# PRIVACY AND ELECTRONIC COMMUNICATIONS

**(Comments on the modifications to Directive 2002/58/EC introduced by Directive 2009/136/EC, supposed to be brought into UK law by 25th May, 2011)**

AMBERHAWK

A DATA PROTECTION ANALYSIS
FROM AMBERHAWK TRAINING LTD
DR. C. N. M. POUNDER, MAY 2010





# PRIVACY AND ELECTRONIC COMMUNICATIONS

## *SUMMARY OF KEY ISSUE: BEHAVIOURAL MARKETING*

Article 13 of Directive 2002/58/EC dealing with electronic marketing has been modified. **The analysis that follows shows that the new Article 13 allows Member States to introduce consent/opt-out requirements for ALL forms of electronic marketing including behavioural marketing. Whether Member States offer this option to its citizens when they implement the required legislative changes is the only unanswered question.**

However, new Article 13 also allows a continuation of a minimum privacy protection policy with respect to the use of electronic marketing by organisations. For example, the current position in the UK is the bare minimum; Article 13 allows that minimum to continue.

The objective of this document is to help organisations and individuals to understand what the changes are envisaged in advance of national implementation. In this way, it should become easier to identify where national Governments are **not** taking advantage of that flexibility to protect individual privacy.

**As the changes to Directive 2002/58/EC have to be implemented by the end of May 2011, it will be an early test of the privacy credentials of the next Government in the UK.**

## *COMMENTARY*

The annoted text updates Directive 2002/58/EC with the modifications found in Directive 2009/136/EC. I have included all the deletions, changes, additions and new Recitals (at the end of the Directive – from page 19), so that readers can clearly see what has changed from the original. I have not annoted the original Directive text as this has been done by most Data Protection Commissioners (e.g. in the UK, there is detailed PECR Guidance on the ICO website).

I now am convinced that a new Directive allows Member States to introduce consent/opt-out requirements for **ALL** forms of electronic marketing including behavioural marketing. Whether Member States offer this option to its citizens when they implement the required legislative changes by next May is the only unanswered question.

However, the Directive also allows a continuation of a minimum privacy protection policy with respect to the use of electronic marketing by organisations. For

example, the current position in the UK is the bare minimum; the Directive allows that minimum to continue.

The requirement for consent or opt-out of behavioural advertising from users and subscribers can be seen from a published analysis of the Directive (see references below). Although, other provisions include the requirement to report a data loss, consent for cookies (rather than an "opt-out"), it is the marketing provisions that could have significant impact.

The argument I am using is derived by reading the Directive text in between the lines. For example, "electronic mail" is a defined term in the Directive; so when it is **NOT** used in some of the marketing provisions (in Article 13), one can make the inference that the provision is intended to apply to other forms of marketing that extends beyond "electronic mail" (e.g. behavioural marketing). The assumption being made that if the text wanted to say "electronic mail" it would have done so.

The text uses the term "direct marketing" which is not defined. So if one assumes a definition of "direct marketing" similar to that in Section 11 of the Data Protection Act ("direct marketing" means "the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals"), then one can see that behavioural marketing is captured. For example, if a marketing message depends on an individual's browsing habits, then any individual who exhibits a required browsing behaviour, receives a particular advert directed to them.

In Article 13 there is a conspicuous absence of the use of "personal data" in its provisions although obviously personal data are subject to these rules (e.g. an email address of an individual is usually personal data – fred.bloggs@amberhawk.com). So where the term "personal data" is **NOT** used, then provisions are clearly intended to apply in circumstances where other data (i.e. beyond the narrow confines of personal data) are processed for a marketing purpose. Behavioural marketing involves such "not personal data" (according to Google and other behavioural marketers).

Article 9 uses an interesting undefined term: "geographical position". It is not clear whether a "geographical position" means "in the UK", or "in London", or "in Covent Garden", or "postcode E5 6PT" or does it need precise GPS co-ordinates? Note that the less precise the meaning of "geographic position" the more impact that this provision could have, especially if marketing activities are linked to the use of "location data". For example, certain types of behavioural marketing targeted at users or subscribers whose address can be ascertained from the location data.

Finally, I remind readers of my view that data such as an IP address can be transformed unambiguously into personal data; see **"Reclaiming Privacy on the Internet – 2009" (**also on http://www.amberhawk.com/policydoc.asp). Please feel free to contact info@amberhawk.com with any comments. You are free to copy and distribute this text, so long as Amberhawk is identified as the source

**Dr C. N. M. Pounder**
**4 May 2010**





# CHANGES TO DIRECTIVE 2002/58/EC

**Article 1**

Scope and aim

~~1. This Directive harmonises 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, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.~~

'1.This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.';

2. The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.

3. This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.

**Article 2**

Definitions

Save as otherwise provided, the definitions in Directive 95/46/EC and in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)(8) shall apply.

The following definitions shall also apply:

(a) "user" means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service;

(b) "traffic data" means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;

**Comment [U1]:** Not much change as far as I can see – the addition of "confidentiality" seems to add little to the word "privacy".

The "right to privacy" is a reference to Article 1 of Directive 95/46/EC which links the "right to Privacy" to Article 8 of the Human Rights Convention.

The text "...provides for the harmonisation..." refers to provisions in the Directive that require Member States to adopt the same standards. It infers that there is a mechanism to make sure that recalcitrant Member States can be brought into line.

