ISPA Regulatory and Legal Working Group

Position of Principle on the matter of DATA RETENTION

Abstract of the Directive

The European Directive on the retention of data processed in connection with the provision of publicly available electronic communications services or of public communications networks (the '***Data Retention Directive***') was published on 15 March 2006 and came into force on 4 April 2006.

Aim of the Directive

Data retention aims at preventing, investigating, detecting and prosecuting serious criminal offences, in particular organised crime and terrorist attacks.

Parties concerned

The Data Retention Directive applies to providers of publicly available electronic communications services and of public communications networks, such as Internet Service Providers, operators of fixed and mobile telephony.

Data to be retained

The data retention obligations relate to traffic data, localisation data and identification data of fixed, mobile and IP communication.

They include the source, destination, type and the date, time and duration of the communication as well as the equipment used and the location thereof.

Data revealing the content of communication is explicitly excluded from the scope of the obligation.

Duration of the obligation

The duration of the retention will have to be between 6 months and 24 months from the date of the communication.

Implementation of the Directive

The Data Retention Directive has to be implemented in Belgian law at the latest by 15 September 2007.

As far as Internet communication data such as Internet access, Internet telephony and Internet e-mail are concerned, application of the Directive may be postponed until 15 March 2009.

ISPA Belgium vzw/asbl
Rue Montoyerstraat, 39 BP3
B-1000 Brussels
Belgium
Bank: GEBABE 210-0047888-22
VAT BE 461 515 409
Tel: +32 2 503 23 28
Fax: +32 2 503 42 95
info@ispa.be
www.ispa.be
Registration number 17982/97

Purpose of this position of principle

While communications service providers recognise the importance of constructive and effective cooperation with law enforcement authorities, there are some key issues of concern to point out in view of the implementation of the Data Retention Directive in Belgium.

The purpose and goal of this document is to set the commonly defined and agreed position by ISPA in relation to such implementation. Internet based data retention, including e-mail and VoIP, is of particular interest to ISPA members.

ISPA would like to recall that the Data Retention Directive was adopted very quickly without adequately reflecting on the necessity and proportionality of the measure, e.g. by outweighing the framework against other solutions (such as legal interception) and by reflecting on the overall consequences for society. As such, it makes all 450 million European citizen potential suspects, may endanger the competitive position of Belgian ISPs and will inevitably increase the digital divide because of unnecessary costs it causes. Also, there are many technological ways to circumvent the retention measures. It can be estimated that organised crime will know these techniques very well and will make it virtually impossible for law enforcement authorities to actually trace them down.

The Data Retention Directive leaves several open questions and room for implementation choices by Member States. The data retention principles imply interference in the right to privacy, as laid down in international treaties, the Belgian constitution and other laws. Any justified interference must be stipulated by law. It needs to be checked whether article 126 of the Electronic Communications Act of 13 June 2005 is a sufficient legal basis for the implementation of the Data Retention Directive.

ISPA is of the opinion that an integrated approach should be adopted taking into account existing legislation, technological developments and standards. ISPA would therefore like to call upon a formal dialogue between the industry and the Belgian government to ensure a well thought through implementation process which introduces retention obligations in a reasonable and proportionate way. This particularly implies legal compliance as well as technical and economical feasibility of any data retention obligations.

ISPA is of the opinion that the development of data retention procedures for Internet services and the implementation thereof will have to be agreed with and coordinated between the authorities and ISPA in appropriate working groups.

ISPA Belgium vzw/asbl
Rue Montoyerstraat, 39 BP3
B-1000 Brussels
Belgium
Bank: GEBABE 210-0047888-22
VAT BE 461 515 409
Tel: +32 2 503 23 28
Fax: +32 2 503 42 95
info@ispa.be
www.ispa.be
Registration number 17982/97

	KEY ISSUES OF CONCERN	ISPA BELGIUM RECOMMENDATIONS
1. Costs	- The amount of data is very high, making the retention obligation, including the retention of unsuccessful calls, a heavy and costly duty for ISPs, in particular small ones. - Data retention also involves high set-up and operational costs (e.g. security and qualified staff). If any costs for data retention are to be borne by ISPs, such additional cost will inevitably be passed on to end consumers. This will increase the Internet barrier to those people who are already lacking behind, whereas the government is doing everything to combat the digital divide.	The government should ensure that - costs for data retention are economically viable and realistically justifiable by carrying out an independent cost analysis study before introducing regulatory measures; - industry bears no extra costs for technical and organisational measures resulting from data retention obligations.
2. Scope	- The scope of data to be retained is very large even if data revealing the content of communication is explicitly excluded from the scope of the obligation. - In practice, it may not always be easy to separate traffic data from content. - Also, it is not totally clear which parties are envisaged by the obligations.	The government should ensure that - the list of data to be retained is well specified; - the type of service providers and services subject to the data retention obligation is well specified; - the responsibilities of ISPs (service providers), AP (access providers) and NWO (network operators) in relation to collection, storage and retrieval are clearly defined; - the proportionality principle of Belgian and European privacy regulations is observed to the maximum extent allowed by the Data Retention Directive, so that the monitoring of human behaviour is carried out technologically neutral.

