

EN

EN

EN



COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 6.11.2008  
COM(2008)723 final

2007/0248 (COD)

Amended proposal for a

**DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

**Amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sectors and Regulation (EC) No 2006/2004 on consumer protection cooperation**

**(Text with EEA relevance)**

Amended proposal for a

## **DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

**Amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sectors and Regulation (EC) No 2006/2004 on consumer protection cooperation**

**(Text with EEA relevance)**

### **1. PROCEDURAL STAGES**

The proposal — COM(2007) 698 – 2007/0248 (COD) — was adopted by the Commission on 13 November 2007 and was sent to the European Parliament and to the Council on 15 November 2007.

The European Economic and Social Committee adopted its opinion on the proposal from the Commission on 29 May 2008.

The Committee of the Regions adopted its opinion on the Commission's proposal on 18 June 2008.

The European Parliament adopted 155 amendments at first reading on 24 September 2008.

### **2. OBJECTIVE OF THE PROPOSAL**

This legislative proposal covers changes to the Universal Service Directive and the Directive on privacy and electronic communications. The aim is to adapt the regulatory framework for electronic communications by strengthening certain consumer and user rights and by ensuring that electronic communications are trustworthy, secure and reliable and provide a high level of protection for individuals' privacy and personal data.

More specifically, the objectives of the present proposals are two-fold:

1. Strengthening and improving consumer protection and user rights in the electronic communications sector, by — among other aspects — giving consumers more information about prices and supply conditions, and facilitating access to and use of e-communications, including emergency services, for disabled end-users.
2. Enhancing the protection of individuals' privacy and personal data in the electronic communications sector, in particular through strengthened security-related provisions and improved enforcement mechanisms.

### 3. OBJECTIVE OF THE AMENDED PROPOSAL

The amended proposal adapts the original proposal on a number of points as suggested by the European Parliament.

### 4. OBSERVATIONS ON THE AMENDMENTS ADOPTED BY THE EUROPEAN PARLIAMENT

#### 4.1 Amendments accepted by the Commission

The Commission can accept amendments 2, 4, 5, 7, 8, 11, 15, 16, 20, 27, 32, 38, 41, 43, 48, 51, 54, 55, 56, 60, 61, 62 (except for first indent), 63, 64, 65, 66, 68, 70, 72, 73, 77, 79, 80, 88, 89, 90, 92 (last paragraph), 97, 100, 110, 111, 112, 114 (last paragraph), 115, 116, 118, 129, 137, 141, 143, 145, 149, 150, 151, 152, 182, 191, 192.

#### 4.2 Amendments accepted by the Commission in part or subject to rewording

Amendments 3, 6, 12, 14, 18, 19, 21, 22, 23, 25, 26, 31, 37, 44, 47, 53, 67, 71, 75, 76, 82, 85, 86, 87, 91, 93, 99, 103, 105, 106, 109, 122, 127, 131, 132, 135, 136, 138, 139, 165, 180, 181, 183, 184, 185, 187, 188, 189, 193, 194.

##### – Amendment 3

The amendment clarifies the new obligations for Member States to ‘promote the availability of appropriate terminal equipment’ introduced in Article 7(2). The description needs, however, be revised in order to reflect the text of Article 7(2).

Recital 4b (new)

**‘Member States should introduce measures to ensure that disabled end-users can take advantage of the choice of undertakings and service providers available to the majority of end-users, and to promote the availability of appropriate terminal equipment to promote the creation of a market for widely available products and services incorporating facilities for disabled users. Such measures may include, for example, ~~This can be achieved inter alia by making~~ referring to European standards, ~~by introducing electronic accessibility (eAccessibility) requirements for public procurement procedures and the provision of services relating to calls for tender relating to the provision of services~~, and by implementing legislation upholding the rights of the disabled.’**

##### – Amendment 6

The Commission considers that all calls to the emergency services should offer caller location information so as to increase the protection of citizens of the European Union. The reference to caller location is thus deleted as this would have implied that caller location may not be provided. In any case, calls to the emergency services do not provide access as such to caller location. However, information on the accuracy of caller location information should be provided to ensure the more effective and rapid provision of emergency services.

## Recital 12

‘Providers of electronic communications services should ensure that their customers are adequately informed as to whether or not access to emergency services ~~and caller location information~~ is provided, and are given clear and transparent information in the initial customer contract and at regular intervals thereafter, for example in customer billing information. ***This information should include any limitations as to territorial coverage, on the basis of the planned technical operating parameters of the service and the available infrastructure. Where the service is not provided over a switched telephony network, the information should also include the level of reliability of the access to and accuracy of caller location information compared to a service that is provided over the switched telephony network, taking into account current technology and quality standards, as well as any quality of service parameters specified under Directive 2002/22/EC. Voice calls remain the most robust and reliable form of access to emergency services. Other means of contact, such as text messaging, may be less reliable and may suffer from lack of immediacy. Member States should, however, if they deem it appropriate, be free to promote the development and implementation of other means of access to emergency services capable of ensuring access equivalent to voice calls.*** Customers should also be kept well informed of possible ***types of*** actions that the providers of electronic communications services may take to address security threats or in response to a security or integrity incident, since such actions could have a direct or indirect impact on the customer’s data, privacy or other aspects of the service provided.’

## - Amendment 12

The amendment is aimed at clarifying the changes proposed to Article 22(3). The wording needs to be clarified in the interest of legal certainty: the words ‘guidelines’ and ‘basic tier of unrestricted service’ are unclear and are therefore replaced.

## Recital 14a (new)

***‘A competitive market should also ensure that users are able to have the quality of service they require, but in particular cases it may be necessary to ensure that public communications networks attain minimum quality levels so as to prevent degradation of service, usage restrictions and/or limitations and the slowing of traffic. Where there is a lack of effective competition, national regulatory authorities should use the remedies available to them under the Directives establishing the regulatory framework for electronic communications networks and services to ensure that users’ access to particular types of content or applications is not unreasonably restricted. It should also be possible for national regulatory authorities to issue guidelines setting minimum quality of service requirements under Directive 2002/22/EC and to take other measures where such other remedies have, in their judgement, not been effective, with regard to the interests of users and all other relevant circumstances. Such guidelines or measures could include the provision of a basic tier of unrestricted service’***

- Amendment 14

The amendment refers to ‘remedies’, ‘guidelines’ and ‘other measures’ that the Commission may need to assess for consistency. It should however refer to ‘quality of service requirements’ in line with amendment 12.

