EUROPEAN PARLIAMENT

2004 *2009*

Committee on Civil Liberties, Justice and Home Affairs

PROVISIONAL
2005/0182(COD)

19.10.2005

***I
DRAFT REPORT

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

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Alexander Nuno Alvaro

Symbols for procedures

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

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

Amendments to a legislative text

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

CONTENTS

Page

DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION

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

(Codecision procedure: first reading)

The European Parliament,

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

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

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

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

1. Approves the Commission proposal as amended;

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

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

Text proposed by the Commission	Amendments by Parliament
Amendment 1 RECITAL 4	
(4) Article 15(1) of Directive 2002/58/EC sets out the conditions under which Member States may restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1)(2)(3) and (4), and Article 9 of the Directive; any such derogations need to be necessary, appropriate and proportionate within a democratic society for specific public order purposes, i.e. to safeguard national security (i.e. State security) defence, public security or the ***prevention***, investigation, detection and prosecution of criminal offences or of	(4) Article 15(1) of Directive 2002/58/EC sets out the conditions under which Member States may restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1)(2)(3) and (4), and Article 9 of the Directive; any such derogations need to be necessary, appropriate and proportionate within a democratic society for specific public order purposes, i.e. to safeguard national security (i.e. State security) defence, public security or the investigation, detection and prosecution of criminal offences or of

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

unauthorised use of the electronic communications systems.	unauthorised use of the electronic communications systems. *(This amendment applies throughout the text. Adopting it will necessitate corresponding changes throughout).*

Amendment 2
RECITAL 5

(5) ***Several*** Member States have adopted legislation providing for the retention of data by service providers for the prevention, investigation, detection, and prosecution of crime and criminal offences; the provisions of the various national legislations vary considerably.	(5) ***Ten of the 25*** Member States have adopted legislation providing for the retention of data by service providers for the prevention, investigation, detection, and prosecution of crime and criminal offences***: Belgium, France, Italy, Ireland, Latvia, Lithuania, the Netherlands, Poland, Spain, Czech Republic***; the provisions of the various national legislations vary considerably.

Amendment 3
RECITAL 7

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

Amendment 4
RECITAL 8

(8) The Conclusions of the Justice and Home Affairs Council of 19 December 2002 underline that, because of the significant growth of the possibilities of electronic communications, data relating to the use of electronic communications is	***deleted***

particularly important and therefore a valuable tool in the prevention, investigation, detection and prosecution of crime and criminal offences, in particular against organised crime.

Amendment 5
RECITAL 9

(9) The Declaration on combating Terrorism adopted by the European Council on 25 March 2004 instructed the Council to examine measures for establishing rules on the retention of communications traffic data by service providers.	***deleted***

Amendment 6
RECITAL 10

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

Amendment 7
RECITAL 11

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

Amendment 8
RECITAL 11 A (new)

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

Amendment 9
RECITAL 12

(12) ***The categories of information to be retained reflect an appropriate balance between the benefits for the prevention, investigation, detection, and prosecution of the serious offences involved and the level of invasion of privacy they will cause; the applicable retention period of one year, respectively six months where data relate to electronic communications taking place using solely the Internet Protocol, also strikes a reasonable balance between all the interests involved.***	(12) ***The retention period of three months reflects a sensible approach to harmonisation, in the light of current practice in the European Union and given that the period can be extended if necessary, following an evaluation.***

Amendment 10
RECITAL 13

(13) Given the fact that retention of data generates significant additional costs for electronic communication providers, whilst the benefits in terms of public security impact on society in general, it is appropriate ***to foresee*** that Member States reimburse demonstrated additional costs incurred in order to comply with the obligations imposed on them as a consequence of this Directive.	(13) Given the fact that retention of data generates significant additional costs for ***public*** electronic communication providers, whilst the benefits in terms of public security impact on society in general, it is appropriate that Member States ***fully*** reimburse demonstrated additional costs incurred in order to comply with the obligations imposed on them as a consequence of this Directive.

Amendment 11
RECITAL 14

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

Amendment 12
RECITAL 17

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

Amendment 13
RECITAL 19

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

Amendment 14
ARTICLE 1, PARAGRAPH 1

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

1. This Directive aims to harmonise the provisions of the Member States concerning obligations on the providers of publicly available electronic communications services or of a ***public*** communications network with respect to the processing and retention of certain data, in order to ensure that the data is available for the purpose of the ***prevention,*** investigation, detection and prosecution of ***serious*** criminal offences***, such as terrorism and organised crime***.	1. This Directive aims to harmonise the provisions of the Member States concerning obligations on the providers of publicly available electronic communications services or of a ***publicly accessible electronic*** communications network with respect to the processing and retention of certain data, ***and to ensure that the rights to respect for private life and to the protection of personal data in the access 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 criminal offences ***referred to in paragraph 2a.***

Amendment 15
ARTICLE 1, PARAGRAPH 2

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

Amendment 16
ARTICLE 1, PARAGRAPH 2 A (new)

