September 2004

ETNO Reflection Document on Traffic Data retention

Executive Summary

ETNO is seriously concerned over new proposal for a Council Framework Decision re-opening the debate on data retention tabled by four Member States on 28 April 2004. The proposal entails unpredictable financial and confidentiality implications for industry and individual users.

Under the current Data Protection framework, network operators are only permitted to store and process traffic data for a limited period and for billing and other specified legitimate businesses purposes.

Any additional storage requirements to meet the requests of law enforcement authorities must be justified in terms of all the costs and benefits for society as a whole: in particular, the requests need to be balanced against the fundamental principles protecting human rights as stipulated in the General Data Protection Directive.

The proposed Framework Decision aims to oblige communications companies to undertake large-scale storage of communications data on all users for periods between 12 to 36 months and longer. The data definition used is very broad including traffic data, location data and other forms of data such as subscriber data. The scope is thereby broader than traffic data and location data covered by the Electronic Communications Data Protection Directive, and the area of obligations thus is somewhat diffuse.

Communication operators already co-operate with law enforcement and police forces on a case-by-case and individual basis following an authorisation or warrant. This cooperation includes: real time ***interception*** of phone conversations, faxes and other forms of communications; ***preservation of*** communications data over a certain limited period; and ***access to traffic data*** stored for legitimate business purposes.

ETNO welcomes the Commission's initiative to launch a wide Consultation. All parties concerned should have the opportunity to be heard. Discussions in the Council on a general data retention obligation for operators emerged long before the 11th September 2001. It is worth noting that when debating the Patriot Act in response to the terrorist attacks, the United States rejected this approach repeatedly.

Background

In its Declaration on combating terrorism on 25 March 2004, the European Council called on Member States to examine proposals for establishing rules on the retention of communications traffic data to be put in place by June 2005.

Following the Declaration, on 28 April four Member States, France, Ireland, Sweden and the UK submitted a "Draft Framework Decision on the retention of data processed and stored in the connection and provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crimes and criminal offences including terrorism".

The new Draft Framework Decision provides for an EU wide mandatory data retention period of "*at least 12 months and not more than 36 months*", though "*Member States may have longer periods of retention dependent upon national criteria*".

It should be noted, that data retention consists of the retention of electronic communications traffic and mobile phone location data for all users for a set period of time, as compared to data preservation, which consists of retention of specified traffic data of a particular person or persons pursuant to a request by law enforcement agencies (LEAs).

ETNO companies lawfully assist their national law enforcement agencies on a daily basis in their prevention and investigation of criminal cases by making traffic data collected for telephone billing purposes available according to national legislation. Other lawful forms of assistance include real time interception and the preservation and disclosure of data on specific requests. This has all proven effective and there are very few occasions when communications service providers are unable to satisfy a request to disclose data. So far the proposed Framework Decision fails to provide evidence why data preservation and other existing tools are insufficient. The new proposal will considerably extend the scope of data to areas where in a normal course of business, companies would not keep such data.

ETNO supports the efforts to improve and facilitate the prosecution of organised crime and terrorism. However, cost and benefits must be appropriate and proportionate in relation to the economic and societal costs and the objectives to be achieved. Law enforcement measures imposed on industry and citizens should not exceed what is absolutely necessary to reach law enforcement's objectives.

The proposed measures go far beyond of what is proportionate. They would require electronic communications network operators, Internet access providers, and a not clearly defined range of other Internet service providers (like e-mail providers, Voice of the Internet services and host

providers) to retain all kinds of traffic and location data over very long periods. This imposes an unacceptable burden on the parties involved with serious economic, technical and social consequences. It entails among others the following risks:

- Significant economic burden on communications companies that are obliged to retain traffic data
- Reduced user confidence for individuals and businesses due to privacy and confidentiality concerns
- Legal conflicts between different requirements – data retention vs. data protection and human rights
- Considerable interest in accessing the data by a wide number of public agencies that are not involved in fighting terrorism and serious crime
- Increased security and liability risks to keep data safe against misuse, manipulation and unauthorised access
- Prohibitive market entrant costs for new businesses and distortion of competition in the internal market as in its current form, the proposed Framework Decision does not provide for a harmonised approach on cost recovery
- Even with a cost recovery scheme, data retention will move communications service provider away from being a commercial entity towards a public authority resource
- Technical problems due to the fact that storing larger volumes of traffic data would considerably slowdown the retrieval process
- Overall negative implications on the development of the information society and the aims of Lisbon strategy 2010

Detailed Considerations

The Legal Context

The proposed Framework Decision raises a delicate situation for operators of electronic communications networks and service providers. On one hand these companies must comply with data protection requirements, whilst on the other, they must retain information relating to their customers personal data and privacy for LEA (communication habits, Internet behaviour…).

