

Data retention directive voting recommendations

by FFII, Privacy International and EDRI

Wed Dec 14 12:28:05 CET 2005

Contents

1	Plenary Amendments Data Retention: Voting list and summary	2
1.1	Voting list	2
1.2	Plenary amendments: Draft voting advice on Data Retention Directive	2
1.3	Rejection/Acceptance	9
1.4	Draft legislative resolution Paragraph 2	10
1.5	Draft legislative resolution Paragraph 2.a	10
1.6	Draft legislative resolution Paragraph 2.b	11
1.7	Article 1.1	11
1.8	Article 1.2	12
1.9	Article 2.2.point(a)	12
1.10	Article 2.2.point(ba)(new)	13
1.11	Article 2.2.point(bb)(new)	13
1.12	Article 2.2.point(bc)(new)	14
1.13	Article 2.2.point(bd)(new)	14
1.14	Article 3a(new)	14
1.15	Article 3b(new)	16
1.16	Article 3.1	17
1.17	Article 3.2	18
1.18	Article 3.2.a(new)	19
1.19	Article 4	19
1.20	Article 4.2.a(new)	23
1.21	Article 5	23
1.22	Article 6	23
1.23	Article 7	23
1.24	Article 7a(new)	24
1.25	Article 7.1.point(a)(new)	25
1.26	Article 8	25
1.27	Article 8a(new)	26
1.28	Article 8.1.point(a)(new)	26
1.29	Article 9.point(a)(new)	27
1.30	Article 9.1	27
1.31	Article 10	28
1.32	Article 11 “Article 15.1.point(a) (Directive 2002/58/EC)”	28
1.33	Article 11a(new)	29
1.34	Article 11b(new)	29
1.35	Article 12.1	30

1.36 Article 12.2	31
1.37 Article 13.1.1	31
1.38 Article 13.2a(new)	31
1.39 Article 14a (new)	32
1.40 Recital 3	32
1.41 Recital 4	33
1.42 Recital 4(a)(new)	34
1.43 Recital 6	34
1.44 Recital 6(a)(new)	34
1.45 Recital 7	35
1.46 Recital 8	35
1.47 Recital 9.point(a)(new)	35
1.48 Recital 10	36
1.49 Recital 10(a)(new)	37
1.50 Recital 11	37
1.51 Recital 11(a)(new)	38
1.52 Recital 12	38
1.53 Recital 12.point(a)(new)	39
1.54 Recital 13	39
1.55 Recital 14	39
1.56 Recital 15.point(a)(new)	40
1.57 Recital 16	40
1.58 Recital 16.point(a)(new)	41
1.59 Recital 16.point(b)(new)	41
1.60 Recital 17	42
1.61 Recital 17.point(a)(new)	42
1.62 Recital 18	42
1.63 Recital 18(various)(new)	43
1.64 Recital 19	44
1.65 Recital 19(a)(new)	44
1.66 Recital 19(b)(new)	45
1.67 Recital 19(c)(new)	45
1.68 ANNEX	46

1 Plenary Amendments Data Retention: Voting list and summary

1.1 Voting list

- **Voting list:** MS Word | PDF
- Summary of most important amendments: MS Word | PDF

Older reparative stuff below

1.2 Plenary amendments: Draft voting advice on Data Retention Directive

Clause	Topic	Amend nr	Source	Advice	Comment
REJECTION	Reject the directive outright	47	Greens; GUE;	+++	First prove necessity and proportionality of data retention, only then propose directive.
Draft legislative resolution Paragraph 2	Impact assessment study	48	EPP+PSE	-	impact assessments should be done before making laws and studies should be made by independent bodies
Draft legislative resolution Paragraph 2 a	Directive necessary first step	49	EPP+PSE	-	Necessity of this directive has not been demonstrated
Draft legislative resolution Paragraph 2 b	National constitution applicable, professional secrecy	50	EPP+PSE	-	a lawyers exception is unethical and impractical to implement
ARTICLES					
A1.1	Subject matter and scope	19	LIBE	-	link to the European Arrest Warrant may lead to broadening of use of retained data
		69	EPP+PSE	--	“Generated or processed” data broadens what data must be retained, no call for harmonisation of access safeguards
A1.2		20	LIBE	+	It is important to minimise the amount of data subject to this Directive.
A2.2a	Access to data	21	LIBE	++	Harmonise who can access the gathered data
A2.2ba	Serious crim. offense	22	LIBE	-	Broadens, without clear limits, what is a “serious criminal offense”, for instance, places the extremely vague “computer-related crime” in the same line of thought as terrorism, rape, etc...
	Telephone service	70	EPP+PSE	-	Extends reach without prior impact assessments
A2.2bb	Definition unsuccessful call	23	LIBE	0	Unnecessary to expand the breadth of data subject to this Directive
	User ID	71	EPP+PSE	-	Makes assumptions about how services are commercialised
A2.2bc	Cell ID	72	EPP+PSE	-	Provides for permanent real-time tracking of everyone with a mobile phone

A2.2bd	Unsuccessful call attempt	73	EPP+PSE	-	Unnecessary to expand the breadth of data subject to this Directive
A3a	Access to retained data	27	LIBE	++	Lays down rules for access to privacy-sensitive data
		76	EPP+PSE	-	Leave rules for access to privacy-sensitive data to member states
A3b	Data protect. & security	28	LIBE	+	Harmonisation of security and confidentiality rules applicable to privacy-sensitive data
A3.1	Ref. Directive 2002/58/EC	24	LIBE	0	
		74	EPP+PSE	0	
A3.2	Only provided to the competent national authorities	25	LIBE	0	Good to provide only with judicial authorisation, but list of crimes not fixed
	Unsuccessful call attempt	75	EPP+PSE	-	Retention should only apply to data that is logged and stored in the process of necessary business and engineering activities
A3.2a	List of competent authorities	26	LIBE	+	The public has a right to know who has access to the gathered data
A4	Types of data to be retained	29 and 31	LIBE	0	
		30	LIBE	0	
		77	EPP+PSE	-	
A4.2a	No content retention	78	EPP+PSE	+	Excludes retaining data that can reveal content (for instance, if web links are registered, they directly reveal the content). However, it is neither meaningful nor a compromise since it's only reinstating what can't be done anyway.
A5	Revision of the annex	32=79	LIBE / EPP+PSE	+	Access to types of traffic data must be balanced in full consideration of parliament's review.
A6	Committee 1	33=80	LIBE / EPP+PSE	+	Access to types of traffic data must be balanced in full consideration of parliament's review.
A7	Period of retention	34	LIBE	+	Defines maximum time limits for retention (service provider and competent authorities) after which data must be erased.