	2a. The following shall be criminal offences within the meaning of paragraph 1: ***- membership of a criminal organisation,*** ***- terrorism,*** ***- arms trafficking,*** ***- trafficking in persons,*** ***- sexual exploitation of children and child***

	pornography,
	- illegal trading in drugs and psychotropic substances,
	- laundering of the proceeds of crime,
	- counterfeiting, including counterfeiting of the euro,
	- environmental crime, including illegal trading in threatened animal or plant and tree species,
	- homicide, grievous bodily harm,
	- illegal trading in organs and human tissue,
	- kidnapping, holding persons against their will and hostage-taking,
	- forging of official documents and trading in such forged documents,
	- forging of means of payment,
	- illegal trading in nuclear and radioactive substances,
	- rape,
	- arson,
	- crimes which fall within the jurisdiction of the International Criminal Court,
	- hijacking of aircraft and ships,
	- sabotage,
	- stalking.

Amendment 17
ARTICLE 2, PARAGRAPH 2, POINT (A)

(a) 'data' means traffic data and ***location data, as well as the related*** data necessary to identify the subscriber or user;	(a) 'data' means traffic data and ***those*** data necessary to identify the subscriber or user;

Amendment 18
ARTICLE 2, PARAGRAPH 2, POINT (B A) (new)

	(ba) 'serious criminal offences' means the offences referred to in Article 1

paragraph 2a.

Amendment 19
ARTICLE 2, PARAGRAPH 2, POINT (B B) (new)

(bb) 'competent law enforcement authorities' means the judicial authorities and the other authorities responsible for the detection, investigation and prosecution of serious criminal offences.

Amendment 20
ARTICLE 3, PARAGRAPH 1

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

Amendment 21
ARTICLE 3, PARAGRAPH 2

2. Member States shall adopt measures to ensure that data retained in accordance with this Directive are only provided to the competent ***national*** authorities, in specific cases and in accordance with national legislation, for the purpose of the prevention, investigation, detection and prosecution of ***serious*** criminal offences***, such as terrorism and organised crime***.	2. Member States shall adopt measures to ensure that data retained in accordance with this Directive are only provided to the competent ***law enforcement*** authorities, in specific cases and in accordance with national legislation, for the purpose of the prevention, investigation, detection and prosecution of ***the*** criminal offences ***referred to in Article 1(2a)***. ***Member States shall ensure that the undertakings concerned which are located on their territory set up a body to liaise with the competent law enforcement authorities in cases when access to data is requested.***

Amendment 22
ARTICLE 3 A (new)

Article 3a

Access to retained data

1. Member States shall adopt measures to ensure that the competent law enforcement authorities are granted access to data retained in accordance with this Directive only subject to the following conditions:
(a) access is granted for the purpose of the investigation, detection and prosecution of serious criminal offences only;

(b) access is granted for an amount of data which is proportionate to the purpose for which the data are sought;

(c) the competent law enforcement authorities erase the data once those data are no longer necessary for the purpose for which they were sought;

(d) the competent law enforcement authorities keep the data in a form which allows data subjects to be identified only for as long as is necessary for the purpose for which the date were collected or processed further;

(e) the competent law enforcement authorities safeguard the confidentiality and integrity of the data;

(f) the competent law enforcement authorities do not forward the data to third countries under any circumstances.

2. The Commission shall adopt a Directive laying down detailed rules giving effect to the principles stated in paragraph 1 of this article. This Directive shall comply with the principles laid down in the Council Framework Decision on [data protection].

Amendment 23

ARTICLE 4, TITLE

Categories of data to be retained	Categories ***and types*** of data to be retained

Amendment 24
ARTICLE 4, POINT (F)

(f) data necessary to identify the location of mobile communication equipment.	***deleted***

Amendment 25
ARTICLE 4, PARAGRAPH 1 A (new)

The following types of data shall be retained under the categories identified in paragraph 1:

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

(1) concerning fixed network telephony:

(a) the calling telephone number;

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

(2) concerning mobile telephony:

(a) the calling telephone number;

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

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

(1) concerning fixed network telephony:

(a) the telephone number(s) called;

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

(2) concerning mobile telephony:

(a) the telephone number(s) called;

(b) the name(s) and address(es) of the subscriber(s) or registered

user(s);

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

(1) concerning fixed network telephony and mobile telephony:

(a) the date and the exact time of the start and end of the communication;

(d) data necessary to identify the type of communication:

(1) concerning fixed network telephony:

(a) the telephone service used, e.g. voice telephony, conference call, fax, messaging services;

(2) concerning mobile telephony:

(a) the mobile telephony service used, e.g. voice telephony, conference call, short message service, enhanced media service or multi-media service;

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

(1) concerning mobile telephony:

(a) the international mobile subscriber identity (IMSI) of the calling and called party;

(b) the international mobile equipment identity (IMEI) of the calling and called party.