Harmonisation definitely applies to personal data. However, the use of "in particular" means that the provisions could be harmonised beyond the circumstances when personal data are processed.

**Comment [U2]:** There is no change to the range of organisations that are caught by the Directive – basically we are looking at ISPs and Telcos except in the area of electronic marketing.

**Comment [U3]:** An electronic communications service is defined in the Communications Act 2003 as 'a service consisting of, or having as its principal feature, the conveyance by means of an electronic communications network of signals, except in so far as it is a content service'.

In general terms, an electronic communications service is a conveyance service for signals, for example a fixed or mobile telephone service.

A public electronic communications service is any service as described above that is provided so as to be available for use (free or by subscription) by members of the public.

**Comment [U4]:** The electronic communications network is the infrastructure through which the electronic communications service is provided.

~~(c) "location data" means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;~~

'(c) "location data" means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;';

(d) "communication" means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;

~~(e) "call" means a connection established by means of a publicly available telephone service allowing two-way communication in real time;~~ (no replacement)

(e~~f~~) "consent" by a user or subscriber corresponds to the data subject's consent in Directive 95/46/EC;

(f~~g~~) "value added service" means any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof;

(g~~h~~) "electronic mail" means any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

(h) "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 a publicly available electronic communications service in the Community.';

~~Article 3~~ **REMOVED**

~~Services concerned~~

~~1. This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community.~~

~~2. Articles 8, 10 and 11 shall apply to subscriber lines connected to digital exchanges and, where technically possible and if it does not require a disproportionate economic effort, to subscriber lines connected to analogue exchanges.~~

**Comment [U5]:** Location data extended to include that location data derived from the use of "an electronic communications service". **Could be important for Article 9.**

What is the precision needed for "geographic position"? I don't know. Because the Directive does not use "precise geographic position" or "geographic co-ordinates", the term could be broader than a "GPS fix". Note also that the location data do not have to be personal data.

**Comment [U6]:** The removal of this definition leaves "call" to be defined either by national legislation or by the courts when considering cases.

It future proofs the meaning of "call", in much the same way the Computer Misuse Act does not define the meaning of "computer". Misuse of a "computer" is something the court decides.

**Comment [U7]:** Note that the removal of the "call definition" has changed the paragraphs designation of later definitions (e.g. para g becomes para f).

**Comment [U8]:** Examples are text, email, voicemail etc. Note that when 'electronic mail' is not used in an Article, the implication is that the provisions inthe Article apply wider than "electronic mail".

**Comment [U9]:** I read this to mean that there has to be an actual loss of personal data. Suspicions of a loss of personal data might not trigger the provisions.

**Comment [U10]:** Note the words "otherwise processed ...in connection with" an electronic communications service is not a high threshold. Could easily related to the use of personal data from the service.





~~3. Cases where it would be technically impossible or require a disproportionate economic effort to fulfil the requirements of Articles 8, 10 and 11 shall be notified to the Commission by the Member States.~~

**NEW Article 3**

**Services concerned**

This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices.';

**Article 4**

(new title)'**Security of processing**';

1. ~~1.~~ The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

**New 1(a) added**

'1a. Without prejudice to Directive 95/46/EC, the measures referred to in paragraph 1 shall at least:

— ensure that personal data can be accessed only by authorised personnel for legally authorised purposes,

— protect personal data stored or transmitted against accidental or unlawful destruction, accidental lossor alteration, and unauthorised or unlawful storage, processing, access or disclosure, and

— ensure the implementation of a security policy with respect to the processing of personal data.

Relevant national authorities shall be able to audit the measures taken by providers of publicly available electronic communication services and to issue recommendations about best practices concerning the level of security which those measures should achieve.'

2. ~~2.~~ In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

**Comment [U11]:** Changes to Article 3 remove the exemptions that applied to calls using non-digital (e.g. "analogue" technology)

**Comment [U12]:** New title of Article 4; changed from mere "security"

**Comment [U13]:** "at least" allows Member States to add to the list of security items

**Comment [U14]:** These provisions in the next three bullets extend the detail of the interpretation of the 7th Data Protection Principle of the UK Act in relation to online electronic communications services delivered electronically.

These items should be added to any checklist used in connection with the 7th Principle.

**Comment [U15]:** Extension of mandatory audit to publicly available electronic communications services Remember the "otherwise processed in connection with...." extension in the definition. – this also could extend the ICO's power of audit.

Basically if the ICO can audit an electronic communications service he will be able to audit those details "connected with" that service.

This would, when implemented, extend the audit powers of the ICO beyond Government Departments to telcos etc.

Add new paragraphs 3-5

"3. In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority.

When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay.

Notification of a 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 that 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 it.

Without prejudice to the provider's obligation to notify subscribers and individuals concerned, if the provider has not already notified the subscriber or individual ofthe personal data breach, the competent national authority, having considered the likely adverse effects of the breach, may require it to do so.

The notification to the subscriber or individual shall at least describe the nature of the personal data breach and the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data breach. The notification to the competent national authority shall, in addition, describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach.

4. Subject to any technical implementing measures adopted under paragraph 5, the competent national authorities may adopt guidelines and, where necessary, issue instructions concerning the circumstances in which providers are required to notify personal data breaches, the format of such notification and the manner in which the notification is to be made. They shall also be able to audit whether providers have complied with their notification obligations under this paragraph, and shall impose appropriate sanctions in the event of a failure to do so.