		81	EPP+PSE	-	Although it defines clear time limits, maximum is too long.
A7a	Data security principles	82	EPP+PSE	0	Applicability Directive 95/46/EC not in doubt, fact that this is tabled indicates EPP+PSE not certain about conflicts of this directive with previous privacy directives
A7.1a	EP duly informed	35	LIBE	+	Member States must inform European Parliament
A8	Transmission to authorities	36	LIBE	0	Traditional legal requirements as required by Directive 95/46/EC must continue to apply regardless.
		83	EPP+PSE	-	Traditional legal requirements as required by Directive 95/46/EC must continue to apply regardless.
A8a	Sanctions	38	LIBE	+	Any illegal use of sensitive data such as traffic data, without regard to its retention, must be sanctioned.
	Supervisory authority	84	EPP+PSE	0	Traditional legal requirements as required by Directive 95/46/EC must continue to apply regardless.
A8.1a	Contact point	37	LIBE	+	Require due process and due care for handling and access to the data
A9a	Supervisory authorities	40	LIBE	+	Independent authorities that supervise the application and security of stored data are important in preventing abuse.
A9.1	Statistics yearly sent to CEC	39	LIBE	++	Statistics on suspected and factual security breaches is crucial
A10	Reimbursement	41=93	LIBE / Cederschiold	++	Costs must not be put on consumers, guarantee proper democratic process with two readings
	Deleted	85	EPP+PSE	--	No cost reimbursement is in conflict with TEU art 95
A11	Ref. Directive 2002/58/EC	42	LIBE	0	
		86	EPP+PSE	-	We don't want speculative use of personal data
A11a	Future measures	87	EPP+PSE	--	This negates all the safeguards and protections within this directive.

A11b	Remedies, liability sanctions	88	EPP+PSE	0	
A12.1	Eval. necessity, effectiveness	43	LIBE	0	Shows case for data retention still has to be made
	Application & impact study	89	EPP+PSE	--	Proposes turning a safeguard (questioning retention after a period of time) into a power grab (extending retention after a period of time)
A12.2	Include observations EU Data Protection Supervisor	44	LIBE	+	The EDPS is currently ignored, so at least listen to him next time.
A13.1.1	Period for adoption	90	EPP+PSE	0	
A13.2a	Extra deferral on internet data	91	EPP+PSE	0	
A14a	Revision	45	LIBE	+	Periodic revision is a must, though this amendment only proves that the case for retention has not yet been made.
RECITALS					
R3	Ref 2002/58/EC	1	LIBE	+	Processing of personal communications data must be done in accordance with data protection principles.
R4	Scope of the rights and obligations	2	LIBE	+	Limit interference with with private lives of individuals to minimum
R4a	Respect for private life	3	LIBE	+	Stress importance of both ECHR and EU standards when assessing need for data retention
R6	Types of data and ret. period	4	LIBE	0	This type of data retention only exists in less than 5 EU countries currently, and contravene ECHR
R6a	Better and more equal access to justice and appeal	5	LIBE	+	Traditional legal requirements as required by Directive 95/46/EC must continue to apply
R7	Deleted	6=51	LIBE / EPP+PSE	+	Insincere to use the language of combating terrorism within a directive
R8	Data ret. may be a valuable tool	7	LIBE	0	Case for data retention has not yet been made

R9a	Private life and correspondence	52	EPP+PSE	--	Unsubstantiated claim that data retention has proven to be necessary enough that it justifies violating the ECHR, or is even mandated by the ECHR
R10	Need to adopt common measures	8	LIBE	0	Overgeneralisation of particular cases, disregarding outcome of studies
		53	EPP+PSE	-	Data retention is in place in the United Kingdom, and yet the UK Presidency is insisting on going well beyond its own national policy and circumventing the UK Parliament's decisions by going to the EU with this policy
R10a	Tasks laid down in Article 30 95/46/EC	9	LIBE	0	
R11	Need to ensure harmonised period of time	10	LIBE	0	Any increase of data collection will likely aid policing but it is up to policy-makers to do so in accordance with constitutional and legal requirements, i.e. in accordance with the ECHR
		54	EPP+PSE	--	Misrepresentation of study results, generalisation of particular cases
R11a	Balance againsts invasion of privacy	11	LIBE	0	
R12	Periodic review of such provisions	12	LIBE	+	Support the development of a multi-stakeholder structure or institution that reviews surveillance policies
	Deleted	55	EPP+PSE	-	Continued insistence by the Council, EPP and PSE amendments to ignore any form of safeguards seriously detracts from the integrity of their position
R12a	2002/58/EC apply other than that covered by this Directive	56	EPP+PSE	-	Negates the promises of harmonisation

R13	Does not relate to data that is the content	57	EPP+PSE	-	Much of the data that is being retained relates to communications content and will thus disclose the nature of the communication itself
R14	Sharing of experience of best practice	58	EPP+PSE	-	Addresses by am 12 (LIBE)
R15a	Concerning measures to ensure data quality	59	EPP+PSE	0	
R16	Data ret. only provided to the competent national authorities	60	EPP+PSE	-	Weak attempt to divert attention from fact that this directive lacks a proper basis
R16a	Sanction infringements of the provisions	61	EPP+PSE	-	Any access to the data, as established under the rubric of combating terrorism, must be strictly limited
R16b	Unlawful processing operation	62	EPP+PSE	0	
R17	Deleted	13=63	LIBE / EPP+PSE	?	
R17a	Convention on Cybercrime & for the Protection of Individuals	64	EPP+PSE	-	False statement, CoE convention on cybercrime only calls for data preservation for specific investigations of specific individuals
R18	It is unclear whether this Directive does not go beyond what is necessary and proportionate	14	LIBE	++	Mentions concerns by EDPS, civil society and industry
	This Directive does not go beyond what is necessary	65	EPP+PSE	--	Simply wrong, see am 14
R18a	Highest standards of data storage security	15	LIBE	+	Common sense
R18b	Security of data	16	LIBE	+	Common sense
R19	This Directive could better respect the fundamental rights and the principles recognised	17	LIBE	++	Refers to two ECJ judgements to back up assertions, confirmed by EDPS

R19a	Implementation takes place following consultations with the business sector, particularly as regards feasibility and cost of retention	18	LIBE	++	Feasibility has never been properly studied before
	Not intended to harmonise the technology	66	EPP+PSE	--	Extrapolation based on one Dutch case study, which is currently contested by Dutch Senate
R19b	Tables that illustrate the correlation between directives and the transposition	67	EPP+PSE	--	Self-contradiction between call for harmonisation and keeping maximum freedom for member states
R19c	Member States to adopt legislative measure concerning the right of access to and use of data	68	EPP+PSE	0	Similar to am 67 above
Annex	Types of data to be retained	92	EPP+PSE	+	It's better to have types of data in a proper article than in an annex, consistent with amendment 77

1.3 Rejection/Acceptance

number	submitter	recmnd	text
47	Greens+GUE	+++	The European Parliament rejects the Commission proposal.