Recital 14d (new)

***‘Since inconsistent ~~remedies~~ quality of service requirements will significantly impair the achievement of the internal market, the Commission should assess any ~~guidelines or other measures~~ adopted by national regulatory authorities for possible regulatory intervention across the Community and, if necessary, adopt technical implementing measures in order to achieve consistent application throughout the Community.’***

- Amendment 18

A substantial part of the text of the Commission’s proposal has been moved to a new Recital 14a (see amendment 12). The reference to comitology — which is also retained in Article 22(3) — is included in the revised Recital 14c covered by amendment 14 above.

- Amendment 19

The amendment refers to the wholesale obligation of undertakings to collect and pass on directory data, under certain conditions, for the purposes of providing publicly available directory and directory enquiry services. As this is already stipulated by Article 25(2), the description of the amendment needs to be revised. Furthermore, it has to be aligned to the revised wording of amendment 85.

Recital 18a (new)

***‘Directory enquiry services should be, and frequently are, provided ~~in~~ under competitive market conditions ~~competition~~, pursuant to Article 5 of Commission Directive 2002/77/EC of 16 September 2002 on competition in the markets for electronic communications networks and services\*. ~~Wholesale~~ Measures ensuring ~~concerning~~ the inclusion of end-user data (of all undertakings that assign telephone numbers to subscribers both fixed and mobile) in databases should respect the safeguards for the protection of personal data, including Article 12 of Directive 2002/58/EC, and the The cost-oriented supply of that data for the purposes of publicly available directory and directory enquiry services to service providers and the provision of network access in cost-oriented, reasonable and transparent conditions should be in place in order to ensure so that end-users benefit fully from competition ~~reasonable and transparent conditions in competitive offers~~ reasonable and transparent conditions in competitive offers ~~with the ultimate aim of enabling the removal of retail regulation from these services.~~’***

\* OJ L 249, 17.9.2002, p. 21.

- Amendment 21

The amendment indicates that the Commission could delegate the responsibility for the management of ETNS. This is not possible as the Member States — and not the Commission — are assigned the ETNS code. The amendment is revised to reflect the fact that only those countries to which the ITU has assigned the ‘3883’ code can delegate the responsibility for its management.

Recital 21

*‘**Development of** the international code “3883” (the European Telephony Numbering Space (ETNS)) is currently **hindered** by insufficient awareness, lack of demand, overly bureaucratic procedural requirements and, in consequence, lack of demand~~insufficient awareness~~. In order to foster the development of ETNS, ~~the Commission~~ the countries to which the International Telecommunications Union has assigned the international code “3883” *should delegate responsibility for its management, number assignment and promotion either to [xxx] or, following the example of the implementation of the “.eu” top-level domain, to a separate organisation, designated by the Commission on the basis of an open, transparent and non-discriminatory selection procedure, and with operating rules which form part of Community law.*’*

- Amendment 22

The first sentence of Recital 22 has been amended to align it with the changes made in the enacting provisions of the Directive (see amendment 86 modifying Article 25(4) of the Universal Service Directive). The EP amendment is not in conformity with the principle of technology neutrality, so has been replaced by one of more general scope, clarifying that access to numbers and services in the Community is necessary to facilitate exchanges between end-users.

Recital 22

*‘A single market implies that end-users are able to access all numbers included in the national numbering plans of other Member States, and to access services, including Information Society services, using non-geographic numbers within the Community, including, among others, freephone and and premium-rate numbers and directory enquiry services. End-users should also be able to access numbers from the European Telephone Numbering Space (ETNS) and a Universal iInternational ~~f~~Freephone ~~n~~Numbers (UIFN). This will facilitate cross-border exchanges between end-users, regardless of the operator they choose. Cross-border access to numbering resources and to the associated service should not be prevented except in objectively justified cases, such as when this is necessary to combat fraud, and abuse e.g. in connection with certain premium-rate services, or when the number is defined as having a national scope only (e.g. national short code). Users should be fully informed in advance in a clear manner of any charges applicable to freephone numbers, such as international call charges for numbers accessible through standard international dialling codes. ~~End users should also be able to connect to other end user (especially via IP numbers) in order to exchange data, regardless of the operator they choose.~~ In order to ensure that end-users have effective access to*

numbers and services in the Community, the Commission should be able to adopt implementing measures.’

- Amendment 23

This amendment supports the amendments to Article 30(4) to provide protection against ‘slamming’.

Recital 23

‘In order to take full advantage of the competitive environment, consumers should be able to make informed choices and to change providers when it is in their interest. It is essential to ensure that they can do so without being hindered by legal, technical or practical obstacles, including contractual conditions, procedures, charges etc. This does not preclude imposing reasonable minimum contractual periods in consumer contracts. Number portability is a key facilitator of consumer choice and effective competition in competitive markets for electronic communications, and should be implemented with the minimum of delay, **ordinarily within no more than one day from the request of the consumer. In the case of abuse or delay in porting, national regulatory authorities should be able to impose appropriate sanctions. Moreover, without making the switching process less attractive for consumers, national regulatory authorities should be able to impose proportionate measures to minimise the risk of consumers being switched without their consent.** ~~However, experience in a certain Member State has shown that there is a risk of consumers being switched without consent. While that is a matter that should primarily be addressed by law enforcement authorities, Member States should be able to impose such minimum proportionate measures regarding the switching process as are necessary to minimise such risks, without making the process less attractive for consumers.~~ In order to be able to adapt number portability to market and technological evolution, including the possible porting of subscriber’s personal directories and profile information stored within the network, the Commission should be able to take technical implementing measures in this area. Assessment of whether technology and market conditions are such as to allow for porting of numbers between networks providing services at a fixed location and mobile networks should in particular take into account prices for users and switching costs for undertakings providing services at fixed locations and mobile networks.’