Regarding the data retention periods, the current EU regulatory framework, as an exception, lays down a provision for Member States to adopt legislative measures allowing retention of data under certain limited conditions for a justified period (art.15 of the Electronic Communications Data Protection Directive 2002/58/EC[1]), whereas the draft Framework

[1] In this sense Recital 11 of this Directive stresses the link to the European Convention on Human Rights and the ruling of the European Court to Human Rights: "Like Directive 95/46/EC, this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take such measures, as are referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications or take other measures, if necessary for any of these purposes and in accordance with the European Convention of Human

Decision considers the general obligation (not any more the possibility) of retaining data for a period of twelve months up to thirty-six months or even more, in specific cases.

The draft Framework Decision uses the data definition included in the Electronic Communications Data Protection Directive. As this Directive aims to grant a very high protection to the privacy of users of electronic communications, its definition is very broad. Using the same definition in the Framework Decision on data retention leads to the absurd situation that all the data to be protected under Directive 2002/58/EC needs to be retained for the purpose of a possible criminal investigation and anti-terrorism measure.

ETNO member companies consider the Draft Framework Decision and, in particular, the proposed retention periods and data definition inappropriate and disproportionate. The draft proposal should provide a clear justification of the proposed measures and carefully consider the potential impact on industry as well as on a democratic society as a whole. The economic consequences of the current draft Framework Decision would be substantial, but this proposal has not been accompanied with any kind of impact assessment (as required by the Commission White Paper on governance of July 2001). In the absence of effective consultation with industry and other interested parties no such impact assessment can be established. The situation is all the more important in respect of data retention as there are very few international precedents for such measures that could be used as a proxy either for calculating the impact or assessing any possible benefits.

In this context, ETNO would remind that in the Council Conclusions of 19 December 2002 Member States established that **reinforced consultation specifically in the area of data retention was needed**. The Council urged "*all parties concerned (governments, parliaments, law enforcement and judicial authorities, industry, data protection authorities and other interested parties), as a matter of priority, to engage in an open and constructive dialogue at national and EU level aimed at finding solutions to the issue of traffic data retention that satisfies both the need for effective tools for prevention, detection, investigation and prosecution of criminal offences and the protection of fundamental rights and freedoms of natural persons, and in particular their right to privacy, data protection and secrecy of correspondence*".

ETNO therefore very much welcomes the Commission's initiative to facilitate such a consultation.

Proportionality

Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights. **Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention on Human Rights and Fundamental Freedoms**".

The principle of proportionality requires that any imposed measure must guarantee the achievement of the intended aim and not go beyond what is necessary to achieve it. In this context ETNO believes that "data preservation" provides for a more practical, proportionate and far less intrusive approach.

There are a number of fundamental principles that need to be fulfilled in accordance to Article 8 (2) of the European Convention for the Protection of Human Rights. Of these, the obligation to respect the principle of proportionality in relation to any measure restricting the fundamental right to privacy, which implies that any measure taken must correspond to an "imperative social need". Measures that are simply useful or desirable do not fulfil this proportionality test as has been established by European case law[2]. With the concept of Data Retention all European Citizens would be part of surveillance activities but never be part of a criminal procedure. Against this backdrop proportionality of data retention methods are more than questionable.

The fundamental principles also include the establishment of a legal basis that must precisely define the limits and means of applying exceptional measures. This includes the purpose for which the data may be processed, the length of time it may be kept (if at all) and that access to the data must be strictly limited. Large-scale exploratory or general surveillance is not permissible.

Impact on Industry

a) Data retention costs

Traffic storage data will result in heavy extra costs, due to increased storage capacity, changes in systems' design, additional security measures, verification and responses to access requests, retrieval of raw data, providing evidences in Courts about authenticity and reliability of the data in question.

The draft proposal is not only silent on these costs issues but it does not provide for any reimbursement schemes. Cost reimbursement is not only crucial from an industry perspective, it would also provide a safeguard from a public policy perspective to keep traffic data retention limited and ensure a better degree of accountability for data retrieval requests.

