EUROPEAN PARLIAMENT

2004 *2009*

Session document

FINAL
A6-0000/2005

25.11.2005

***I
REPORT

on the proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC
(COM(2005)0438 – C6-0293/2005 – 2005/0182(COD))

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Alexander Nuno Alvaro

Symbols for procedures

*	Consultation procedure *majority of the votes cast*
**I	Cooperation procedure (first reading) *majority of the votes cast*
**II	Cooperation procedure (second reading) *majority of the votes cast, to approve the common position* *majority of Parliament's component Members, to reject or amend the common position*
***	Assent procedure *majority of Parliament's component Members except in cases covered by Articles 105, 107, 161 and 300 of the EC Treaty and Article 7 of the EU Treaty*
***I	Codecision procedure (first reading) *majority of the votes cast*
***II	Codecision procedure (second reading) *majority of the votes cast, to approve the common position* *majority of Parliament's component Members, to reject or amend the common position*
***III	Codecision procedure (third reading) *majority of the votes cast, to approve the joint text*

(The type of procedure depends on the legal basis proposed by the Commission.)

Amendments to a legislative text

In amendments by Parliament, amended text is highlighted in ***bold italics***. Highlighting in *normal italics* is an indication for the relevant departments showing parts of the legislative text for which a correction is proposed, to assist preparation of the final text (for instance, obvious errors or omissions in a given language version). These suggested corrections are subject to the agreement of the departments concerned.

CONTENTS

Page

DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION

on the proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM(2005)0438 – C6-0293/2005 – 2005/0182(COD))

(Codecision procedure: first reading)

The European Parliament,

– having regard to the Commission proposal to the European Parliament and the Council (COM(2005)0438)[1]

– having regard to Article 251(2) and Article 95 of the EC Treaty, pursuant to which the Commission submitted the proposal to Parliament (C6-0293/2005),

– having regard to Rule 51 of its Rules of Procedure,

– having regard to the report of the Committee on Civil Liberties, Justice and Home Affairs and the opinions of the Committee on Industry, Research and Energy (A6-0000/2005) and of the Committee on the Internal Market and consumer Protection (A6-0000/2005)

1. Approves the Commission proposal as amended;

Amendment 1
Paragraph 1 a (new)

1a. Calls on the Commission, prior to the entry into force of this Directive, to commission an impact assessment study from an independent body representing all stakeholders, covering all internal market and consumer protection issues;

2. Calls on the Commission to refer the matter to Parliament again if it intends to amend the proposal substantially or replace it with another text;

3. Instructs its President to forward its position to the Council and Commission.

Text proposed by the Commission	Amendments by Parliament

Amendment 1
Recital 3

(3) Articles ***5,*** 6 and 9 of Directive	(3) Articles 6 and 9 of Directive 2002/58/EC

[1] OJ C ...., ..., p. .....

2002/58/EC define the rules applicable to the processing by network and service providers of traffic and location data generated by using electronic communications services. ***Such*** data must be erased or made anonymous when no longer needed for the purpose of the transmission of a communication, ***except for the data necessary for*** billing ***or*** interconnection payments; ***subject to consent, certain data may also be processed for marketing purposes and the provision of value added services.***	define the rules applicable to the processing by network and service providers of traffic and location data generated by using electronic communications services. ***In principle such*** data ***should*** be erased or made anonymous when no longer needed for the purpose of the transmission of a communication. ***For the purposes of subscriber*** billing ***and*** interconnection payments ***data may be processed, but only up to end of the period during which the bill may lawfully be challenged or payment may be pursued;***

Amendment 2
Recital 4

(4) Article 15(1) of Directive 2002/58/EC sets out the conditions under which Member States may restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1)(2)(3) and (4), and Article 9 of the Directive; any such derogations need to be necessary, appropriate and proportionate within a democratic society for specific public order purposes, i.e. to safeguard national security (i.e. State security) defence, public security or the ***prevention,*** investigation, detection and prosecution of criminal offences ***or of unauthorised use of the electronic communications systems.***	(4) Article 15(1) of Directive 2002/58/EC sets out the conditions under which Member States may restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1)(2)(3) and (4), and Article 9 of the Directive; any such derogations need to be necessary, appropriate and proportionate within a democratic society for specific public order purposes, i.e. to safeguard national security (i.e. State security) defence, public security or the investigation, detection and prosecution of ***serious*** criminal offences. *(The first part of the amendment to delete 'prevention' applies throughout the text. Adopting it will necessitate corresponding changes throughout).*

Amendment 3
Recital 4 a (new)

	4a Article 7 of the Charter of Fundamental Rights explicitly recognises the right to respect for private life and Article 8 thereof the right to protection of personal data.

Amendment 4
Recital 6

(6) The legal and technical differences ***between national provisions concerning the retention of data for the purpose of prevention, investigation, detection and prosecution of criminal offences present obstacles to the internal market for electronic communications; service providers are faced with different*** requirements regarding the types of traffic data to be retained as well as the conditions and the periods of retention.	(6) The ***provisions so far adopted present*** legal and technical differences ***and the*** requirements regarding the types of traffic data to be retained as well as the conditions and the periods of retention ***also differ.***

Amendment 5
Recital 6 a (new)

	(6) a The harmonisation of the internal market in the field of data retention highlights the need for a better and more equal access to justice and appeal for citizens, throughout the EU. Every citizen should have the same right to legal protection and compensation against misuse of information regardless if it originates from an authority or a provider.

Amendment 6
RECITAL 7

(7) The Conclusions of the Justice and Home Affairs Council of 20 September 2001 call for ensuring that law enforcement authorities are able to investigate criminal acts which involve the use of electronic communications and to	***deleted***

take legal measures against perpetrators of these crimes, while striking a balance between the protection of personal data and the needs of law enforcement authorities to gain access to data for criminal investigation purposes.

Amendment 7
Recital 8

(8) The Conclusions of the Justice and Home Affairs Council of 19 December 2002 underline that, because of the significant growth of the possibilities of electronic communications, data relating to the use of electronic communications ***is particularly important and therefore*** a valuable tool in the prevention, investigation, detection and prosecution of crime and criminal offences, in particular against organised crime.	(8) The Conclusions of the Justice and Home Affairs Council of 19 December 2002 underline that, because of the significant growth of the possibilities of electronic communications, data relating to the use of electronic communications ***may be*** a valuable tool in the prevention, investigation, detection and prosecution of crime and criminal offences, in particular against organised crime.

Amendment 8
Recital 10

(10) The declaration adopted by the special informal Council of 13 July 2005 reinforces the need to adopt measures related to the retention of electronic communications traffic data as soon as possible.	(10) The declaration adopted by the special informal Council of 13 July 2005 reinforces the need to adopt ***common*** measures related to the retention of electronic communications traffic data as soon as possible.

Amendment 9
Recital 10 a (new)

	(10a) The Working Party on the protection of individuals with regard to processing of personal data established according to Article 29 of Directive 95/46/EC shall carry out the tasks laid down in Article 30 of the abovementioned Directive also with regard to the protection of fundamental rights and freedoms and of legitimate interests in the

sector which is subject to this Directive.

Amendment 10
RECITAL 11

(11) ***Given the importance of traffic data for the prevention, investigation, detection, and prosecution of serious criminal offences, such as terrorism and organised crime, as demonstrated by research and the practical experience of several Member States,*** there is a need to ensure that data which are processed by electronic communication providers when offering public electronic communication services or public communication networks are retained for a ***certain*** period of time.	(11) ***The practical experience of some Member States has demonstrated that traffic data can be important for the investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime. Consequently,*** there is a need to ensure that data which are processed by ***public*** electronic communication providers when offering public electronic communication services or public communication networks are retained for a ***harmonised*** period of time.

Amendment 11
RECITAL 11 A (new)

	(11a) The drawing up of any lists of types of data to be retained should reflect a balance between the benefit to the investigation, detection and prosecution of serious criminal offences against the degree of invasion of privacy which will result.

Amendment 12
Recital 14

(14) Technologies relating to electronic communications are changing rapidly and the legitimate requirements of the competent authorities may evolve; to advise on these matters the Commission envisages ***to create a*** platform composed of representatives of the law enforcement authorities, associations of the electronic communications industry and data protection authorities.	(14) Technologies relating to electronic communications are changing rapidly and the legitimate requirements of the competent authorities may evolve; to advise on these matters the Commission envisages ***a periodic review of the strict necessity of such provisions and the evaluation of the types of data that are needed. A*** platform composed of representatives of the ***European Parliament,*** law enforcement

	authorities, associations of the electronic communications industry***, consumer protection organisations*** and ***European and national*** data protection authorities ***may assist the Commission.***

Amendment 13
RECITAL 17

(17) The measures necessary for the implementation of this Directive should be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission[1].	***deleted***

Amendment 14
Recital 18

(18) The objectives of the action to be taken, namely to harmonise the obligations on providers to retain certain data and to ensure that these data are available for the purpose of the ***prevention,*** investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime, cannot be sufficiently achieved by the Member States and can, by reason of the scale and effects of the action, be better achieved at Community level. Therefore the Community may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.	(18) The objectives of the action to be taken, namely to harmonise the obligations on providers to retain certain data and to ensure that these data are available for the purpose of the investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime, cannot be sufficiently achieved by the Member States and can, by reason of the scale and effects of the action, be better achieved at Community level. Therefore the Community may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, ***it is unclear whether*** this Directive does not go beyond what is necessary ***and proportionate*** in order to achieve those objectives, ***as also pointed out by the European Data Protection Supervisor.***

[1] OJ L 184, 17.7.1999, p. 23.

Amendment 15
Recital 18 a (new)

(18a) Since the security of data retained under this Directive is of paramount importance for the safeguarding of consumers' rights, Member States should ensure that the highest standards of data storage security are applied, in particular the protection of data from alteration and unauthorized access, as well as from internet and non-internet related threats.

Amendment 16
Recital 18 A (new)

(18a) The security of data under this Directive must be in compliance with the data protection provisions of Directive 2002/58/EC.

Amendment 17
Recital 19

(19) This Directive *respects* the fundamental rights and ***observes*** the principles recognised, in particular, by the Charter of Fundamental Rights of the European Union; in particular, this Directive together with Directive 2002/58/EC, seeks to ensure full respect of the fundamental rights to respect the private life and communications of citizens and the protection of personal data (Articles 7 and 8 of the Charter),

(19) This Directive ***could better*** *respect* the fundamental rights and the principles recognised, in particular, by the Charter of Fundamental Rights of the European Union; in particular, this Directive together with Directive 2002/58/EC, ***and*** seek to ensure full respect of the fundamental rights to respect the private life and communications of citizens and the protection of personal data (Articles 7 and 8 of the Charter) ***as well as the judgments of the European Court of Human Rights[1].***

[1] See in particular the judgments in the cases Amann v. Switzerland (no. 27798/95, ECHR 2000-II of 16 February 2000, where the storing of information about an individual was considered to be an

interference with private life, (even though it contained no sensitive data) and the judgment in Malone v. the United Kingdom (no. 8691/79, of 2 August 1984), where the same applied to the practice of 'metering' of telephone calls, which involves the use of a device that registers automatically the numbers dialled on a telephone and the time and duration of each call).