Providers shall maintain an inventory of personal data breaches comprising the facts surrounding the breach, its effects and the remedial action taken which shall be sufficient to enable the competent national authorities to verify compliance with the provisions of paragraph 3.The inventory shall only include the information necessary for this purpose.

5. In order to ensure consistency in implementation of the measures referred to in paragraphs 2, 3 and 4, the Commission may, following consultation with the European Network and Information Security Agency(ENISA), the Working Party on the Protection of Individuals with regard to the Processing of Personal Data

**Comment [U16]:** Paras 1 and 2 untouched from the original

**Comment [U17]:** The use of "personal data ***or*** privacy" covers those individuals who might need to be informed when their privacy is at risk.

For example, suppose subscribers personal data have been lost. Contact might be needed with the users of the subscription if there is consequence for the privacy of the user (e.g. lost subscribers data is linked to a site giving AIDS or ABORTION advice. It might be the users associated with a subscriber that needs the data loss alert – not the subscriber).

However, I can see that care needs to be taken here. Do you alert the subscriber that a user has visited such sites?

**Comment [U18]:** As far as I can see the rules are very similar to that which currently apply at the moment, where data controllers tell the ICO of a breach.

These provision really kick in cases where the data controller decides not to report a breach when he should have done.

I would not take any risk here if there were to be a personal data loss in relation to a publicly available electronic communications service; if in doubt report the data loss.





established by Article 29 of Directive 95/46/EC and the European Data Protection Supervisor, adopt technical implementing measures concerning the circumstances, format and procedures applicable to the information and notification requirements referred to in this Article. When adopting such measures, the Commission shall involve all relevant stakeholders particularly in order to be informed of the best available technical and economic means of implementation of this Article.

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).';

**Article 5**

Confidentiality of the communications

1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

2. Paragraph 1 shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.

**New Article 5(3)**

~~3. Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.~~

'3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in

**Comment [U19]:** The effect of this change is that services AND networks need consent for cookies inserted into computers.

There appears to be an ambiguity here: consent is from the "subscriber or user concerned". Does this mean the consent of each user and each subscriber? It should do so – but I am not at all sure on this.

This is because the Article can be read as meaning that subscriber consent, once obtained, could cover any user. Also, it is also not clear whether the consent of the user could cover the subscriber or other users of the computer Recital 65 and 66 focuses on the plural "users" – so is not much of a help.

Use of "information" rather than personal data means that the information referred to in the provision does not have to be personal data

accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.';

**Article 6**

Traffic data

1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).

2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.

**New para 6(3)**

~~3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his/her consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.~~

'3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his or her prior consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time';

4. The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in paragraph 2 and, prior to obtaining consent, for the purposes mentioned in paragraph 3.

5. Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.

**Comment [U20]:** The change to "prior consent" removes any "post consent wheeze" that marketing people might try! I don't know what these wheezes are – but the provision kills them off.

Prior consent – where "consent" has the same meaning as in Directive 95/46/EC.

"User or subscriber" again: same ambiguity exists as mentioned in Article 5(3).

However, either user or subscriber can change their mind at any time; procedures for withdrawal of consent essential therefore.





6. Paragraphs 1, 2, 3 and 5 shall apply without prejudice to the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.

**Article 7**

Itemised billing

1. Subscribers shall have the right to receive non-itemised bills.

2. Member States shall apply national provisions in order to reconcile the rights of subscribers receiving itemised bills with the right to privacy of calling users and called subscribers, for example by ensuring that sufficient alternative privacy enhancing methods of communications or payments are available to such users and subscribers.

**Article 8**

Presentation and restriction of calling and connected line identification

1. Where presentation of calling line identification is offered, the service provider must offer the calling user the possibility, using a simple means and free of charge, of preventing the presentation of the calling line identification on a per-call basis. The calling subscriber must have this possibility on a per-line basis.

2. Where presentation of calling line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge for reasonable use of this function, of preventing the presentation of the calling line identification of incoming calls.

3. Where presentation of calling line identification is offered and where the calling line identification is presented prior to the call being established, the service provider must offer the called subscriber the possibility, using a simple means, of rejecting incoming calls where the presentation of the calling line identification has been prevented by the calling user or subscriber.

**Comment [U21]:** Remember the definition of "call" has been removed from Article 2. It is no longer a defined term.

This provision has the potential to be extended to any "call" – whatever a call is.

4. Where presentation of connected line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge, of preventing the presentation of the connected line identification to the calling user.

5. Paragraph 1 shall also apply with regard to calls to third countries originating in the Community. Paragraphs 2, 3 and 4 shall also apply to incoming calls originating in third countries.

6. Member States shall ensure that where presentation of calling and/or connected line identification is offered, the providers of publicly available

electronic communications services inform the public thereof and of the possibilities set out in paragraphs 1, 2, 3 and 4.

**Article 9**

Location data other than traffic data

1. Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.

2. Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

3. Processing of location data other than traffic data in accordance with paragraphs 1 and 2 must be restricted to persons acting under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service.

