

CONSULTATION DOCUMENT

**IMPLEMENTATION OF THE DIRECTIVE ON PRIVACY
AND ELECTRONIC COMMUNICATIONS**

Department of Trade and Industry

March 2003

Contents

Introduction	Page 3
Summary of questions	Page 5
Chapter one: background, current rules and impact of new Directive	Page 7
Draft Regulations	
Chapter two: scope, aim and definitions	Page 18
Chapter three: security and confidentiality, cookies and other tracking devices	Page 21
Chapter four: network and service providers' requirements: traffic data, itemised billing, calling line identification, location data services, call tracing and forwarding	Page 27
Chapter five: subscriber directories	Page 31
Chapter six: unsolicited commercial communications: automated calling systems, fax, phone, e-mail and SMS	Page 36
Chapter seven: enforcement and sanctions, technical standards, and exemptions for national security and law enforcement purposes	Page 43
Annex 1	Directive on Privacy and Electronic Communications 2002/58/EC
Annex 2	Draft SI: The Privacy and Electronic Communications (EC Directive) Regulations 2003
Annex 3	ICO Guidance
Annex 4	Partial Regulatory Impact Assessment
Annex 5	Consultation Criteria

Introduction

The Directive on privacy and electronic communications (Directive 2002/58/EC) (the “Privacy Directive”) is part of the new European regulatory framework for electronic communications networks and services. The Privacy Directive updates the current Telecoms Data Protection Directive (Directive 97/66/EC) in the light of new technologies and ensures that the privacy rules which apply to phone and fax services also apply to e-mail and use of the internet. It aims to protect the confidentiality of communications, sets conditions on the use of traffic, location and subscriber data, and subscriber directories, and regulates the use of communications networks for unsolicited direct marketing by phone, fax, e-mail and SMS.

There are new provisions in the Directive on:

- **value added services based on traffic and location data**
- **unsolicited commercial e-mail and SMS**
- **cookies and similar internet tracking devices, and**
- **subscriber directories**

This Directive is of interest to phone/internet users, communications network and service providers, website and online content businesses, subscriber directory providers and anyone who direct markets by phone, fax, SMS or e-mail.

The purpose of this consultation is to seek your views on how the UK should implement the new rules in the Directive and whether there are any other changes we should make to the existing rules in this area. In particular, you are invited to comment on the draft Privacy Regulations at Annex 2. You are also invited to comment on the costs and benefits of the options identified in the draft regulatory impact assessment at Annex 4. This paper asks a number of questions (summarised on pages 5 and 6) and your comments on these and any other issues raised by the implementation are welcome.

How to submit your comments

Responses should be sent in by 19 June 2003 to:

Mrs Buki Edoja
Department of Trade and Industry
Bay 202
151 Buckingham Palace Road
London SW1W 9SS
Tel: 020 7215 5000

Or by e-mail to:

cdpd@dti.gsi.gov.uk

Further copies of this consultation paper are available from:

DTI Publications Orderline
ADMAIL 528
London
SW1W 8YT

Tel: 0870 1502 500

Fax: 0870 1502 333

E-mail: publications@dti.gsi.gov.uk

Order online: <http://www.dti.gov.uk/publications/>

The reference number to quote on orders is URN 03/762.

Publication of responses

We plan to publish the responses we receive except where respondents prefer to remain private. Please indicate on your response if you would like it to be treated as confidential.

Consultation guidelines

The DTI follows Government guidelines on consultations. Details of the guidelines are set out in Annex 5. If you have any comments or complaints about the consultation process or timetable you should contact the DTI's consultation coordinator:

Mr Philip Martin
Department of Trade and Industry
1 Victoria Street
London

Next steps

The final version of the Regulations is expected to be laid in Parliament in August this year, and brought into force on 31 October 2003.

Summary of questions

General issues:

How should we implement the Privacy Directive in those areas where the rules have changed or new requirements have been introduced, on the use of cookies and similar tracking devices, on value added services based on traffic and location data, on subscriber directories, and on unsolicited commercial e-mail and SMS?

Are there any aspects of the current regime which we should change (for example, on telephone and fax selling)?

Do the draft Privacy Regulations deliver the intended results?

How should the existing guidance in this area be updated? What guidance should be provided on the new rules?

Draft Privacy Regulations

Chapter two – definitions

Should the draft Privacy Regulations redefine the split between corporate and individual subscribers?

Chapter three – security, confidentiality and cookies

What information should operators provide about cookies and similar devices, and how should internet users be given the opportunity to refuse them?

Should the Privacy Regulations apply to all cookies and similar devices, or should they only apply to cookies where they involve processing of personal data?

Should the Privacy Regulations specify whether a user should have the right to override a subscriber's consent to a cookie?

Chapter four – network and service providers' requirements

How should service providers gain consent to processing of traffic and location data and what information should they provide?

Should service providers be under a stronger requirement to provide the full range of CLI services, as proposed?

Chapter five – subscriber directories

Should subscribers be allowed to opt for inclusion in a subscriber directory as the default option, as proposed, or should active choice be required?

What entry options should be available to subscribers and should service providers be able to determine the core list, as proposed?

Are the draft Privacy Regulations right to specify that additional consent is needed for inclusion in any directory with a reverse search function?

Should corporate subscribers be entitled to some or all of the new rights accorded to individual subscribers?

Chapter six – unsolicited commercial communications

How should “customer relationship” and “similar products” be interpreted for the purposes of unsolicited e-mail and SMS marketing and do you agree with the approach adopted in the draft Privacy Regulations?

Should individual phone subscribers be given opt-in or prior consent rights in relation to phone marketing?

Should corporate subscribers be given the right to register on the Telephone Preference Service, as proposed? Should corporate subscribers have stronger rights in relation to fax, e-mail and SMS marketing?

Is the new definition of automated calling system right?

Chapter seven – enforcement and sanctions, technical standards and exemptions for national security and law enforcement purposes

Should network and service providers be required to disclose the source of unsolicited commercial communications?

Should new enforcement sanctions be available against breaches of the rules on unsolicited commercial communications? If so, what should they be?

Chapter one: background, current rules and impact of the new Directive

The Privacy Directive, known during negotiations as the Communications Data Protection Directive, is one of the measures that arose from the European Commission's 1999 review of the regulatory regime for electronic communications. The other key elements include the Framework, Access, Authorisation and Universal Service Directives, which will be implemented via the Communications Bill once that is enacted. Further information about the Communications Bill is available on:

<http://www.communicationsbill.gov.uk/>

The Privacy Directive, like most of the other measures in the new framework, was subject to co-decision procedures and was therefore subject to agreement both by Member States and by the European Parliament. Negotiations on the draft Directive started in spring 2001 and the Directive was finally adopted, following amendments, in July 2002. Information about the different stages of negotiation and how the Directive changed is available on the European Commission's website at:

http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/index_en.htm#dp

Other relevant European legislation includes:

- the Data Protection Directive (95/46/EC) which sets cross-sectoral rules on the processing of personal data
- the E-Commerce Directive (2000/31/EC) which applies to online service providers and intermediaries

The Privacy Directive updates the existing Telecoms Data Protection Directive or TDPD (Directive 97/66/EC) in the light of new technologies and ensures that the rules which apply to phone and fax services also apply to e-mail and use of the internet. The new Directive requires the confidentiality of communications to be protected, enables the provision of value added services with the consent of subscribers, and regulates the use of phone, fax, e-mail and mobile text messages for unsolicited direct marketing. The aim is to ensure that people can be confident that their privacy will be respected when they use electronic networks and services of all kinds, and that network and service providers are given a clear framework in which to operate.

What does the existing Telecoms Data Protection Directive cover and how was it implemented in the UK?

The TDPD was agreed and adopted in 1997. It requires EU Member States including the UK to ensure that their national legislation:

- provides for the security of networks and the confidentiality of communications and ensures that any interception or surveillance for national security, law

enforcement, or essential business purposes is properly regulated

- requires network operators to erase or anonymise traffic data as soon as it is no longer needed for billing and traffic management purposes, and enables them to use it for their own marketing purposes only with the consent of the subscriber. This applies, for instance, to records of what phone/fax messages have been made, their origin, destination and length
- gives subscribers the right to have non-itemised bills if they prefer and takes account of the need for scope to allow other privacy preferences
- requires a range of calling and connected line identification (CLI) services to be provided by operators, including the ability to withhold identification on outgoing calls both per-line and on a call-by-call basis, and the ability to bar incoming calls where the identity of the caller has been withheld
- sets out clearly when the withholding of CLI may be overridden (e.g. to trace the source of malicious or nuisance calls, or calls to the emergency services)
- gives individual subscribers the right to be ex-directory or to have a partial entry, or to specify that their entry may not be used for direct marketing purposes
- requires prior consent for unsolicited direct marketing by fax and by automated calling systems without human intervention, and requires either prior consent or the right to opt-out of other forms of unsolicited direct marketing (e.g. by phone), the choice to be decided by Member States

The TDPD was brought into force here in stages in 1999 and 2000. Most of the Directive was implemented via the Telecommunications (Data Protection and Privacy) Regulations 1999 (the TDPP Regulations). The provisions on confidentiality were implemented under the Regulation of Investigatory Powers Act 2000.

Further information about the TDPD and the TDPP Regulations is available on the website below:

http://www.dti.gov.uk/cii/regulatory/telecomms/telecommsregulations/ec_telecomms_data_protection.shtml

The Telephone Preference Service

Of all these provisions, it is the rules on unsolicited phone and fax marketing which have had most impact and generated the most interest. The TDPD allows Member States a degree of flexibility about the rights of individual and corporate users in relation to unsolicited commercial communications. The TDPP Regulations give individual phone subscribers the right to opt-out of unsolicited direct marketing phone calls either from particular sources or on a global basis by registering with an opt-out scheme, the Telephone Preference Service (TPS), run under supervision from Ofcom by the Direct Marketing Association (DMA). The TDPP Regulations also stipulate that

direct marketing callers must give their name, and, on request, a freephone number or postal address by which they can be contacted.

Corporate subscribers (e.g. limited companies and, in Scotland, partnerships) do not currently have the right to register on the TPS. They do have some rights to opt out on a case by case basis by instructing individual callers not to make further direct marketing calls, under the terms of the Telecommunications Act 1984 licensing regime.

Fax Preference Service

The TDPP Regulations give individual subscribers prior consent rights in relation to unsolicited direct marketing faxes (i.e. the sender must get the addressee's consent before sending a direct marketing fax to them); this is in accordance with the harmonised opt-in requirement in the Directive. Because of the cost of unwanted faxes to the addressee, the TDPP Regulations give opt-out rights to corporate subscribers, both on a case by case basis and through registration with the Fax Preference Service (FPS), an opt-out scheme run, like the TPS, by the DMA under supervision by Ofcom. This register is open to individual subscribers who want to reinforce their opt-in rights; no-one may therefore send an unsolicited direct marketing fax to any subscriber, corporate or individual, who is registered with the FPS or who has previously instructed the direct marketer not to fax them. As with phone calls, anyone direct marketing by fax must identify themselves and provide either a freephone number or a postal address at which they can be contacted.