Amendment 26
ARTICLE 4, PARAGRAPH 2

The types of data to be retained under the abovementioned categories of data are specified in the Annex.	***Data that reveals the content of a communication must not be included.***

Amendment 27
ARTICLE 5

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

Amendment 28
ARTICLE 6

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

Amendment 29
ARTICLE 7

Member States shall ensure that the categories of data referred to in Article 4 are retained for a period of ***one year*** from the date of the communication***, with the exception of data related to electronic communications taking place using wholly or mainly the Internet Protocol. The latter shall be retained for a period of six months.***	Member States shall ensure that the categories of data referred to in Article 4 are retained for a period of ***three months*** from the date of the communication***; thereafter, the data must be erased.***
	The retention period may be extended to up to six months if this proves necessary in the light of the evaluation conducted pursuant to Article 12.

Amendment 30
ARTICLE 7, PARAGRAPH 1 A (new)

	Competent law enforcement authorities

shall ensure that transferred data are erased by automated means once the investigation for which access to the data was granted is completed.

Amendment 31
ARTICLE 7, PARAGRAPH 1 B (new)

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

Amendment 32
ARTICLE 7 A (new)

Article 7a

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 of Directive 2002/58/EC and the following data security principles:

(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 loss, alteration, unauthorised or unlawful disclosure or access, and against all other unlawful forms of processing;

(c) 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;
	(d) that providers keep log lists and undertake regular and systematic self-auditing to ensure that the applicable rules on data protection are respected;
	(e) the data cannot under any circumstances be transmitted to third countries;
	(f) all data shall be destroyed at the end of the period for retention except those data which have been accessed and preserved.

Amendment 33
ARTICLE 8

Member States shall ensure that the data are retained in accordance with this Directive in such a way that the data retained and any other necessary information related to such data can be transmitted upon request to the competent ***authorities*** without undue delay.	Member States shall ensure that the data are retained in accordance with this Directive in such a way that the data retained and any other necessary information related to such data can be transmitted upon request to the competent ***law enforcement authority*** without undue delay.

Amendment 34
ARTICLE 8, PARAGRAPH 1 A (new)

	Member States shall ensure that the undertakings concerned located on their territory set up a body to deal with requests for access to data.

Amendment 35
ARTICLE 8 A (new)

	Article 8a
	Penalties
	1. Member States shall lay down penalties for infringements of the national provisions adopted to implement this

	Directive. The penalties shall be effective, proportionate and dissuasive.
	2. Member States shall ensure that persons against whom proceedings are brought with a view to imposing penalties have effective rights of defence and appeal.

Amendment 36
ARTICLE 9

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

Amendment 37
ARTICLE 10

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

Amendment 38
ARTICLE 11
Article 15, paragraph 1a (Directive 2002/58/EC)

In Article 15 of Directive 2002/58/EC ***the following paragraph 1a is inserted:***	Article 15 of Directive 2002/58/EC ***shall be replaced by the following:***
'1a. Paragraph 1 shall not apply to obligations relating to the retention of data for the prevention, investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime, deriving from Directive 2005/../EC*. * OJ L nr. …. of ….'.	***'The rights and obligations provided for in Article 5, Article 6, Article 8 (1), (2), (3) and (4), and Article 9 may only be restricted by the national provisions adopted to implement this Directive.***

Amendment 39
ARTICLE 12, PARAGRAPH 1

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

Amendment 40
ARTICLE 12, PARAGRAPH 2

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

Amendment 41
ARTICLE 12, PARAGRAPH 2 A (new)

	2a. Where the outcome of the evaluation justifies extending the retention period laid down in Article 7 by three months, the Commission shall, in accordance with Article 251 of the Treaty, submit a proposal to the European Parliament and to the Council to amend that Article.

Amendment 42
ARTICLE 14 A (new)

	Article 14a ***Confirmation of the Directive***
	This Directive must be confirmed five years after its transposition, in accordance with the procedure laid down in Article 251 of the Treaty; otherwise, it shall cease to be operative.
	Legal provisions enacted on the basis of the operative nature of this Directive shall not be affected.

Amendment 43
ANNEX

Types of data to be retained under the categories identified in Article 4 of this Directive:	***deleted***

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

(1) Concerning Fixed Network Telephony:

(a) The calling telephone number;

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

(2) Concerning Mobile Telephony:

(a) The calling telephone number;

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

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

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

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

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

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

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

(1) Concerning Fixed Network Telephony:

(a) The called telephone number or numbers;

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

user(s);

(2) Concerning Mobile Telephony:

(a) The called telephone number or numbers;

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

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

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

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

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

(1) Concerning Fixed Network Telephony and Mobile Telephony:

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

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

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

d) Data necessary to identify the type of communication:

(1) Concerning Fixed Network Telephony:

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

(2) Concerning Mobile Telephony:

(a) The telephone service used,

e.g. voice, conference call, Short Message Service, Enhanced Media Service or Multi-Media Service

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

(1) Concerning Mobile Telephony:

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

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

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

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

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

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

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

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

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