**Article 10:** Exceptions

Member States shall ensure that there are transparent procedures governing the way in which a provider of a public communications network and/or a publicly available electronic communications service may override:

(a) the elimination of the presentation of calling line identification, on a temporary basis, upon application of a subscriber requesting the tracing of malicious or nuisance calls. In this case, in accordance with national law, the data containing the identification of the calling subscriber will be stored and be made available by the provider of a public communications network and/or publicly available electronic communications service;

(b) the elimination of the presentation of calling line identification and the temporary denial or absence of consent of a subscriber or user for the processing of location data, on a per-line basis for organisations dealing with emergency calls and recognised as such by a Member State, including law

**Comment [U22]:**
Location data" means any data processed in an electronic communications network ***or by an electronic communications service***, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.

I do not know what "geographic position" means? Is it "in the UK" or "in London" or "in Covent Garden" or "postcode E5 6PT" or precise GPS co-ordinates?

The fact that the definition of location data could have said "precise geographic position", means that "geographic position" could be broader than precise co-ordinates?

Note that the less precise the "geographic position", the more impact that this provision could take, especially if electronic direct marketing activities are linked to the use of "location data".

For example, where the message associated with the behavioural marketing message has a geographic characteristic and it is targeted at users or subscribers whose geographic position can be ascertained from the location data.





enforcement agencies, ambulance services and fire brigades, for the purpose of responding to such calls.

**Article 11**

Automatic call forwarding

Member States shall ensure that any subscriber has the possibility, using a simple means and free of charge, of stopping automatic call forwarding by a third party to the subscriber's terminal.

**Comment [U23]:** Remember the definition of "call" has been removed from Article 2.

**Article 12**

Directories of subscribers

1. Member States shall ensure that subscribers are informed, free of charge and before they are included in the directory, about the purpose(s) of a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which their personal data can be included and of any further usage possibilities based on search functions embedded in electronic versions of the directory.

2. Member States shall ensure that subscribers are given the opportunity to determine whether their personal data are included in a public directory, and if so, which, to the extent that such data are relevant for the purpose of the directory as determined by the provider of the directory, and to verify, correct or withdraw such data. Not being included in a public subscriber directory, verifying, correcting or withdrawing personal data from it shall be free of charge.

3. Member States may require that for any purpose of a public directory other than the search of contact details of persons on the basis of their name and, where necessary, a minimum of other identifiers, additional consent be asked of the subscribers.

4. Paragraphs 1 and 2 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to their entry in public directories are sufficiently protected.

**New Article 13 totally**

~~Unsolicited communications~~

~~1. The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.~~

~~2. Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.~~

~~3. Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation.~~

~~4. 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 without a valid address to which the recipient may send a request that such communications cease, shall be prohibited.~~

~~5. Paragraphs 1 and 3 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected.~~

**Article 13: Unsolicited communications**

1. The use of automated calling and communication systems without human intervention automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may be allowed only in respect of subscribers or users who have given their prior consent.

2. Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner to such use of electronic contact details at the time of their collection and on the occasion of each message incase the customer has not initially refused such use.

**Comment [U24]:** In Article 13 there is a conspicuous absence of the use of "personal data" although obviously personal data are subject to these rules (eg. Email addresses are usually personal data – chris.pounder@amberhawk.com).

This means the provisions in A.13 apply in circumstances where "non-personal" data are processed. Behavioural marketing involves "not personal data", according to the behavioural marketers.

The Article uses "user or subscriber" in some provisions, so the ambiguity raised in connection with Article 5(3) also exists here.

Also, "electronic mail" is a defined term; so when it is **NOT** used, one can make the inference that the provision can apply to other forms of marketing that extends beyond "electronic mail".

The Article defines the minimal approach as applying to individual subscribers; **it does not stop Member States going beyond the minimum.**

Because of all these factors, I think these provisions ***could*** be applied by a Member State to behavioural advertising which does not use personal data but details such as IP addresses and "anonymous" details of the web-sites visited by a user or subscriber.

See Hawktalk Blog of 4/May/2010 for detailed argument.

**Comment [U25]:** A minimalistic implementation of this provision could maintain the status quo in the UK (e.g. the provision can be implemented by only applying these provisions to an "individual subscriber"– see para 3 & 5).

**Comment [U26]:** This provision maintains the "similar product" rule for electronic mail. Remember this rule is of diminishing effect because its intent was to ease the entry of the original 2002 Directive text into national law.





3. Member States shall take appropriate measures to ensure that unsolicited communications for the purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers or users concerned or in respect of subscribers or users who do not wish to receive these communications, the choice between these options to be determined by national legislation, taking into account that both options must be free of charge for the subscriber or user.

4. In any event, the practice of sending electronic mail for the purposes of direct marketing which disguise or conceal the identity of the sender on whose behalf the communication is made, which contravene Article 6 of Directive 2000/31/EC, which do not have a valid address to which the recipient may send a request that such communications cease or which encourage recipients to visit websites that contravene that Article shall be prohibited.