Enforcement and sanctions

The enforcement authority for the TDPP Regulations is the Information Commissioner (previously called the Data Protection Commissioner). The Information Commissioner's Office (ICO) has powers to investigate and issue enforcement notices to individuals or companies which breach the TDPP Regulations. Breach of an enforcement notice is a criminal offence liable to a fine of up to £5,000 if handled in a magistrates court, or an unlimited fine if the trial is in front of a jury. In addition, anyone who has suffered damages because the TDPP Regulations have been breached has the right to sue the person responsible for compensation.

Ofcom has responsibility under the TDPP Regulations for overseeing the running of the TPS and FPS. This involves putting the schemes out to tender every five years and supervising the performance of the scheme managers.

How effectively is the current regime working?

Registration levels: the DMA, which runs the TPS and FPS, reports that since the introduction of statutory controls in 1999, registration on the TPS has risen from 297,746 (the number registered in May 1999 on what was then a voluntary scheme) to 2,632,435 as of 20 February 2003. Over the same period, registration on the FPS has risen from 18,577 to 1,276,546.

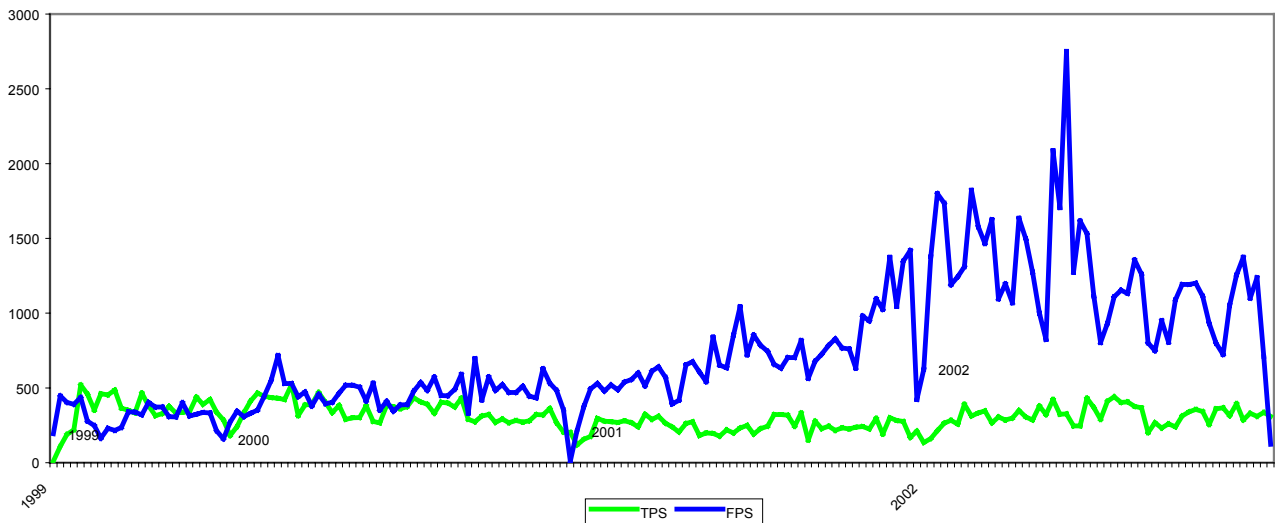
Compliance with the regime: the DMA sends a report to the ICO every two months on their complaint handling activities. Based on analysis of a typical TPS report, 88% of companies complained against receive between 1-5 complaints. Fewer than 1% of companies complained against received over 50 complaints. The profile for FPS is different in that a handful of companies are responsible for the majority of the complaints. Whilst 83% of companies receive between 1-5 complaints, fewer than 1%

of companies are responsible for 52% of complaints received (in one typical period, seven companies received over 500 complaints each).

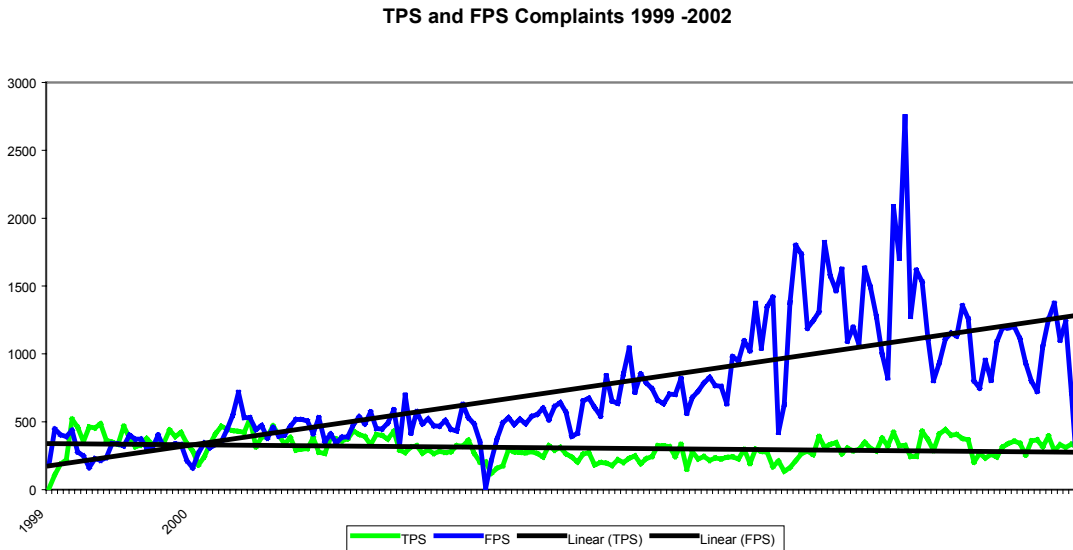
Number of Complaints Received

	TPS	FPS
1999 (from May)	9,000	8,000
2000 (Jan- December)	18,000	23,500
2001	12,000	36,500
2002	16,000	64,000
Total	55,000	132,000

TPS and FPS Complaints 1999 -2002



TPS and FPS Complaint Trendline 1999 -2002



Use by Telephone and Fax Marketers

Companies have a number of options of checking the registers. They can either choose to take the full file or choose selections by telephone code area. They can take the file on an annual or ad hoc basis. There are currently 300 companies taking the TPS file and 71 taking the FPS file on an annual basis. A total of 217 companies take the files on an ad hoc basis.

The TPS also offers three checking services for smaller companies. These include an internet interrogation service where for a minimum of £50 a month they can check up to 500 numbers, extra numbers cost 10p per look up; a call barring service whereby a company can arrange that their sales calls go through a filter system whereby calls to TPS numbers are stopped, and a premium rate number checking service. The call barring service and the premium rate service are both charged at a comparable rate to the internet interrogation service.

TPS and FPS subscribers offer their own list screening services for third parties; a variety of services are available from 33 TPS subscribers and 12 FPS subscribers. The services range from call barring services offered by telecommunications companies to list enhancement and screening services. TPS collects a royalty fee from subscribers offering third party screening.

Business/subscriber awareness

The DMA is responsible for an ongoing PR campaign aimed at centres of information for businesses and the trade and business press.

The following tables shows the most quoted sources of information for TPS and FPS.

Most Often Quoted Sources of Information for TPS	Percent
--	---------

Word of Mouth	16%
DMA	13%
TPS	10%
Press	7%
Colleague	7%
Oftel	4%
BT	4%
OIC	3%
Website	3%
Directory Enquiries	2%
Admar	2%
Chamber of Commerce	2%
DTI	2%
Business Link	1%
Others	24%

In all 51 sources of information were quoted by at least 10 companies.

Most Often Quoted Sources of Information for FPS	Percent
Word of Mouth	20%
Colleague	9%
DMA	9%
FPS	7%
TPS	6%
Website	4%
BT	4%
Oftel	4%
Chamber of Commerce	3%
Customer Contact	3%
Press	3%
Admar	2%
ICO	2%
Directory Enquiries	2%
FPS Letter of Complaint	2%
Others	20%

In all 40 sources of information were quoted by at least 5 companies.

Promotion to the Consumer

Promotional activity has been PR led. There is continual coverage in national and local press and radio. TPS is a media contact for queries on telephone marketing and good practice; both FPS and TPS have been recently featured by BBC Watchdog.

Annual mailings distribute leaflets to consumer points of contact such as libraries and Citizens Advice Bureaux.

The TPS and FPS websites are linked to many other consumer related sites. The DMA site includes information pages on the services as well as banner advertising. Currently 11% of TPS registrations are through the web and 25% of fax registrations.

The TPS benefits from the DMA's PR. It was featured in the DMA's consumer campaign entitled It's Your Choice. Reference to the TPS is included in all press releases concerning the other preference services.

Consumer Awareness

Research on consumer awareness of the TPS has been carried out annually by MORI, and each year has seen an increase in awareness. In 2002 29% of consumers had heard of TPS, in 2000, the first year the research was carried out, it was 22%. In the latest research carried out in the summer of 2002 consumers mentioned that they have heard about TPS from the following sources:

How Consumers Heard of TPS	Percent
From a friend, colleague or relative	28%
BT	16%
Newspaper	14%
Television	9%
Through work	6%
Radio	5%
Magazine	3%
Library	1%
Trading Standards Office	1%
Phone Book	1%
Internet	1%
Don't know, can't remember	15%
Total	100%

Information Commissioner: enforcement action

The table below gives a breakdown of complaints received by the ICO about breaches of the TDPP Regulations and enforcement notices issued.

Complaints received under Telecommunications (Data Protection and Privacy) Regulations 1999 since 1 April 2000

Reporting period	Total	Fax		Phone (inc SMS)		CLI	
		No.	% of Total	No.	% of Total	No.	% of Total
1 April 2000 to 31 March 2001	8835	1631	18%	153	2%	2	N/A
1 April 2001 to 31 March 2002	12210	2435	20%	170	1%	9	N/A
1 April 2002 – 27 Feb 2003	10910	1339	12%	210	2%	3	N/A

The percentage of total columns show the percentage of complaints about breaches of the TDPP Regulations in relation to total complaints to the ICO.

Information Notices – None, although two Preliminary Information Notices likely to be issued shortly.

Enforcement Notices

Reporting period	No. of Notices	Caller(s)
1 April 2000 to 31 March 2001	1	Second Telecom/Top 20 – appealed. (Amended notice then issued which was not appealed)
1 April 2001 to 31 March 2002	2	Planet Telecom/192 Enquiries (plus directors) - not appealed Insiders – appealed. (Amended notice then issued which was not appealed)
1 April 2002 – 27 Feb 2003	2	21 Century Faxes, Info 4 U, Right 2 Vote, Green Freephone Pages, Hyperos Systems, Lord’s Witnesses (plus director) – appealed (Appeal ongoing) Petworth Publishing (plus director) - not appealed

Fines issued - None

Problem areas

Complaints to the DTI, ICO, Oftel and the Preference Services have thrown up a number of issues over the past few years. Use of power diallers and similar systems for direct marketing or other purposes can generate silent or failed calls where insufficient call centre staff are available to handle the calls; the DMA believes that the growth in use of such systems has accounted for many new TPS registrations and last year introduced its own guidelines for members, which require power dialler users, among other things, to ensure that the number of failed calls is limited and that system users always provide a relevant calling line identification number (CLI), so that subscribers can find out who rang them and why.