Amendment 18
RECITAL 19 A (new)

19a. The Member States should ensure that the implementation of this Directive takes place following consultations with the business sector, particularly as regards feasibility and cost of retention. In view of the fact that retention entails a practical and financial effort from businesses, the Member States should guarantee full compensation for additional costs incurred by businesses as a result of obligations or commitments relating to the transposition of this Directive.

Justification

Combating crime and guaranteeing public security are core duties of the modern state: accordingly, such measures must be fully funded from the public purse, and not at the expense of business, otherwise the attractiveness of Europe as a business location will be diminished. The full (investment and operational) costs of all obligations arising out of this Directive must therefore be entirely borne by the Member States. The same applies to the compilation of statistics, which should primarily be the task of the Member States.

Amendment 19
Article 1, paragraph 1

1. This Directive aims to harmonise the provisions of the Member States concerning obligations on the providers of publicly available electronic communications services or of a public communications	1. This Directive aims to harmonise the provisions of the Member States concerning obligations on the providers of publicly available electronic communications services or of a communications network

network with respect to the processing and retention of certain data, ***in order to*** ensure that the data is available for the purpose of the prevention, investigation, detection and prosecution of serious criminal offences, ***such as terrorism and organised crime.***	with respect to the processing and retention of certain data, ***and to ensure that the rights to the respect for private life and to the protection of personal data in the access and use of these data are fully respected,*** in order to ensure that the data is available for the purpose of the investigation, detection and prosecution of serious criminal offences, ***as referred to in Article 2 (2) of Council Framework Decision 2002/584/JHA.***

Amendment 20
ARTICLE 1, PARAGRAPH 2

2. This Directive shall apply to traffic ***and location*** data of both private and legal persons, as well as the ***related*** data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network.	2. This Directive shall apply to traffic ***and location*** data of both private and legal persons, as well as the data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network. *(This amendment applies throughout the text. Adopting it will necessitate corresponding changes throughout).*

Amendment 21
Article 2, paragraph 2, point a) and a)a

a) 'data' means traffic data and location data, as well as the ***related*** data necessary to identify the subscriber or user;	a) 'data' means traffic data and location data, as well as the data necessary to identify the subscriber or user; ***a)a 'competent national authorities' means the judicial authorities and national authorities responsible for the investigation, detection and prosecution of serious criminal offences.***

Amendment 22
Article 2, paragraph 2, point ba) (new)

ba) 'serious criminal offences' means the offences referred to in Article 2(2) of the Council Framework Decision 2002/584/JHA[1].

[1] Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States.

Amendment 23
Article 2, paragraph 2, point bb) new

bb) 'unsuccessful call attempt' means a communication in which a telephone call has been successfully connected but is unanswered or there has been a network management intervention.

Amendment 24

Article 3, paragraph 1

1. By way of derogation to Articles ***5,*** 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that data which are generated ***or*** processed ***by providers of publicly available electronic communications services or of a public communications network within their jurisdiction*** in the process of supplying communication services ***are retained*** in accordance with the provisions of this Directive.	1. By way of derogation to Articles, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that***, in the event of a successfully established communication, providers of publicly accessible electronic communications services or of a public communications network providing the service in question retain and make available*** data which are generated ***and*** processed in the process of supplying communication services in accordance with the provisions of this Directive ***by that provider who has offered the respective used electronic communication service.***

Or. en

Amendment 25
Article 3, paragraph 2

2. Member States shall adopt measures to ensure that data retained in accordance with this Directive are only provided to the competent national authorities, in specific cases and in accordance with ***national legislation***, for the purpose of the prevention, investigation, detection and prosecution of serious criminal offences, ***such as terrorism and organised crime.***	2. Member States shall adopt measures to ensure that data retained in accordance with this Directive are only provided to the competent national authorities***, following the approval of the judicial authorities and of other competent authorities according to national legislation,*** in specific cases and in accordance with ***the provisions of this Directive,*** for the purpose of the investigation, detection and prosecution of serious criminal offences, ***as referred to in Article 2(2) of Council Framework Decision 2002/584/JHA.)*** ***This Directive shall comply with the principles laid down in the Council Framework Decision on [data protection].***

Amendment 26
Article 3, paragraph 2 a (new)

	2a. To this end an updated list of the designated competent law enforcements authorities should be publicly available.

Amendment 27
Article 3 a (new)

	Access to retained data ***1. Each Member State shall ensure that providers of publicly available electronic communications services or of a communications network shall only grant access to data retained under this Directive under the following minimum conditions, and shall establish judicial remedies in line***

with the provisions of Chapter III of Directive 95/46/EC:

(a) data is accessed only for the specified, explicit and legitimate purposes defined by this Directive,by competent national authorities duly authorised by a judicial authority or other competent independent national authority, on a case by case basis and with respect for professional secrecy in accordance with national law;
(b) the data shall not be further processed in a way, which is incompatible with those purposes; any further processing of retained data by competent national authorities for other related proceedings should be limited on the basis of stringent safeguards;
(c) any access to the data by other government bodies or private companies is forbidden;
d) the process to be followed in order to get access to retained data and to preserve accessed data is defined by each Member State in their national law; providers are not allowed to process data retained under this Directive for their own purposes;
(e) the data requested must be necessary relevant and proportionnal in relation to the purposes for which they were accessed. Data are processed fairly and lawfully: in any case access is restricted to those data that are necessary in the context of a specific investigation and does not include large-scale data-mining in respect of travel and communications patterns of people unsuspected by the competent national authorities;
(f) any accessing of retained data is recorded in a data processing register that enables identification of the requester, the data controllers, the personnel authorised to access and process the data, the judicial authorisation in question, the data consulted and the purpose for which they have been consulted,
(g) the data shall be in a form which allows data subjects to be identified only for as

long as is necessary for the purpose for which the data were collected or processed further;
(h) the confidentiality and integrity of the data shall be safeguarded, including respect for professional secrecy; any retrieval of the data shall be recorded and make these records available to the national data protection authorities;
(i) data accessed are accurate and, every necessary step is taken to ensure that personal data which are inaccurate, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.
(j) data are erased once those data are no longer necessary for the purpose for which they are sought;
(k) the competent national authorities may only forward the data to third countries by means of an International Agreement concluded on the basis of Article 300, of the Treaty and only if the assent of the European Parliament has been obtained to this agreement (Article 300, paragraph 3, subparagraph 2 of the Treaty).

Amendment 28
Article 3 b (new)

Data protection and data security

Each Member State shall ensure that data retained under this Directive is subject, as a minimum, to the rules implementing Article 17 of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movements of such data, to the provisions of Article 4 and 5 of Directive 2002/58/EC and the following data security principles:

(a) the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction or loss, alteration, unauthorised or unlawful disclosure or

access, and against all other unlawful forms of processing;

(b) the data shall be subject to appropriate technical and organisational measures to ensure that disclosure of, and access to data is undertaken only by authorised persons whose conduct is subject to oversight by a competent judicial or administrative authority;

c) providers of publicly available electronic communications services or networks as well as Member State authorities accessing the data shall record all acces and take the appropriate security measures to prevent unauthorized or other inappropriate or unlawful storage, access, processing, disclosure, or use, including through fully updated technical systems to protect the integrity of data and through the designation of specially authorized personnel who can have exclusive access to the data;

d) providers of publicly accessible electronic communications services or networks create a separate system of storage of data for public order purposes, the data of this separate system cannot under any circumstance be used for business purposes or other purposes not explicitly authorized under this Directive;

e) the competent national authorities forward the data to third countries by means of an International Agreement on the basis of Article 300, of the Treaty and only if the assent of the European Parliament has been obtained to this agreement (Article 300, paragraph 3, subparagraph 2 of the Treaty);

(f) all data shall be destroyed at the end of the period for retention except those data which have been accessed and preserve;.

(g) the data protection authority or another competent independent authority in each member State, as prescribed by national

law is designated to oversee the lawful implementation of this Directive.

Amendment 29
Article 4, paragraph 1

Categories of data to be retained	Categories ***and types*** of data to be retained
Member States shall ensure that the following categories of data are retained under this Directive:	***1.*** Member States shall ensure that the following categories of data are retained under this Directive:
(a) data necessary to trace and identify the source of a communication;	(a) data necessary to trace and identify the source of a communication;
(b) data necessary to trace and identify the destination of a communication;	(b) data necessary to trace and identify the destination of a communication;
(c) data necessary to identify the date, time and duration of a communication;	(c)data necessary to identify the date, time and duration of a communication;
(d) data necessary to identify the type of communication;	(d) data necessary to identify the type of communication
(e)data necessary to identify the communication device or what purports to be the communication device;	(e) data necessary to identify the communication device or what purports to be the communication device;
(f) data necessary to identify the location of mobile communication equipment.	(f) data necessary to identify the location of mobile communication equipment.
The types of data to be retained under the abovementioned categories of data are specified in the Annex.	***No data revealing the content of the communication can be retained.***

Amendment 30
Article 4, paragraph 1 a (new)

Types of data to be retained

1) Concerning Fixed Network Telephony

a) Data necessary to trace and identify the source of a communication:

(a) The calling telephone number;

(b) Name and address of the subscriber or registered user;

b) Data necessary to trace and identify the

destination of a communication:

(a) The called telephone number or numbers;

(b) Name(s) and address(es) of the subscriber(s) or registered user(s);

c) Data necessary to identify the date, time and duration of a communication:

(a) The date and time of the start and end of the communication.

d) Data necessary to identify the type of communication:

(a) The telephone service used, e.g. voice, conference call, fax and messaging services.