- the European Data Protection Officer thinks the directive is not necessary and has concerns regarding respect for human rights
- the Article 29 Working Party from across Europe have called for numerous safeguards that are almost entirely lacking
- Privacy Commissioners, civil liberties organisations, consumer organisations and service providers from across Europe have endorsed our statement calling for the rejection of this directive (www.privacyinternational.org/retention)
- 58,000 individuals from across Europe have signed a petition opposing data retention (www.dataretentionisnosolution.com)
- the directive is being rushed through Parliament in 3 months (making a mockery of the codecision procedure)
- countless countries have already rejected data retention, e.g. U.S. and Canada have no plans for data retention

- where national debate have occurred, retention policies are very limited
- studies have been misrepresented by the Commission and the Council
- criminals have plenty of ways to get around the proposed measures
- anyone who uses Hotmail or Gmail are circumventing the proposed system
- the telecom industry and civil society have serious concerns and were barely heard during the preparation of the text
- the proposed measures indicate a serious lack of understanding regarding how the Internet actually works
- deals are being struck behind the scenes to pre-empt a proper democratic process
- the responsible EP Committee (LIBE) was extremely critical
- the discussion in national parliaments is not over, and in some have not yet begun
- some national governments are using the European Parliament to launder this policy after they have already been rejected by their national parliaments

1.4 Draft legislative resolution Paragraph 2

number	submitter	recmnd	text
***	Commission	N/A	
##	LIBE+IMCO	++	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;
48	EPP+PSE	-	Calls on the Commission for an impact assessment study (deletion) covering all internal market and consumer protection issues;

This is an irregularity since the text marked as ## was originally an amendment in the IMCO committee. It was carried both there and in LIBE and incorporated in the LIBE report. Nevertheless, it is not tabled in plenary for some reason. Of course impact assessments should be done before making laws and such studys should be made by independent bodies.

1.5 Draft legislative resolution Paragraph 2.a

number	submitter	recmnd	text
***	Commission	N/A	
49	EPP+PSE	-	(2a) Considers that, concerning access to data, the present directive constitutes just a necessary first step and calls on the Council for loyal cooperation for the swift adoption of appropriate guarantees in the context of the framework decision on data protection and data treatment in judicial and police co-operation in criminal matters;

1.6 Draft legislative resolution Paragraph 2.b

number	submitter	recmnd	text
***	Commission	N/A	
50	EPP+PSE	-	(2b) Considers that the Member States have the right to apply their national constitutional principles and considers especially that professional secrecy will also be respected in the application of the present directive;

The “professional secrecy” clause here means lawyers activities. It is unethical to give a privacy privilege to only one field of profession. Many other activities that are usually considered to be highly sensitive and protected by constitutional law will be captured by this mandatory retention regime: free expression, access to religious and political information, communications and interactions with medical information sources, etc.

It has been known for many years that the mandatory data retention policy fails to discriminate protected-privileged activities and is thus overly broad and illegal according to ECHR jurisprudence. To include a “lawyers only” proposal recognises the ECHR conflict.

1.7 Article 1.1

number	submitter	recmnd	text
***	Commission	N/A	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.
19	LIBE	-	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 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(1). (1) Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.7.2002, p. 1).

69	EPP+PSE	--	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 retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.
----	---------	----	---

Commission proposal makes a narrow interpretation of which crimes retained data can be used for possible, since it refers to “terrorism and organised crime”, it also true to the directive’s original justification to “prevent terrorism”. If not amended, this article makes the whole directive easier to take to court.

LIBE refers to the crimes in the European Arrest Warrant, which is an open ended list of crimes (including fraud and piracy). The European Arrest Warrant is deemed unconstitutional in Germany and is put on suspension in Poland. It may also lead to a broadening of use of the retained data.

EPP+PSE does not impose any limitation at all to which crimes retained data can be used for and also widens the scope of which data communication providers must retain by extending it from data processed to data “generated or processed”. The Council and EPP+PSE are calling for the harmonisation of data retention even while there are very few countries that have implemented data retention on this scale (less than five); and yet are not calling for the harmonisation of access safeguards. It is thus clear that the Directive’s goal is to increase the powers of governments whilst reducing safeguards and minimising national debate.

1.8 Article 1.2

number	submitter	recmnd	text
***	Commission	N/A	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.
20	LIBE	+	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).

LIBE is deleting the word “related”, thus minimising the amount of data subject to this Directive.

1.9 Article 2.2.point(a)

number	submitter	recmnd	text
***	Commission	N/A	(a) “data” means traffic data and location data, as well as the related data necessary to identify the subscriber or user;

21	LIBE	++	(a) “data” means traffic data and location data, as well as the data necessary to identify the subscriber or user; (aa) ‘competent national authorities’ means the judicial authorities and national authorities responsible for the investigation, detection and prosecution of serious criminal offences.
----	------	----	---

It is essential to harmonise the safeguards for access and providing that this access is regulated through judicial authorities. Access to traffic data in the U.S. is permitted only through court order; yet in the UK it is self-authorized by law enforcement officials. Access to this sensitive data must be highly controlled.

1.10 Article 2.2.point(ba)(new)

number	submitter	recmnd	text
***	Commission	N/A	-
22	LIBE	-	(ba) “serious criminal offences” means the offences referred to in Article 2(2) of Framework Decision 2002/584/JHA.
70	EPP+PSE	-	(ba) “telephone service” means calls (including voice, voicemail, conference or data), supplementary services (including call forwarding and call transfer), messaging and multi-media services (including Short Message Services, Enhanced Media Services and Multi-Media Services).

Regarding am 22, we are concerned that the list of ‘serious crimes’ will only increase. Every country within the EU has been working hard to ensure that anti-terror laws established in recent years apply to all forms of investigations; we do not believe that it will be long before the same happens here. By hinging it on the list within Arrest Warrant, this will ensure that both the arrest warrant and the retention regime will expand in use over time.

For am 70, prior to expanding the list of services we require impact assessments.

1.11 Article 2.2.point(bb)(new)

number	submitter	recmnd	text
***	Commission	N/A	-
23	LIBE	0	(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.
71	EPP+PSE	-	(bb) “User ID” means an unique identifier allocated to a person as they subscribe or register to an Internet Access Service or Internet Communication Service;

Regarding am 23, we do not believe that it is necessary to expand the breadth of data subject to this Directive

Am 71 makes assumptions about technical details of the services, but suscription is not always necessary, nor is registration and a unique UserID. This directive must not prescribe the provision of services within nascent markets.

1.12 Article 2.2.point(bc)(new)

number	submitter	recmnd	text
***	Commission	N/A	-
72	EPP+PSE	-	(bc) “Cell ID” means the identity of the cell from which a mobile telephony call originated or in which it terminated;

CellIDs may denote places and this is tantamount to the tracking of locations of all individuals. Recording the location when calls are completed is tantamount to tracking the movement of all individuals.

1.13 Article 2.2.point(bd)(new)

number	submitter	recmnd	text
***	Commission	N/A	-
73	EPP+PSE	-	(bd) “unsuccessful call attempt” means a communication where a telephone call has been successfully connected but is unanswered or there has been a network management intervention;

We do not believe it is necessary to expand the breadth of data subject to this Directive.