The Communications Bill includes a new offence of persistent misuse of a communications system, which will enable the Office of Communications (Ofcom) to

take action against people whose careless or reckless use of the communications system causes serious inconvenience to other users. This will apply to situations where the problem is caused by misuse of power dialling equipment.

Calls from overseas marketers have started to generate complaints; the Directive does not apply outside the EU (although the TDPP Regulations do allow action to be taken against the business which commissions a direct marketing campaign, if based here, even if they use a non-EU call centre).

Subscribers sometimes complain that operators are unwilling to disclose the source of problem calls where these are made for direct marketing purposes, rather than being more serious nuisance or malicious calls.

The premium rate sector has grown significantly since 1999; some premium rate service providers have generated complaints that they are breaching both the rules on unsolicited commercial communications and the code of practice administered by the premium rate services regulator, ICSTIS (particularly when these services are marketed by unsolicited faxes and SMS or text messages to mobiles). Further information about ICSTIS, and the sanctions they apply for breaches of the code is available from the following website:

<http://www.icstis.org.uk>

The ICO takes the view that SMS should be regarded as phone calls for the purposes of the TDPP Regulations, although they are not explicitly covered by the TDPD (this is one of the grey areas that the Privacy Directive will clarify).

Conclusions

Working experience of the rules on unsolicited phone and fax marketing has been mixed. On the positive side, both the evidence that we get from complaints to the DTI, Information Commissioner and Ofcom, and analysis of DMA registration and complaint levels indicate that the TPS can be very effective in blocking unsolicited direct marketing calls to subscribers who do not want to receive them. For businesses advertising their own products or services or direct marketers advertising on behalf of others, the TPS is easy and cheap to use and, arguably, saves businesses the cost of approaching subscribers who do not want to receive such calls and will not respond to them.

The take-up of more than two and a half million subscribers on the TPS shows that a significant number of individuals do object to unsolicited phone calls and are prepared to opt-out if given the choice. Despite the large increase in the number of TPS registrations since the scheme was put on a statutory basis, however, the number of complaints from subscribers with numbers registered has held relatively stable, indicating that registration does have a significant impact. This accords with the ICO and Ofcom experience: they found a steep rise in complaints about unsolicited phone calls when the new rules were introduced, followed by a significant drop as the new rules bedded down.

There is however a significant difference between phone and fax marketing. Registration of the FPS stand at around 60 per cent of TPS levels, despite the fact that

phone use is higher; this may indicate greater relative resistance to unsolicited fax marketing as a medium. There have been far more complaints about breaches of the FPS, and a much higher proportion of complaints generated by the same marketers, suggesting less willingness to comply with the rules.

There may be a technical explanation for some of the complaints received about unwanted faxes – there is reason to believe that many faxes that come through on FPS registered numbers have been diverted from another number by the subscribers' own equipment, where this re-routes incoming communications automatically. However, regulatory experience suggests that the most significant underlying factor is the relative cost of phone and fax marketing. Faxes are quick and cheap to send, without the cost of a human element in making a one-to-one direct marketing call, and the response rate required to validate a fax marketing campaign is lower than it would be for a comparable phone campaign. There is a corresponding danger that campaigns may be badly planned and researched or the marketer may take a conscious decision to risk breaking the rules. The implication is that the cheaper the communications medium, the less effective the relevant statutory or self-regulatory control. In this scenario, technical and network-based solutions become all the more important. In the case of phone and fax marketing, these include automatic barring facilities on incoming and outgoing calls and faxes.

What is new about the Directive on privacy and electronic communications?

The Directive carries over much of the existing regime. There are some important changes, however. The Privacy Directive now talks throughout about electronic communications networks and services rather than traditional telecommunications and voice telephony services. It clears up some grey areas which had emerged under the existing Directive, for instance, about the regulation of unsolicited direct marketing SMS.

- The Directive now allows the provision of **value added services** based on traffic or location data, by network or service providers on their own or in conjunction with third parties. There is no restriction on the type of services that may be provided as long as subscribers give their consent and are informed of the data processing implications. This will provide a much clearer legal framework for the provision of value added services such as location based advertising to mobiles.
- **Unsolicited commercial e-mail (UCE)** will be subject to a prior consent requirement, so that UCE may not be sent without the prior consent of the addressee, except in the context of an existing customer relationship, where companies may continue to e-mail on an “opt-out” basis.
- **Cookies** and similar software tracking devices used to access and store data on internet linked computer terminals will be subject to a new transparency requirement – anyone who uses them on a website or as part of another online service must normally provide information and a chance to refuse to subscribers or users who are not content to accept them.
- Subscribers will have a stronger right to decide whether they want to be listed in **subscriber directories** or not, and they must be given clear information about

the directories in question, including any reverse search-type functions which allow directory users to identify names/addresses by searching against numbers rather than the other way round.

Other changes

On **data retention**, the Directive now explicitly allows the retention of traffic data (e.g. records of the length, origin and destination of phone calls) for national security and law enforcement purposes, once it is no longer required for billing or other essential management purposes, provided that any measures taken by Member States (such as the data retention provisions in the Anti-Terrorism, Crime and Security Act 2001) are proportionate and necessary.

How and when will the new rules be brought into force?

The transposition deadline for the Directive is **31 October 2003** and implementation in the UK will be by means of secondary legislation under the European Communities Act 1972 (effectively, an update of the existing TDPP Regulations). In order to finalise the new Privacy Regulations and guidance in time to meet this deadline, we are seeking comments by **19 June**. We plan to lay the Regulations in Parliament in August this year, to come into force on 31 October.

Main issues

The key issues raised in this consultation are:

How should we implement the Privacy Directive in those areas where the rules have changed or new requirements have been introduced, on the use of cookies and similar tracking devices, on value added services based on traffic and location data, on subscriber directories, and on unsolicited commercial e-mail and SMS?

Are there any aspects of the current regime which we should change (for example, on telephone and fax selling)?

Do the draft Privacy Regulations deliver the intended results?

How should the existing guidance in this area be updated? What guidance should be provided on the new rules?

Chapter two: scope, aim and definitions

The requirements in the Directive

- Articles 1, 2 and 3
- Recitals 1 to 19

Article 1 sets out the scope and aim of the Privacy Directive – to ensure that all EU Member States apply an equivalent level of privacy protection with respect to the processing of personal data in the electronic communication sector, and to ensure that those safeguards do not obstruct the free movement of data or equipment, or the provision of services within the Community. This Article makes a link to the Data Protection Directive (Directive 95/46/EC), which this Directive is intended to complement.

Article 2 sets out how the terms used in the Directive should be interpreted. Article 3 sets out what the Directive applies to: the processing of personal data in connection with the provision of publicly available electronic communications services. It also specifies that the provisions on calling and connected line identification (CLI) and call forwarding in later Articles of the Directive should apply to analogue as well as digital systems, except where this would be technically impossible or require a disproportionate economic effort. The Recitals set out further information on the rationale for the Directive, how it relates to other legislation, and how it should be applied; numbers 1 – 19 in particular apply to the aims, scope and definitions used in the Directive.

Much of the content of the Privacy Directive is carried over from the existing Telecoms Data Protection and Privacy Directive or TDPD (Directive 97/66/EC). The Privacy Directive is, however, now worded in terms of electronic communications rather than telecommunications, to ensure that it applies to e-mail and use of the internet as well as traditional phone networks. There are new definitions of traffic and location data, the kind of communication covered by the Directive (which excludes point to multipoint broadcasting but is meant to include point to point services like video on demand), value added services and e-mail, where the definition in the Directive is worded to include SMS.

Approach to the Privacy Regulations

- Regulation 2

Unlike EU legislation like the Privacy Directive, UK legislation does not incorporate a statement of the aim of the measure, although we must ensure that this is reflected in the detailed provisions. The draft Privacy Regulations set out the definitions used in Regulation 2. These largely reflect the wording used in the existing Telecommunications (Data Protection and Privacy) Regulations (the TDPP Regulations); where there are new definitions in the Directive we have followed the wording used in Article 2 and the relevant recitals, where these expand on the interpretation. The wording used in the draft Privacy Regulations also reflects the

approach used in the Communications Bill (currently going through Parliament and expected to be enacted later this year).

Issues

Definition of corporate and individual subscriber: the Directive relies on the definition of subscriber used in the Framework Directive 2002/21/EC (“any natural person or legal entity who or which is party to a contract with the provider of publicly available electronic communications services for the supply of such services”). The Privacy Directive also makes a distinction between subscribers who are natural and legal persons (e.g. individuals and corporate subscribers). This distinction is important because the Directive requires Member States to apply the rights set out in Article 12 on subscriber directories, and the rights set out in Article 13 on unsolicited commercial communications, to natural persons, but leaves it to Member States to decide how to protect the legitimate interests of subscribers who are legal persons. The rationale for this is that business/corporate subscribers do not always need the same level of protection as individuals, and safeguards justified for business-to-individual transactions could be unnecessarily burdensome to business-to-business dealings.

The split between natural and legal persons in the UK does not always follow a neat corporate/residential subscriber divide, however. Under English, Welsh and NI law, both sole traders and partnerships other than limited liability partnerships fall into the definition of natural rather than legal persons. Under Scottish law sole traders but not partnerships count as individual persons. This means that some businesses (in some cases quite large businesses) automatically benefit from the safeguards attached to individuals.

Two possible solutions to this issue have been identified, although there are problems with both of them. Firstly, we could apply the rules to individual subscribers in a way which excludes them when they are acting in their business capacity (e.g. along the lines of the E-Commerce Directive, which excludes individuals from the consumer definition when they are acting in a trade, business or professional capacity). The problem is that the Privacy Directive does not make this distinction, so for the UK to do so in its implementing regulations would lessen the protections accorded to individuals under the Directive. It would also create scope for abuse (e.g. an unscrupulous direct marketer could routinely ring individuals despite their TPS registration or e-mail them without their prior consent, by claiming that they were approaching them in their business capacity). This distinction works in the context of the E-Commerce Directive because it enables individuals in their business capacity to opt out of some of the information requirements imposed on business to consumer transactions, if they want to (the detailed requirements relating to online contracts may be waived in business to business cases if both parties agree). It is much harder to see this kind of distinction working in the context of the Privacy Directive.

The second way would be to tailor the definition of corporate subscribers for the purposes of the Privacy Regulations; in particular, to include partnerships in the corporate subscriber definition. Although this would create a more logical division it would not be easy to achieve, and the benefits in terms of the end results for the purposes of these Regulations may be fairly marginal.

The draft Privacy Regulations maintain the current split between corporate and individual subscribers but consultees are invited to comment on this.

Questions for consultees

Should the draft Privacy Regulations redefine the split between corporate and individual subscribers?

Chapter three: security and confidentiality, cookies and other tracking devices

The requirements in the Directive

- Articles 4 and 5
- Recitals 20 - 26

Article 4 of the Directive requires network and service providers to work together to safeguard network security. Service providers are required to inform subscribers of any particular security risk and, in the case of a risk that they cannot reasonably exclude themselves, to inform subscribers of other possible remedies and the likely costs. The wording of Article 4 is not significantly different from current requirements, although Recital 20 now includes a reference to the issue of charging for information about security risks: it says that this should be free of charge except for any nominal costs which the subscriber may incur while receiving or collecting the information, for instance, by downloading an e-mail.