5. Paragraphs 1 and 3 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected.

6. Without prejudice to any administrative remedy for which provision may be made, inter alia, under Article 15a(2), Member States shall ensure that any natural or legal person adversely affected by infringements of national provisions adopted pursuant to this Article and therefore having a legitimate interest in the cessation or prohibition of such infringements, including an electronic communications service provider protecting its legitimate business interests, may bring legal proceedings in respect of such infringements. Member States may also lay down specific rules on penalties applicable to providers of electronic communications services which by their negligence contribute to infringements of national provisions adopted pursuant to this Article.';

**Article 14**

Technical features and standardisation

1. In implementing the provisions of this Directive, Member States shall ensure, subject to paragraphs 2 and 3, that no mandatory requirements for specific technical features are imposed on terminal or other electronic communication equipment which could impede the placing of equipment on

**Comment [U27]:** Please look at para 5 first and then come back to para 3.

Assume the definition of "Direct Marketing in the UK DP Act : "direct marketing" means the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals".

Behavioural ads are directed at the user – the choice of ad being dependent on user activity. I conclude this text has the flexibility for Member States to introduce legislation that applies to behavioural marketing ***if Member States want to enact it.***

**Comment [U28]:** Opt in or opt-out is left to Member States. One can expect no change to the current regime if the Member State opts to do the minimum.

In the UK, I expect the current confusion with respect of "unsolicited" calls to be tidied up (e.g. when an individual who has returned an unticked opt-out box about email marketing has neither solicited a email marketing communication nor is any email marketing communication unsolicited).

**Comment [U29]:** No secret marketing emails. texts or phone calls etc etc. Note: this provision is NOT excluded by para 5 – So it applies to electronic marketing sent to users (e.g. staff of organisations). A significant change.

**Comment [U30]:** Could be a big let out as the provisions in paras 1 and 3 **MUST** apply to subscribers who are also "individual subscribers" (i.e. data subjects) as a **MINIMUM POSITION**.

However, the Directive does not stop a Member State going beyond the **MINIMUM. Member States can go further.**

Member States also left to their own devices for other subscribers (e.g. corporate subscribers) So the UK could keep the status quo with respect to users of their organisation's email except for para 4 above **(if the UK does the minimum)**.

**Comment [U31]:** I expect the enhanced enforcement mechanism to apply to the new regulations (e.g. Monetary Penalty Notices).

Organisations who are concerned about the effect of junk mail could sue to protect their staff. ISPs could sue if their reputation is damaged by spammers. The use of "any natural or legal person" is very broad.

the market and the free circulation of such equipment in and between Member States.

2. Where provisions of this Directive can be implemented only by requiring specific technical features in electronic communications networks, Member States shall inform the Commission in accordance with the procedure provided for by Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services(9).

3. 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(10).

**New Article 14a**

'Article 14a

**Committee procedure**

1. The Commission shall be assisted by the Communications Committee established by Article 22 of Directive 2002/21/EC (Framework Directive).

2. Where reference is made to this paragraph, Article 5a(1) to (4) and Article 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.

3. Where reference is made to this paragraph,Article 5a(1), (2), (4) and (6) and Article 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.';

**Comment [U32]:** If anyone has a translation of the effect of these provisions in this Article, I will add it.

I really haven't got the time. I think it is an example of how opaque the Commission is – as one does not know what these Committees do unless you work with them!

These guys could have powers to change the Directive as far as I know. However, I think the word "assist" provides the clue. It usually means the Committee can be ignored.

The European Data Protection Supervisor (EDPS) regularly "assists" the Commission in its understanding of privacy concerns. In relation to Third Pillar, the advice the EDPS provides is often ignored (see Hawktalk blog of 14/04/2010).

**Article 15**

Application of certain provisions of Directive 95/46/EC

1. ~~1.~~ Member States may adopt legislative measures to 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 this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the





retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

**New paragraph 1b)**

'1b. Providers shall establish internal procedures for responding to requests for access to users' personal data based on national provisions adopted pursuant to paragraph 1. They shall provide the competent national authority, on demand, with information about those procedures, the number of requests received, the legal justification invoked and their response.

**Comment [U33]:** Worded so that Member States can keep the statistics of the detail of a request very opaque.

Note the use of the plural "users' personal data". A request from the authorities could be about 1,000 users or 1 user; both would still be counted as 1 request. This provision also maintains the weak regulatory structure in the UK with respect of national security.

Governments have a vested interest in the operation of the state security apparatus. Its "national provisions" could provide for a very weak regulatory system (which are outwith the Directive's responsibilities at the moment – Third Pillar is excluded)

The provision should have empowered the competent national authority (e.g. in the UK, Communications Commissioner or ICO) to dictate what records to keep and procedures to follow. This would allow the Regulator to be informed and to regulate.

See my "Nine Principles for controlling a surveillance society – Part II" on the Amberhawk web-site (www.amberhawk.com under Public policy)

2. The provisions of Chapter III on judicial remedies, liability and sanctions of Directive 95/46/EC shall apply with regard to national provisions adopted pursuant to this Directive and with regard to the individual rights derived from this Directive.

3. 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 shall also carry out the tasks laid down in Article 30 of that Directive with regard to matters covered by this Directive, namely the protection of fundamental rights and freedoms and of legitimate interests in the electronic communications sector.

**New Article 15(a)**

**Implementation and enforcement**

1. Member States shall lay down the rules on penalties, including criminal sanctions where appropriate, applicable to infringements of the national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for must be effective, proportionate and dissuasive and may be applied to cover the period of any breach, even where the breach has subsequently been rectified. The Member States shall notify those provisions to the Commission by 25 May 2011, and shall notify it without delay of any subsequent amendment affecting them.