1.14 Article 3a(new)

number	submitter	recmnd	text
***	Commission	N/A	-

27	LIBE	++	<p>Article 3a 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:</p> <p>(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;</p> <p>(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;</p> <p>(c) any access to the data by other government bodies or private companies is forbidden;</p> <p>(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;</p> <p>(e) the data requested must be necessary relevant and proportionate 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;</p> <p>(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;</p> <p>(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;</p> <p>(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;</p> <p>(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;</p> <p>(j) data are erased once those data are no longer necessary for the purpose for which they are sought;</p> <p>(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(3), second subparagraph of the Treaty).</p>
----	------	----	--

76	EPP+PSE	-	Access to data 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. The process to be followed and the conditions to be fulfilled in order to get access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in national law, subject to relevant provisions of Union law or public international law, in particular the European Convention on Human Rights, as interpreted by the European Court of Human Rights.
----	---------	---	---

Am 27 recognises that data protection and ECHR protections of the right to privacy must be maintained. Even if data retention is not implemented across the EU we must regulate access to this sensitive data as others have already done. For instance, in the U.S. and Canada judicial authorisation must be sought, and in some circumstances, e.g. internet traffic data and location data, the judicial review requires the highest degree of proof from the state. Such protects are seriously lacking in Europe.

Am 76 leves these essential protections to national law and thereby negates the need for harmonising the retention of this data. It is improper to ensure greater surveillance across the EU with no clear requirements for essential safeguards.

1.15 Article 3b(new)

number	submitter	recmnd	text
***	Commission	N/A	-

28	LIBE	+	<p>Article 3b 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:</p> <p>(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;</p> <p>(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;</p> <p>(c) providers of publicly available electronic communications services or networks as well as Member State authorities accessing the data shall record all access and take the appropriate security measures to prevent unauthorised 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;</p> <p>(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;</p> <p>(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(3), second subparagraph of the Treaty);</p> <p>(f) all data shall be destroyed at the end of the period for retention except those data which have been accessed and preserve;</p> <p>(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.</p>
----	------	---	---

Essential treatment for any form of data processed by communications service providers even if under a data preservation regime. Data retention is not necessary, proportionate, technologically reasonable and will seriously damage consumer confidence and international competitiveness.

1.16 Article 3.1

number	submitter	recmnd	text
--------	-----------	--------	------

***	Commission	N/A	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.
24	LIBE	0	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.
74	EPP+PSE	0	By way of derogation to Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 4, to the extent it is 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 the communication services concerned, are retained in accordance with the provisions of this Directive.

Data retention is not necessary, proportionate, technologically reasonable and will seriously damage consumer confidence and international competitiveness. Neither amendment substantially improves the Commission text.

1.17 Article 3.2

number	submitter	recmnd	text
***	Commission	N/A	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.
25	LIBE	0	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 Framework Decision 2002/584/JHA. This Directive shall comply with the principles laid down in the Council Framework Decision on [data protection].

75	EPP+PSE	-	This shall include the retention of data specified in Article 4 in relation to unsuccessful call attempts where that data is generated or processed and stored (as regards telephony data) or logged (as regards Internet data) by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communication services concerned. This Directive shall not require the retention of data in relation to unconnected calls.
----	---------	---	--

Data retention is not necessary, proportionate, technologically reasonable and will seriously damage consumer confidence and international competitiveness.

Regarding am 25, we agree that any access to traffic data at communications service providers requires judicial authorisation, but we are concerned that over time the list of crimes for which this data will be sought will expand.

Regarding am 75, any regime for access to traffic data should only apply to data that is logged and stored in the process of necessary business and engineering activities.

1.18 Article 3.2.a(new)

number	submitter	recmnd	text
***	Commission	N/A	
26	LIBE	+	To this end an updated list of the designated competent law enforcement authorities should be publicly available.

The public has a right to know who has access to the gathered data, as traffic data can detail all the activities, interests and movements of an individual.

1.19 Article 4

number	submitter	recmnd	text
***	Commission	N/A	Categories of data to be retained 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; (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; (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; (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.

29 and 31	LIBE	0	<p>Categories and types of data to be retained 1. Member States shall ensure that the following categories of data are retained under this Directive:</p> <ul style="list-style-type: none"> (a) data necessary to trace and identify the source 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; (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; (f) data necessary to identify the location of mobile communication equipment. 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. No data revealing the content of the communication can be retained.
--------------	------	---	---

30	LIBE	0	<p>1a. Types of data to be retained:</p> <p>(1) Concerning Fixed Network Telephony</p> <p>(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;</p> <p>(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);</p> <p>(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.</p> <p>(d) Data necessary to identify the type of communication: (a) The telephone service used, e.g. voice, conference call, fax and messaging services.</p> <p>(2) Concerning Mobile Telephony:</p> <p>(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;</p> <p>(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);</p> <p>(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.</p> <p>(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</p> <p>(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.</p> <p>(f) Data necessary to identify the location of mobile communication equipment: (a) The location label (Cell ID) at the start of the communication;</p> <p>(3) Concerning the Internet and its services:</p> <p>(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.</p> <p>(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.</p> <p>(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;</p>
----	------	---	---

77	EPP+PSE	-	<p>(a) data necessary to trace and identify the source of a communication:</p> <p>(1) Concerning Fixed Network Telephony and Mobile Telephony (a) The calling telephone number; (b) Name and address of the subscriber or registered user; (2) Concerning Internet Access, Internet e-mail and Internet telephony: (a) The User ID(s) allocated. (b) The User ID and telephone number allocated to any communication entering the public telephone network. (c) Name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, User ID or telephone number was allocated at the time of the communication.</p> <p>(b) data necessary to identify the destination of a communication:</p> <p>(1) Concerning Fixed Network Telephony and Mobile Telephony: (a) The number(s) dialled (the called telephone number or numbers), and in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed. (b) Name(s) and address(es) of the subscriber(s) or registered user(s).</p> <p>(2) Concerning Internet e-mail and Internet telephony: (a) The User ID or telephone number of the intended recipient(s) of an Internet telephony call. (b) Name(s) and address(es) of the subscriber(s) or registered user(s) and User ID of the intended recipient of the communication.</p> <p>(c) data necessary to identify the date, time and duration of a communication:</p> <p>(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 Access service based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet Access Service provider to a communication, and the User ID of the subscriber or registered user. (b) The date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service based on a certain time zone.</p> <p>(d) data necessary to identify the type of communication:</p> <p>(1) Concerning Fixed Network Telephony and Mobile Telephony: (2) Concerning Internet e-mail and Internet telephony: (a) The Internet service used.</p> <p>(e) data necessary to identify users' communication equipment or what purports to be their equipment:</p> <p>(1) Concerning Fixed Network Telephony (a) The calling and called telephone numbers. (2) Concerning Mobile Telephony (a) The calling and called telephone numbers. (b) The International Mobile Subscriber Identity (IMSI) of the calling party. (c) The International Mobile Equipment Identity (IMEI) of the calling party. (d) The International Mobile Subscriber Identity (IMSI) of the called party. (e) The International Mobile Equipment Identity (IMEI) of the called party. (f) In case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the activation was made. (3) 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 of the originator of the communication.</p> <p>(f) data necessary to identify the location of mobile communication equipment:</p> <p>(1) The location label (Cell ID) at the start of the communication. (2) Data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data is retained.</p>
----	---------	---	--

Data retention is not necessary, proportionate, technologically reasonable and will seriously damage consumer confidence and international competitiveness.