2) Concerning Mobile Telephony:

a) Data necessary to trace and identify the source of a communication:

(a) The calling telephone number;

(b) Name and Address of the subscriber or registered user;

b) Data necessary to trace and identify the destination of a communication:

(a) The called telephone number or numbers;

(b) Name(s) and address(es) of the subscriber(s) or registered user(s);

c) Data necessary to identify the date, time and duration of a communication:

(a) The date and time of the start and end of the communication.

d) Data necessary to identify the type of communication:

(a) The telephone service used, e.g. voice, conference call,

Short Message Service, Enhanced Media Service or Multi-Media Service

e) Data necessary to identify the communication device or what purports to be the communication device:

(a) The International Mobile Subscriber Identity (IMSI) of the calling and called party;

(b) In case of pre-paid anonymous cards/services, the date and time of the initial activation of the card and the label (Cell ID) from which the activation was made.

f) Data necessary to identify the location of mobile communication equipment:

(a) The location label (Cell ID) at the start of the communication;

3) Concerning the Internet :

a) Data necessary to trace and identify the source of a communication:

(a) The Internet Protocol (IP) address, whether dynamic or static, allocated by the Internet access provider to a communication;

(b) The Connection Label or telephone number allocated to any communication entering the public telephone network;

(c) Name and address of the subscriber or registered user to whom the IP address or Connection Label was allocated at the time of the communication.

b) Data necessary to identify the date, time and duration of a communication:

(a) The date and time of the log-in and log-off of the Internet

sessions based on a certain time zone.

c) Data necessary to identify the communication device or what purports to be the communication device:

(a) The calling telephone number for dial-up access;

(b) The digital subscriber line (DSL) or other end point identifier of the originator of the communication;

Amendment 31
Article 4, paragraph 2

The types of data ***to be retained under the abovementioned*** categories of data ***are specified in the Annex.***	***Member States shall be free to request to providers of publicly available electronic communications services or of a communications network to retain*** data ***concerning unsuccessful call attempts to secure a communication, within these*** categories of data ***according to their national laws.***
	Data that reveals the content of a communication must not be included.

Amendment 32
Article 5

Revision of the annex	***deleted***
The Annex shall be revised on a regular basis as necessary in accordance with the procedure referred to in Article 6(2).	

Amendment 33
Article 6

Committee	***deleted***
1. The Commission shall be assisted by a Committee composed of representatives of the Member States and chaired by the representative of the Commission.	
2. Where reference is made to this paragraph, Article 5 and 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.	
3. The period laid down in Article 5(6) of Decision 1999/468/EC shall be three months.	

Amendment 34
Article 7

Member States shall ensure that the categories of data referred to in Article 4 are retained for a period of ***one year*** from the date of the communication, ***with the exception of data related to electronic communications taking place using wholly or mainly the Internet Protocol. The latter shall be retained for a period of six months.***	Member States shall ensure that the categories of data referred to in Article 4 are retained for a period of ***6-12 months*** from the date of the communication***; thereafter, the data must be erased.***
	Competent law enforcement authorities shall ensure that transferred data are erased by automated means once the investigation for which access to the data was granted is completed.

Amendment 35
ARTICLE 7, PARAGRAPH 1 B (new)

The Commission shall keep the European Parliament duly informed of the notifications made by Member States under Article 95 (4) of the Treaty.

Amendment 36
Article 8

Member States shall ensure that the data are retained in accordance with this Directive in such a way that the data retained and any other necessary information related to such data can be transmitted upon request to the competent authorities without undue delay.	Member States shall ensure that the data ***as specified in Article 4*** are retained ***by providers of publicly available electronic communications services or of a public communicating network,*** in accordance with this Directive in such a way that the data retained and any other necessary information related to such data can be transmitted upon request to the competent ***national*** authorities ***of the Member States concerned*** without undue delay. ***The processing of the data takes place in accordance with the provisions of Article 17 of Directive 95/46/EC and Article 4 of Directive 2002/58/EC.***

Amendment 37
Article 8, paragraph 1 a (new)

Member States shall ensure that the providers of publicly available electronic communication services or a public communication network concerned located on their territory set up a contact point to deal with requests for access to data.

Amendment 38
Article 8 a (new)

Sanctions

1. Member States shall lay down effective,

proportionate and dissuasive sanctions (including criminal and administrative sanctions) for infringements of the national provisions adopted to implement this Directive.

2. Member States shall ensure that persons against whom proceedings are brought with a view to imposing sanctions have effective rights of defence and appeal.

Amendment 39
Article 9

Member States shall ensure that statistics on the retention of data processed in connection with the provision of ***public*** electronic communication services are provided to the European Commission on a yearly basis. Such statistics shall include	Member States shall ensure that statistics on the retention of data processed in connection with the provision of electronic communication services are provided to the European Commission on a yearly basis. ***ENISA may provide help to Member States in collecting these statistics.*** Such statistics***, to be drawn up by the competent national authorities,*** shall include
- the cases in which information has been provided to the competent authorities in accordance with applicable national law,	- the cases in which information has been provided to the competent authorities, in accordance with applicable national law,
- the time elapsed between the date on which the data were retained and the date on which the competent authority requested the transmission of the data;	- the time elapsed between the date on which the data were retained and the date on which the competent authority requested the transmission of the data;
- the cases where ***requests for data could not be met.***	- the ***number of*** cases where ***the data requested did not directly lead to the successful conclusion of the relevant investigations;***
	- the number of cases where data requested was not available to the undertakings concerned.
	- the cases where suspected and factual security breaches occurred.
	The European Commission shall submit these statistics to the European Parliament

	each year and then each three years.
Such statistics shall not contain personal data.	Such statistics shall not contain personal data.

Amendment 40
<Article>Article 9 a (new)

	1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive regarding the security of the stored data. ***2. These authorities shall act with complete independence in exercising the functions referred to in paragraph 1.***

Amendment 41
Article 10

Member States shall ensure that providers of publicly available electronic communication services or of a public communication network are reimbursed for demonstrated additional costs they have incurred in order to comply with obligations imposed on them as a consequence of this Directive.	Member States shall ensure that providers of publicly available electronic communication services or of a public communication network are reimbursed for demonstrated additional ***investment and operating*** costs they have incurred in order to comply with obligations imposed on them as a consequence of this Directive ***including the demonstrated additional costs of data protection and any future amendments to it. The reimbursement should include demonstrated costs arising from making the retained data available to competent national authorities.***

Amendment 42
Article 11

In Article 15 of Directive 2002/58/EC the	In Article 15 of Directive 2002/58/EC the

following paragraph 1a is inserted:

”1a. Paragraph 1 shall not apply to obligations relating to the retention of data for the ***prevention,*** investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime, deriving from Directive 2005/../EC*. * OJ L nr. …. of ….”.

following paragraph 1a is inserted:

"1a. Paragraph 1 shall not apply to obligations relating to the retention of data for the investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime, deriving from ***the transposition of*** Directive 2005/../EC. * * OJ L nr. ..... of .....

Member States shall refrain from adopting legislative measures in the sectors covered by this Directive.

Amendment 43
Article 12, paragraph 1

1. Not later than ***three*** years from the date referred to in Article 13(1), the Commission shall submit to the European Parliament and the Council an evaluation of ***the application of this Directive and its*** impact on economic operators and consumers, taking into account the statistical elements provided to the Commission pursuant to Article 9 ***with a view to determining whether it is necessary to modify the provisions of this Directive, in particular with regard to the period of retention provided for in Article 7.***

1. Not later than ***two*** years from the date referred to in Article 13(1) the Commission shall submit to the European Parliament and the Council an evaluation of ***the necessity and effectiveness of the provisions contained in the Directive, and of the*** impact on ***fundamental rights of the data subjects. The evaluation will also consider the impact of the measures on*** economic operators and consumers, taking into account the statistical elements provided to the Commission pursuant to Article 9.

The results of the evaluations will be publicly available.

Amendment 44
Article 12, paragraph 2

2. To that end, the Commission shall examine all observations communicated to it by the Member States or by the Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

2. To that end, the Commission shall examine all observations communicated to it by the Member States or by the Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC ***or by the European Data***

Protection Supervisor.

Amendment 45
Article 14 a, paragraph 1 (new)

Revision

No later than two years after the date referred to in Article 13(1), this Directive shall be revised in accordance with the procedure laid down in Article 251 of the Treaty. In particular, the types of data retained and the retention periods shall be assessed to determine their relevance to the fight against terrorism and organised crime in the light of the statistics compiled pursuant to Article 9. The revision shall take place every three years.

Amendment 46
ANNEX

Types of data to be retained under the categories identified in Article 4 of this Directive:	***deleted***
a) Data necessary to trace and identify the source of a communication:	
(1) Concerning Fixed Network Telephony:	
(a) The calling telephone number;	
(b) Name and address of the subscriber or registered user;	
(2) Concerning Mobile Telephony:	
(a) The calling telephone number;	

(b) Name and Address of the subscriber or registered user;

(3) Concerning Internet Access, Internet e-mail and Internet telephony:

(a) The Internet Protocol (IP) address, whether dynamic or static, allocated by the Internet access provider to a communication;

(b) The User ID of the source of a communication;

(c) The Connection Label or telephone number allocated to any communication entering the public telephone network;

(d) Name and address of the subscriber or registered user to whom the IP address, Connection Label or User ID was allocated at the time of the communication.

b) Data necessary to trace and identify the destination of a communication:

(1) Concerning Fixed Network Telephony:

(a) The called telephone number or numbers;

(b) Name(s) and address(es) of the subscriber(s) or registered user(s);

(2) Concerning Mobile Telephony:

(a) The called telephone number or numbers;

(b) Name(s) and address(es) of the subscriber(s) or registered user(s);

(3) Concerning Internet Access , Internet e-mail and Internet telephony:

(a) The Connection Label or User ID of the intended recipient(s) of a communication;

(b) Name(s) and address(es) of the subscriber(s) or registered user(s) who are the intended recipient(s) of the communication.

c) Data necessary to identify the date, time and duration of a communication:

(1) Concerning Fixed Network Telephony and Mobile Telephony:

(a) The date and time of the start and end of the communication.

(2) Concerning Internet Access, Internet e-mail and Internet telephony:

(a) The date and time of the log-in and log-off of the Internet sessions based on a certain time zone.

d) Data necessary to identify the type of communication:

(1) Concerning Fixed Network Telephony:

(a) The telephone service used, e.g. voice, conference call, fax and messaging services.

(2) Concerning Mobile Telephony:

(a) The telephone service used, e.g. voice, conference call, Short Message Service, Enhanced Media Service or Multi-Media Service

e) Data necessary to identify the communication device or what purports to be the communication device:

(1) Concerning Mobile Telephony:

(a) The International Mobile Subscriber Identity (IMSI) of the

calling and called party;

(b) The International Mobile Equipment Identity (IMEI) of the calling and called party.

(2) Concerning Internet Access, Internet e-mail and Internet telephony:

(a) The calling telephone number for dial-up access;

(b) The digital subscriber line (DSL) or other end point identifier of the originator of the communication;

(c)The media access control (MAC) address or other machine identifier of the originator of the communication.

f) Data necessary to identify the location of mobile communication equipment:

(1) The location label (Cell ID) at the start and end of the communication;

(2) Data mapping between Cell IDs and their geographical location at the start and end of the communication.