Article 5 is split into three parts. Parts one and two require Member States to guarantee the confidentiality of communications and the related traffic data (defined as “any data processed for the purpose of the conveyance of a communication ... or for the billing thereof”). They prohibit interception and surveillance except where authorised for national security, law enforcement and related purposes, or to record evidence of commercial transactions or other business transactions where this is necessary and authorised under national law. These requirements are largely the same as under the Telecoms Data Protection Directive (the TDPD), although the existing provision applies to communications only without reference to the related traffic data; in relation to monitoring for business purposes, recital 23 now says that “parties to the communications should be informed prior to the recording about the recording, its purposes and the duration of its storage”.

The third part of Article 5 introduces a new requirement to ensure that when electronic communications networks are used to store information or gain access to information stored in the terminal equipment of a subscriber or user, clear and comprehensive information must be provided, in accordance with the Data Protection Directive 95/46/EC, about the purposes of such storage, and the subscriber or user concerned must be offered the right to refuse such processing. This does not apply to technical storage or access, however, or where strictly necessary in order to provide an information society service requested by the subscriber or user. Recitals 24 and 25 make it clear that these new provisions apply to the use of “cookies” and similar software which is designed to be sent to the terminal equipment of a user for tracking or recognition purposes.

Approach to the Privacy Regulations

- Regulation 4 (Security)
- Regulation 5 (Confidentiality)

Security

The security provisions in Article 4 are implemented in Regulation 4 of the draft Privacy Regulations. These largely reflect the wording of current requirements except that they now include the wording used in Recital 20 on the provision of information free except for a nominal charge.

Confidentiality

The confidentiality requirements in the TDPD, on which the new Directive's wording is closely based, were implemented in the UK by the Regulation of Investigatory Powers Act 2000 (RIPA), which prohibits interception and recording of communications (including e-mail) without consent, except as authorised for national security and law enforcement purposes, or essential business purposes. RIPA provides for the terms on which public authorities may access communications and traffic data (such as a phone operator's records of the time, duration and destination of calls). The Home Office is currently consulting on proposals for secondary legislation under RIPA setting out which additional public authorities might use these provisions; further information on this is available from the Home Office at:

<http://www.homeoffice.gov.uk/ripa/part1/consult.htm>

Because the new Privacy Directive's provisions are close to existing requirements under the TDPD, and RIPA already applies to e-mail communications, we do not propose to include any further confidentiality provisions in the implementing regulations.

The terms on which businesses may intercept and record communications without consent are set out under the Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000 ("the Lawful Business Practice Regulations"), secondary legislation under RIPA. Further information, and the text of these Regulations, is available from the following website:

http://www.dti.gov.uk/cii/regulatory/telecomms/telecommsregulations/lawful_business_practice_regulations.shtml

The Lawful Business Practice Regulations do not require that businesses monitoring or recording communications under the terms of the Regulations must inform both parties that this is happening, although they are required to try to ensure that users of the same system (e.g. employees) are aware of this and best practice guidelines for the Information Commissioner in any case recommend informing all the parties of such monitoring. Given this, and the controls on personal data processing under the Data Protection Act 1998, we do not propose to include any substantial amendments to the Lawful Business Practice Regulations in the implementing regulations for the Privacy Directive.

Cookies and similar devices

Article 5.3 introduces new transparency and consent controls on the use of cookies and similar tracking devices; the implementing provisions are set out in Regulation 5 of the draft Privacy Regulations.

What are cookies and what are these new controls designed to safeguard? Cookies are normally defined as software sent to and stored in the terminal of an internet user by a service provider: the device then acts as a marker or identifier that can be recognised automatically by the service provider. They may be used for a wide range of purposes: some operators use them, for example, to log how many visits a particular website, or page of a website, is getting, or the order in which visitors navigate around a site; they can therefore be used to monitor how attractive a site is, for design or advertising purposes. Cookies can be used to monitor repeat visits from the same terminal, enabling site providers to record their language preferences, or vary the banner adverts sent to that visitor. They may be used in conjunction with other information provided by the visitor to provide a picture of what a web-visitor has previously bought or expressed an interest in, or to facilitate online purchasing procedures or security/identity checks. They may be used to send a return message – to prompt the visitor to buy from the site, for instance.

There are technical controls which internet users can place on cookies – internet users can choose to set browser controls to alert to or reject certain forms of cookies automatically.

The Privacy Directive recognises that there are good and bad uses of cookies and similar devices and indeed that some internet functions would be either impossible or very difficult to use without them; the aim is to address devices used in a way which “may seriously intrude upon the privacy” of terminal users and subscribers and to ensure that users are aware when such devices are used, and have a chance to refuse, although cookie-free access does not have to be provided where the cookie is essential to an online service that has been requested or being used for “a legitimate purpose” on a website.

It is worth emphasising that the new requirements in the Directive are not technology specific – i.e. they do not just apply to what is now currently understood as a cookie but to any device used to store information or gain access to information stored on a user’s terminal. The new requirement should also be seen in the context of existing EU and UK law; for instance, the controls on lawful interception under the RIPA, the Data Protection Act 1998, which requires the fair processing of personal data whatever the technology involved, and the Computer Misuse Act 1990, which makes unauthorised access to computers illegal.

We believe that the key aim in implementing the new provisions of the Privacy Directive should be to enable internet users to make an informed choice about cookies, without placing unnecessary constraints on the technical development of online services. The Privacy Regulations should build on existing good practice and use of the technical controls on cookies available in internet browsers.

Many online operators already routinely include information about cookies on their websites. The Interactive Advertising Bureau (IAB), is an industry body which

develops standards and guidelines to support online business processes and increase customer confidence in the e-commerce environment. The IAB has set up a specialist team to develop a practical approach to compliance with the requirements of Privacy Directive, including advice for online service providers on how to identify whether cookies are being used, how they can be categorised, and how to explain to site visitors how they can be switched off. The central feature of the IAB's recommended approach is the creation of an accessible and impartial source of information for users about cookies, the technology involved, their benefits and potential abuses. This resource will be in the form of a website to which service providers will be able to link their own cookie or privacy statements. A draft version of the contents of this project is available on the following website:

<http://www.iabuk.net/index.php?class=news&view=688>

For more information about the IAB project or to make comments or suggestions directly to the IAB:

iab-cookies@europe-analytica.com

Issues

Implementing these provisions raises a number of questions:

What kind of information should cookie users provide and where should they provide it? The draft Privacy Regulations specify that there should be clear and comprehensive information about the purposes for which any cookies are being used. They do not specify where and how this information should be set out, but we would envisage it being included in a clearly signposted privacy or cookie statements on the online service provider's website. Where use of cookies involves processing of personal data, they are already subject to the Data Protection Act's requirements on fair processing of personal data. Guidance from the Information Commissioner is available from:

<http://www.dataprotection.gov.uk/dpr/dpdoc.nsf>
under "Compliance advice: Internet : Protection of Privacy"

How should users be given the opportunity to refuse a cookie?

The draft Privacy Regulations do not specify how this should be done but we envisage two broad options: service providers could make their own switch-off facilities available, or they could explain to users how to use the switch-off and alert facilities provided independently in browser programmes. There is nothing in the draft Regulations to stop operators from offering opt-in consent rather than simply the opportunity to refuse a cookie, but this is not a requirement. Finally, the draft Regulations specify that the opportunity to refuse need not be offered more than once.

When should service providers be entitled to refuse cookie-free access to their services?

The draft Privacy Regulations specify that service providers should not have to provide either information or the chance to refuse where the cookie is intended for the sole purpose of enabling or facilitating the transmission of a communication (e.g. to enable

technical access to some site formats) or where the cookie is strictly necessary for the provision of an online service requested by the subscriber or user. Where service providers believe that a cookie is important without being strictly necessary to the provision of a service, including access to a site, they may still make acceptance of the cookie a condition of access, although they would have to provide information about the cookie to the potential service recipients so that they can decide whether to proceed or not.

Should the requirement to provide information and a chance to refuse apply to all cookies or just those which involve the processing of personal data?

We interpret the new provisions in the Directive as applying to all cookies, regardless of the kind of data they process; to be sure of complying with the Privacy Regulations, service providers should therefore provide information and a chance to refuse in relation to all cookies, even where they involve the processing of data on an anonymised basis or are session specific. Where use of the cookie will result in the processing of personal data, service providers will need to ensure that they comply with existing Data Protection Act requirements (see above).

Should users have the right to override a subscriber's consent?

The Directive gives both users and subscribers the right to information and a right to refuse cookies, but does not make it clear whether a user has the right to override the subscriber's consent to the same cookie (Article 5 is framed in terms of users or subscribers, but the recitals talk about the importance of the user's right to refuse where users other than the original user have access to the terminal equipment and therefore to any data containing privacy-sensitive information stored on such equipment).

In most cases where terminals are shared (for example, on workplace systems where the subscriber is the employer but the user is an employee, or in an internet café) this will not matter. However, there could be a problem with programmes or services designed for corporate use if an individual user (for example, a company employee) blocked or disabled a cookie which was important to the functioning of the programme, thereby undermining the effectiveness or the price basis for the product (where they prevent a product from being copied in breach of contract terms, for instance).

This could argue for seeking to define in the Privacy Regulations whose consent should take precedence, but there would be strong objections to this. It would be difficult to make this distinction without running the risk of undercutting rights granted either under the Privacy Directive or other legislation. The Privacy Directive itself gives rights to both users and subscribers in relation to cookies, and we would have to be careful not to sweep away legitimate user rights (for example, leaving privacy sensitive data exposed to employers without any legitimate operational justification).

We believe that in almost all cases where a cookie was being used as part of this kind of service, the service provider (and the system subscriber) would be able to rely on the provisions of the Directive which apply to cookies which are strictly necessary to the provision of a service requested by the user (in which case, the Directive does not require either information or the opportunity to refuse a cookie to be provided). Where the cookie was not strictly necessary but the service provider believed it was none-the-less important to the working of the service, they would still be entitled to refuse cookie-free access although they would still have to provide information about the

cookie and why it was being used. The Privacy Regulations as drafted do not seek to define whether users and subscribers should have the right to overrule each other in any circumstances.

Questions for consultees

What information should operators provide about cookies and similar devices, and how should internet users be given the opportunity to refuse them?

Should the Privacy Regulations apply to all cookies and similar devices, or should they only apply to cookies where they involve processing of personal data?

Should the Privacy Regulations specify whether a user should have the right to override a subscriber's consent to a cookie?

Chapter four: network and service providers' requirements – traffic data, itemised billing, calling line identification, location data services, call tracing and forwarding

The requirements in the Directive

- Articles 6, 7, 8, 9 and 10
- Recitals 26 – 37

Article 6 of the Directive sets out what electronic communications network and service providers may do with traffic data (data which is processed for the purpose of conveying communications within a network, and for billing purposes, such as the length and destination of phone calls). It requires providers to delete or anonymise traffic data once it is no longer required for network management, billing or dispute resolution purposes (but see also Article 15 and Chapter 7 for provisions on the retention of data for national security and law enforcement purposes).