As an example, we would like to provide with some figures[3] showing the additional expense for larger fixed and mobile telephony operators and Internet Service providers, based on the requirements of the draft framework decision and for a period of 12 month.

[2] Especially the Klass judgment of 6 September 1978, Series A N° 28, pp. 23 et seq., and the Malone judgment of 2 August 1984, Series A n° 82, pp. 30 et seq. – see also Art. 29 Working Party recommendation on the respect of privacy in the context of interception of telecommunications of 3 May 1999.

[3] Figures related to Germany according to the Position Paper of the Federation of German Industry (BDI): http://www.bdi-online.de

Since the framework decision is ambiguous in its wording, it has been assumed that the envisaged storage obligations do not only cover data that is already stored by companies for other purposes (billing), but also every type of data stipulated in Article 2 of the framework decision, even if that is not stored by companies:

- Larger fixed and mobile telephony provider: in the traditional circuit-switched telephony sector capital expenditure would amount to a three-digit million figure for adjustment of software, server, security and in addition an annual overhead expense of at least 50 million euros (including depreciation of investment costs) would be expected. The additional expense is mainly needed for the necessary adjustment of technical systems, the implementation of processes to guarantee secure storage of data and to deal adequately with requests of the law enforcement agencies.

- Internet (big ISP): the capital expenditure necessary for the network of a big ISP will be even much higher, since the volume of data is much higher than the volume of fixed and mobile telephony. In the Internet business also the cost to store data will therefore be extremely high.

b) Technical challenges and effectiveness of data retention

Considering the large volume of data to be stored according to the draft framework decision, it is doubtful whether the retrieval of raw data is actually possible, since even elaborate search techniques would still generate huge volumes of data.

To illustrate this point we would like to provide an estimation[4] on the volume of data for a period of 12 month, based on the requirements of the draft framework decision:

- **Larger fixed and mobile telephony providers** in the traditional circuit-switched telephony sector about a volume of 8 terabytes (1 terabyte = 1million megabyte)

- **Larger ISP**: about 20.000 – 40.000 terabytes of data, much more than in the fixed or mobile sector, if traffic data of all IP packages is stored or 100 – 1000 terabyte, in the case of traffic data of email, voice over IP, web server, etc.

  As seen above, the data volume of retained data is enormous. With the existing systems, and without additional investments, a single sequential search through a volume of 20.000 – 40.000 terabyte would take decades.

[4] Figures related to Germany according to the Position Paper of the Federation of German Industry (BDI): http://www.bdi-online.de

Besides the large volumes of data and the extension of storage periods, there are other challenges that need to be taken into consideration when assessing the efficiency of the proposed measures:

- The integrity of information concerning Internet communications is much less robust that that associated with voice calls. In addition the data volumes are much higher than in traditional voice telephony. Internet data retrieval is a difficult process and its accuracy cannot be guaranteed. There is 'dynamic' allocation of addresses (i.e. for the duration of the communication), encryption can be used, the data transmission may pas through several time zones, networks, servers etc., all which are 'timed' independently.

- There are several possibilities to circumvent the retention of traffic data of for example email or accesses to web server. One can send e-mails using re-mailers which anonymise the traffic data of the sender. Using mixing server for surfing the Internet prevents the storage of web access traffic data.

- There are several possibilities of anonymous access to the Internet, for example Internet cafes. The same holds for telephony services. One can use public telephony boxes to make anonymous calls.

- Wireless LAN enables a given group of people within a certain limited geographic area to build their own private network and to communicate without relying on any operator at all.

- Using peer-to-peer connections, it is possible to communicate via Internet without leaving any marks.

- Platforms for calling cards do not store any data.

- Last, but not least, the origin or destination of traffic data can be in a foreign country on a foreign server, where no obligation to store traffic data exists. Therefore, these data records are senseless, since no relationship to the sender or receiver can be established.

Further considerations

Restriction of citizens' rights to determine how his or her personal data is handled

According to article 8 of the European Charter of Human Rights every person has the right to determine how their personal data is handled. This right is an integral part of European culture and a significant basis of the European legal system. The proposed Framework Decision restricts this right considerably. For example, for certain professions, such as journalists or lawyers, it would no longer be possible to guarantee the confidentiality of their sources as ultimately any electronic communication can be traced

back to its origin. In order not to violate these fundamental values it should be weighed up very carefully if it is adequate to put under surveillance millions of respectable European citizens in this way.