EXPLANATORY STATEMENT

1. Rückblick

Im Rahmen der Ratstagung für Justiz und Inneres am 29./30. April 2004 haben Frankreich, Großbritannien, Irland und Schweden einen gemeinsamen Vorschlag[1] für einen Rahmenbeschluss zur Vorratsspeicherung von Kommunikationsdaten vorgelegt. Hintergrund der Initiative ist eine am 25. März 2004 vom Europäischen Rat verabschiedeten Erklärung zum Kampf gegen den Terrorismus[2], in der der Rat beauftragt wurde, Maßnahmen für die Erarbeitung von Rechtsvorschriften über die Aufbewahrung von Verkehrsdaten durch Diensteanbieter zu prüfen.

Ziel des Vorschlages ist eine Harmonisierung der justiziellen Zusammenarbeit in Strafsachen, indem die Rechtsvorschriften der Mitgliedstaaten über die Vorratsdatenspeicherung, die durch Diensteanbieter eines öffentlich zugänglichen elektronischen Kommunikationsdienstes verarbeitet und gespeichert werden, für die Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus, angeglichen werden.

Das Europäische Parlament hat diesen Ratsvorschlag für einen Rahmenbeschluss zur Vorratsdatenspeicherung in seinen Plenarsitzungen im Juni und September 2005 einstimmig zurückgewiesen. Nach Auffassung des Europäischen Parlaments hatte der Rat die falsche Rechtsgrundlage gewählt. Der Rat ging von seiner alleinigen Gesetzgebungsbefugnis gemäß Titel VI des Vertrages über die Europäische Union (EUV) aus und berief sich auf Art. 31 Abs. 1 Buchstabe c i. V. m. Art. 34 Abs. 2 Buchstabe b EUV.
Gemeinsam mit den juristischen Diensten von Rat und Kommission ist das Parlament der Auffassung, dass Art. 95 EGV die richtige Rechtsgrundlage ist. Hiernach ist das Parlament vollständig in den Gesetzgebungsprozess eingebunden und Mitentscheider.

Am 21. September 2005 hat die Europäische Kommission einen eigenen Richtlinienentwurf zur Vorratsdatenspeicherung unter Art. 95 EGV vorgelegt und somit die Grundlage für Verhandlungen mit dem Rat gelegt. In der Folge sind die Diskussionen zwischen Rat und Parlament intensiver geworden, obwohl der Rat es sich weiterhin vorbehält seinen Rahmenbeschluss durchzusetzen.

Das Europäische Parlament hatte neben der formalen Zuständigkeitsfrage erhebliche Bedenken gegenüber dem Inhalt des Rahmenbeschlusses zur Vorratsdatenspeicherung geäußert. Diesen Bedenken sind in dem Richtlinienentwurf der Kommission teilweise berücksichtigt worden.

Am 24. November hat der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres seine Position zum vorliegenden Richtlinienentwurf formuliert.

[1] Ratsdokument 8958/04 v. 28. April 2004
[2] Ratsdokument 7764/04 v. 28. März 2004

2. Ausgangslage nach Vorlage des Kommissionsentwurfs

a. inhaltlich

Der Richtlinienentwurf der Kommission zur Vorratsdatenspeicherung sieht folgende Regelungen vor:

Scope	Traffic data on fixed and mobile telephony, internet , e-mail and IP telephony – location data and unsuccessful calls included
Purpose of retention	Prevention, detection, investigation and prosecution of serious crime, such as terrorism and organised crime
Authorities to have access	Competent authorities determined by MS
Access to data	Not included
Retention periods	12 months telephony, 6 months internet
Costs	Reimbursement of demonstrated additional costs as a consequence of the Directive
Flexibility under Article 15 (1) of Directive 2002 (58)	Flexibility: it allows the use of data retention for other purposes – but harmonised dataset for combating serious crime
Data protection provisions	Not necessary – covered by existing Directives (95/46 and 2002/58)
Penal sanctions	Not included, covered by Framework Directive on attacks against information systems and data protection Directives
Comitology procedure to update list of data	Included
Review clause	Three years
Data to be retained (Annex)	

b. formal

Der Vorschlag der Kommission zur Regelung der Vorratsdatenspeicherung ist dem Parlament am 21. September mitgeteilt worden. Die Richtlinie lag zum Abstimmungszeitpunkt im Ausschuss somit gerade mal zwei Monate vor.
Die britische Ratspräsidentschaft hat ihr Interesse zum Ausdruck gebracht, dass eine Regelung noch vor Ende des Jahres 2005 als Kompromiss in erster Lesung verabschiedet werden solle. Die Konferenz der Präsidenten bestätigte das Interesse des Parlaments gleichfalls einen Kompromiss vor Ablauf des Jahres zu erreichen.
Das Parlament hat seine Arbeit zügigst aufgenommen, um eine gemeinsame Position zu formulieren und so seinen Teil zur Schaffung eines Kompromisses beizutragen. Die letzte Gelegenheit einen Kompromiss in erster Lesung zu verabschieden ist die Plenarwoche vom 12.-15. Dezember. Dieses extrem beschleunigte Gesetzgebungsverfahren hat unter anderem wegen der Übersetzungsfristen mangelnde Beratungszeiten oder teilweise fehlende Übersetzungen zur Folge gehabt. Ebenso fehlt es an einer Technikfolgen-Abschätzung oder einer Studie zu den Auswirkungen auf den Binnenmarkt.
Gerade mit Blick auf die Maßnahmen und Vorhaben zur „better regulation“ auf europäischer

Ebene wird das Verfahren bei den Beratungen zur Vorratsdatenspeicherung hoffentlich kein Regelfall.

Um am 24. November einen Vorschlag im Ausschuss für bürgerliche Freiheiten, Justiz und Inneres abstimmen zu können und die zahlreichen strittigen inhaltlichen Fragen zu lösen traf sich regelmäßig eine Arbeitsgruppe zur Vorratsdatenspeicherung. In dieser haben der Berichterstatter, die Schattenberichterstatter, Berichterstatter von IMCO und ITRE, Ausschussvorsitz und –sekretariat, die Koordinatoren sowie Mitarbeiter innerhalb von 7 Wochen Kompromissanträge erarbeitet. Während dieser Zeit erfolgten regelmäßige Treffen mit Rat und Kommission, um den Sachstand in den jeweiligen Institutionen zu besprechen.

3. Votum des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres

Am 24. November 2005 hat der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres seine Position zum Richtlinienentwurf der Kommission mit einer deutlichen 3/4 Mehrheit formuliert. Im Vorfeld der Abstimmung haben sich die Abgeordneten von PPE-ED, PSE und ALDE auf 21 Kompromissanträge verständigen können, die einen Großteil der 250 eingereichten Änderungsanträge ersetzen konnten.

LIBE position based on compromise amendments (committee vote, 1st reading)

Scope	Traffic data on fixed and mobile telephony – location data (at the start of a call) (Comp. AM 9: opt-in system for MS for unsuccessful calls Respect private life/protection of personal data in access/use of data (Comp. AM 1)
Purpose of retention	Detection, investigation, and prosecution of specified forms of **serious** criminal offences to define this list of offences is taken which is used for the European Arrest Warrant. '**prevention**' is excluded because it is a vague concept and makes the retained data more vulnerable from abuses (Comp. AM 1)
Authorities to have access	Access **by judicial authorities** and other authorities responsible for detection, investigation and prosecution of **serious criminal offences** (following the list of the European Arrest Warrant). In any case, national authorities must be subject to **judicial authorisation.** (Comp. AM 2, 4)
Access to data	A provision on **conditions** on access to the data has been introduced by the committee: - only for specific purposes, defined by the directive and on a case by case basis

	- The reasons must be necessary/proportionate - erase data when no longer necessary / when inaccurate - providers are prohibited to use data - any accessing of retained data is recorded - confidentiality/integrity of data shall be ensured - data **can only** be transmitted to **third countries** by means of an International Agreement, on the basis of Article 300, par. 3, subpar. 2 of the Treaty (Comp. AM 5)
Retention periods	6 -12 months for everything. After such period, all data must be erased. (Comp. AM 12)
Costs	Member States will ensure the reimbursement of demonstrated additional costs for telecom industry (including 'investment and operating costs', also costs resulting from further modifications of the directive). *in the Council the tendency is to exclude reimbursement of the directive. (Comp. AM 18)
Flexibility under Article 15 (1) of Directive 2002 (58)	MS shall refrain from adopting legislative measures in the sectors covered by the Directive (AM 224)
Data protection provisions	Additional provisions on data security, proposed in line with existing Directives (see a detailed list in the compromise amendment) (Comp. AM 6)
Penal sanctions	Effective, proportionate and dissuasive penalties for infringements of the national provisions adopted to implement Directive. (Comp. AM 15)
Comitology procedure to update list of data	Not included
Review clause	Review after 2 years of its implementation and periodic review every 3 years. (Comp. AM 21)
Data to be retained (Annex)	Committee has voted in favour of placing the Annex into the main text Includes pre-paid anonymous cards/services, the date and time of the initial activation of the card and the label (Cell ID) from which the activation was made" -"types" of data to be retained: FIXED PHONE: - Name/address of person who calls + phone number - Name/address of person/s who receive the call + phone number

	- Date and time of the start and end of the conversation MOBILE PHONE: - Name/address of person who calls + phone number - Name/address of person/s who receive the call + phone number - Date and time of the start and end of the conversation - international mobile subscriber Identity (IMSI) = sim card - location label **at the start** of the communication INTERNET: - IP address of computer - Telephone number connecting to the internet - Name/address of subscriber - Date / time of log-in and log-off - ADSL-calling telephone number for dial-up access and the digital ADSL subscriber (Comp. AM 8)

Diese mit Mehrheit beschlossenen Anträge zeigen, dass das Parlament sehr gut in der Lage war sich fraktionsübergreifend auf wesentliche Punkte zur Vorratsdatenspeicherung zu einigen. Der Rat hat vergleichbares, zumindest zum Zeitpunkt der Berichtserstellung, noch nicht erreicht. Insofern bleibt die Entwicklung im Rat abzuwarten. Der Berichterstatter ist aber der Auffassung, dass für substanzielle Änderungen an den erreichten Kompromissanträgen kein Spielraum besteht.

4. Tendenz der bisherigen Meinungsbildung im Rat

Entsprechend der Abstimmung im Ausschuss für bürgerliche Freiheiten, Justiz und Inneres am 24. November ergeben sich folgende Abweichungen von der Tendenz der Meinungen im Rat.