**Comment [U34]:** Can be the custodial S.55 offence when (if) implemented in the UK.

**Comment [U35]:** Includes the Monetary Penalty Notice perhaps

**Comment [U36]:** Note the date of implementation – May next year

2. Without prejudice to any judicial remedy which might be available, Member States shall ensure that the competent national authority and, where relevant, other national bodies have the power to order the cessation of the infringements referred to in paragraph 1.

**Comment [U37]:** Reference to competent national authority means that this might not be the ICO.

The power to stop the processing would be new in a DPA context, especially if the cessation applied immediately.

3. Member States shall ensure that the competent national authority and, where relevant, other national bodies have the necessary investigative powers and resources, including the power to obtain any relevant information they might need to monitor and enforce national provisions adopted pursuant to this Directive.

**Comment [U38]:** Reference to suitable audit powers implied – but one needs to see what the UK Government deem "necessary".

4. The relevant national regulatory authorities may adopt measures 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 national regulatory authorities shall provide the Commission, in good time before adopting any such measures, with a summary of the grounds for action, the envisaged measures and the proposed course of action. The Commission may, having examined such information and consulted ENISA and 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, make comments or recommendations thereupon, in particular to ensure that the envisaged measures do not adversely affect the functioning of the internal market. National regulatory authorities shall take the utmost account of the Commission's comments or recommendations when deciding on the measures'.

**Article 16**

Transitional arrangements

1. Article 12 shall not apply to editions of directories already produced or placed on the market in printed or off-line electronic form before the national provisions adopted pursuant to this Directive enter into force.

2. Where the personal data of subscribers to fixed or mobile public voice telephony services have been included in a public subscriber directory in conformity with the provisions of Directive 95/46/EC and of Article 11 of Directive 97/66/EC before the national provisions adopted in pursuance of this Directive enter into force, the personal data of such subscribers may remain included in this public directory in its printed or electronic versions, including versions with reverse search functions, unless subscribers indicate otherwise, after having received complete information about purposes and options in accordance with Article 12 of this Directive.

**Article 17**

Transposition

1. Before 31 October 2003 Member States shall bring into force the provisions necessary to comply with this Directive. They shall forthwith inform the Commission thereof.

When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall communicate to the Commission the text of the provisions of national law which they adopt in the field governed by this Directive and of any subsequent amendments to those provisions.





**Article 18**

Review

The Commission shall submit to the European Parliament and the Council, not later than three years after the date referred to in Article 17(1), a report on the application of this Directive and its impact on economic operators and consumers, in particular as regards the provisions on unsolicited communications, 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. Where appropriate, the Commission shall submit proposals to amend this Directive, taking account of the results of that report, any changes in the sector and any other proposal it may deem necessary in order to improve the effectiveness of this Directive.

**Article 19:** Repeal

Directive 97/66/EC is hereby repealed with effect from the date referred to in Article 17(1).

References made to the repealed Directive shall be construed as being made to this Directive.

**Article 20:** Entry into force

This Directive shall enter into force on the day of its publication in the Official Journal of the European Communities.

**Article 21:** Addressees

This Directive is addressed to the Member States.

Done at Brussels, 12 July 2002.

For the European Parliament
The President
P. Cox

For the Council
The President
T. Pedersen

(1) OJ C 365 E, 19.12.2000, p. 223.

(2) OJ C 123, 25.4.2001, p. 53.

(3) Opinion of the European Parliament of 13 November 2001 (not yet published in the Official Journal), Council Common Position of 28 January 2002 (OJ C 113 E, 14.5.2002, p. 39) and Decision of the European Parliament of 30 May 2002 (not yet published in the Official Journal). Council Decision of 25 June 2002.

(4) OJ L 281, 23.11.1995, p. 31.

(5) OJ L 24, 30.1.1998, p. 1.

(6) OJ L 178, 17.7.2000, p. 1.

(7) OJ L 91, 7.4.1999, p. 10.

(8) OJ L 108, 24.4.2002, p. 33.

(9) OJ L 204, 21.7.1998, p. 37. Directive as amended by Directive 98/48/EC (OJ L 217, 5.8.1998, p. 18).

(10) OJ L 36, 7.2.1987, p. 31. Decision as last amended by the 1994 Act of Accession.

## Recitals in Directive 2009/136/EC that relate to the changes to Directive 2002/58/EC

(51) Directive 2002/58/EC (Directive on privacy and electronic communications) provides for the harmonisation of the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, in particular the right to privacy and the right to confidentiality, 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. 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 of 22 December 1986 on standardization in the field of information technology and telecommunications [OJ L 36, 7.2.1987, p. 31] (1), such measures should respect the principle of technology neutrality.

**Comment [U39]:** Preamble justifying the changes to Directive 2002/58/EC and linking in other relevant Directives etc

(52) Developments concerning the use of IP addresses should be followed closely, 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 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [OJ L 281, 23.11.1995, p. 31], and in the light of such proposals as may be appropriate.

**Comment [U40]:** As comment above

(53) The processing of traffic data to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by providers of security technologies and services when acting as data controllers is subject to Article 7(f) of Directive 95/46/EC. This could, for example, include preventing unauthorised

**Comment [U41]:** Links to Article 2(b) of Directive 2002/58/EC which is unchanged from the original





access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.