Negative implications for the Information Society

The draft framework decision under discussion might have a negative effect on the development of the information society and the Lisbon strategy.

Consumer confidence is important because it affects the readiness to use innovative telecommunication services and the development of new innovative services (Internet Broadband via DLS, UMTS). Extensive data retention can undermine this confidence in security and may have a negative impact on the use of new electronic communication services and products, its development and innovation. Especially the development of the Internet, which would be clearly affected by the proposed measures, is considered to be essential for the competitiveness of Europe. **Only serious data protection can build up and strengthen the trust of customers** and is therefore an essential basis for the economic success of Europe.

Preservation of data - the better alternative

Before imposing such intrusive measures as data retention, Member States should justify why less intrusive measures such as data preservation (requiring a storage and preservation of data on a case by case basis following a specific request) won't achieve the same objectives. Without providing any justification, Recital 6 of the draft Framework Decision concludes that data preservation is not sufficient. By contrast, the Council of Europe Convention on Cyber Crime does not require retention, but considers data preservation as fully sufficient to achieve the objective of fighting all crimes relying on modern electronic communications and computing technologies.

Preservation of data is less intrusive as only data of a specific individual or group clearly identified as the subject of an investigation can be stored and analysed. In addition this would allow retrieval of data being more targeted. Preservation of data can therefore help built a more adequate database that together with optimised search systems may even be the most efficient way. In this sense, in the United States preservation of data is considered as sufficient and US Administration has expressed this view repeatedly since 11 September 2001[5].

[5] www.heise.de/newsticker/meldung/46800, 23 April 2004.
See also Prepared Statement by Mark Richard, Criminal Division of the United States Department of Justice on 27 November 2001 at EU Forum on Cybercrime : "The United States recognizes that access to electronic evidence is critical to the success of computer crime and terrorist investigations….. In the United States, we have balanced the competing interests through laws governing data preservation. Public safety officials rely on

Harmonisation. Distortion of competition in the Internal Market

As it stands the draft Framework Decision will create a patchwork of different national measures across the EU, due to **lack of harmonization** in important issues.

Furthermore, a harmonized approach would help reduce **compliance** costs as the new technologies that would need to be developed specifically to meet law enforcement's needs would then be appropriate for the entire European Union, and will help ensure that data retention requirements do not **distort competition** within the single market.

Indeed, for operators obliged to retain data, it is of the utmost importance that the draft Framework Decision establishes the basic parameters for a cost reimbursement scheme in Member States. Otherwise there will be a distortion of competition in the internal market. France and Italy provide for some kind of compensation for lawful interception, Germany only partial[6], Spain does not consider at all any kind of compensation for operators.

Also, the draft Framework Decision raises questions on compliance and enforcement. The national regulators must ensure that all operators and service providers (which can amount to several hundreds of actors in some countries) actually retain data in an accurate manner. How will compliance be ensured by the authorities? What will happen with data retained by companies that decide to leave a market or run out of business? Needless to say, larger operators would retain the majority of data but there are, as pointed out above, a range of other actors also affected by this proposal and which are integral parts of the data retention 'value chain'.