	European Parliament	**Tendency of negociations in Council**
Length of retention	6-12 months for all (telephony and internet)	6 months for internet, 6-24 months for telephony
Scope	Uses the European Arrest Warrant definition of "serious crime" (catalogue + 3 years imprisonment),	All crimes are included
Cost reimbursement	Mandatory for all additional costs that the Directive pose + costs related to data protection requirements,	An optional national scheme
Unsuccessful calls	An opt-in where MS can choose to oblige telecoms	Mandatory retention of unsuccessful calls

Penal sanctions	Criminal sanctions for misuse of the data	Against

MINORITY OPINION

Wir lehnen diesen Bericht ab, da er den Richtlinienvorschlag über die "Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden" weder politisch noch rechtlich im erforderlichen Maß korrigiert.

Der von der Kommission vorgeschlagene Rechtsakt verstößt auch mit den Änderungsvorschlägen dieses Berichts gegen das Verhältnismäßigkeitsprinzip. Er ist zudem weder notwendig, noch effektiv. Die vorgesehene Speicherdauer der Daten ist viel zu lang, und das Ausmaß der zu speichernden Datentypen ist zu weitreichend. Unpräzise ist die Definition der zuständigen Behörden, die Zugriff auf die Daten haben, der Zugang von Geheimdiensten wird nicht ausgeschlossen. Unzureichend geregelt sind die Kontrollmechanismen zur Datensicherheit.

Der Richtlinienvorschlag stellt einen tiefen Eingriff in die Grundrechte der Bürgerinnen und Bürger dar, den wir nicht unterstützen können. Die Bürgerinnen und Bürger der Union dürfen nicht unter Generalverdacht gestellt werden. Rat und Kommission sind bislang den Nachweis schuldig geblieben, dass schwere Straftaten durch die Vorratsspeicherung einer Unmenge verschiedenster Kommunikationsdaten tatsächlich erfolgreicher aufgeklärt werden können.

Darüber hinaus bestehen Bedenken, dass der Richtlinienentwurf oder Teile dessen - sowohl in der Fassung der Kommission als auch in der des Ausschusses - nicht in den Anwendungsbereich der gewählten Rechtsgrundlage gemäß Artikel 95 EGV fallen.

23.11.2005

OPINION OF THE COMMITTEE ON INDUSTRY, RESEARCH AND ENERGY

for the Committee on Civil Liberties, Justice and Home Affairs

on the proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC
(COM(2005)0438 – C6-0293/2005 – 2005/0182(COD))

Draftswoman: Angelika Niebler

SHORT JUSTIFICATION

Background

On 21 September 2005 the Commission published a proposal for a directive on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC. In so doing the Commission has presented, on the basis of Article 95 of the EC Treaty, a deliberate counter-proposal to the Council's Draft Framework Decision on data retention drafted in 2004 by France, Ireland, the UK and Sweden.[1]

This development is a welcome one from the European Parliament's point of view. The Commission has chosen a legal basis which allows Parliament the right of codecision on this issue of great importance both for citizens and businesses. By contrast, the Framework Decision, based on Articles 31(1)(c) and 34(2)(b) of the EU Treaty, gives Parliament only the right to be consulted.

In terms of substance, the Commission's proposed directive and the Draft Framework Decision tend in the same direction. Both seek to improve the fight against terrorism and serious crime by requiring the providers of public communication networks to retain certain data in accordance with harmonised provisions.

The data covered are traffic and location data within the meaning of Article 2 of Directive 2002/58/EC, including user and subscriber data. This means that the data to be retained are the following: all information about place, time, duration and number called in telephone

[1] DOC. 8958/04 of 28 April 2004.

conversations, faxes, e-mails, text messages and Internet protocols. The content of conversations is specifically excluded.

Evaluation

The Member States currently have different regulations governing retention times for individual items of communications data. From the point of view of effective cross-border action against terrorism and crime this is undoubtedly a disadvantage, since criminals increasingly operate across borders and use modern means of communication to do so. The proposed directive may accordingly become an important instrument in the fight against crime.

Your draftswoman considers, however, that it raises a number of serious issues which should be addressed by the Committee on Industry, Research and Energy in particular so as to take account of the specific aspects of the communications and information society on which the directive touches.

Like the Council in its above-mentioned Draft Framework Decision, the Commission uses a very broad brush to demonstrate that the proposed measures will actually lead to an improvement in the fight against crime and terrorism. It is, however, essential for this to be proved in order to justify the significant effects and burdens on citizens and businesses. It appears, however, that the data requested by the prosecuting authorities in practice are not normally more than 3 months old. The legal retention times should therefore be adapted to take account of actual needs.

For telecoms firms the proposal would mean having to retain an inconceivably large amount of data. To store, archive and make available this volume of data would require expensive system adjustments. Calculations within the industry estimate that these adjustments would entail costs in the hundreds of millions of euro for some companies, not counting the follow-on costs for system maintenance and servicing.

As well as reducing retention time, then, it is also necessary to cut down the number of types of data to be retained (as set out in the Annex). Calls which fail to establish a connection, which are covered by the Commission proposal and would lead to major additional costs especially in fixed network telephony – without yielding any crime-fighting benefits, are an obvious candidate for the axe, as are data relating to the mobile phone identity, the MAC address or the location during or at the end of a mobile communication.

It causes your draftswoman serious concern that under Articles 5 and 6 of the proposal, the Annex and thus the substantive provisions of the directive governing the types of data to be retained, may be altered using the comitology procedure. This would mean that Parliament was entirely excluded from decisions on this sensitive issue. The provisions to this effect should therefore be deleted.

The requirement, in Article 9 of the proposal, for Member States to submit statistics relating to data retention, should not lead to extra bureaucratic demands on businesses, though in fact these statistics could also be used to provide evidence of the number of cases in which the requests actually led to successful investigations.

Finally, on this issue of great public sensitivity, Parliament should not allow itself to be hustled into action. Understandable though the desire is to conclude this legislative procedure as quickly as possible, stress must be laid on the importance of thoughtful debate. Furthermore, in the interest of the credibility of the European Union we must avoid a situation where work is under way simultaneously on two legal acts trying to achieve the same objective. In your draftswoman's view, the Council should therefore in future concern itself exclusively with the directive proposed by the Commission.

AMENDMENTS

The Committee on Industry, Research and Energy calls on the Committee on Civil Liberties, Justice and Home Affairs, as the committee responsible, to incorporate the following amendments in its report:

Text proposed by the Commission[1]	Amendments by Parliament
Amendment 1 RECITAL 12	
(12) The categories of information to be retained reflect an appropriate balance between the benefits for the prevention, investigation, detection, and prosecution of the serious offences involved and the level of invasion of privacy they will cause; the applicable retention period of ***one year***, respectively ***six months*** where data relate to electronic communications taking place using solely the Internet Protocol, also strikes a reasonable balance between all the interests involved.	(12) The categories of information to be retained reflect an appropriate balance between the benefits for the prevention, investigation, detection, and prosecution of the serious offences involved and the level of invasion of privacy they will cause; the applicable retention period of ***six months***, respectively ***three months*** where data relate to electronic communications taking place using solely the Internet Protocol, also strikes a reasonable balance between all the interests involved.
Justification	
A maximum period of six months is in keeping with the proportionality principle, given that almost all investigations are dealt with using data less than six months old.	
Amendment 2 RECITAL 13	
(13) Given the fact that retention of data generates significant additional costs for electronic communication providers, whilst the benefits in terms of public security impact on society in general, it is appropriate to foresee that Member States reimburse demonstrated additional costs incurred in order to comply with the obligations	(13) Given the fact that retention of***, and affording access to,*** data generates significant additional costs for electronic communication providers, whilst the benefits in terms of public security impact on society in general, it is appropriate to foresee that Member States ***ensure full reimbursement to all electronic***

[1] Not yet published in OJ.

imposed on them as a consequence of this Directive.	***communication providers for*** demonstrated additional costs incurred in order to comply with the obligations imposed on them as a consequence of this Directive.

Justification

The additional costs arising from a procedure intended to strengthen the security of the Member States must not be borne by operators.

Amendment 3
RECITAL 14

(14) Technologies relating to electronic communications are changing rapidly and the legitimate requirements of the competent authorities may evolve; to advise on these matters the Commission envisages *to create* a platform composed of representatives of the law enforcement authorities, associations of the electronic communications industry and data protection authorities.	(14) Technologies relating to electronic communications are changing rapidly and the legitimate requirements of the competent authorities may evolve; to advise on these matters the Commission envisages *creating* a platform composed of representatives of the law enforcement authorities, associations of the electronic communications industry and data protection authorities. ***The Commission undertakes to consult the European Parliament on any possible adaptation of the provisions of this Directive.***

Justification

It is essential for Parliament to be involved in any revision of the directive, given the potential risk that fundamental freedoms and rights might be violated.

Amendment 4
RECITAL 16

(16) It is essential that Member States provide legislative measures to ensure that data retained under this Directive are only provided to the competent national authorities in accordance with national legislation in full respect of the fundamental rights of the persons concerned; such measures include in particular appropriate	(16) It is essential that Member States provide legislative measures to ensure that data retained under this Directive are only provided to ***and used by*** the competent national authorities in accordance with national legislation in full respect of the fundamental rights of the persons concerned; such measures include in particular

conditions, limits and safeguards in order to ensure the conformity of the provision of the data retained with fundamental rights as guaranteed in particular in the European Convention for the Protection of Human Rights and Fundamental freedoms.	appropriate conditions, limits and safeguards in order to ensure the conformity of the provision of the data retained with fundamental rights as guaranteed in particular in the European Convention for the Protection of Human Rights and Fundamental freedoms.

Justification

Respect for fundamental freedoms and rights demands that national authorities alone be allowed to make use of the data concerned.

Amendment 5
RECITAL 17

(17) The measures necessary for the implementation of this Directive should be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission.	***deleted***

Justification

The comitology procedure proposed by the Commission, whereby representatives of the Commission and the Member States may add to the list of the data to be retained without any participation by the European Parliament or by businesses affected, is unacceptable. Any extension of the types of data to be retained is an interference in fundamental rights which should be subject to review by Parliament. Accordingly this recital should be deleted.

Amendment 6
RECITAL 19 A (new)

	19a. The Member States should ensure that the implementation of this Directive takes place following consultations with the business sector, particularly as regards feasibility and cost of retention. In view of the fact that retention entails a practical and financial effort from businesses, the Member States should guarantee full compensation for additional costs incurred by businesses as a result of obligations or

commitments relating to the transposition of this Directive.

Justification

Combating crime and guaranteeing public security are core duties of the modern state: accordingly, such measures must be fully funded from the public purse, and not at the expense of business, otherwise the attractiveness of Europe as a business location will be diminished. The full (investment and operational) costs of all obligations arising out of this Directive must therefore be entirely borne by the Member States. The same applies to the compilation of statistics, which should primarily be the task of the Member States.