Providers may however retain and use traffic data to market communications services. The Directive also now explicitly allows the provision of value added services based on traffic data. The Article does not restrict the involvement of third parties in the provision of value added services, or place a limit on the kinds of services that may be offered, but there are some important provisos. The subscriber or user must be informed of the data processing implications of any services, and they must give their consent to the service or marketing; they must also be allowed to withdraw that consent at any time.

Article 7 gives subscribers the right to receive non-itemised bills and puts an obligation on Member States to ensure that privacy-enhancing methods of communications or payments are available to users and subscribers. Recital 33 gives other billing options that Member States may use – for instance, bills which are itemised but where some of the digits of the called number are deleted.

Article 8 sets out the range of calling and connected line identification (CLI) services to be provided by service providers.

Article 9 introduces new provisions on location data (e.g. data processed within a communications network which indicates the geographical position of a user's terminal equipment, such as a mobile phone). This new Article enables network and service providers to introduce value added services based on location data as well as traffic data. As with Article 6, there is no restriction on the kinds of services that may be offered or the involvement of third parties, but such services can only be provided where the data involved has been anonymised, or with the consent of the individual concerned; before consent, the subscriber or user must be informed of the data processing implications of the service, and they must be allowed to withdraw their consent at any time. They must also be allowed to temporarily withhold their consent, free of charge.

Article 10 enables network and service providers to override a subscriber or user's CLI or location data preferences in order trace malicious or nuisance calls, or to enable the emergency services to respond to calls for help.

Article 11 specifies that subscribers must have a simple and free means of blocking automatic call forwarding by a third party.

Approach to the Privacy Regulations

- Regulations 6 and 7 (traffic data)
- Regulation 8 (itemised billing)
- Regulations 9 -12 (CLI)
- Regulation 13 (location data)
- Regulations 14 and 15 (tracing of malicious, nuisance and emergency calls)
- Regulation 16 (call forwarding)

Traffic data

The requirements to delete and anonymise traffic data in Article 6 are largely based on existing requirements under the Telecommunications Data Protection Directive (TDPD), although they now apply to providers of services and networks on the internet as well as conventional telecommunications networks and services. These provisions, and the new rules on value added services based on traffic data, are set out in Regulations 6 and 7 of the draft Privacy Regulations. The new provisions on value added services follow the text of the Directive; like the Directive, the draft Regulations do not limit the kind of value added services that may be provided, as long as the subscriber or user's consent is gained. The draft Regulations require that network and service providers must inform subscribers and users about the data processing implications of value added services before gaining their consent, but they do not specify how this must be done.

Itemised billing

This provision is transposed in Regulation 8 of the draft Privacy Regulations. Like the billing requirement in the current regulations, it gives subscribers the right to request non-itemised bills (so that where a phone is shared between several users, they can opt simply to split the bill if they do not want to disclose details of calls made). The draft Regulation also places a duty on the Secretary of State and Ofcom to take privacy issues into account when exercising their wider policy and regulatory functions under the Communications Act; for example, this means that Ofcom would need to have regard to the need for access to private communications when setting conditions in relation to the provision of electronic communications services.

Calling and connected line identification (CLI)

The Directive's requirements on CLI are continued from the TDPD. They require service providers to offer a range of CLI services to their subscribers, including the right to withhold CLI on outgoing calls on a per-call or per-line basis (so that the call receiver cannot trace the call by dialling 1471), and the right to block incoming calls where the CLI has been withheld (anonymous caller rejection). This balances the right of callers to withhold their CLI and for subscribers, and can be a very useful service (among other things, it is an effective network-based way of blocking cold calls from unidentified numbers). Where this service is used the caller should an automatic

message explaining why the call has been barred and how lift the block on CLI to enable the call to go through. Some CLI services must be provided free of charge, including the suppression of CLI on outgoing calls. Operators may make a charge for others, including anonymous caller rejection services.

Not all telecommunications operators currently provide the full range of CLI services, however, and there is a dispute over whether the current rules on CLI provision require operators to provide CLI services directly where subscribers could achieve a similar effect by using the options available in terminal equipment. Mobile service providers in particular do not generally offer anonymous caller rejection as a network service. There is an argument that subscribers may effectively exercise their rights by using phones which display the caller's identity or lack of it, and just not answer, or press the "busy" button if the CLI is withheld, and that network based blocking solutions are too expensive to justify the additional benefits to subscribers. Both the ICO and Oftel regard this as a less than satisfactory solution, since the subscriber may still be disturbed by the call which could end up on their voicemail or answerphone, and there is an issue over whether this fully reflects the intention of the CLI requirements in the Directive. We believe there is a case for a stronger requirement on service providers and this and the other provisions on CLI are set out in regulations 9 to 12 of the draft Regulations.

Location Data

The new provisions in the Directive are intended to allow service providers to offer value added services based on location as well as traffic data. This will open the door to a range of new services such as location-based advertising to mobile phones, or traffic or weather alert services. Like value added services based on traffic data, it is important that subscribers and users give their informed consent and understand the data processing implications of this kind of service. The draft Privacy Regulations specify that information is provided before consent is obtained but we do not propose to specify exactly how service providers should go about this in the Regulations.

Call tracing and forwarding

It is currently an offence under section 43 of the Telecommunications Act 1984 to make a malicious or nuisance call; this will also be an offence under the Communications Act. Regulation 14 of the draft Privacy Regulations enables network providers to override the suppression of CLI on a call in order to trace the source of a nuisance or malicious call at the request of a subscriber, and to pass the results of that search on to the appropriate authorities (see also Chapter 7 on the tracing of subscriber details for the purpose of investigating breaches of the rules on unsolicited commercial communications). Regulation 15 enables network providers to override the suppression of both CLI and location data, if applicable, in order to trace a call to the emergency services (where the caller is unable, for instance, to provide a clear indication of where they are). Regulation 16 requires service providers to ensure that subscribers can stop unwanted call forwarding, free of charge. All of these are largely based on existing provisions.

Questions for consultees

How should service providers gain consent to processing of traffic and location data and what information should they provide?

Should service providers be under a stronger requirement to provide the full range of CLI services, as proposed?

Chapter five: subscriber directories

The requirements in the Directive

- Articles 12 and 16
- Recitals 38, 39, 49

The Privacy Directive introduces a number of changes to the rules on subscriber directories, designed to give subscribers clearer rights and to simplify the regime for network operators and directory providers. Article 12 requires, firstly, that subscribers are informed about the kind of subscriber directories in which they may be listed and how those directories will be used, including any non-standard search functions available in any electronic versions. Recital 39 makes it clear that the obligation to inform subscribers should be imposed on the party collecting the data for inclusion (in the UK, this would normally be the network or service provider).

Secondly, they must be given an opportunity to determine whether they are going to be listed, and if so, what personal data should be included, subject to the rider that this must be relevant for the purposes of the directory, as determined by the provider of the directory. This is a change from the Telecoms Data Protection Directive (TDPD) requirement which simply gives subscribers the right to be ex-directory, to specify that their entries may not be used for direct marketing purposes, or to omit part of their address or any reference to their gender. Not being in a directory or correcting or otherwise changing an entry must now be free of charge.

Thirdly, the Directive now addresses the issue of “reverse searches” i.e. functions which allow a directory user to search for a subscriber’s name and/or address on basis of their phone number, rather than the other way round. The Directive gives Member States the right to impose a separate consent requirement for inclusion in any directory which includes this kind of function. Subscribers must in any case be informed if any of the subscriber directories in which they may be entered may be used in this way.

Finally, the Directive specifies that these rights must be applied to subscribers who are natural persons (e.g. individuals) although they may be extended to legal persons (e.g. corporate subscribers such as limited companies in the UK).

Article 16 of the Directive applies transitional arrangements to directory entries; it specifies that the new rules do not apply to existing editions of directories, and that subscribers who already have entries in directories will stay listed unless they decide to withdraw or change their entry, having been informed of their new rights.

Approach to the Privacy Regulations

- Regulations 17 and Schedule 2

The rules in the Privacy Directive address privacy issues, and apply to e-mail addresses as well as phone and fax contact details. However, they have to be read alongside provisions elsewhere in the new regulatory framework for electronic communications (specifically the Universal Service and Competition Directives), which underpin the importance of comprehensive subscriber directories as a facility. These require Member States to ensure the availability at least one comprehensive subscriber directory, and at least one directory enquiries service, in a form approved by the relevant regulator. These obligations will be achieved through the imposition of conditions by Ofcom under the Communications Act regime. Oftel consulted on draft general conditions of entitlement, including conditions 8 and 22 on the provision of subscriber directories and directory enquiry services in May last year.

The responses were published on 21 March 2003 as part of the Department's consultation on the implementation of the four Communications Directives and are available from the Communications Bill website: www.communicationsbill.gov.uk (as Annex B to the document published on 21 March). Oftel's revised proposals for the general conditions to be made once the Communications Bill has been passed are set out in Annex C to the consultation document of 21 March, and the general conditions that would apply from 25 July 2003 if the relevant provisions of the Bill are not being brought into force on that date are set out in Annex A to that consultation document.

In the UK all publicly available directories and directory enquiries services run off a central pool of subscriber data. This is operated by British Telecom (BT) as the largest telephone services provider but is available to all network and service providers, who feed in their own subscribers' data; this ensures that the directories and enquiries services available cover subscribers to all networks. Data from this pool is entered into the residential and business subscriber directories provided by BT, Yell and Thomson. Directory enquiries (DQ) services are being opened to competition. This process was launched in December 2002 with the introduction of new 118 codes for DQ services. The old codes (192 and 153) will be withdrawn in August 2003. There are approximately twelve new services at present. There is currently no parallel universal subscriber directory of mobile phone, fax numbers or e-mail addresses although some network and service providers do provide listings of their own subscribers.

We believe our objectives in implementing the Privacy Directive should be to ensure that subscribers can make an informed decision about being listed, and what kind of entry to have, but also to maximise the chance of subscribers choosing to be listed and minimise the complexity of consent procedures.

Issues

What kind of directory do the new requirements apply to?

The requirements in the Privacy Directive apply to publicly available directories of subscribers of electronic communications services. We interpret this to mean any directory whose sole or main function is to list the phone, fax or e-mail contact details of network subscribers, including universal directories of phone service subscribers of the kind required under the regulatory framework for electronic communications. The Directive would not apply to other forms of directory (for example, trade directories) where electronic communications contact details do not constitute the sole or major component. In the UK this means that only directories of residential, and arguably also business, subscribers are covered by the new rules. This does not mean that other

forms of directory are either outlawed or unregulated from a privacy viewpoint – all UK-based directories which process personal data are subject to the requirements of the Data Protection Act 1998.

What kind of consent should be required?

While the Directive makes it clear that subscribers must be given the opportunity to choose whether they are listed or not, the text does not specify how that choice must be exercised and whether it should be active or passive, which raises the question of how we should implement this here. The message we have had so far both from network operators and directory operators, supported by the ICO, is that it is acceptable for subscribers to be presented with inclusion as the default position provided the choice is well explained and flagged up for subscribers and they have a clear opportunity to decide otherwise. Allowing this form of choice would also make it less likely that subscribers would drop out of directories by default and this is the basis on which Regulation 17 should be read. Against this, requiring active consent would arguably give subscribers stronger protection against accidental inclusion by forcing them to make a positive decision to be listed. Consultees' views on this would be welcome.