1.20 Article 4.2.a(new)

number	submitter	recmnd	text
***	Commission	N/A	
78	EPP+PSE	+	2a. No data revealing the content of the communication can be retained pursuant to this Directive.

1.21 Article 5

number	submitter	recmnd	text
***	Commission	N/A	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).
32 = 79	LIBE / EPP+PSE	+	deleted

Access to types of traffic data must be balanced in full consideration of parliament's review.

1.22 Article 6

number	submitter	recmnd	text
***	Commission	N/A	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.
33 = 80	LIBE / EPP+PSE	+	deleted

Access to types of traffic data must be balanced in full consideration of parliament's review.

1.23 Article 7

number	submitter	recmnd	text
--------	-----------	--------	------

***	Commission	N/A	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.
34	LIBE	+	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.
81	EPP+PSE	-	Member States shall ensure that the categories of data referred to in Article 4 are retained for periods of not less than 6 months and for a maximum of two years from the date of the communication.

Regarding am 34, governments have not made the case for the retention of this information even while other countries prefer to implement the less invasive and more specific means of 'data preservation'. Under this process only the required amount of information is preserved in specific cases involving specific investigations of specific individuals.

Even when studies have been done to investigate how long data should be retained, in only the most exceptional cases was this data needed for more than three months.

If data retention is to occur, in accordance with safeguards announced by the Article 29 Working Party, this data must be kept for the shortest period of time.

Regarding am 81, the EU can not claim that the purpose of this directive is to harmonise retention when it continues to permit countries to retain data for more than one year when the Commission originally proposed that it was reasonable to limit the period to one year. We do not trust the sincerity of the proponents of this policy so long as they appear comfortable in extending the period of retention

Already some countries are calling for this data to be kept for three years (Ireland), if not longer (Poland recently called for 15 years).

1.24 Article 7a(new)

number	submitter	recmnd	text
***	Commission	N/A	

82	EPP+PSE	0	Article 7a Data protection and data security - Without prejudice to the provisions adopted pursuant to Directive 95/46/EC and Directive 2002/58/EC, each Member State shall ensure that providers of publicly available electronic communications services or of a public communications network respect, as a minimum, the following data security principles with respect to data retained in accordance with the present Directive: (a) the retained data shall be of the same quality and shall be subject to the same security and protection as those data on the network; (b) the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, or accidental loss or alteration, unauthorised or unlawful storage, processing, access or disclosure; (c) the data shall be subject to appropriate technical and organisational measures to ensure that access to the data is undertaken only by specially authorised personnel; and (d) the data shall be destroyed at the end of the period for retention except those data which have been accessed and preserved.
----	---------	---	---

Data retention is not necessary, proportionate, technologically reasonable and will seriously damage consumer confidence and international competitiveness. As a result we believe that Directive 95/46/EC should continue to apply without any need to reiterate its principles.

As the two largest parties in the Parliament see a need to reiterate these principles it is arguably necessary for an impact assessment for data retention on communications service providers legal and cost liabilities.

1.25 Article 7.1.point(a)(new)

***	Commission	N/A	
35	LIBE	+	The Commission shall keep the European Parliament duly informed of the notifications made by Member States under Article 95(4) of the Treaty.

It is a good idea to keep the European Parliament informed, as well as the Commission, when a Member State deems it necessary to maintain national provisions as well as the grounds for maintaining them.

1.26 Article 8

number	submitter	recmnd	text
***	Commission	N/A	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.

36	LIBE	0	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.
83	EPP+PSE	-	Member States shall ensure that the data as specified in Article 4 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.

Traditional legal requirements as required by Directive 95/46/EC must continue to apply regardless.

1.27 Article 8a(new)

***	Commission	N/A	-
38	LIBE	+	Article 8a 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.
84	EPP+PSE	0	Supervisory authority 1. Each Member State shall designate one or more public authorities to be responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to Article 7a of this Directive regarding the security of the stored data. These authorities may be same authorities as those referred to in Article 28 of Directive 95/46/EC. 2. These authorities shall act with complete independence in exercising the functions referred to in paragraph 1.

Traditional legal requirements as required by Directive 95/46/EC must continue to apply regardless.

1.28 Article 8.1.point(a)(new)

***	Commission	N/A	-
-----	------------	-----	---

37	LIBE	+	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.
----	------	---	---

1.29 Article 9.point(a)(new)

***	Commission	N/A	-
40	LIBE	+	Supervisory authorities 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.

1.30 Article 9.1

number	submitter	recmnd	text
***	Commission	N/A	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 - 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 cases where requests for data could not be met.
39	LIBE	++	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 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 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 Commission shall submit these statistics to the European Parliament each year and then each three years.

As risks and costs are substantial with large and complex data retention systems it is crucial to collect statistics on many aspects of their function. In the light of recent and costly abuse of surveillance systems in e.g. Germany and the Netherlands it is particularly important to include statistics on suspected and factual security breaches of these systems.

This amendment only highlights the fact that the use of traffic data is inadequately understood, and the case for retention of this data has yet to be made.

1.31 Article 10

number	submitter	recmnd	text
***	Commission	N/A	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.
41=93	LIBE / Cederschiold	++	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.
85	EPP+PSE	--	deleted

Amendment 41=93 is unacceptable to the Council, and therefore would guarantee a second reading with the possibility of proper discussions instead of hasty backroom compromises. This directive needs at least two readings. The deletion of the cost issue also conflicts with the legal basis for this directive, namely art 95 function of internal market.

Particularly as Member States are insisting on their right to retain this data for extended periods of time, these Member States must be required to cover the costs of retention and provision of traffic data to law enforcement authorities. Otherwise consumers in Europe will be forced to bear the costs of retention even as consumers in other countries around the world who have rejected retention, e.g. the U.S. and Canada, will not have these additional costs.

1.32 Article 11 “Article 15.1.point(a) (Directive 2002/58/EC)”

number	submitter	recmnd	text
***	Commission	N/A	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.

42	LIBE	0	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. Member States shall refrain from adopting legislative measures in the sectors covered by this Directive.
86	EPP+PSE	-	1a. Paragraph 1 does not apply to data specifically required to be retained by Directive 2005/././EC for the purposes referred to in Article 1(1) of that Directive.

Data retention is not necessary, proportionate, technologically reasonable and will seriously damage consumer confidence and international competitiveness. Traditional legal requirements as required by Directive 95/46/EC must continue to apply regardless. Speculative use of personal information must not be used, such as in the case of preventing crime.

1.33 Article 11a(new)

number	submitter	recmnd	text
***	Commission	N/A	
87	EPP+PSE	--	Article 11a Future measures 1. A Member State facing particular circumstances warranting an extension for a limited period of the maximum retention period referred to in Article 7 may take the necessary measures. The Member State shall immediately notify the Commission and inform the other Member States of the measures taken by virtue of this Article and indicate the grounds for introducing them. 2. The Commission shall, within six months after the notification as referred to in paragraph 1, approve or reject the national measures involved after having verified whether or not they are a means of arbitrary discrimination or disguised restriction of trade between Member States and whether or not they shall constitute an obstacle to the functioning of the internal market. In the absence of a decision by the Commission within this period the national measures shall be deemed to have been approved. 3. When, pursuant to paragraph 2, the national measures of a Member State derogating from the provisions of this Directive are approved, the Commission may examine whether to propose an adaptation of this Directive.