Validity of the information retained and possible short-term actions

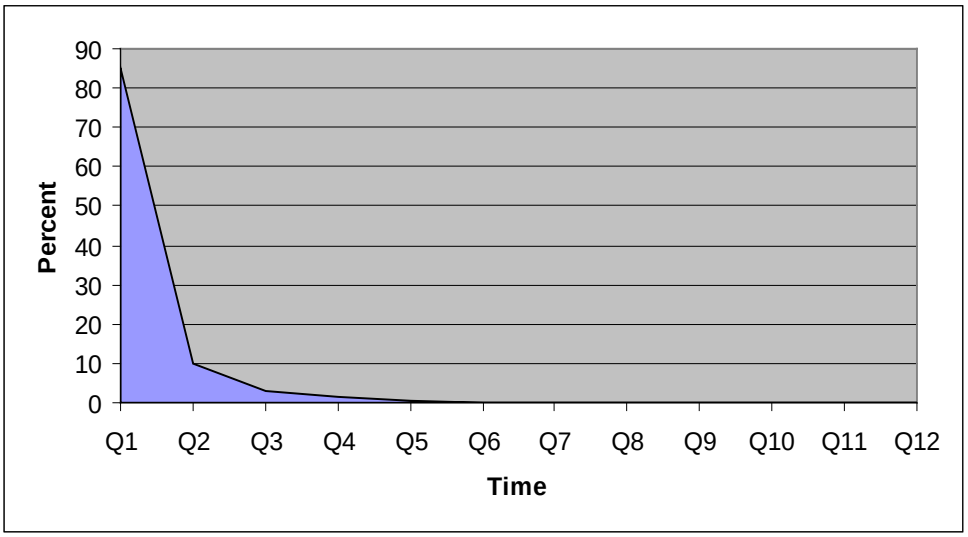
The usefulness and the associated cost of keeping such large volumes of data for a long period of time have been questioned. In addition, police experts work with data from three to six months and only rarely, or never, request data that is older than eight or ten months. For example, a mere 0,5% of requests for call data records (CDR) to TeliaSonera Sweden relates

---

providers to preserve log files, electronic mail, and other records quickly upon notification that such information is necessary for a specific investigation, before such information is altered or deleted. Later access to these historical records is obtained by court order or other statutory processes in conformity with accepted due process protections. Preservation, however, does not require a service provider to collect data prospectively. The Council of Europe Cybercrime Convention contains a similar scheme, reflecting general agreement that, for now, this preservation regime strikes the proper balance between the competing policy interests. With respect to Internet service providers choosing to retain data, the United States has taken an approach that neither requires the destruction of critical data, nor mandates the general collection and retention of personal information. Rather, ISPs are permitted to retain or destroy the records they generate based upon individual assessments of resources, architectural limitations, security, and other business needs. "

[6] WIK Study (WIK „Rechtlicher Rahmen für das Angebot von TK-Diensten und den Betrieb von TK-Anlagen in den G7 Staaten in Bezug auf die Sicherstellung der Überwachbarkeit der Telekommunikation".

to data older than 12 months. At the same time 85% CDR requests concern data recorded during the last three months (see table below).



Requests for call data records to TeliaSonera Sweden

Recommendations

ETNO seriously questions the need for mandatory data retention and actually doubts that it will serve the intended purpose to make law enforcement in the area of serious crime and terrorism more efficient. Before moving ahead, a cost-benefit analysis should be provided and the draft Decision needs important improvements. In particular any proposed measure in this area should be based on the need:

- to maintain the necessary information and not exceeding the volume that is currently stored and which is already satisfactory to investigations developed by Police Forces and law enforcement agencies

- To gather information during an investigation, so that it can be carried out in real time. This model is an evolution of the current one, and is based on investigation of facts that are occurring instead of being based on facts that occurred in the past.

Against this backdrop, the following principles should be observed when examining potential regulations on the retention of traffic data:

- When looking for solutions, the **effectiveness and practicability** of the measures planned have to be taken into account.
- The **existing legal framework and the possibilities should be further examined** before another layer of regulation is introduced.

- Processes for **multilateral assistance in criminal investigations should be speeded-up** to reduce need for "historic" data
- **Law enforcement ICT resources should be optimised**. Based on some ETNO member companies' experience, law enforcement officials have difficulties and lack resources to handle data already under the current regime.
- **Consideration should be given to optimising the preservation of data** in specific cases as an alternative solution.
- In order to avoid competitive distortions in the internal market and internationally, it will be necessary to **introduce harmonized rules for cost recovery. If an EU instrument is adopted, the cost matter should be addressed therein**. If cost allocation is left out of the Framework Decision Member States may decide that providers bear the cost of the proposed measures. Any difference in cost allocation between EU Member States will certainly have a negative impact on the provision of telecommunications services between Member States.
- If data retention is to be made mandatory, the **kinds of data to be retained and retention periods are both to be kept to the absolute minimum**.
- In addition, it is crucial that the proposed **Framework Decision takes into consideration the complex technical implications and challenges** entailed by such a measure. Otherwise, it will not be implemented properly and will not be technically viable.

ETNO is fully committed to co-operate with Governments and Law Enforcement Authorities in raising awareness on technical limitations and possibilities to ensure the development of a proportionate, adequate and efficient approaches and very much welcomes the Commission's initiative to conduct a Consultation on the current draft Framework Decision with all interested parties.