	KEY ISSUES OF CONCERN	ISPA BELGIUM RECOMMENDATIONS
3. Duration	- The longer the data have to be retained, the higher the storage costs become and the more retention becomes incompatible with privacy legislation, i.e. retention of personal data should be no longer than absolutely necessary and deletion of communications data upon completion of the communication should be done immediately, except for billing reasons and disputes regarding interconnection agreements between operators.	The government should ensure that - the retention period is kept short, in accordance with the proportionality principle of Belgian and European privacy regulations; - a consensus is found on data to be kept for 6 months maximum. A longer retention period will increase costs and incompatibility with privacy legislation. An exception should only be available for these data which are already, by law, kept for longer than 6 months, such as invoicing data; - for specific data and in case it is economically and legally justifiable, a maximum period of 12 months is adopted.
4. Storage	- Storing the retained data in a separate, secured database, apart from billing data will have an enormous financial, organisational and legal impact for ISPs.	The government should ensure - to avoid multiple storage of identical data by various service providers; - duplication of retained data is avoided, e.g. by explicitly excluding companies that have no direct contact with the end user.

ISPA Belgium vzw/asbl
Rue Montoyerstraat, 39 BP3
B-1000 Brussels
Belgium
Bank: GEBABE 210-0047888-22
VAT BE 461 515 409
Tel: +32 2 503 23 28
Fax: +32 2 503 42 95
info@ispa.be
www.ispa.be
Registration number 17982/97

	KEY ISSUES OF CONCERN	ISPA BELGIUM RECOMMENDATIONS
5. Retrieval	- The more and the longer data are stored, the more complex it becomes to find them back, thus making data retention less effective.	The government should ensure that - the retrieval of data is only allowed if duly authorised by judicial authorities and if workable modalities and procedures are set up (e.g. criteria, conditions, time lines, formats, etc.) and if conform to ETSI norms/interfaces - once these norms are officially published, technically feasible and cost effective - (ETSI norms/interfaces are recognised European communication protocol for data interoperability, also referred to in the Law on Electronic communications). - the definition of serious crime is as narrow and entirely clear (i.e. not subject to individual appreciation that could cause liability issues); - the costs associated with retrieval are borne by the "requester" i.e. the legal authorities in most cases.
6. Liability	- The retained data will have to be protected against loss, destruction and unauthorised access. In case of lost or stolen data, ISPs face the heavy burden of proof that any damage suffered by a third party is not due to their fault or negligence.	The government should ensure that - ISP liability in case of lost or stolen data is limited; - any obligation on ISPs to secure the retained data is best efforts based.
7. Competition	- Heavy obligations will be detrimental for the industry, competitiveness of Belgian service providers and the	The government should ensure that

	KEY ISSUES OF CONCERN	ISPA BELGIUM RECOMMENDATIONS
	development of new services. Moreover, different regimes for ISPs in the EU risk hindering the development of EU-wide network services.	- data retention obligations imposed on ISPs are clear, specific and feasible, without hindering normal business operations; - regulatory initiatives in Belgium are not more cumbersome to Belgian service providers than similar regulation applicable to their European competitors.
8. Consumer protection	- End users are the key driver of the communications industry, which in its turn is vital for our economy and social system. Too strict and non transparent measures will damage users' trust in the information society. The potential negative impact of increased costs of usage should also be considered, since it is an element that could increase the socio-economical digital divide, at a time when promotion of the use of information society services is an official government objective.	The government should ensure that - a fair balance is struck between privacy protection for users and law enforcement; - any implementing measures are appropriate, necessary and proportionate and preferably not general in nature. - advice from the Privacy Commission is obtained in due time.

Brussels, November 2006

ISPA Belgium vzw/asbl
Rue Montoyerstraat, 39 BP3
B-1000 Brussels
Belgium
Bank: GEBABE 210-0047888-22
VAT BE 461 515 409
Tel: +32 2 503 23 28
Fax: +32 2 503 42 95
info@ispa.be
www.ispa.be
Registration number 17982/97