What entry options should be available to subscribers?

The new version of the Directive allows subscribers a degree of choice over the kind of information that may be listed in a directory or disclosed by a directory enquiry service, subject to the proviso that such data must be relevant for the purpose of the directory as determined by the directory provider. This replaces a provision in the previous version of the Directive which specified that individual subscribers should have the right, among other things, to have their address omitted in part, and “not to have a reference revealing his or her sex, where this is applicable linguistically”.

Our interpretation is that the Directive still entitles operators to present subscribers with a menu of pre-set entry options, provided that they are given a reasonable degree of choice. Because UK network and service providers pool subscriber data for directory entry and enquiry purposes, we believe that it would make sense for service providers to work to a shared core set of options to put to subscribers. This will both lessen the potential for errors and support competition and data sharing. Determining what should be in that core list is not always going to be straightforward, however. Subscribers currently have the choice of a partial address entry and/or the choice of going in with full name or initials only to avoid disclosing the subscriber's gender but there may be both more and less choice in the future. On the one hand, multiple listings of the same family name may make entries increasingly unusable without full address listings, making the existing options less viable; on the other hand, new options for differentiating subscribers may emerge over time.

We think the best model would be for operators to formulate their own core list in liaison with the Information Commissioner's Office (ICO) to ensure that privacy requirements are met, and with Ofcom, to ensure that the choices offered support the availability of comprehensive directory services and competition in this market. Regulation 17 is therefore drafted on the basis that the Privacy Regulations should set out the broad parameters but not specify the list of options available.

Should additional consent be required for directories with a reverse search function?

Negotiations on the Directive demonstrated very diverging approaches to directories with a reverse search function in different Member States; this function is not currently offered by public subscriber directory or enquiry services in the UK (and it has generated some controversy when offered by other directory/database providers here). The problem is that subscribers who agree to this kind of function without fully understanding it risk inadvertently disclosing their name and address when they give out their number. There is also danger that fear of this kind of search may put subscribers off any kind directory entry at all. In some European countries, however, this kind of search function is widely used and seen as useful and legitimate, and the Directive makes it clear that this kind of function is not in itself unacceptable although it may justify special handling.

Given the lack of familiarity with this function in the UK, and the potential for serious abuse of data protection and privacy, we propose exercising the option to require additional consent to directories with a reverse search functions. Regulation 17 is drafted on this basis.

What rights should corporate subscribers have?

The Privacy Directive, like the TDPD, applies the harmonised safeguards on directories to individual subscribers only. It allows, but does not require, Member States to extend some or all of these safeguards to corporate subscribers. The Telecommunications (Data Protection and Privacy) Regulations give corporate subscribers a simple opt-out right in relation to subscriber directories, without specifying that they must also have the partial entry rights currently available to individual subscribers. In practice, this seems to work effectively and Regulation 17 has therefore been drafted on the same basis, without extending the full range of rights available to individual subscribers. We would welcome the views of consultees on this point.

Questions for consultees

Should subscribers be allowed to opt for inclusion in a subscriber directory as the default option, as proposed, or should active choice be required?

What entry options should be available to subscribers and should service providers be able to determine the core list, as proposed?

Are the draft Privacy Regulations right to specify that additional consent should be required for inclusion in any directory with a reverse search function?

Should corporate subscribers be entitled to some or all of the new rights accorded to individual subscribers?

Chapter six: unsolicited commercial communications – automated calling systems, fax, phone, e-mail and SMS

The requirements in the Directive

- Article 13
- Recitals 40 – 45

The Directive retains existing controls on unsolicited direct marketing by means of automated calling systems without human intervention, fax, and phone. It also introduces new controls on unsolicited e-mail and SMS marketing. In the case of automatic calling systems and faxes, Member States are required to ensure that individual subscribers have prior consent or opt-in rights. The opt-in rule also applies to e-mails, which the Directive defines as including SMS, except where the conditions set out in Article 13.2 apply. This part of the Article (the “soft opt-in” exemption) specifies that e-mails may be sent on an opt-out basis in the context of an existing customer relationship, where:

- the sender obtains the addressee’s contact details in the context of the sale of a product or service and in accordance with the data processing rules in the Data Protection Directive; and
- the sender is marketing its own similar products or services; and
- the addressee is always able to opt out of future marketing, in an easy way and free of charge

Recital 41 makes it clear that the “free of charge” condition does not include any basic transmission costs (e.g. the addressee would be expected to cover the cost of e-mailing the sender, but they must not be charged any kind of fee for opting out).

Article 13 also specifies that e-mailers must not conceal their identity.

As with subscriber directories, the rights in Article 13 apply to subscribers who are natural persons (e.g. individuals) although Member States may extend them to legal persons (e.g. corporate subscribers).

Approach to the Regulations

- Regulation 18 (automated calling systems)
- Regulation 19 (faxes)
- Regulation 20 (phone calls)
- Regulation 21 (e-mail and SMS messages)
- Regulation 22 (information to be supplied by direct marketers)

Issues

What is a customer relationship for e-mail marketing purposes?

Implementation of the new rules on unsolicited commercial e-mail and SMS raises a number of questions. Firstly, should customer relationship for these purposes be

confined to situations only where the e-mail addressee has previously bought something or should it apply to prospective customers as well (e.g. where someone has registered an interest in a product and allowed their e-mail address to be recorded for future marketing use but under an opt-out rather than opt-in process)? The text of the Directive does not make it wholly clear what is intended but this is an issue that is clearly going to be of concern for businesses who may have legitimately obtained an e-mail address (through a promotional campaign, for instance, or by providing a quote to a prospective customer) without actually selling its products or services.

Our view is that the most important safeguards here are that contact details are fairly collected and subscribers are clearly informed of, and given a chance to object to, use of their data for direct marketing by that same business. As long as these conditions are met, and there is a direct relationship of some kind between the two parties, it does not seem necessary to insist that there must have been an actual purchase for this exemption to apply. Regulation 21 has been drafted on this basis.

How should the “similar products” rule be interpreted?

The Directive’s condition that opt-out e-mail marketing must be of similar products was intended to reinforce the principle that opt-out consent should only apply to targeted marketing where the products and services concerned will be of interest to the addressee and they already have a relationship with the sender. The exact interpretation of “similar” in this context is not clear, however. Could a supermarket, for example, only e-mail its online customers about special offers on baked beans if that is what they have bought before or should it be able to direct market its whole range of food and other products or services?

We think the way forward on this should be based on existing rules and guidelines under the Data Protection Act 1998. These would restrict a business to direct marketing the kind of products the addressee would have reasonably expected it to market at the time they gave or agreed to use of their contact details i.e. a business could market the products available at the time, but not necessarily those of a business that it took over, or a substantively new product range. The key safeguard here is that addressees’ contact details are fairly obtained in the first place – given that if in doubt, they have the right to opt out in any case (and businesses will have an incentive to monitor their own marketing practices in order to avoid this happening) it seems sensible to give a broader, rather than a narrower, interpretation to the “similar products” restriction. Regulation 21 (3) (b) specifies that for the purposes of this provision, the marketer must take reasonable steps at the time the addressee’s contact details were collected to ensure that the addressee is aware of the kind of products they deal in.

What other solutions are there to unwanted e-mail marketing?

E-mail marketing can be a powerful tool when used in a targeted and responsible way; when used without respect for addressees’ privacy rights or preferences it can cause serious offence and nuisance. Bulk untargeted e-mails or spam also generate problems for internet service providers (ISPs) whose networks can be blocked or slowed down. The new rules on unsolicited commercial e-mail will bolster the rights available to individuals and will reinforce good practice in e-mail marketing. Industry bodies like the Direct Marketing Association and the Advertising Standards Authority already promote their own rules on e-mail marketing through their codes of practice – further

information about this is available from their websites (<http://www.dma.org> and <http://www.asa.org.uk>)

Regulation is only part of the answer, however, particularly given the volume of spam that comes from outside the EU. Internet Service Providers (ISPs) will cut off senders who breach their acceptable use policies by sending spam; they can also offer advice to their customers on how to avoid spam, and the spam prevention and filtering systems available. Further information is available from the Internet Service Providers Association: <http://www.ispa.org.uk/html/consumers/spam.html>

Should individual or corporate subscribers be given further opt-in or opt-out rights against phone, fax, SMS or e-mail marketing?

Although there are harmonised opt-in requirements for unsolicited commercial fax and e-mail (including SMS) messages to individuals, the Directive continues to allow Member States the choice between opt-in and opt-out rules in relation to direct marketing by phone to individual subscribers. It also allows Member States discretion over what level of protection should be extended to corporate subscribers in relation to all forms of unsolicited commercial communications.

Currently, the UK applies opt-out rules to **direct marketing by phone** to individual subscribers, who can opt-out either by registering on the Telephone Preference Service, or by instructing individual marketers not to ring again. Corporate subscribers do not have the right to register on the TPS but they do have some rights under the current Telecommunications Act licensing regime to opt out on a case-by- case basis. Corporate subscribers do have the right to opt out of **fax marketing** by registering on the Fax Preference Service or on a case-by-case basis. In terms of **e-mail** corporate subscribers have case-by-case opt-out rights under the Data Protection Act 1998 where their e-mail address incorporates personal data (i.e. an individual's name). There is no current global opt-out scheme with statutory backing, although the DMA's e-mps opt-out register is backed by industry codes of practice, and is open to both individual and corporate subscribers. The e-mps database is held in the United States and personal data is not therefore covered by UK data protection legislation. **SMS** messages are currently treated in the same way as phone calls so corporate subscribers have no global opt-out rights.

See the table below for summary of individual/corporate opt-in and opt-out rights.

	Individual subscribers	Corporate subscribers
Telephone selling	Member States allowed to choose between opt-in and opt out – UK rules give both individual opt-out rights and the right to register on the TPS	Not entitled to register on the TPS
Fax selling	Opt in rule applies but current regulations allow individuals to register on the FPS as an additional protection	Corporate subscribers may register with the FPS under current regulations
E-mail	The Data Protection Act gives the right to opt-out on an individual basis where the e-mail address includes personal data (e.g. an individual's name). There is a non-statutory, US based preference scheme to opt-out on a global basis (e-mps). Privacy Directive will introduce new opt-in right	Corporate subscribers may register on the e-mps and can also exercise individual opt-out right under the Data Protection Act where their business address incorporates personal data (e.g. an individual's name). Privacy Directive allows but does not require further rights

Options for change

Individual subscribers

The only area where individual subscribers could be given stronger statutory rights would be in relation to telephone sales, where they could be given a prior consent/opt-in right. In favour of the status quo, experience of the TPS suggests that this is a reasonably effective protection for people who do not want to receive cold calls. It is easy and cheap for direct marketers to comply with and arguably allows them to target campaigns more effectively because it saves them the cost of phoning people who do not respond to this form of marketing.

Some aspects of commercial phone use cause particular problems: one of them is the use of power diallers (often but not exclusively for direct marketing) which can cause silent calls when used without enough operators being available (see also below on automatic calling systems). Another emerging issue is the difficulty of regulating calls made by overseas call centres which are not subject to EU controls. It is not clear that an opt-in right would impact on these problems, however, and it would cut back on the marketing opportunities now available to businesses; this would undoubtedly carry a cost for businesses. Against this, however, there is a body of opinion (supported by Ofcom) that individuals should in principle have opt-in rights and that there is a case for re-opening this option.