Member States who have been pushing for data retention because of the need for harmonising rules must not be equally permitted to expand the length of the period of retention. This negates all the safeguards and protections within this directive.

1.34 Article 11b(new)

number	submitter	recmnd	text
***	Commission	N/A	

88	EPP+PSE	0	Article 11b Remedies, liability and sanctions 1. Each Member State shall take the necessary measures to ensure that the national measures implementing Chapter III of Directive 95/46/EC providing for judicial remedies, liability and sanctions are fully implemented with respect to the processing of data under this Directive. 2. Each Member State shall in particular take the necessary measures to ensure that the intentional access to or transfer of data retained in accordance with the present Directive which is not permitted under national law adopted pursuant to this Directive, shall be punishable by sanctions, including administrative or criminal sanctions, which are effective, proportionate and dissuasive.
----	---------	---	---

Data retention is not necessary, proportionate, technologically reasonable and will seriously damage consumer confidence and international competitiveness. Traditional legal requirements as required by Directive 95/46/EC must continue to apply regardless.

1.35 Article 12.1

number	submitter	recmnd	text
***	Commission	N/A	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.
43	LIBE	0	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 shall 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 shall be publicly available.
89	EPP+PSE	--	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 further developments in electronic communications technology and 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 list of data in Article 4, and the periods of retention provided for in Article 7. The results of the evaluation will be made publicly available.

This clause and amendment 43 only prove that the case for retention has not yet been made and yet the Parliament is being asked to move forward on this and to then reconsider this after two years. Governments have a duty to prove that their interferences with the right to privacy are necessary and proportionate prior to enacting laws that enable these interferences. This 'trial and error' approach to civil liberties is unacceptable.

As a matter of habit and course, once taken away liberties are rarely restored.

Amendment 89 proposes turning a safeguard (questioning retention after a period of time) into a power grab (extending retention after a period of time). This is a reflection on all of the amendments proposed by the Council and the EPP and PSE.

1.36 Article 12.2

number	submitter	recmnd	text
***	Commission	N/A	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
44	LIBE	+	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 or by the European Data Protection Supervisor.

The opinion of the European Data Protection Supervisor (namely that this directive is not necessary) is currently be ignored, so it should at least be taken into account in the future.

1.37 Article 13.1.1

number	submitter	recmnd	text
***	Commission	N/A	Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by [no later than 15 months after its adoption at the latest]. They shall forthwith communicate to the Commission the text of those provisions and a correlation table between those provisions and this Directive.
90	EPP+PSE	0	Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by no later than 18 months after its adoption at the latest. They shall forthwith communicate to the Commission the text of those provisions.

If data retention is to be implemented it must be done with great care and a duty to consult with national industry, consumer, and civil liberties organisations. Time limits do not assist in doing so, though the longer and greater the consultation the better.

1.38 Article 13.2a(new)

number	submitter	recmnd	text
***	Commission	N/A	
91	EPP+PSE	0	Each Member State may for a period of up to 18 months from the expiry of the deadline referred to in paragraph 1 defer application of this Directive to the retention of communications data relating to Internet Access, Internet telephony and Internet e-mail. Any Member State which intends to make use of this paragraph shall, by way of a declaration, notify the Commission to that effect upon adoption of this Directive. The declaration shall be published in the Official Journal of the European Union.

Data retention is not necessary, proportionate, technologically reasonable and will seriously damage consumer confidence and international competitiveness.

This is particularly the case for data relating to internet usage. An extension on the period of time to establish this rule does not permit greater flexibility in this rule. At the very least this rule must be extended beyond the so-called two or three year 'sunset' or 'renegotiation' of the directive, permitting Member States to opt out of this highly invasive practice entirely.

This amendment goes to show the lack of sincerity in protections promised by the Council, the EPP and PSE, and reflects accordingly on all of the amendments proposed by the Council and the EPP and PSE.

1.39 Article 14a (new)

number	submitter	recmnd	text
***	Commission	N/A	-
45	LIBE	+	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.

This amendment only proves that the case for retention has not yet been made.

1.40 Recital 3

number	submitter	recmnd	text
--------	-----------	--------	------

***	Commission	N/A	Articles 5, 6 and 9 of Directive 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.
1	LIBE	+	Articles 6 and 9 of Directive 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. 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.

Any processing of personal data in the form of communications data must be done with the utmost care in accordance with data protection principles.

1.41 Recital 4

number	submitter	recmnd	text
***	Commission	N/A	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.
2	LIBE	+	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.

Any interference into the private lives of individuals as provided for in Article 8.1 of the European Convention on Human Rights must be limited to what is strictly necessary in a democratic society, and proportionate. As communications traffic data denotes an individual's communications, interests, and network of associations and movements this data can only be accessed when it is absolutely necessary

and for combating terrorism.

1.42 Recital 4(a)(new)

number	submitter	recmnd	text
3	LIBE	+	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.

The EDPS raised concerns regarding possible conflicts of this directive with the Charter of Fundamental Rights, so explicitly mentioning that it cannot be overruled by this directive is no luxury.

Data retention is not necessary, proportionate, technologically reasonable and will seriously damage consumer confidence and international competitiveness. It is important to emphasise that both international human rights standards (ECHR) and EU standards must be used to assess the case for data retention.

1.43 Recital 6

number	submitter	recmnd	text
***	Commission	N/A	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.
4	LIBE	0	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.

Given that this directive leaves a lot of things to be decided by the member states (including the period of detention), the Commission's statement is curious.

Data retention policies of this form and breadth only exist in less than five EU countries. These proposals already contravene the ECHR and now the EU is planning on extending this illegality.

1.44 Recital 6(a)(new)

number	submitter	recmnd	text
5	LIBE	+	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 of whether it originates from an authority or a provider.

Data retention is not necessary, proportionate, technologically reasonable and will seriously damage consumer confidence and international competitiveness. Traditional legal requirements as required by Directive 95/46/EC must continue to apply regardless.

1.45 Recital 7

number	submitter	recmnd	text
***	Commission	N/A	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 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.
6=51	LIBE / EPP+PSE	+	[deleted]

It is insincere to use the language of combating terrorism within a directive.

1.46 Recital 8

number	submitter	recmnd	text
***	Commission	N/A	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.
7	LIBE	0	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.

Communications traffic data is highly sensitive information regarding the interests, movements and associations of all individuals within Europe. The case for data retention has still not been made; but this amendment improves on Commission language that claims that the case has been made. This amendment goes to prove that retention is still a highly immature policy.