Amendment 7
ARTICLE 1, PARAGRAPH 2

2. This Directive shall apply to traffic and location data of both private and legal persons, as well as the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network.	2. ***Since this Directive provides for derogations, its application shall be regularly reviewed under the supervision of the European Parliament. The European Parliament must have the information required to enable it to establish that application of this Directive does not contravene respect for the Charter of fundamental rights of the European Union, especially as regards the processing of personal data and the protection of privacy in the electronic communications sector.***
	This Directive shall apply to traffic and location data of both private and legal persons, as well as the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network.

Justification

It is essential for Parliament to be involved in any revision of the directive, given the potential risk that fundamental freedoms and rights might be violated.

Amendment 8
ARTICLE 3, PARAGRAPH 1

1. By way of derogation to Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that data ***which*** are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying communication services ***are retained in accordance with the provisions of this Directive***.	1. By way of derogation to Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that***, in cases where a connection was successfully established,*** data ***for the purpose set out in Article 1(1) are retained in accordance with the provisions of this Directive where they*** are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying communication services.

Justification

The amendment to paragraph 1 makes it clear that data retention can only be required when it is generated or processed in the course of the provision of communications services, since such a requirement might otherwise mean that services which do not generate certain types of data (e.g. prepaid telephony services) could no longer be supplied. Rendering such services impossible to supply or placing them under a disproportionate burden would reduce the attractiveness of the whole of Europe as a location for business, and would be in conflict with the Lisbon objectives.

Amendment 9
ARTICLE 3, PARAGRAPH 1 A (new)

	1a. The Member States may provide, having regard to necessity and proportionality, that paragraph 1 shall not apply to providers of publicly available electronic communications services and operators of a public communication network, taking into account their market share, number of their subscribers, and the size of the networks in question in proportion to the size of the market.

Justification

Small service providers would be unable to comply with the proposed comprehensive data retention obligation even given full compensation for costs, since they would be forced to alter their systems and business procedures as well having to field regular queries from the authorities. This would not be affordable and would kill off small and medium-sized service providers, which in turn would have serious negative consequences for the attractiveness of

Europe as a business location, since a large proportion of Europe's innovative power resides with SMEs.

Amendment 10
ARTICLE 3, PARAGRAPH 2

2. Member States shall adopt measures to ensure that data retained in accordance with this Directive are only provided to the competent national authorities, in specific cases and in accordance with national legislation, for the purpose of the prevention, investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime.	2. Member States shall adopt measures to ensure that data retained in accordance with this Directive are only provided to ***and used by*** the competent national authorities, in specific cases and in accordance with national legislation, for the purpose of the prevention, investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime. ***The competent national authorities must be in a position to give reasons for their transmission requests on the understanding that the contractual relationship between the provider and its customer must not be undermined and respect for the Charter of fundamental rights of the European Union must not be contravened, especially as regards the processing of personal data and the protection of privacy in the electronic communications sector.***

Justification

The contractual relationship between an operator and its customer must not be altered by these data retention measures. The authorities concerned have to be able to prove that their requests will be of use from the point of view of preventing, investigating, detecting, or prosecuting serious criminal offences such as terrorism and organised crime.

Amendment 11
ARTICLE 4, INTRODUCTORY PART

Member States shall ensure that the following categories of data are retained under this Directive	Member States shall ensure that***, in cases where a successful connection was established,*** the following categories of data are retained under this Directive ***for the purpose described in Article 1(1), provided that they are generated or processed in the course of the provision of communications***

	services by providers of publicly available electronic communications services or of a public communications network:

Justification

Telecoms firms already retain many of the types of data called for in the proposed directive. The extended data retention requirement would, however, entail significant costs, since existing data banks would have to be expanded and adjusted. The retention requirement should therefore apply only where a connection was successfully established.

Amendment 12
ARTICLE 4, POINT (A)

(a) data necessary to trace and identify the source of a communication;	(a) data necessary to trace and identify the source of a communication; ***(1) Concerning fixed network telephony:*** ***(a) The calling telephone number;*** ***(b) Name and address of the subscriber or registered user;*** ***(2) Concerning mobile telephony:*** ***(a) The calling telephone number;*** ***(b) Name and address of the subscriber or registered user;*** ***(3) Concerning Internet access:*** ***(a) The Internet Protocol (IP) address, whether dynamic or static, allocated by the Internet access provider to a communication;*** ***(b) The User ID of the source of a communication;*** ***(c) Name and address of the subscriber or registered user to whom the IP address, Connection Label or User ID was allocated at the time of the communication.***

Amendment 13
ARTICLE 4, POINT (B)

(b) data necessary to ***trace and*** identify the destination of a communication	(b) data necessary to identify the destination

	of a communication*:*
	(1) Concerning fixed network telephony:
	(a) The called telephone number or numbers;
	(2) Concerning mobile telephony:
	(a) The called telephone number or numbers;
	(3) Concerning Internet access :
	(a) The Connection Label or User ID of the intended recipient(s) of a communication;

Amendment 14
ARTICLE 4, POINT (C)

(c) data necessary to identify the date, time and duration of a communication	(c) data necessary to identify the date, time and duration of a communication*:*
	(1) Concerning fixed network telephony and mobile telephony:
	(a) The date and time of the start and end of the communication.
	(2) Concerning Internet access:
	(a) The date and time of the log-in and log-off of the Internet sessions based on a certain time zone.

Amendment 15
ARTICLE 4, POINT (D)

(d) data necessary to identify the type of communication	(d) data necessary to identify the type of communication*:*
	(1) Concerning fixed network telephony:
	(a) The telephone service used, e.g. voice, fax and messaging services.
	(2) Concerning mobile telephony:
	(a) The telephone service used, e.g. voice, Short Message Service (SMS).

Amendment 16
ARTICLE 4, POINT (E)

(e) data necessary to identify the communication device or what purports to be the communication device	(e) data necessary to identify the communication device or what purports to be the communication device***:***
	(1) Concerning mobile telephony:
	(a) The International Mobile Subscriber Identity (IMSI) of the calling party;
	(2) Concerning Internet access:
	(a) The calling telephone number for dial-up access;
	(b) The digital subscriber line (DSL) or other end point identifier of the originator of the communication.

Justification

Mobile telephone serial numbers are issued more than once by the manufacturers and can be manipulated by users .
The machine ID number of a computer's network card cannot be reliably identified, since it may also be issued more than once by the manufacturers and can subsequently be easily manipulated by the user. The retention of these two types of data will not bring about a perceptible improvement in the fight against crime.

Amendment 17
ARTICLE 4, POINT (F)

(f) data necessary to identify the location of mobile communication equipment.	(f) data necessary to identify the location of mobile communication equipment***:***
	(1) The location label (Cell ID) at the start of the communication;

Justification

The proposal that the Cell ID should be retained at the end as well as at the start of a call would entail significant additional costs. At present, only the location at the start of the call is retained in some Member States. In any case the Cell ID retained at the beginning of each new call makes it possible in retrospect to form a sufficiently accurate movement profile.

Amendment 18
ARTICLE 4, PARAGRAPH 2

The types of data to be retained under the abovementioned categories of data are specified in the Annex.	***deleted***

Amendment 19
ARTICLE 5

Article 5	***deleted***
Revision of the annex	
The Annex shall be revised on a regular basis as necessary in accordance with the procedure referred to in Article 6(2).	

Justification

The comitology procedure proposed by the Commission, whereby representatives of the Commission and the Member States may add to the list of the data to be retained without any participation by the European Parliament or by businesses affected, is unacceptable. Any extension of the types of data to be retained is an interference in fundamental rights which should be subject to review by Parliament. Accordingly the provisions to this effect should be deleted.

Amendment 20
ARTICLE 6

Article 6	***deleted***
Committee	
1. The Commission shall be assisted by a Committee composed of representatives of the Member States and chaired by the representative of the Commission.	
2. Where reference is made to this paragraph, Article 5 and 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.	
3. The period laid down in Article 5(6) of Decision 1999/468/EC shall be three months.	

Justification

The comitology procedure proposed by the Commission, whereby representatives of the Commission and the Member States may add to the list of the data to be retained without any participation by the European Parliament or by businesses affected, is unacceptable. Any extension of the types of data to be retained is an interference in fundamental rights which should be subject to review by Parliament. Accordingly the provisions to this effect should be deleted.

Amendment 21
ARTICLE 7

Member States shall ensure that the categories of data referred to in Article 4 are retained for a period of ***one year*** from the date of the communication, with the exception of data related to electronic communications taking place using wholly or mainly the Internet Protocol. The latter shall be retained for a period of ***six months***.	Member States shall ensure that the categories of data referred to in Article 4 are retained for a period of ***six months*** from the date of the communication, with the exception of data related to electronic communications taking place using wholly or mainly the Internet Protocol. The latter shall be retained for a period of ***three months***. ***At the end of the retention period, the data must be erased or made anonymous, in accordance with Directive 2002/58/EC.***

Justification

A maximum period of six months is in keeping with the proportionality principle, given that almost all investigations are dealt with using data no more than six months old.

Amendment 22
ARTICLE 8

Member States shall ensure that the data are retained in accordance with this Directive in such a way that ***the data retained and any other necessary information related to such data*** can be transmitted upon request to the competent authorities ***without undue delay***.	Member States shall ensure that the data are retained in accordance with this Directive in such a way that ***they*** can be transmitted ***in due course*** upon ***written*** request***, stating reasons,*** to the competent authorities.

Justification

The provisions of the proposed directive constitute a derogation from Articles 5, 6 and 9 of Directive 2002/58/EC. Consequently the data to be transmitted should be definitively specified. A procedure should also be provided for their transmission, in the interest of legal certainty and data protection. Past experience shows that transmission may cause delays for

technical reasons, so that transmission without delay is not always possible.

Amendment 23
ARTICLE 9, PARAGRAPH 1

Member States shall ensure that statistics on the retention of data processed in connection with the provision of public electronic communication services are provided to the *European* Commission on a yearly basis. Such statistics shall include	Member States shall ensure that statistics on the retention of data processed in connection with the provision of public electronic communication services are provided to the Commission ***and the European Parliament*** on a yearly basis ***by the competent authorities***. Such statistics shall include
- the cases in which information has been provided to the competent authorities in accordance with applicable national law,	- the cases in which information has been provided to the competent authorities in accordance with applicable national law,
- the time elapsed between the date on which the data were retained and the date on which the competent authority requested the transmission of the data;	- the time elapsed between the date on which the data were retained and the date on which the competent authority requested the transmission of the data;
- the cases where requests for data could not be met.	- the cases where requests for data could not be met
	- the cases in which requests for specific types of data led to, or significantly contributed to, successful investigations.