Corporate subscribers

There are three broad options in relation to corporate subscribers – leave things as they are, give corporate subscribers further opt-out rights, or go the whole way and give corporate subscribers exactly the same rights as individuals (including opt-in rights in relation to fax, e-mail and text messaging).

In defence of the status quo, businesses as a group are arguably better placed to deal with direct marketing communications than individual subscribers at home may be. Any new restrictions on business-to-business marketing would undoubtedly carry a cost, especially for new entrants trying to build up a client base who would have to attract interest by other, more expensive forms of advertising where they could not use direct marketing by phone, fax, or e-mail. This is most true of opt-in consent requirements but registration with the TPS, for instance, will prevent all marketers from making the initial contact with that subscriber by phone, regardless of the kind of products they are promoting and the interest they are likely to generate.

Against this, corporate subscribers (particularly small ones) can suffer a real loss from badly targeted communications. Corporate subscribers already have opt-out rights in relation to fax marketing because of the cost of receiving faxes. Phone calls also carry a cost, however – it can be a real bone of contention with small shops, for example, when staff find they have to leave customers to answer direct marketing calls which are of no relevance to their own business activity. The way that the split between individual and corporate subscribers works under UK law (see Chapter two) can throw up some anomalies – sole traders and partnerships (except in Scotland) can register on the TPS because they count as individuals, limited companies, however small, cannot. Many register anyway by simply not declaring their status and have to be subsequently removed from the list.

The picture on e-mail including SMS is more complex; there is no existing statutory opt-out scheme which corporate users could rely on although they are able to register with the DMA's voluntary e-mps scheme. Because e-mail is an international medium, and because individual subscribers here must in any case now be given opt-in rights, there would be little point trying to establish a statutory opt-out register only for corporate users, and only for the UK. Another option would be to grant statutory recognition to global registers like the e-mps although this would mean effectively backing a scheme outside UK control. It is not clear how much value this would add to a scheme which is already built into DMA and other codes of practice. Corporate subscribers already have the right to opt-out of e-mail from particular senders where their e-mail address incorporates personal data (e.g. an individual's name). This protection will not apply to SMS, however, since they are sent to a phone number.

The most radical option would be to extend all the rights available to individual subscribers to corporate subscribers, including an opt-in right in relation to fax and e-mail, including SMS. This would have the benefit not just of giving corporate users rights against unwanted advertising but would ensure that no-one could direct market individuals on the pretence that they thought they were corporate subscribers. Against this, it would have a significant impact on business-to-business marketing – the opt-in consent would be a much costlier option, particularly for new market entrants, because it means that they could not make an unsolicited approach by phone, fax or e-mail/SMS, to any corporate users, even those who might potentially have been

receptive to their marketing – they must instead use other forms of advertising to attract clients’ interest and consent to further marketing.

Regulations 17 to 21 have been drafted on the basis that we should:

- Maintain the existing opt-out right for individuals in relation to phone selling
- Give corporate subscribers the right to register on the TPS or opt out on a case by case basis, in line with their rights to opt-out of faxes

We would welcome the views of consultees on these and on all the other options available.

What are automated calling systems and how should they be regulated?

The Directive maintains the existing requirement for prior consent to unsolicited direct marketing by automated calling systems without human intervention, also referred to as automatic calling machines. This term is not defined, however, and there has been some debate in the past over exactly what systems are covered by this term in the Telecommunications (Data Protection and Privacy) or TDPP Regulations. Our understanding is that this provision in the Directive was designed to target systems which automatically deliver a recorded voice message; the prior consent requirement was needed because of the potential nuisance of a pre-recorded advertising message in this form and the danger that this form of bulk communication could overload networks. Regulation 18 has now been drafted to apply specifically to systems which deliver a pre-recorded message.

Grey areas under the current rules include the status of systems which send SMS automatically and power dialler-type systems which dial numbers automatically but are designed to establish a voice link with a live operator rather than a pre-recorded message. Lack of certainty about the application of the TDPP Regulations has made it harder to deal with the problems that these kinds of systems can cause. Power diallers, for instance, can cause problems to subscribers where they are used without enough call centre staff available to answer the calls being dialled, resulting in single or repeated silent calls, or calls which cut off after a few rings, in addition to any annoyance caused if they are used to ring subscribers who have registered on the TPS.

Limiting the definition of automated calling system does not mean that these areas will be unregulated. The sending of unsolicited SMS for advertising purposes is now explicitly covered by the Privacy Directive which treats them in the same way as e-mail messages. The use of power diallers and similar systems is also currently regulated under the Telecommunications Act licensing regime. Ofcom will have new powers to regulate this kind of system under the Communications Act, which creates a new offence of the persistent misuse of communications networks. This will enable Ofcom to take action against anyone who uses systems in a way which causes avoidable nuisance, annoyance or anxiety.

Questions for consultees

How should “customer relationship” and “similar products” be interpreted for the purposes of unsolicited e-mail and SMS marketing and do you agree with the approach adopted in the draft Privacy Regulations?

Should individual phone subscribers be given opt-in or prior consent rights in relation to phone marketing?

Should corporate subscribers be given the right to register on the Telephone Preference Service, as proposed? Should corporate subscribers have stronger rights in relation to fax, e-mail and SMS marketing?

Is the new definition of automated calling system right?

Chapter seven: enforcement and sanctions, technical standards, and exemptions for national security and law enforcement purposes

The requirements of the Directive

- Articles 14 and 15
- Recitals 11 and 46 – 47

Article 14 provides that any technical standards on networks or terminal equipment in support of the requirements of the Directive must be introduced in accordance with EU rules, including rules on the free circulation of equipment, on notification of draft technical standards, and terminal equipment standards.

Article 15 allows Member States to make exemptions to the privacy rules set out in the Directive for national security and law enforcement purposes. The Directive now specifies that Member States may adopt legislative measures providing for the retention of data for a limited period for national security and law enforcement purposes. Recital 11 sets out the parameters for Member States' legislation, which must comply with European Convention for the Protection of Human Rights and Fundamental Freedoms, and must be appropriate and strictly proportionate.

Article 15 and recital 47 require Member States to apply the provisions of Chapter III on judicial remedies, liability and sanctions of the Data Protection Directive to national implementation of the Directive, and to ensure that there are judicial remedies and penalties for failure to comply with the Directive.

Approach to the Privacy Regulations

- Regulation 24 (contracts)
- Regulations 25 and 26 (national security and legal requirements)
- Regulations 27, 28 and 29 (enforcement and compensation)

Technical standards

Like the existing Telecommunications (Data Protection and Privacy) Regulations (the TDPP Regulations), the draft Privacy Regulations do not provide for technical standards.

Exemptions for national security and law enforcement purposes

In the UK, the Regulation of Investigatory Powers Act 2000 (RIPA) provides for the terms on which national security and law enforcement agencies may intercept communications and access traffic data (such as a phone operator's records of the time, duration and destination of calls). The Home Office is currently consulting on proposals for secondary legislation under RIPA setting out which additional public authorities might use these provisions. Further information on this is available from the Home Office at:

<http://www.homeoffice.gov.uk/ripa/part1/consult.htm>

The Anti-Terrorism, Crime and Security Act 2001 introduced provisions for the retention of traffic data for national security and law enforcement purposes. The Home Office is conducting a separate consultation on how these provisions should operate: further information on this is available at:

http://www.homeoffice.gov.uk/oicd/antiterrorism/vol_retention.pdf

Regulations 25 and 26 specify that communications providers are exempt from the requirements of the Directive if necessary for the purposes of safeguarding national security, or for law enforcement purposes.

Enforcement and Sanctions

The Information Commissioner is the UK body responsible for enforcement of the rights granted under the Directive. The draft Privacy Regulations continue to give the Commissioner the right to take action either in response to a complaint or on his own initiative. In addition, anyone who suffers damage as a result of a breach of the Regulations is entitled to compensation from the person responsible.

Issues

Should network and service providers be required to disclose the source of unsolicited commercial communications?

How can subscribers, and the ICO, trace the source of unsolicited direct marketing communications which breach the rules (for example, direct marketing calls made to a subscriber who is registered on the Telephone Preference Service)? The current TDPP Regulations allow, but do not require, operators to disclose to anyone with a legitimate interest (including the police) the source of nuisance or malicious calls or faxes, where the caller has withheld their CLI. Network providers are committed to investigate complaints about such calls from their subscribers and currently invest a great deal of time and effort in their nuisance call bureaux.

However, there is a problem under the current regime where nuisance call bureaux trace a call on behalf of a subscriber but find that the source is a call centre or other direct marketer rather than a deliberately malicious or nuisance caller. Although bureaux will normally contact the call centre or direct marketer to pass on the complaint, they are not usually prepared to rely on the current TDPP provisions to disclose the source of this kind of call to the regulatory authorities. The Information Commissioner does have the right, under current provisions, to issue information notices requiring the provision of information to enable investigation and/or enforcement action to be taken for breach of the TDPP rules, among other things, but it is questionable whether these notices may be issued to bodies (such as, in the present case, network or service providers), who have no involvement in the suspected breach. This can leave subscribers powerless to enforce their opt-in or opt-out rights. All callers are entitled to withhold their CLI under the Regulations, but direct marketers are required to disclose their identity and valid contact details, either on request in the case of a live phone call, automatically on other forms of communication. If they do not comply with this, they will be untraceable without the help of the relevant network operator.

This raises the issue of whether network and service providers should be under a requirement to disclose the source of a call and/or other form of electronic communication which is suspected of breaching the rules on unsolicited direct marketing. Arguably, this kind of requirement would not encroach on the legitimate privacy rights of direct marketers because they are in any case required to disclose their identity and contact details under the Regulations. It would be consistent with the powers available to Ofcom to require information from network and service providers under the Communications Act. This would however clearly place a new obligation on operators with attendant implications for their relationship with their subscribers. We would welcome the views of consultees on whether this form of requirement is justified and if so, how it should be exercised.

Should the enforcement procedures and sanctions in relation to the rules on unsolicited commercial communications be strengthened? If so, how?

The current enforcement powers and sanctions for breaches of the TDPP Regulations are those available to the Information Commissioner under the Data Protection Act 1998. Where there is a breach, the Information Commissioner has the power to issue an enforcement notice requiring remedial action to be taken; failure to comply with an enforcement notice is a criminal offence punishable by a fine. If the Information Commissioner needs more information before deciding to issue an enforcement notice, he can, but is not obliged to, issue an information notice. The information and enforcement notices can be appealed against and the effect of the notice is lifted during the appeal, although where the Commissioner considers there are special circumstances he may require the notice to be complied with as a matter of urgency. In such cases the notice can take effect after seven days, even if it is appealed against.