- Amendment 25

The changes below are introduced to avoid duplication of the existing Recital 47 of the Universal Service Directive 2002/22/EC.

Recital 25a (new)

***‘The procedure for out-of-court dispute resolution should be strengthened by ensuring that independent dispute resolution bodies are used, and that the procedure conforms at least to the minimum principles established by Commission Recommendation 98/257/EC of 30 March 1998 on the principles applicable to the bodies responsible for out-of-court settlement of consumer disputes\*. Member States may either use existing dispute resolution bodies for that purpose, provided those bodies meet the applicable requirements, or establish new bodies.’***

---

~~\* — OJ L115, 17.4.1998, p.31.~~

- Amendment 26

The amendment is a statement of objectives, supporting the substantive provisions of the Directive.

Recital 26a (new)

***‘(26a) Directive 2002/58/EC provides for the harmonisation of the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and the right to confidentiality and security of information technology systems, with respect to the processing of personal data in the electronic communications sector, and to ensure the free movement of such data and of electronic communications equipment and services in the Community.’***

- Amendment 31

The amendment clarifies the scope of the security measures to be adopted pursuant to Article 4. The formulation ‘without prejudice to [...] the [Data Retention] Directive 2006/24/EC’ is not appropriate since the Data Retention Directive constitutes *lex specialis* with respect to Directive 2002/58/EC.

Recital 28a (new)

***‘(28a) The provider of a publicly available electronic communications service should take appropriate technical and organisational measures to ensure the security of its services. Without prejudice to the provisions of Directive 95/46/EC and 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, such measures should ensure that personal data can be accessed only by authorised personnel for legally authorised purposes and that the personal data stored or transmitted as well as the network and services are protected. Moreover a security policy with respect to the processing of personal data should be established in order to identify vulnerabilities in the system and regular monitoring and preventive, corrective and mitigating action should be carried out.’***

- Amendment 37

The amendment emphasises the role of awareness-raising in preventing the distribution of malicious software.

Recital 34

‘Software that surreptitiously monitors actions of the user and/or subverts operation of the user’s terminal equipment for the benefit of a third party (so-called “spyware”) poses a serious threat to users’ privacy. A high and equal level of protection of the private sphere of users needs to be ensured, regardless of whether unwanted spying

programmes are inadvertently downloaded via electronic communications networks or are delivered and installed hidden in software distributed on other external data storage media, such as CDs, CD-ROMs, or USB keys. **Member States, for instance through awareness-raising campaigns, shall encourage should inform end-users about available precautions and encourage them to take the necessary steps to protect their terminal equipment against viruses and spy-ware.**

- Amendment 44

The reference to consumer legislation is modified to include the Unfair Commercial Practices Directive 2005/29/EC.

Article 1, point 1, of the amending act; Article 1, paragraph 2a (new), of Directive 2002/22/EC

***'The provisions of this Directive shall apply without prejudice to Community rules on consumer protection, in particular Directives 93/13/EC, ~~and~~ 97/7/EC and 2005/29/EC, and national rules in conformity with Community law.'***

- Amendment 47

This amendment concerns the possible deletion of the definition of Network Termination Point from the Universal Service Directive 2002/22/EC and is acceptable in principle in the event this definition is moved to the Framework Directive 2002/21/EC. However, as the EP has not tabled such an amendment, it is suggested that the latter Directive should be amended to this effect (see amendment introduced by the Commission to Article 1, point 2(ba) (new), of the amending act; Article 2, point (da) (new), of Directive 2002/21/EC.

- Amendment 53

The amendment clarifies the original proposal. However, the Commission cannot accept the replacement of 'shall' by 'may' as it undermines the objective of the provision.

Article 1, point 5, of the amending act; Article 7(2)(a) (new) of Directive 2002/22/EC

***'Member States ~~may~~shall take specific measures, shown through an assessment by the national regulatory authorities to be needed in the light of national conditions and specific disability requirements, to ensure that disabled end-users can take advantage of the choice of undertakings and service providers available to the majority of end-users, and to promote the availability of appropriate terminal equipment. They shall ensure that in any event the needs of specific groups of disabled users are met by at least one undertaking.'***

- Amendment 67

The amendment describes information to be provided in contracts by the relevant public authorities. It aims to ensure that end-users are clearly informed before concluding the contract of their obligations, for instance in relation to copyright, and of means of protection against risks to personal security and privacy. In this regard,

the reference to ‘any’ information is too wide: the provision of too much information to subscribers would render the provision ineffective.

Article 1, point 12, of the amending act; Article 20(2), second subparagraph, of Directive 2002/22/EC

***‘The contract shall also include ~~any~~ information provided by the relevant public authorities on the use of electronic communications networks and services to engage in unlawful activities or to disseminate harmful content, and on the means of protection against risks to personal security, privacy and personal data, as referred to in Article 21(4a) and relevant to the service provided.’***

- Amendment 71

The amendment concerns Article 20(6) of the Universal Service Directive. Some changes to the amendment are necessary to ensure that all elements covered by Article 20(6) as initially proposed by the Commission are kept. Amendment 76 — which is closely related to amendment 71 — is revised accordingly. (Amendment 71 is related to the new compromise proposals in Article 20(2), second subparagraph, (amendment 67) and Article 21(4a) (amendment 76)).

- Amendment 75

The amendment covers tariff information to be provided to subscribers and aims to increase transparency. However, the wording ‘prior to connecting the call’ in the last part of the point (a) might be interpreted very broadly. The text proposed by the Commission was meant to ensure that users are fully informed about any additional charge ‘at the time and point of purchase’; it is therefore specified that such information is provided ‘immediately’ prior to connecting the call. As regards point (d), subscribers also have the right to decide not to include their personal data in a directory, in accordance with the provisions of Article 12 of Directive 2002/58/EC.

Article 1, point 12, of the amending act; Article 21(4) of Directive 2002/22/EC

‘Member States shall ensure that national regulatory authorities are able to oblige undertakings providing ***connection to a public electronic communications network and/or*** electronic communications services to ***inter alia***:

***(a) provide applicable tariff information to subscribers regarding any number or service subject to particular pricing conditions; with respect to individual categories of services, national regulatory authorities may require such information to be provided immediately prior to connecting the call;***

....