(54) The liberalisation of electronic communications networks and services markets and rapid technological development have combined to boost competition and economic growth and resulted in a rich diversity of end-user services accessible via public electronic communications networks. It is necessary to ensure that consumers and users are afforded the same level of protection of privacy and personal data, regardless of the technology used to deliver a particular service.

**Comment [U42]:** Recitals 54- 56 link to Harmonisation objectives of revised Article 1 and revised scope of the Directive 2002/58/EC in Article 3

(55) In line with the objectives of the regulatory framework for electronic communications networks and services and with the principles of proportionality and subsidiarity, and for the purposes of legal certainty and efficiency for European businesses and national regulatory authorities alike, Directive 2002/58/EC (Directive on privacy and electronic communications) focuses on public electronic communications networks and services, and does not apply to closed user groups and corporate networks.

**Comment [U43]:** See comment above

(56) Technological progress allows the development of new applications based on devices for data collection and identification, which could be contactless devices using radio frequencies. For example, Radio Frequency Identification Devices (RFIDs) use radio frequencies to capture data from uniquely identified tags which can then be transferred over existing communications networks. The wide use of such technologies can bring considerable economic and social benefit and thus make a powerful contribution to the internal market, if their use is acceptable to citizens. To achieve this aim, it is necessary to ensure that all fundamental rights of individuals, including the right to privacy and data protection, are safeguarded. When such devices are connected to publicly available electronic communications networks or make use of electronic communications services as a basic infrastructure, the relevant provisions of Directive 2002/58/EC (Directive on privacy and electronic communications), including those on security, traffic and location data and on confidentiality, should apply.

**Comment [U44]:** See comment above

(57) 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 Directive 95/46/EC, 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 monitoring and preventive, corrective and mitigating action should be regularly carried out.

**Comment [U45]:** Links to revised Article 4 dealing with security

(58) The competent national authorities should promote the interests of citizens by, inter alia, contributing to ensuring a high level of protection of personal data and privacy. To this end, competent national authorities should have the necessary means to perform their duties, including comprehensive and reliable data about security incidents that have led to the personal data of individuals being compromised. They should monitor measures taken and disseminate best practices among providers of publicly available electronic communications services. Providers should therefore maintain an inventory of personal data breaches to enable further analysis and evaluation by the competent national authorities.

**Comment [U46]:** Links to Revised Article 4 dealing with security

(59) Community law imposes duties on data controllers regarding the processing of personal data, including an obligation to implement appropriate technical and organisational protection measures against, for example, loss of data. The data breach notification requirements contained in Directive 2002/58/EC (Directive on privacy and electronic communications) provide a structure for notifying the competent authorities and individuals concerned when personal data has nevertheless been compromised. Those notification requirements are limited to security breaches which occur in the electronic communications sector. However, the notification of security breaches reflects the general interest of citizens in being informed of security failures which could result in their personal data being lost or otherwise compromised, as well as of available or advisable precautions that they could take in order to minimise the possible economic loss or social harm that could result from such failures. The interest of users in being notified is clearly not limited to the electronic communications sector, and therefore explicit, mandatory notification requirements applicable to all sectors should be introduced at Community level as a matter of priority. Pending a review to be carried out by the Commission of all relevant Community legislation in this field, the Commission, in consultation with the European Data Protection Supervisor, should take appropriate steps without delay to encourage the application throughout the Community of the principles embodied in the data breach notification rules contained in Directive 2002/58/EC (Directive on privacy and electronic communications), regardless of the sector, or the type, of data concerned.

(60) Competent national authorities should monitor measures taken and disseminate best practices among providers of publicly available electronic communications services.

(61) A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the subscriber or individual concerned. Therefore, as soon as the provider of publicly available electronic communications services becomes aware that such a breach has occurred, it should notify the breach to the competent national authority. The subscribers or individuals whose data and privacy could be adversely affected by the breach should be notified without delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the data or privacy of a subscriber or individual where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation in connection with the provision of publicly available communications services in the Community. The notification should include information about measures taken by the provider to address the breach, as well as recommendations for the subscriber or individual concerned.

(62) When implementing measures transposing Directive 2002/58/EC (Directive on privacy and electronic communications), the authorities and courts of the Member States should not only interpret their national law in a manner consistent with that Directive, but should also ensure that they do not rely on an interpretation of it which would conflict with fundamental rights or general principles of Community law, such as the principle of proportionality.

(63) Provision should be made for the adoption of technical implementing measures concerning the circumstances, format and procedures applicable to information and notification requirements in order to achieve an adequate level of privacy protection

**Comment [U47]:** Links to Revised Article 4 dealing with security

**Comment [U48]:** Links to Revised Article 4 dealing with security

**Comment [U49]:** Revised Article 4 dealing with security

**Comment [U50]:** Not sure which Article this is linked to – could be Article 1

**Comment [U51]:** Revised Article 4





and security of personal data transmitted or processed in connection with the use of electronic communications networks in the internal market.

(64) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of the breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law enforcement authorities in cases where early disclosure could unnecessarily hamper the investigation of the circumstances of a breach.