Justification

The requirement set out in Article 9 of the proposal for Member States to submit statistics in connection with data retention should not lead to extra bureaucratic demands on businesses. However, such statistics could also be used as evidence of the number of cases in which requests actually led to successful investigations.

Amendment 24
ARTICLE 10

Member States shall ensure that providers of publicly available electronic communication services or of a public communication network are reimbursed for demonstrated additional costs they have incurred in order to comply with obligations imposed on them as a consequence of this Directive.	Member States shall ensure that ***all*** providers of publicly available electronic communication services or of a public communication network are ***fully*** reimbursed for ***all*** demonstrated additional costs they have incurred in order to comply with obligations imposed on them as a consequence of this Directive

Justification

The fact that the Commission proposal provides for the reimbursement to businesses of investment and operating costs is to be welcomed. The proposed amendment is purely for purposes of clarification. At the same time the reimbursement of costs is an important regulatory instrument for reducing requests by the prosecuting authorities to the minimum necessary, and preventing distortions of competition on the basis of differing reimbursement procedures.

Amendment 25
ARTICLE 12, PARAGRAPH 1

1. Not later than three years from the date referred to in Article 13(1), the Commission shall submit to the European Parliament and the Council an evaluation of the application of this Directive and its impact on economic operators and consumers, taking into account the statistical elements provided to the Commission pursuant to Article 9 with a view to determining whether it is necessary to modify the provisions of this Directive, in particular with regard to ***the period of retention provided for in Article 7***.	1. Not later than three years from the date referred to in Article 13(1), the Commission shall submit to the European Parliament and the Council an evaluation of the application of this Directive and its impact on economic operators and consumers, taking into account the statistical elements provided to the Commission pursuant to Article 9 with a view to determining whether it is necessary to modify the provisions of this Directive, in particular with regard to ***the types of data set out in Article 4***.

Justification

In line with the proposed deletion of the comitology procedure in Article 5, an evaluation of all provisions of the directive, without distinction, should take place. Since the requirement of data retention is imposed on businesses and will entail significant costs for them, these costs should be taken into account in an evaluation of the directive.

Amendment 26
ARTICLE 12, PARAGRAPH 2

2. To that end, the Commission shall examine all observations communicated to it by the Member States or by the Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.	2. To that end, the Commission shall examine all observations communicated to it by the Member States***, by the commercial sector*** or by the Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC***, together with any report drawn up by the European***

Parliament pursuant to Article 1 of this Directive.

Justification

It is essential for Parliament to be involved in any revision of the directive, given the potential risk that fundamental freedoms and rights might be violated.

Amendment 27
ANNEX

This annex deleted

Justification

The Annex should be deleted in its entirety and placed in Article 4. The list of data constitutes the substance of the proposed directive and not merely a technical detail. The nature of the data to be retained determines the usefulness, feasibility, cost and proportionality of data retention. Accordingly the data list should not form part of an Annex separate from the operative text of the directive but should appear directly in Article 4.

PROCEDURE

Title	Proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC
References	COM(2005)0438 – C6-0293/2005 – 2005/0182(COD)]
Committee responsible	LIBE
Opinion by Date announced in plenary	ITRE 15.11.2005
Enhanced cooperation – date announced in plenary	No
Drafts(wo)man Date appointed	Angelika Niebler 5.10.2005
Previous drafts(wo)man	
Discussed in committee	22.11.2005 23.11.2005
Date adopted	23.11.2005
Result of final vote	+: 37 –: 4 0: 1
Members present for the final vote	Ivo Belet, Jan Březina, Philippe Busquin, Jerzy Buzek, Joan Calabuig Rull, Pilar del Castillo Vera, Jorgo Chatzimarkakis, Giles Chichester, Den Dover, Lena Ek, Nicole Fontaine, Adam Gierek, Norbert Glante, Umberto Guidoni, András Gyürk, Fiona Hall, David Hammerstein Mintz, Ján Hudacký, Romana Jordan Cizelj, Werner Langen, Anne Laperrouze, Nils Lundgren, Eluned Morgan, Angelika Niebler, Reino Paasilinna, Umberto Pirilli, Miloslav Ransdorf, Vladimír Remek, Herbert Reul, Mechtild Rothe, Paul Rübig, Britta Thomsen, Patrizia Toia, Catherine Trautmann, Claude Turmes, Nikolaos Vakalis, Alejo Vidal-Quadras Roca, Dominique Vlasto
Substitute(s) present for the final vote	Avril Doyle, Erna Hennicot-Schoepges, Vittorio Prodi, Hannes Swoboda
Substitute(s) under Rule 178(2) present for the final vote	
Comments (available in one language only)	...

22.11.2005

OPINION OF THE COMMITTEE ON THE INTERNAL MARKET AND CONSUMER PROTECTION

for the Committee on Civil Liberties, Justice and Home Affairs

on the proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC
(COM(2005)0438 – C6-0293/2005 – 2005/0182(COD))

Draftswoman: Charlotte Cederschiöld

SHORT JUSTIFICATION

As the Commission proposal is based on Article 95 of the Treaty - the Internal Market article - it is vital that the Committee on the Internal Market and consumer protection can deliver an opinion.

Data retention measures affect all parts of society with wide-ranging economic, social and industrial implications. Harmonising data retention provisions in the EU has severe implications not only for European consumers but also for European industry and ultimately the internal market. Unless harmonisation is carefully introduced, both citizens' fundamental rights and European competitiveness will be at risk.

Current situation

All the Member States have different regimes in place in terms of data retention periods, types of data to be retained and reimbursement for costs incurred for industry. A harmonised European approach could improve the situation if carefully designed while respecting the balance between all interests and affected parties.

Data retention represents a paradigm shift in the way society looks at traffic data. Under current laws electronic communications providers are only allowed to keep traffic data for specific legitimate business purposes and are obliged to erase traffic data once the purpose has been completed. Under the new proposal, operators would be required to store large quantities of new data specifically for law enforcement purposes which puts the European Union in a unique position, as no other democratic country in the world has introduced such far reaching obligations. This fact needs careful consideration, both in terms of privacy, competitiveness and security.

In the interest of better regulation it is questionable whether the EU should introduce such obligations at this stage without carefully examining the long-term consequences, with a thorough impact assessment. The system of data preservation and "quick freeze" could be a better way of enhancing cooperation between industry and law enforcement agencies and ought to be analysed from a consumer and internal market point of view.

The proposed comitology procedures are not acceptable – a wider solution has to be found, which includes all stakeholders that were not sufficiently consulted before the proposal was presented.

Impact on the internal market and European competitiveness

Heads of State and Government have repeatedly identified electronic communications as a cornerstone of the European economy: essential for sustainable growth and maximising employment. Any regulation, including data retention, must be carefully examined before it is introduced in order not to hamper competitiveness and development of EU businesses.

Costs

Successful collection of large amounts of data as foreseen in the proposed Directive is difficult and expensive. Trying to make sense of the different data formats and interpret them into something that is of value for law enforcement agencies is even more difficult.

Based on the volume of retained data, the cost will increase heavily due to changes in the design of the management systems, more powerful and sophisticated platforms, greater security measures, storage and support infrastructures as well as the necessary human resources to handle this type of systems.

It is obvious that data retention will put a heavy burden of cost on the European communications industry. The risk of a fragmented approach to the cost issue is obvious: If some Member States reimburse the electronic communications providers for data retention, while others don't, the internal market for communications services will suffer from grave distortions of competition.

Investments

European communications operators are currently rolling out next generation networks to meet the need for new e-services in both the private and public domain. Introducing data retention without a full cost compensation would force operators to dedicate resources to comply with the new regime, resources that would otherwise flow into building tomorrow's networks.

Competition

Irrespective of the question if full harmonisation is achieved within the EU, the fact remains that non-EU service providers will not be subjected to the same obligations and constraints. This will affect the competitive landscape and balance between the EU and competing economies. Many providers of electronic communications services, especially providers of Internet services, are based outside the EU while competing on the internal market. Service platforms can be set-up anywhere in the world: thus non-EU providers will even find themselves in a position to offer "*non-retention services*", and possibly build their business case on users' concern of their integrity and privacy. Far reaching data retention obligations

could deter European consumers from using European services.

In the case where an European operator provides Internet access, while the customer uses an e-mail provider in the US (e.g. Hotmail, Gmail, Yahoo), the European access provider does not have access to the traffic data as required by the Commission's proposal. In addition, many of the larger e-mail providers are based outside the EU and will in any case not be subject to the requirements.

Security

It might be possible to achieve high levels of information security, but a total security guarantee is virtually impossible to obtain. It will be paramount to safeguard that data stored are authentic and secured from any alteration, that access controls are strong and show a clearly auditable trail and chain of custody. The retention and storage of such large amounts of sensitive data will also face challenges at the software and network level (malware, spyware, spam, phishing) as well as non-internet based threats (for example the physical theft of data retention tapes).

Furthermore, the proposal lacks security provisions on proceedings once the information is collected in the Member State, if and how it can be transferred to other Member States as well as provisions forbidding the transfer of retained data to countries outside the EU. All these security aspects are a potential threat to the European Consumer.

AMENDMENTS

The Committee on the Internal Market and Consumer Protection calls on the Committee on Civil Liberties, Justice and Home Affairs, as the committee responsible, to incorporate the following amendments in its report:

Draft legislative resolution

Amendment 1
Paragraph 1 a (new)

1a. Calls on the Commission, prior to the entry into force of this Directive, to commission an impact assessment study from an independent body representing all stakeholders, covering all internal market and consumer protection issues;

Proposal for a directive

Text proposed by the Commission[1]	Amendments by Parliament

Amendment 2
RECITAL 13

[1] OJ C ... / Not yet published in OJ.

(13) Given the fact that retention of data generates significant additional costs for electronic *communication* providers, whilst the benefits in terms of public security impact on society in general, it is appropriate to *foresee* that Member States reimburse demonstrated additional costs incurred in order to comply with the obligations imposed on them as a consequence of this Directive.	(13) Given the fact that the retention of data generates significant additional costs for electronic *communications* providers, whilst the benefits in terms of public security impact on society in general, ***and in order to avoid distortions in the internal market,*** it is appropriate to *provide* that ***all*** Member States ***must ensure that providers of publicly available electronic communications services or of a public communications network are given full, harmonised reimbursement for*** demonstrated additional costs incurred in order to comply with the obligations imposed on them as a consequence of this Directive.

Amendment 3
RECITAL 13 A (new)

	(13a) Costs must be kept to a minimum in order to avoid putting EU companies at a competitive disadvantage as compared to non-EU companies.