***(d) inform subscribers of their right to determine whether or not to include their personal data in a directory and of the types of data concerned in accordance with Article 12 of the Directive on privacy and electronic communications; and***

- Amendment 76

This amendment is related to the new compromise proposals in Article 20(2), second subparagraph, (amendment 67) and Article 20(6) (amendment 71). However, the amendment does not cover the reference to the Electronic Commerce Directive 2000/31/EC, which should be kept. This is re-inserted in point (a) of amendment 76 as revised by the Commission. Furthermore, the text should refer to ‘legal’ consequences of breaches of copyright and related rights, so as to make it clear that other consequences (e.g. economic) are not covered. Finally, the reference to ‘respect for the rights and freedoms of others’ is vague and potentially very wide, and is accordingly deleted.

Article 1, point 12, of the amending act; Article 21(4a) (new) of Directive 2002/22/EC

*‘Member States shall ensure that national regulatory authorities oblige the undertakings referred to in paragraph 4 to distribute public interest information to existing and new subscribers when appropriate. Such information shall be produced by the relevant public authorities in a standardised format and shall inter alia cover the following topics:*

*(a) without prejudice to Directive 2000/31/EC on electronic commerce, the most common uses of electronic communications services to engage in unlawful activities or to disseminate harmful content, ~~particularly where it may prejudice respect for the rights and freedoms of others~~, including infringements of copyright and related rights, and their legal consequences; and*

*(b) means of protection against risks to personal security, privacy and personal data in using electronic communications services.*

*Significant additional costs incurred by an undertaking in complying with these obligations shall be reimbursed by the relevant public authorities.’*

- Amendment 82

The amendment clarifies that the requirement to ensure availability is limited to feasible objectives.

Article 1, point 14, of the amending act; Article 23 of Directive 2002/22/EC

*‘Member States shall take all necessary **measures** to ensure the highest fullest possible level of availability of publicly available telephone services in the event of catastrophic network breakdown or in cases of force majeure. Member States shall ensure that undertakings providing publicly available telephone services take all **necessary measures** to ensure uninterrupted access to emergency services ~~from any place within the territory of the EU.~~’*

- Amendment 85

The extension of the scope of the provision to all electronic communications services and the reference to cost orientation cannot be accepted. The reference to fair, objective, non-discriminatory, and transparent conditions is changed to reflect the relevant provisions of Article 5 of the Access Directive 2002/19/EC.

Article 1, point 15, sub-point b, of the amending act; Article 25(3) of Directive 2002/22/EC

‘Member States shall ensure that all end-users **provided with a publicly available telephone of an electronic communications** service can access directory enquiry services, ~~and that~~ **National regulatory authorities shall be able to impose obligations and conditions on undertakings that operators controlling access to end-users for the provision of directory enquiry services in accordance with the provisions of Article 5 of Directive 2002/19/EC (Access Directive). Such obligations and conditions shall be such services provide access on terms which are fair, cost-oriented, objective, proportionate, non-discriminatory and transparent.**’

- Amendment 86

This amendment clarifies that the provision applies to voice calls and SMS. The last part of the amendment has been taken into account by amending the first sentence of Recital 22 of the amending act (see amendment 22 above).

Article 1, point 15, sub-point ba (new), of the amending act; Article 25(4) of Directive 2002/22/EC

‘Member States shall not maintain any regulatory restrictions which prevent end-users in one Member State from accessing directly the directory enquiry service in another Member State ***by voice call or SMS, and shall take measures to ensure such access pursuant to Article 28.***’

- Amendment 87

The amendment clarifies that different parties (NRAs, emergency authorities, providers of electronic communications) should cooperate to ensure access to emergency services. However, the description needs to be revised as the wording ‘reliable’ is unclear (there is a risk that operators could claim that their services are ‘not reliable enough’, in order to avoid having to deliver emergency services). Moreover, the reference to ‘international’ calls is unnecessary and misleading as it is not possible to access emergency numbers from abroad.

Article 1, point 16, of the amending act; Article 26(2) of Directive 2002/22/EC

‘Member States, ***in cooperation with national regulatory authorities, emergency services and providers***, shall ensure that undertakings providing ***an electronic communications*** service for originating national ~~and/or international~~ calls through **to** a number or numbers in a national ~~or international~~ telephone numbering plan provide ~~reliable~~ access to emergency services.’

- Amendment 91

The amendment clarifies the wording of the original proposal. However, the Commission cannot accept the deletion of the annual reporting obligation of the Member States.

Article 1, point 16, of the amending act; Article 26(6) of Directive 2002/22/EC

‘Member States shall ensure that *in addition to information about their national emergency numbers, all* citizens *of the Union* are adequately informed about the existence and use of the single European emergency call number “112”, in particular through initiatives specifically targeting persons travelling between Member States. **Member States shall submit an annual report to the Commission and the Body on the measures taken in this regard.**’

- Amendment 93

The amendment transfers the future management of ETNS to an organisation designated by the Commission. Some redrafting is proposed in order to allow the Commission to lay down the implementing rules governing the legal entity as to the management of ETNS.

Article 1, point 16, of the amending act; Article 27(2) of Directive 2002/22/EC

‘Those Member States to which the ITU **has** assigned the international code ‘3883’ shall entrust **a legal entity, established within the Community** ~~an organisation established by Community law and designated by the Commission on the basis of an open, transparent and non-discriminatory selection procedure, or [xxx]~~, with sole responsibility for **the** management, *including number assignment, and promotion* of the European Telephony Numbering Space. **The Commission shall lay down the necessary implementing rules.**’

- Amendment 99

The amendment provides a complementary tool (withholding revenues) to fight effectively against fraud or misuse. A minor drafting improvement is proposed.

Article 1, point 16, of the amending act; Article 28(1), second subparagraph, of Directive 2002/22/EC

‘National regulatory authorities shall be able to block on a case-by-case basis access to numbers or services where this is justified by reasons of fraud or misuse, *and to ensure that in such cases, including where an investigation is pending, providers of electronic communications services may withhold relevant interconnection or other service revenues.*’

- Amendment 103

The amendment provides protection against ‘slamming’, which is a serious problem in a number of Member States. However, the explicit extension of the one working-day limit for number portability cannot be accepted. The sentences have been rearranged.