(65) Software that surreptitiously monitors the actions of the user or subverts the operation of the user's terminal equipment to the benefit of a third party (spyware) boses a serious threat to the privacy of users, as do viruses. A high and equal level of protection of the private sphere of users needs to be ensured, regardless of whether unwanted spying programmes or viruses are inadvertently downloaded via electronic communications networks or are delivered and installed in software distributed on other external data storage media, such as CDs, CD-ROMs or USB keys. Member States should encourage the provision of information to end-users about available precautions, and should encourage them to take the necessary steps to protect their terminal equipment against viruses and spyware.

(66) Third parties may wish to store information on the equipment of a user, or gain access to information already stored, for a number of purposes, ranging from the legitimate (such as certain types of cookies) to those involving unwarranted intrusion into the private sphere (such as spyware or viruses). It is therefore of paramount importance that users be provided with clear and comprehensive information when engaging in any activity which could result in such storage or gaining of access. The methods of providing information and offering the right to refuse should be as user-friendly as possible. Exceptions to the obligation to provide information and offer the right to refuse should be limited to those situations where the technical storage or access is strictly necessary for the legitimate purpose of enabling the use of a specific service explicitly requested by the subscriber or user. Where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user's consent to processing may be expressed by using the appropriate settings of a browser or other application. The enforcement of these requirements should be made more effective by way of enhanced powers granted to the relevant national authorities.

(67) Safeguards provided for subscribers against intrusion into their privacy by unsolicited communications for direct marketing purposes by means of electronic mail should also be applicable to SMS, MMS and other kinds of similar applications.

(68) Electronic communications service providers make substantial investments in order to combat unsolicited commercial communications (spam). They are also in a better position than end-users in that they possess the knowledge and resources necessary to detect and identify spammers. E-mail service providers and other service providers should therefore be able to initiate legal action against spammers, and thus defend the interests of their customers, as part of their own legitimate business interests.

**Comment [U52]:** Revised Article 4

**Comment [U53]:** Mixture of Articles 4 and 5

**Comment [U54]:** New Article 5(3) but does not use the word consent (as does the Article)

**Comment [U55]:** Mainly Article 13(1) – 13(3)

**Comment [U56]:** Mainly Article 13(6)

(69) The need to ensure an adequate level of protection of privacy and personal data transmitted and processed in connection with the use of electronic communications networks in the Community calls for effective implementation and enforcement powers in order to provide adequate incentives for compliance. Competent national authorities and, where appropriate, other relevant national bodies should have sufficient powers and resources to powers to obtain any relevant information they might need, to decide on complaints and to impose sanctions in cases of non-compliance.

(70) The implementation and enforcement of the provisions of this Directive often require cooperation between the national regulatory authorities of two or more Member States, for example in combating cross-border spam and spyware. In order to ensure smooth and rapid cooperation in such cases, procedures relating for example to the quantity and format of information exchanged between authorities, or deadlines to be complied with, should be defined by the relevant national authorities, subject to examination by the Commission. Such procedures will also allow the resulting obligations of market actors to be harmonised, contributing to the creation of a level playing field in the Community.

(71) Cross-border cooperation and enforcement should be reinforced in line with existing Community cross-border enforcement mechanisms, such as that laid down in Regulation (EC) No 2006/2004 (the Regulation on consumer protection cooperation)[OJ L 364, 9.12.2004, p. 1] by way of an amendment to that Regulation.

(72)The measures necessary for the implementation of Directives 2002/22/EC (Universal Service Directive) and 2002/58/EC (Directive on privacy and electronic communications) 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 [OJ L 184, 17.7.1999, p. 23].

(73) In particular, the Commission should be empowered to adopt implementing measures on effective access to '112' services, as well as to adapt the Annexes to technical progress or changes in market demand. It should also be empowered to adopt implementing measures concerning information and notification requirements and security of processing. Since those measures are of general scope and are designed to amend non-essential elements of Directives 2002/22/EC (Universal Service Directive) and 2002/58/EC (Directive on privacy and electronic communications) by supplementing them with new non-essential elements, they must be adopted in accordance with the regulatory procedure with scrutiny provided for in Article 5a of Decision 1999/468/EC. Given that the conduct of the regulatory procedure with scrutiny within the normal time limits could, in certain exceptional situations, impede the timely adoption of implementing measures, the European Parliament, the Council and the Commission should act speedily in order to ensure the timely adoption of those measures.

(74) When adopting implementing measures on security of processing, the Commission should consult all relevant European authorities and organisations (the European Network and Information Security Agency (ENISA), the European Data Protection Supervisor and 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), as well as all other relevant stakeholders, particularly in order to be informed of the best available technical and economic means of improving the

**Comment [U57]:** All the rest appear to be Article 15(a), changes to Article 15 and Article 14(a) which deals with harmonisation of the level of protection and co-operation re enforcement

I apologise for no further commentary but I don't understand the finer points of EU Commitology.





implementation of Directive 2002/58/EC (Directive on privacy and electronic communications).

(75) Directives 2002/22/EC (Universal Service Directive) and 2002/58/EC (Directive on privacy and electronic communications) should therefore be amended accordingly.

(76) In accordance with point 34 of the Interinstitutional Agreement on better law-making [OJ C 321, 31.12.2003, p. 1], Member States are encouraged to draw up, for themselves and in the interests of the Community, their own tables illustrating, as far as possible, the correlation between Directives 2002/22/EC (Universal Service Directive) and 2002/58/EC (Directive on privacy and electronic communications) and the transposition measures, and to make them public.

# *APPENDIX: ADVERTS*