Amendment 4
RECITAL 14

(14) Technologies relating to electronic communications are changing rapidly and the legitimate requirements of the competent authorities may evolve; to advise on these matters ***the Commission envisages*** to create ***a platform composed*** of representatives of the law enforcement authorities, ***associations of*** the electronic communications industry and data protection authorities.	(14) Technologies relating to electronic communications are changing rapidly and the legitimate requirements of the competent authorities may evolve; *in order* to advise on these matters ***it is necessary*** to create ***a standing committee*** of representatives of the ***European Parliament,*** law enforcement authorities, the electronic communications industry***, consumer protection organisations*** and data protection authorities.

Amendment 5
RECITAL 18 A (new)

(18a) Since the security of data retained under this Directive is of paramount importance for the safeguarding of consumers' rights, Member States should ensure that the highest standards of data storage security are applied, in particular in the protection of data from alteration and unauthorized access and from internet and non-internet related threats.

Amendment 6
RECITAL 18 B (new)

-	***(18b) The security treatment of data retained under this Directive must comply with the data protection provisions of Directive 2002/58/EC.***

Amendment 7
ARTICLE 1, PARAGRAPH 1

1. This Directive aims to harmonise the provisions of the Member States concerning obligations on the providers of publicly available electronic communications services or of a public communications network with respect to the processing and retention of certain data, in order to ensure that the data is available for the purpose of the prevention, investigation, detection and prosecution of ***serious*** criminal offences, ***such as terrorism and organised crime***.	1. This Directive aims to harmonise the provisions of the Member States concerning obligations on the providers of publicly available electronic communications services or of a public communications network with respect to the processing and retention of certain data, in order to ensure that the data is available for the purpose of the prevention, investigation, detection and prosecution of criminal offences.

Justification

This proposal is related to Article 15 of the Directive on data protection in the electronic communications sector (2002/58) which states that Member States may adopt data retention rules "to safeguard national security…, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system". The scope of the Commission proposal however is much more limited than the "mandate" given by Article 15 and should be extended. Data retention requirements are of primary importance to allow law enforcement measures and judicial proceedings to be taken against all forms of online crimes. Without a requirement to retain

data, authorities face significant obstacles in tracking illegal activities and identifying suspected infringers, and in talking actions to enforce offences and legal rights. In addition, the definition of "serious" may be subject to many different interpretations, which could create much legal uncertainty.

Amendment 8
ARTICLE 3

1. By way of derogation *to* Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that data which are ***generated or*** processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the *process* of supplying *communication* services are retained in accordance with the provisions of this Directive.	1. By way of derogation *from* Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that data which are processed ***and stored*** by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the *course* of supplying *communications* services are retained in accordance with the provisions of this Directive.

Justification

It is essential that the scope of the Directive is clearly defined: the word 'generated' being very broad and unclear it should be replaced by language which is already in use in European legislation. Processing is defined in the general Data Protection Directive (article 2b), while the Electronic Communication Directive on Data Retention refers to both processing and storing in its article 6.

Amendment 9
ARTICLE 3, PARAGRAPH 2

2. Member States shall adopt measures to ensure that data retained in accordance with this Directive are ***only*** provided to the competent national authorities, in specific cases and in accordance with national legislation, for the purpose of the prevention, investigation, detection and prosecution of ***serious*** criminal offences, ***such as terrorism and organised crime.***	2. Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided to the competent national authorities, in specific cases and in accordance with national legislation, for the purpose of the prevention, investigation, detection and prosecution of criminal offences***.***

Justification

The Commission proposal is too restricted compared to the "mandate" provided by Article 15 of the Directive on data protection in the electronic communications sector (2002/58) and should therefore be extended. Data retention requirements are of primary importance to allow law enforcement measures and judicial proceedings to be taken against all forms of online crimes. Without a requirement to retain data, authorities face significant obstacles in tracking illegal activities and identifying suspected infringers, and in talking actions to enforce offences and legal rights. In addition, the definition of "serious" may be subject to many different interpretations, which could create much legal uncertainty. Finally, this instrument must not prejudice any other Community/national measures for the enforcement of rights.

Amendment 10
ARTICLE 5

Revision of the annex	***deleted***
The Annex shall be revised on a regular basis as necessary in accordance with the procedure referred to in Article 6(2).	

Amendment 11
ARTICLE 6

Committee	***deleted***
1. The Commission shall be assisted by a Committee composed of representatives of the Member States and chaired by the representative of the Commission. ***2. Where reference is made to this paragraph, Article 5 and 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.*** ***3. The period laid down in Article 5(6) of Decision 1999/468/EC shall be three months.***	

Amendment 12
ARTICLE 7

Member States shall ensure that the categories of data referred to in Article 4 are retained for a period of one year from the date of the communication***, with the exception of data related to electronic***	Member States shall ensure that the categories of data referred to in Article 4 are retained for a period of one year from the date of the communication. ***Member States shall ensure that all data is erased at the***

communications taking place using wholly or mainly the Internet Protocol. The latter shall be retained for a period of six months.	***end of this retention period.***

Justification

The period of retention should be sufficiently long to enable national authorities to find evidence and prosecute law breakers. It can take a lot of time to conduct investigations into possible online infringements and some cases can involve complex online structures. It is therefore vital that the Commission's proposal provide that Member States implement procedures that offer enforcement bodies flexible and reliable means of ensuring that this critical evidence is stored for as long as possible in order to prepare a strong case.

Amendment 13
ARTICLE 8

Member States shall ensure that the data are retained in accordance with this Directive in such a way that the data retained and any other necessary information related to such data can be transmitted upon request to the competent authorities without undue delay.	Member States shall ensure that data are retained in accordance with this Directive in such a way that the data retained and any other necessary information related to such data can be transmitted upon request to the competent authorities without undue delay. ***Every request for data access between Member States must be accompanied by a guarantee that data retained under this Directive will be forwarded only to duly authorised law enforcement authorities and that they will not be forwarded to third countries.***

Amendment 14
ARTICLE 10

Member States shall ensure that providers of publicly available electronic *communication* services or of a public *communication* network are reimbursed for demonstrated additional costs they have incurred in order to comply with obligations imposed on them as a consequence of this Directive.	Member States shall ensure that providers of publicly available electronic *communications* services or of a public *communications* network are reimbursed for demonstrated additional ***investment and operating*** costs *which* they have incurred in order to comply with *the* obligations imposed on them as a consequence of this Directive***, including the demonstrated additional costs of data protection and any***

future amendments to it. The reimbursement should include demonstrated costs arising from making the retained data available to competent national authorities.

Justification

Compromise amendment as proposed by LIBE.

PROCEDURE

Title	Proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC
References	COM(2005)0438 – C6-0293/2005 – 2005/0182(COD)
Committee responsible	LIBE
Opinion by Date announced in plenary	IMCO 15.11.2005
Enhanced cooperation – date announced in plenary	
Drafts(wo)man Date appointed	Charlotte Cederschiöld 24.10.2005
Previous drafts(wo)man	
Discussed in committee	21.11.2005
Date adopted	22.11.2005
Result of final vote	+: 27 –: 5 0: 2
Members present for the final vote	Mia De Vits, Janelly Fourtou, Evelyne Gebhardt, Malcolm Harbour, Christopher Heaton-Harris, Anna Hedh, Edit Herczog, Anneli Jäätteenmäki, Pierre Jonckheer, Henrik Dam Kristensen, Alexander Lambsdorff, Kurt Lechner, Lasse Lehtinen, Toine Manders, Arlene McCarthy, Manuel Medina Ortega, Bill Newton Dunn, Zita Pleštinská, Zuzana Roithová, Luisa Fernanda Rudi Ubeda, Heide Rühle, Leopold Józef Rutowicz, Andreas Schwab, Eva-Britt Svensson, József Szájer, Marianne Thyssen, Jacques Toubon, Bernadette Vergnaud, Phillip Whitehead, Joachim Wuermeling,
Substitute(s) present for the final vote	Charlotte Cederschiöld, Joel Hasse Ferreira, Othmar Karas, Joseph Muscat, Alexander Stubb
Substitute(s) under Rule 178(2) present for the final vote	
Comments (available in one language only)	...

PROCEDURE

Title	Proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC
References	COM(2005)0438 – C6-0293/2005 – 2005/0182(COD)
Date submitted to Parliament	0.0.0000
Committee responsible Date announced in plenary	LIBE 15.11.2005
Committee(s) asked for opinion(s) Date announced in plenary	ITRE IMCO 15.11.2005 15.11.2005
Not delivering opinion(s) Date of decision	
Enhanced cooperation Date announced in plenary	
Rapporteur(s) Date appointed	Alexander Nuno Alvaro 26.09.2005
Previous rapporteur(s)	
Simplified procedure – date of decision	
Legal basis disputed Date of JURI opinion	
Financial endowment amended Date of BUDG opinion	
European Economic and Social Committee consulted – date of decision in plenary	
Committee of the Regions consulted – date of decision in plenary	
Discussed in committee	5.9.2005 26.92005 5.10.2005 13.10.2005 24.10.2005
	14.11.2005 24.11.2005
Date adopted	24.11.2005
Result of final vote	+: 33 –: 8 0: 5
Members present for the final vote	Alexander Nuno Alvaro, Edit Bauer, Johannes Blokland, Mario Borghezio, Mihael Brejc, Kathalijne Maria Buitenweg, Maria Carlshamre, Michael Cashman, Giusto Catania, Charlotte Cederschiöld, Carlos Coelho, Agustín Díaz de Mera García Consuegra, Rosa Díez González, Patrick Gaubert, Elly de Groen-Kouwenhoven, Adeline Hazan, Timothy Kirkhope, Ewa Klamt, Magda Kósáné Kovács, Wolfgang Kreissl-Dörfler, Barbara Kudrycka, Stavros Lambrinidis, Sarah Ludford, Edith Mastenbroek, Martine Roure, Inger Segelström, Antonio Tajani, Ioannis Varvitsiotis, Manfred Weber, Stefano Zappalà, Tatjana Ždanoka
Substitute(s) present for the final vote	Richard Corbett, Panayiotis Demetriou, Gérard Deprez, Lutz Goepel, Genowefa Grabowska, Jeanine Hennis-Plasschaert, Luis Herrero-Tejedor, Sylvia-Yvonne Kaufmann, Katalin Lévai, Bill Newton

	Dunn, Herbert Reul, Marie-Line Reynaud
Substitute(s) under Rule 178(2) present for the final vote	Sharon Margaret Bowles, Daniel Caspary, Othmar Karas, Gabriele Zimmer
Date tabled	24.11.2005
Comments (available in one language only)	...