Article 1, point 18, of the amending act; Article 30(4) of Directive 2002/22/EC

‘Porting of numbers and their subsequent activation shall be executed within the shortest possible delay, no later than one working day from the initial request by the subscriber. **National regulatory authorities shall be able to impose appropriate sanctions on providers, including an obligation to compensate subscribers, in cases of delay in porting or abuse of porting by them or on their behalf.** *National*

~~regulatory authorities may extend the one day period and prescribe take appropriate measures where necessary to ensure that subscribers are not switched against their will. National regulatory authorities may impose appropriate sanctions on providers, including an obligation to compensate customers, in case of delay in porting or abuse of porting by them or on their behalf.'~~

- Amendment 105

The amendment provides for contracts lasting 24 months. However, requiring operators to offer the possibility of 12-month contracts for all types of service and terminal equipment would limit the provision of innovative offerings in the market and the business freedom of operators.

Article 1, point 18, of the amending act; Article 30(5a) (new) of Directive 2002/22/EC

~~'Member States shall ensure that the duration of contracts concluded between users and undertakings providing an electronic communications service does not exceed 24 months. They shall also ensure that undertakings offer users the possibility to subscribe to a contract with a maximum duration of 12 months for all types of service and terminal equipment.'~~

- Amendment 106

The amendment recognises the fact that national bodies other than NRAs may be responsible for the matters at hand, which is a useful addition. On the other hand, it is necessary to retain the reference to 'conditions'.

Article 1, point 18, of the amending act; Article 30(6) of Directive 2002/22/EC

'Without prejudice to any minimum contractual period, **Member States** shall ensure that conditions and procedures for termination of **contracts** do not act as a disincentive for changing suppliers or services.'

- Amendment 109

The objective of this amendment is sound, i.e. to ensure equivalent access for disabled users. The description should, however, ensure that economic viability is also taken into account and that national regulatory authorities can take proactive action. The EP amendment is modified to this effect.

Article 1, point 19a (new), of the amending act; Article 31a (new) of Directive 2002/22/EC

**'Ensuring equivalent access and choice for disabled end-users**

**Member States shall ensure that national regulatory authorities are able to impose appropriate requirements on undertakings providing publicly available electronic communications services so as to ensure, on a sustainable and comprehensive basis, that disabled end-users:**

*(a) have access to electronic communication services equivalent to that enjoyed by the majority of end-users; and*

*(b) can take advantage of the choice of undertakings and services available to the majority of end-users.'*

- Amendment 122

The detailed technical suggestions are maintained, inasmuch as they refer to the security of personal data, which is the focus of the provision at hand. Auditing powers for NRAs can contribute to improving the implementation of the provisions relating to data protection and security.

Article 2, point 3, sub-point aa (new), of the amending act; Article 4(1a) and (1b) (new) of Directive 2002/58/EC

*'(aa) the following paragraphs are inserted:*

***"1a. Without prejudice to the provisions of Directive 95/46/EC and Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks<sup>1</sup>, these measures shall at least:***

*~~— appropriate technical and organisational measures to ensure~~ **ensure** ~~that personal data can be accessed only by authorised personnel for legally authorised purposes and to protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration and unauthorised or unlawful storage, processing, access or disclosure;~~*

***- protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure; and***

*~~— appropriate technical and organisational measures to protect the network and services against accidental, unlawful or unauthorised usage or interference with or hindering of their functioning or availability;~~*

***- implement a security policy with respect to the processing of personal data;***

*~~— a process for identifying and assessing reasonably foreseeable vulnerabilities in the systems maintained by the provider of electronic communications services, which shall include regular monitoring for security breaches; and~~*

*~~— a process for taking preventive, corrective and mitigating action against any vulnerabilities discovered in the process described under the fourth indent and a process for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach.~~*

***1b. National regulatory authorities shall be able to audit the measures taken by providers of publicly available electronic communication services and information society services and to issue recommendations about best practices and***

*performance indicators concerning the level of security which these measures should achieve.”*

---

---

*1 — OJ L 105, 13.4.2006, p. 54.”*

- Amendment 127

It is necessary to maintain the comitology procedure for technical implementing measures to ensure consistent and harmonised implementation of the provisions relating to security of personal data, including notifications of privacy breaches. A broad consultation of relevant stakeholders may contribute to the quality and acceptance of these measures.

Article 2, point 3, sub-point b, of the amending act; Article 4(4) of Directive 2002/58/EC

‘In order to ensure consistency in implementation of the measures referred to in **paragraphs 1 to 3bd**, the Commission ~~shall~~ **may**, following consultation with the European Data Protection Supervisor, **the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC, relevant stakeholders and ENISA, adopt recommend** technical implementing measures concerning *inter alia* the **measures set out in paragraph 1a and the** circumstances, format and procedures applicable to information and notification requirements **referred to in paragraphs 3a and to 3bd**.

***The Commission shall involve all relevant stakeholders, particularly in order to be informed of the best available technical and economic methods for improving the implementation of this Directive.’***

Those measures designed to amend non-essential elements of this Directive by supplementing it shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 14a (2). On imperative grounds of urgency, the Commission may use the urgency procedure referred to in Article 14a (3).

- Amendment 131

The amendment provides clarification that MMS and similar technologies are covered by the definition of ‘electronic mail’ in Article 2(h).

New recital

**‘Safeguards provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes by means of electronic mail are also applicable to SMS, MMS and similar technologies.’**

- Amendment 132

The proposed redrafting improves the clarity of the text while maintaining the intention of the amendment to cover certain ‘phishing’ messages (at least those which fall within the scope of the Directive; i.e. those of a commercial nature).

Article 2, point 4d (new), of the amending act; Article 13(4) of Directive 2002/58/EC

*(4d) Article 13(4) is replaced by the following:*

***‘In any event, the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, ~~or in contravention of Article 6 of Directive 2000/31/EC, or that contain links to sites that have a malicious or fraudulent intent,~~ or without a valid address to which the recipient may send a request that such communications cease, or soliciting recipients to visit websites that contravene Article 6 of Directive 2000/31/EC, shall be prohibited.’***

- Amendment 135

The amendment seeks to emphasise the importance of the principle of technology neutrality, but it seems more appropriate to include such a reference in a new recital.