1.47 Recital 9.point(a)(new)

number	submitter	recmnd	text
--------	-----------	--------	------

***	Commission	N/A	N/A
52	EPP+PSE	--	Under Article 8 of the European Convention of Human Rights, everyone has the right to respect for his private life and his correspondence. Interference by a public authority with the exercise of that right may only be made in accordance with the law and if it is necessary in a democratic society, inter alia, in the interests of national security, public safety, for the prevention of disorder or crime, or for the protection of the rights and freedoms of others. Because retention of data has proven to be such a necessary and effective investigative tool for law enforcement in investigations in several Member States and in particular into serious cases such as organized crime and terrorism, it is therefore necessary to ensure availability of retained data to law enforcement for a certain period of time under the conditions provided for in the present Directive. The adoption of an instrument on data retention is therefore a necessary measure in accordance with the requirements of Article 8 of the European Convention of Human Rights.

Numerous officials, experts, and legal bodies have declared that the indiscriminate collection of data on all individuals without any foreseeability contravenes the ECHR. Additionally, data retention has not proven to be necessary and effective, as required by the ECHR.

To turn the ECHR on its head and argue that a retention directive is necessary is indicative of the problems with the EPP and PSE amendments. These amendments turn safeguards into power grabs, limitations into extensions, protections of individual rights into interferences with the private lives of individuals.

Article 8 by no means requires data retention. Article 8 and the jurisprudence of the European Court of Human Rights actually abhors policies such as indiscriminate retention of personal data.

1.48 Recital 10

number	submitter	recmnd	text
***	Commission	N/A	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.
8	LIBE	0	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.
53	EPP+PSE	-	The declaration adopted by the Council on 13 July 2005 reinforces the need to adopt common measures related to the retention of electronic communications traffic data as soon as possible.

Data retention is not necessary, proportionate, technologically reasonable and will seriously damage consumer confidence and international competitiveness.

Data retention is in place in the United Kingdom, and yet the UK Presidency is insisting on going well beyond its own national policy and circumventing the UK Parliament's decisions by going to the European Union with this policy, as it has been doing for years. Reference to a special meeting of the

Council after the July terrorist atrocities in London states nothing new.

1.49 Recital 10(a)(new)

number	submitter	recmnd	text
9	LIBE	0	The Working Party on the protection of individuals with regard to processing of personal data established pursuant 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.

Data retention is not necessary, proportionate, technologically reasonable and will seriously damage consumer confidence and international competitiveness. Traditional legal requirements as required by Directive 95/46/EC must continue to apply regardless.

1.50 Recital 11

number	submitter	recmnd	text
***	Commission	N/A	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.
10	LIBE	0	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.
54	EPP+PSE	--	Given the importance of traffic data for the investigation, detection, and prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States, there is a need to ensure at a European level 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 under the conditions provided for in the present Directive.

Data retention is not necessary, proportionate, technologically reasonable and will seriously damage consumer confidence and international competitiveness. Any increase of data collection will likely aid policing but it is up to policy-makers to do so in accordance with constitutional and legal requirements, i.e. in accordance with the ECHR. As a result this entire amendment continues to make a leap of logic

even as it tries to lessen the Commission’s original logical flaws.

Despite numerous attempts, proponents of data retention have yet to make the specific case that indiscriminate and extended retention of communications traffic data is necessary in a democratic society and proportionate. There is a serious lack of research on the need for retention, and what little research exists does not make a conclusive case for retention by any means. In fact many countries that have implemented new powers after terrorist attacks, e.g. the U.S. have also rejected data retention policies. So any declarations of the absolute need for retention are based on weak grounds.

1.51 Recital 11(a)(new)

number	submitter	recmnd	text
11	LIBE	+	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.

Any policy on communications surveillance must be proportionate and necessary in a democratic society, in accordance with the ECHR. Whilst data retention is clearly in contravention with the requirements of the ECHR, policies on access to traffic data must certainly be proportionate and necessary in a democratic society, and thus require careful consideration of the benefits of the interferences and the level of the intrusion.

The principle of proportionality needs to be stressed, as the EDPS also noted it is threatened by this directive.

1.52 Recital 12

number	submitter	recmnd	text
***	Commission	N/A	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.
12	LIBE	+	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.
55	EPP+PSE	-	deleted

Data retention is not necessary, proportionate, technologically reasonable and will seriously damage consumer confidence and international competitiveness. As technologies changes the legal, regulatory, and technological challenges only increase. As such we support the development of a multi-stakeholder

structure or institution that reviews surveillance policies to cater for new developments in technology. We would like to see some representation from civil liberties organisations.

The continued insistence by the Council, EPP and PSE amendments to ignore any form of safeguards seriously detracts from the integrity of their position.

1.53 Recital 12.point(a)(new)

number	submitter	recmnd	text
***	Commission	N/A	N/A
56	EPP+PSE	-	Article 15(1) of Directive 2002/58/EC would continue to apply in relation to data, including data related to unsuccessful call attempts, which are not specifically required to be retained under the present Directive and therefore fall outside the scope of this Directive, and for retention for purposes, including judicial purposes, other than that covered by this Directive.

This amendment negates the promises of harmonisation. This view is supported by the statement of Commissioner Frattini on December 7th stating the Commission's opposition to this Council amendment.

1.54 Recital 13

number	submitter	recmnd	text
***	Commission	N/A	Given the fact that retention of data generates significant additional costs for electronic communications 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.
57	EPP+PSE	-	This Directive relates only to data generated or processed as a consequence of a communication or a communication service and does not relate to data that is the content of the information communicated. Retention of data should be done in a way avoiding data to be retained more than once. Generating or processing data, when supplying the communications services concerned (Article 3), refers to data which is accessible. In particular when retaining data related to Internet e-mail and Internet Telephony, the scope may be limited to the providers' own services or the network providers'.

Much of the data that is being retained relates to communications content and will thus disclose the nature of the communication itself.

1.55 Recital 14

number	submitter	recmnd	text
***	Commission	N/A	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.
58	EPP+PSE	-	Technologies relating to electronic communications are changing rapidly and the legitimate requirements of the competent authorities may evolve; to obtain advice and encourage the sharing of experience of best practice on these matters the Commission intends to establish a group composed of Member States' law enforcement authorities, associations of the electronic communications industry, European Parliament representatives and data protection authorities, including the European Data Protection Supervisor.

Addressed by Amendment 12 (LIBE).

1.56 Recital 15.point(a)(new)

number	submitter	recmnd	text
***	Commission	N/A	N/A
59	EPP+PSE	-	It should also be recalled that the obligations incumbent on service providers concerning measures to ensure data quality which derive from Article 6 of Directive 95/46/EC as well as their obligations concerning measures to ensure confidentiality and security of processing of data which derive from Articles 16 and 17 of Directive 95/46/EC, are fully applicable to data being retained within the meaning of the present Directive.

Data retention is not necessary, proportionate, technologically reasonable and will seriously damage consumer confidence and international competitiveness. Traditional legal requirements as required by Directive 95/46/EC must continue to apply regardless.

1.57 Recital 16

number	submitter	recmnd	text
--------	-----------	--------	------

***	Commission	N/A	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 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.
60	EPP+PSE	-	It is essential that Member States provide legislative measure 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.