Article 2, point 5b (new), of the amending act; Article 14(3) of Directive 2002/58/EC

***‘Where required, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data, in accordance with Directive 1999/5/EC and Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and communications. ~~Such measures shall respect the principle of technology neutrality.~~***

**New recital:**

***‘Where measures aiming to ensure that terminal equipment is constructed so as to safeguard the protection of personal data and privacy are adopted pursuant to Directive 1999/5/EC or Council Decision 87/95/EEC, such measures should respect the principle of technology neutrality to the greatest extent possible.’***

- Amendment 136

The proposed reporting is a useful addition in the interest of greater transparency. The language should be aligned with the wording of Directive 95/46/EC, which defines the supervisory authority in its Article 28. In contrast, the inclusion of providers of information society services goes beyond the current scope of the regulatory framework for electronic communications and is accordingly deleted.

Article 2, point 6a (new), of the amending act; Article 15(1b) (new) of Directive 2002/58/EC

***‘(6a) in Article 15, the following paragraph is inserted:***

***“1b. Providers of publicly available communications services ~~and providers of information society services~~ shall notify the ~~independent data protection authorities~~ supervisory authority established in accordance with Article 28 of Directive 95/46/EC, without undue delay, of all requests for access to users’ personal data received pursuant to paragraph 1, including the legal justification given and the legal procedure followed for each request; the supervisory***

***~~independent data protection authority concerned shall notify the appropriate judicial authorities of those cases in which it deems that the relevant provisions of national law have not been complied with.~~***”

- Amendment 138

The provisions in question concern data protection issues with a cross-border dimension (including the enforcement of national data protection laws), which in some cases do not come under the current scope and tasks of ENISA. The reference is therefore adapted accordingly. The reference to the Article 29 Working Party should be worded as in the existing Article 15(3).

Article 2, point 7, of the amending act; Article 15a(4), first subparagraph, of Directive 2002/58/EC

‘In order to ensure effective cross-border cooperation in the enforcement of the national laws adopted pursuant to this Directive and to create harmonised conditions for the provision of services involving cross-border data flows, the Commission may adopt technical implementing measures, following consultation with ~~ENISA, the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC ("Article 29 Data Protection Working Party")~~ the relevant regulatory authorities and, where appropriate, ENISA.’

- Amendment 139 and 186/rev

The deadline for the report on the operation of the amended ePrivacy Directive must allow for the necessary collection of data and should be aligned with the review clauses in other parts of the regulatory framework (i.e. 3 years). A reporting obligation referring to ‘purposes not covered by this Directive’ is not appropriate. The references to the Article 29 Data Protection Working Party and the EDPS are acceptable. A reference to the Lisbon Treaty is not appropriate here. In addition, while the Commission is prepared to undertake the work on IP addresses suggested by the Parliament, a substantive provision of a directive is not the appropriate way of addressing the issue.

Article 2, point 7a (new), of the amending act; Article 18 of Directive 2002/58/EC

‘(7a) Article 18 is replaced by the following:

**“Article 18**

**Review**

**By ...+Not later than three years after <time limit for implementation of the amending act>, the Commission shall submit to the European Parliament and the Council, having consulted the ~~Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC~~ and the European Data Protection Supervisor, a report on the application of ~~this Directive 2002/58/EC~~ and its impact on economic operators and consumers, in particular as regards the provisions on unsolicited communications, and breach notifications ~~and the use of personal~~**

~~data by public or private third parties for purposes not covered by this Directive, taking into account the international environment. For this purpose, the Commission may request information from the Member States, which shall be supplied without undue delay. The Commission may submit proposals to amend this Directive, taking account of the results of that report, any changes in the sector, the Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community<sup>1</sup>, in particular the new competences in matters of data protection as laid down in Article 16, and any other proposal it may deem necessary in order to improve the effectiveness of this Directive.~~

~~No later than two years from the date of entry into force of Directive 2008/.../EC [amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation], the Commission shall submit to the European Parliament, the Council and the European Economic and Social Committee a report, based on an in-depth study, with recommendations on standard uses of IP addresses and the application of the ePrivacy and Data Protection Directives as regards their collection and further processing, following the consultation of the EDPS, the Article 29 Working Party, and other stakeholders to include industry representatives.~~

---

~~+ Two years from the date of entry into force of this Directive.~~

~~1 — OJ C 306, 17.12.2007, p. 1.”~~

- Amendment 165

The Commission accepts the wording of the amendment with minor linguistic improvements. It is also clarified that the provision concerns tariff information.

Article 1 — point 12 of the amending act; Article 21(3) of Directive 2002/22/EC

‘National regulatory authorities shall encourage the provision of **comparable** information to enable end-users and consumers to make an independent evaluation of the cost of alternative usage patterns, by means of interactive guides or similar techniques. Member States shall ensure that **when such guides or similar techniques are not available on the market, free of charge or at a reasonable price,** national regulatory authorities make such guides or techniques **them** available ~~themselves or through third parties, free of charge or at a reasonable price~~. Third parties shall have a right to use without charge the **tariff information** published by undertakings providing electronic communications networks and/or services, for the purposes of selling or making available such interactive guides or similar techniques.’

- Amendment 180

Traffic data enjoy a high level of protection under the Directive due to their sensitive nature. The recital clarifies that the processing of traffic data where necessary for the

provision of security products and services is permissible insofar as it is done in a responsible way and in compliance with the existing data protection safeguards.

Recital 26b (new)

***‘The processing of traffic data for the purpose of ensuring network and information security purposes, including ensuring the availability, authenticity, integrity and confidentiality of stored or transmitted data, by providers of security services acting as data controllers would, under normal circumstances, be considered to be will enable the processing of such data for the legitimate interest of the data controller within the meaning of Article 7(f) of Directive 95/46/EC. This could for example include for the purpose of preventing unauthorised access to electronic communications networks, and malicious code distribution, stopping the or denial of service attacks, and damages to computer and electronic communication systems. The European Network and Information Security Agency (ENISA) should publish regular studies with the purpose of illustrating the types of processing allowed under Article 6 of this Directive.’***

- Amendment 181

The amendment provides for a new legal basis for the processing of traffic data for security purposes. In view of the sensitive nature of traffic data, appropriate safeguards must be applied to the processing activities, while the scope of the provision should be brought into line with the scope of the Directive and the regulatory framework for electronic communications as a whole.

Article 2, point 4b (new), of the amending act; Article 6(6a) (new) of Directive 2002/58/EC

***‘(4b) in Article 6, the following paragraph is added:***

***“6a. Without prejudice to compliance with the provisions other than Article 7 of Directive 95/46/EC and Article 5 of this Directive, traffic Traffic data may be processed for the legitimate interest of the data controller for the purpose of implementing technical measures to ensure the network and information security, as defined by Article 4(c) of Regulation (EC) 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency\*, of a public electronic communication service, a public or private electronic communications network, an information society service or related terminal and electronic communication equipment, except where such interests are overridden by the interests ~~for~~of the fundamental rights and freedoms of the data subject. Such processing ~~must~~shall be restricted to that which is strictly necessary for the purposes of such security activity.***

---

\* OJ L 77, 13.3.2004, p. 1.”

- Amendment 183

The amendment gives useful examples of situations in which immediate notification of privacy breaches to the individuals concerned is essential in order to avoid potential harm.

Recital 29

*‘A breach of security resulting in the loss or compromising of personal data of a subscriber **or individual** may, if not addressed in an adequate and timely manner, result in substantial harm **to users, such as economic loss, social harm or identity theft**. Therefore, subscribers concerned by such security incidents ~~the national regulatory authority or other competent national authority~~ should be notified ~~by the relevant service provider of every security breach~~ without delay **in order to be able to take the necessary precautions**. ~~The competent authority should determine the seriousness of the breach and should require the relevant service providers to give an appropriate notification without undue delay to the persons affected by the breach, as appropriate. Furthermore, and~~ **In particular, in cases where there is an imminent and direct danger for consumers’ rights and interests (such as in cases of unauthorised access to the content of e-mails, access to credit card records, etc.), it is essential that the relevant service providers should, in addition to the competent national authorities, immediately notify affected users immediately directly. Finally, Providers should also annually notify affected users once a year of all breaches of security under this Directive that occurred during the relevant time period the preceding twelve months.** The notification to the national authorities and to users should include information about measures taken by the provider to address the breach, as well as recommendations for **the protection of** the users affected.’*

- Amendment 185

The recital is related to the broader debate on the legal status of IP addresses that has been ongoing among the relevant stakeholders in Europe in recent months. While the Commission is prepared to undertake the work on IP addresses suggested by the Parliament, an explicit reference to this in a directive does not seem appropriate.

Recital 27a (new)

*‘IP addresses are essential to the working of the internet. They are unique numbers assigned to identify network participating devices participating in a computer network using the Internet Protocol for communication between its nodes, such as computers or mobile smart devices by a number. In practice, they may also be used to identify the user of a given device. Considering the different scenarios in which IP addresses are used, and the related technologies, which are rapidly evolving (including the deployment of IPv6), questions have arisen about their use treatment as personal data in certain circumstances. Developments concerning the use of IP addresses should be followed closely ~~Commission should therefore conduct a study regarding IP addresses and their use, taking into consideration the work already done by, among others, the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC, and in the light of such present such proposals as may be appropriate.~~*

The amendment proposes an alternative solution for the mandatory notification of security breaches involving personal data, taking into account the concerns about possible 'notification fatigue' (i.e. the need to avoid notification in cases of minor importance or where appropriate technology measures are in place), while ensuring the harmonisation of implementing measures at EU level.

Article 2, point 3, sub-point b, of the amending act; Article 4(3) of Directive 2002/58/EC

'3. In the case of a personal data breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed in connection with the provision of publicly available communications services in the Community, the provider of publicly available electronic communications services, ~~as well as any undertaking operating on the internet and providing services to consumers, which is the data controller and the provider of information society services~~ shall, without undue delay, notify the national regulatory authority ~~or the competent authority according to the individual law of the Member State~~ and the subscriber or individual concerned of such a breach, subject to paragraphs 3a and 3b below. The notification to the ~~competent authority~~ subscriber or individual concerned shall at least describe the nature of the breach and the contact points where more information can be obtained, and shall recommend measures to mitigate its possible negative effects of the personal data breach. The notification to the ~~competent~~ authority shall, in addition, describe the consequences of the personal data breach and the measures proposed or taken by the provider to address the breach.

3a. Notification of a personal data breach to a subscriber or individual concerned shall not be required if ~~the provider of publicly available electronic communications services, as well as any undertaking operating on the Internet and providing services to consumers, which is the data controller and the provider of information society services, shall notify their users beforehand to avoid imminent and direct danger~~ has demonstrated to the satisfaction of the competent authority that no harm to the rights and interests of consumers is reasonably likely to occur as a result of the personal data breach.

3b. Notification of a ~~security~~ personal data breach to a subscriber or individual concerned shall not be required if the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access the data.

3c. Member States shall ensure that the competent national authority is able to set detailed rules and, where necessary, issue instructions concerning the circumstances when the notification of personal data breaches by the provider of a publicly available electronic communications service is required, in compliance with paragraphs 3a and 3b, the format applicable to such

notification, as well as the manner in which the notification is made. Competent national authorities shall also monitor whether companies have complied with their notification obligations under this Article and impose appropriate sanctions and remedies, including publication, as appropriate, in the event of a failure to do so.'

New Article 2(i):

"Personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed in connection with the provision of publicly available electronic communications services in the Community.'

- Amendment 188

The amendment introduces provisions related to '116' numbers and services, in particular the number '116000' for missing children hotlines. However, there is a need to avoid over-strict or unrealistic provisions (e.g. for disabled users in paragraph 2) that may be a barrier to effective implementation. Furthermore, paragraph 4 concerns aspects which are outside the scope of the regulatory framework (the provision of hotlines).