Data retention is not necessary, proportionate, technologically reasonable and will seriously damage consumer confidence and international competitiveness. Traditional legal requirements as required by the ECHR under Article 8 and the Directive 95/46/EC must continue to apply regardless. Any attempts to limit attention to these principles must be rejected.

1.58 Recital 16.point(a)(new)

number	submitter	recmnd	text
***	Commission	N/A	N/A
61	EPP+PSE	-	In this context, it should be recalled that Article 24 of Directive 95/46/EC imposes an obligation on Member States to sanction infringements of the provisions adopted pursuant to Directive 95/46/EC; Article 15(2) of Directive 2002/58/EC imposes the same requirement in relation to national provisions adopted pursuant to Directive 2002/58/EC; Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems provides that the intentional illegal access to information systems, including to data retained therein, shall be made punishable as a criminal offence.

Data retention is not necessary, proportionate, technologically reasonable and will seriously damage consumer confidence and international competitiveness. Traditional legal requirements as required by the ECHR under Article 8 and the Directive 95/46/EC must continue to apply regardless. Any attempts to limit attention to these principles must be rejected.

Moreover any access to this data, as established under the rubric of combating terrorism, must be strictly limited.

1.59 Recital 16.point(b)(new)

number	submitter	recmnd	text
--------	-----------	--------	------

***	Commission	N/A	N/A
62	EPP+PSE	0	It should be borne in mind that the right of any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with national provisions adopted pursuant to Directive 95/46/EC, to receive compensation, which derives from Article 23 of Directive 95/46/EC, applies also in relation to the unlawful processing of any personal data pursuant to the present Directive.

Data retention is not necessary, proportionate, technologically reasonable and will seriously damage consumer confidence and international competitiveness. Traditional legal requirements as required by the ECHR under Article 8 and the Directive 95/46/EC must continue to apply regardless.

1.60 Recital 17

number	submitter	recmnd	text
***	Commission	N/A	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.
13=63	LIBE / EPP+PSE	?	[deleted]

1.61 Recital 17.point(a)(new)

number	submitter	recmnd	text
64	EPP+PSE	-	It should be borne in mind that the 2001 Council of Europe Convention on Cybercrime as well as the 1981 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data also cover data being retained within the meaning of the present Directive.

This statement is entirely false. The CoE documents call for privacy protection, with the exception of the CoE convention on cybercrime which calls only for data preservation for specific investigations of specific individuals. Data retention appears in none of these documents.

1.62 Recital 18

number	submitter	recmnd	text
--------	-----------	--------	------

***	Commission	N/A	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.
14	LIBE	++	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.
65	EPP+PSE	--	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 crime as defined by each Member State in national law, 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.

LIBE properly points out the concerns of the European Data Protection Supervisor (human rights, necessity and proportionality), civil society (idem) and the conclusions of the Erasmus University study (unclear whether the proposed measures will actually help the fight against criminality and terrorism).

The interpretation of EPP+PSE of legal rights of European residents and citizens is faulty and excludes the points of view expressed repeatedly by a number of organisations and EU institutions, as outlined by the LIBE amendment.

1.63 Recital 18(various)(new)

number	submitter	recmnd	text
--------	-----------	--------	------

15	LIBE	+	(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.
16	LIBE	+	(18b) The security of data under this Directive must be in compliance with the data protection provisions of Directive 2002/58/EC.

Common sense. Data retention is not necessary, proportionate, technologically reasonable and will seriously damage consumer confidence and international competitiveness. Traditional legal requirements as required by the ECHR under Article 8 and the Directive 95/46/EC must continue to apply regardless.

1.64 Recital 19

number	submitter	recmnd	text
***	Commission	N/A	(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),
17	LIBE	++	(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.

The LIBE amendment refers to two ECJ judgements to support its assertions, which was also expressed by the European Data Protection Supervisor.

1.65 Recital 19(a)(new)

number	submitter	recmnd	text
18	LIBE	++	(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.

66	EPP+PSE	--	Considering that the obligations on providers of electronic communications services should be proportionate, the Directive requires that they only retain such data which are generated or processed in the process of supplying their communications services; to the extent that such data is not generated or processed by those providers, there can be no obligation to retain it. This Directive is not intended to harmonise the technology for retaining data, the choice of which will be a matter to be resolved at national level.
----	---------	----	---

Data retention places a significant burden on European industry that is unprecedented even as other jurisdictions have rejected similar policies. If the EU is to embark on this unprecedented policy then it must ensure that European consumers are not burdened with additional costs even while it is likely that they will chose instead to use non-EU services, again to the detriment of EU industry.

The concerns of the business sector regarding implementation have been disregarded by the Commission based on one case study performed in the Netherlands. However, the conclusions of that study are being contested by even the responsible Committee in the Dutch Senate (as being outdated already, since e.g. the applicable Internet traffic has more than tripled since it was performed one year ago).

1.66 Recital 19(b)(new)

number	submitter	recmnd	text
67	EPP+PSE	--	It should be remembered that Paragraph 34 of the Inter-institutional agreement on better law-making (OJ C 321, 31.12.2003.) states that the Council “will encourage the Member States to draw up, for themselves and in the interests of the community, their own tables which will, as far as possible, illustrate the correlation between directives and the transposition measures and to make them public”.

The EPP and PSE amendments again point to additional flexibility for Member States to increase surveillance while calling for the harmonisation of increased powers. This is non-sensical.

1.67 Recital 19(c)(new)

number	submitter	recmnd	text

68	EPP+PSE	0	The present Directive is without prejudice to the power of Member States to adopt legislative measure concerning the right of access to and use of data by national authorities as designated by them. Issues of access to data retained pursuant to this Directive by national public authorities for such activities as are referred to in the first indent of Article 3(2) of Directive 95/46/EC fall outside the scope of Community law. However, they may be the subject of national law, or action pursuant to Title VI of the Treaty on European Union, always noting that such laws or action must fully respect fundamental rights as they result from the common constitutional traditions of the Member States and as they are guaranteed by the ECHR. Article 8 ECHR, as interpreted by the European Court of Human Rights, requires that interference by public authorities with privacy rights must respond to requirements of necessity and proportionality and must therefore serve specific, explicit and legitimate purposes and be exercised in a manner which is adequate, relevant and not excessive in relation to the purpose of the interference.
----	---------	---	---

The EPP and PSE amendments again point to additional flexibility for Member States to increase surveillance while calling for the harmonisation of increased powers. It has long been established that indiscriminate data collection contravenes the ECHR. Therefore the EPP and PSE statements are non-sensical.

1.68 ANNEX

number	submitter	recmnd	text
***	Commission	N/A	Types of data to be retained under the categories identified in Article 4 of this Directive: 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) 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, (...missing text...)
92	EPP+PSE	+	deleted

This amendment points to the serious challenges in identifying the appropriate data to be retained under this policy and therefore indicates how complex this policy actually is. Therefore we call for the rejection of the policy in its current form and the amended form as proposed by the EPP and PSE in particular because they ignore these challenges and complexities.