Article 1, point 16, of the amending act; Article 27a (new) of Directive 2002/22/EC

#### **'Article 27a**

#### ***Harmonised numbers for harmonised services of social value, including the missing children hotline number***

~~1. Member States shall promote the specific numbers in the numbering range beginning with '116' identified by Commission Decision 2007/116/EC of 15 February 2007 on reserving the national numbering range beginning with '116' for harmonised numbers for harmonised services of social value.<sup>1</sup> They shall encourage the provision within their territory of the services for which such numbers are reserved.~~

~~2. Member States shall ensure that disabled end users are able to access services provided under the '116' numbering range. In order to ensure that disabled end users are able to access such services while travelling in other Member States, measures taken shall include ensuring compliance with relevant standards or specifications published in accordance with the provisions of Article 17 of Directive 2002/21/EC (Framework Directive).~~

~~3. Member States shall ensure that citizens are adequately informed about the existence and use of services provided under the '116' numbering range, in particular through initiatives specifically targeting persons travelling between Member States.~~

~~4. Member States shall, in addition to measures of general applicability to all numbers in the '116' numbering range taken pursuant to paragraphs 1, 2 and 3,~~

~~ensure citizens' access to a service operating a hotline to report cases of missing children. The hotline shall be available on the number 116000.~~

~~5. In order to ensure the effective implementation of the '116' numbering range the numbers and services identified by Commission Decision 2007/116/EC of 15 February 2007 on reserving the national numbering range beginning with "116" for harmonised numbers for harmonised services of social value\*, in particular the missing children hotline number 116000, in the Member States, including access for disabled end-users when travelling in other Member States, the Commission, having consulted [xxx], may adopt technical implementing measures.~~

*Those measures, designed to amend non-essential elements of this Directive by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 37(2).'*

---

~~1 — OJ L 49, 17.2.2007, p.30~~

~~\* — OJ L 49, 17.2.2007, p.30~~

- Amendment 189

The amendment accompanies amendment 188 above, which introduces provisions related to '116' numbers and services, in particular '116000' for missing children hotlines. The last sentence should be deleted because it would be disproportionate and burdensome to implement for some Member States. Amendments are suggested to reflect the fact that the regulatory framework can include provisions on the assignment of '116' numbers (but not on issues relevant to the functioning of the services), and to foster the use of these numbers in the Member States.

Recital 21a (new)

~~'Pursuant to its Decision 2007/116/EC of 15 February 2007 on reserving the national numbering range beginning with "116" for harmonised numbers for harmonised services of social value\*, the Commission has reserved numbers in the "116" numbering range for certain services of social value. This Decision is based on Article 10(4) of the Framework Directive and therefore relates to numbering issues. The numbers identified in that Decision cannot be used for purposes other than those set out therein, but there is no obligation for Member States to ensure that services associated with the reserved numbers are actually provided. The appropriate provisions of Decision 2007/116/EC should be reflected in Directive 2002/22/EC in order to integrate them more firmly into the regulatory framework for electronic communications networks and services and to ensure accessibility by disabled end-users as well. In order to ensure the effective implementation of numbers and services in the "116" numbering range and to foster the use of these numbers, the Commission should be able to adopt implementing measures. Considering the particular aspects related to reporting missing children and the currently limited availability of that service, Member States should not only reserve a number, but also ensure that a service for reporting missing children is actually available in their territories under the number 116000.'~~

---

~~1\*~~ OJ L 49, 17.2.2007, p.30

- Amendment 193

This amendment is linked to amendment 14. The concepts ‘guidelines’ and ‘other measures’ are not clearly defined. This could lead to diverging implementation across the EU and to legal uncertainty. They are therefore deleted.

Article 1, point 13, point b, of the amending act; Article 22(3) of Directive 2002/22/EC

*~~‘A national regulatory authority may issue guidelines setting minimum quality of service requirements, and, if appropriate, take other measures, in order to prevent degradation of service and slowing of traffic over networks, and to ensure that the ability of users to access or distribute content or to run applications and services of their choice is not unreasonably restricted. Those guidelines or measures Such requirements shall take due account of any standards issued under Article 17 of Directive 2002/21/EC (Framework Directive).~~*

*~~The Commission may, having examined such guidelines or measures requirements and consulted [xxx], adopt technical implementing measures in that regard if it considers that the guidelines or measures requirements set at national level may create a barrier to the internal market. Those Such measures, designed to amend non-essential elements of this Directive by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 37(2).~~*

- Amendment 194

The amendment is acceptable in principle. However, some re-drafting is proposed to ensure a better link between the regulatory framework and the legislation on electronic commerce. The reference to ‘law enforcement’ authorities does not seem appropriate in this context and is therefore deleted.

Recital 14b (new)

*~~‘In the absence of relevant rules of Community law, content, applications and services are deemed lawful or harmful in accordance with national substantive and procedural law. It is a task for the relevant authorities of the Member States, not for providers of electronic communications networks or services, to decide, in accordance with due process, whether content, applications or services are lawful or harmful or not. Directive 2002/22/EC is The Framework Directive and the Specific Directives are without prejudice to Directive 2000/31/EC (Directive on electronic commerce), which inter alia contains a “mere conduit” rule for intermediary service providers, as defined therein. Directive 2002/22/EC The Framework Directive and the Specific Directives does not require providers to monitor information transmitted over their networks or to take punitive action or legal prosecution against their customers due to such information, nor does it make providers liable for the information. Responsibility for any such punitive action or legal prosecution remains with the relevant ~~law enforcement~~ authorities.’~~*

#### **4.3. Amendments not accepted by the Commission**

Amendments 1, 10, 17, 24, 28, 29, 35, 36, 39, 40, 42, 45, 46, 49, 50, 52, 57, 58, 59, 62 (first paragraph), 69, 78, 83, 84, 92 (first paragraph), 95, 96, 98, 101, 102, 104, 107, 108, 113, 114 (first paragraph), 117, 119, 120, 121, 123, 124, 125, 128, 130, 133, 140, 142, 144, 146, 147, 157, 163, 174, 166, 186, 190 cannot be accepted by the Commission.

#### **5. AMENDED PROPOSAL**

Having regard to Article 250(2) of the EC Treaty, the Commission amends its proposal as indicated above.