Enforcement of sanctions against breaches of the rules on unsolicited direct marketing communications raises particular challenges. The current structure inevitably involves some time consuming procedures which do not allow for speedy action. This is becoming a particular issue in the fax marketing area, where the falling cost of faxing is lowering the incentive to comply with the regulatory regime. Although enforcement notices have been issued against some operators, no fines have yet been imposed on a company for breaching the terms of an enforcement notice. For legitimate marketers with a reputation to maintain, the threat of an enforcement notice may be a real deterrent; for others it may not be (and is unlikely in itself to create the kind of publicity that spreads subscriber awareness of their rights and the safeguards available to them).

Are there alternative models? The closest parallel are the sanctions that will be available to Ofcom under the Communications Act. In the case of the new offence of persistent misuse of electronic networks, Ofcom will be able to impose a direct administrative fine of up to £5,000 and/or seek an injunction to ensure that the terms of enforcement notices are complied with. In the case of consumer protection legislation, and where the collective interest of consumers is being harmed, the Office of Fair Trading, Trading Standards authorities and other nominated bodies now have the power to issue "Stop Now" orders; failure to comply with these may leave the offending business liable to contempt of court charges and subject to a fine and/or imprisonment. Alternatively, breaches or repeat breaches could be made a criminal offence, although

this would raise the standard of proof required in individual cases. We would welcome the views of consultees on the case for alternatives to the existing regime, and what they might be.

Questions for consultees

Should network and service providers be required to disclose the source of unsolicited commercial communications?

Should new enforcement sanctions be available against breaches of the rules on unsolicited commercial communications? If so, what should they be?

Official Journal L 201 , 31/07/2002 P. 0037 - 0047

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission(1),

Having regard to the opinion of the Economic and Social Committee(2),

Having consulted the Committee of the Regions,

Acting in accordance with the procedure laid down in Article 251 of the Treaty(3),

Whereas:

(1) 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(4) requires Member States to ensure the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy, in order to ensure the free flow of personal data in the Community.

(2) This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the Charter of fundamental rights of the European Union. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.

(3) Confidentiality of communications is guaranteed in accordance with the international instruments relating to human rights, in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms, and the constitutions of the Member States.

(4) Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector(5) translated the principles set out in Directive 95/46/EC into specific rules for the telecommunications sector. Directive 97/66/EC has to be adapted to developments in the markets and technologies for electronic

communications services in order to provide an equal level of protection of personal data and privacy for users of publicly available electronic communications services, regardless of the technologies used. That Directive should therefore be repealed and replaced by this Directive.

(5) New advanced digital technologies are currently being introduced in public communications networks in the Community, which give rise to specific requirements concerning the protection of personal data and privacy of the user. The development of the information society is characterised by the introduction of new electronic communications services. Access to digital mobile networks has become available and affordable for a large public. These digital networks have large capacities and possibilities for processing personal data. The successful cross-border development of these services is partly dependent on the confidence of users that their privacy will not be at risk.

(6) The Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal data and privacy.

(7) In the case of public communications networks, specific legal, regulatory and technical provisions should be made in order to protect fundamental rights and freedoms of natural persons and legitimate interests of legal persons, in particular with regard to the increasing capacity for automated storage and processing of data relating to subscribers and users.

(8) Legal, regulatory and technical provisions adopted by the Member States concerning the protection of personal data, privacy and the legitimate interest of legal persons, in the electronic communication sector, should be harmonised in order to avoid obstacles to the internal market for electronic communication in accordance with Article 14 of the Treaty. Harmonisation should be limited to requirements necessary to guarantee that the promotion and development of new electronic communications services and networks between Member States are not hindered.

(9) The Member States, providers and users concerned, together with the competent Community bodies, should cooperate in introducing and developing the relevant technologies where this is necessary to apply the guarantees provided for by this Directive and taking particular account of the objectives of minimising the processing of personal data and of using anonymous or pseudonymous data where possible.

(10) In the electronic communications sector, Directive 95/46/EC applies in particular to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals. Directive 95/46/EC applies to non-public communications services.

(11) Like Directive 95/46/EC, this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures

referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(12) Subscribers to a publicly available electronic communications service may be natural or legal persons. By supplementing Directive 95/46/EC, this Directive is aimed at protecting the fundamental rights of natural persons and particularly their right to privacy, as well as the legitimate interests of legal persons. This Directive does not entail an obligation for Member States to extend the application of Directive 95/46/EC to the protection of the legitimate interests of legal persons, which is ensured within the framework of the applicable Community and national legislation.

(13) The contractual relation between a subscriber and a service provider may entail a periodic or a one-off payment for the service provided or to be provided. Prepaid cards are also considered as a contract.

(14) Location data may refer to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded.

(15) A communication may include any naming, numbering or addressing information provided by the sender of a communication or the user of a connection to carry out the communication. Traffic data may include any translation of this information by the network over which the communication is transmitted for the purpose of carrying out the transmission. Traffic data may, inter alia, consist of data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection. They may also consist of the format in which the communication is conveyed by the network.

(16) Information that is part of a broadcasting service provided over a public communications network is intended for a potentially unlimited audience and does not constitute a communication in the sense of this Directive. However, in cases where the individual subscriber or user receiving such information can be identified, for example with video-on-demand services, the information conveyed is covered within the meaning of a communication for the purposes of this Directive.

(17) For the purposes of this Directive, consent of a user or subscriber, regardless of whether the latter is a natural or a legal person, should have the same meaning as the data subject's consent as defined and further specified in Directive 95/46/EC. Consent

may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website.

(18) Value added services may, for example, consist of advice on least expensive tariff packages, route guidance, traffic information, weather forecasts and tourist information.

(19) The application of certain requirements relating to presentation and restriction of calling and connected line identification and to automatic call forwarding to subscriber lines connected to analogue exchanges should not be made mandatory in specific cases where such application would prove to be technically impossible or would require a disproportionate economic effort. It is important for interested parties to be informed of such cases and the Member States should therefore notify them to the Commission.

(20) Service providers should take appropriate measures to safeguard the security of their services, if necessary in conjunction with the provider of the network, and inform subscribers of any special risks of a breach of the security of the network. Such risks may especially occur for electronic communications services over an open network such as the Internet or analogue mobile telephony. It is particularly important for subscribers and users of such services to be fully informed by their service provider of the existing security risks which lie outside the scope of possible remedies by the service provider. Service providers who offer publicly available electronic communications services over the Internet should inform users and subscribers of measures they can take to protect the security of their communications for instance by using specific types of software or encryption technologies. The requirement to inform subscribers of particular security risks does not discharge a service provider from the obligation to take, at its own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of the service. The provision of information about security risks to the subscriber should be free of charge except for any nominal costs which the subscriber may incur while receiving or collecting the information, for instance by downloading an electronic mail message. Security is appraised in the light of Article 17 of Directive 95/46/EC.

(21) Measures should be taken to prevent unauthorised access to communications in order to protect the confidentiality of communications, including both the contents and any data related to such communications, by means of public communications networks and publicly available electronic communications services. National legislation in some Member States only prohibits intentional unauthorised access to communications.

(22) The prohibition of storage of communications and the related traffic data by persons other than the users or without their consent is not intended to prohibit any automatic, intermediate and transient storage of this information in so far as this takes place for the sole purpose of carrying out the transmission in the electronic communications network and provided that the information is not stored for any period longer than is necessary for the transmission and for traffic management purposes, and that during the period of storage the confidentiality remains guaranteed. Where this is necessary for making more efficient the onward transmission of any publicly accessible information to other recipients of the service upon their request, this Directive should not prevent such information from being further stored, provided that this information

would in any case be accessible to the public without restriction and that any data referring to the individual subscribers or users requesting such information are erased.

(23) Confidentiality of communications should also be ensured in the course of lawful business practice. Where necessary and legally authorised, communications can be recorded for the purpose of providing evidence of a commercial transaction. Directive 95/46/EC applies to such processing. Parties to the communications should be informed prior to the recording about the recording, its purpose and the duration of its storage. The recorded communication should be erased as soon as possible and in any case at the latest by the end of the period during which the transaction can be lawfully challenged.

(24) Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned.

(25) However, such devices, for instance so-called "cookies", can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions. Where such devices, for instance cookies, are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using. Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. This is particularly important where users other than the original user have access to the terminal equipment and thereby to any data containing privacy-sensitive information stored on such equipment. Information and the right to refuse may be offered once for the use of various devices to be installed on the user's terminal equipment during the same connection and also covering any further use that may be made of those devices during subsequent connections. The methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible. Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose.

(26) The data relating to subscribers processed within electronic communications networks to establish connections and to transmit information contain information on the private life of natural persons and concern the right to respect for their correspondence or concern the legitimate interests of legal persons. Such data may only be stored to the extent that is necessary for the provision of the service for the purpose of billing and for interconnection payments, and for a limited time. Any further processing of such data which the provider of the publicly available electronic communications services may want to perform, for the marketing of electronic

communications services or for the provision of value added services, may only be allowed if the subscriber has agreed to this on the basis of accurate and full information given by the provider of the publicly available electronic communications services about the types of further processing it intends to perform and about the subscriber's right not to give or to withdraw his/her consent to such processing. Traffic data used for marketing communications services or for the provision of value added services should also be erased or made anonymous after the provision of the service. Service providers should always keep subscribers informed of the types of data they are processing and the purposes and duration for which this is done.

(27) The exact moment of the completion of the transmission of a communication, after which traffic data should be erased except for billing purposes, may depend on the type of electronic communications service that is provided. For instance for a voice telephony call the transmission will be completed as soon as either of the users terminates the connection. For electronic mail the transmission is completed as soon as the addressee collects the message, typically from the server of his service provider.

(28) The obligation to erase traffic data or to make such data anonymous when it is no longer needed for the purpose of the transmission of a communication does not conflict with such procedures on the Internet as the caching in the domain name system of IP addresses or the caching of IP addresses to physical address bindings or the use of log-in information to control the right of access to networks or services.

(29) The service provider may process traffic data relating to subscribers and users where necessary in individual cases in order to detect technical failure or errors in the transmission of communications. Traffic data necessary for billing purposes may also be processed by the provider in order to detect and stop fraud consisting of unpaid use of the electronic communications service.

(30) Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum. Any activities related to the provision of the electronic communications service that go beyond the transmission of a communication and the billing thereof should be based on aggregated, traffic data that cannot be related to subscribers or users. Where such activities cannot be based on aggregated data, they should be considered as value added services for which the consent of the subscriber is required.

(31) Whether the consent to be obtained for the processing of personal data with a view to providing a particular value added service should be that of the user or of the subscriber, will depend on the data to be processed and on the type of service to be provided and on whether it is technically, procedurally and contractually possible to distinguish the individual using an electronic communications service from the legal or natural person having subscribed to it.

(32) Where the provider of an electronic communications service or of a value added service subcontracts the processing of personal data necessary for the provision of these services to another entity, such subcontracting and subsequent data processing should be in full compliance with the requirements regarding controllers and processors of personal data as set out in Directive 95/46/EC. Where the provision of a value added service requires that traffic or location data are forwarded from an electronic

communications service provider to a provider of value added services, the subscribers or users to whom the data are related should also be fully informed of this forwarding before giving their consent for the processing of the data.

(33) The introduction of itemised bills has improved the possibilities for the subscriber to check the accuracy of the fees charged by the service provider but, at the same time, it may jeopardise the privacy of the users of publicly available electronic communications services. Therefore, in order to preserve the privacy of the user, Member States should encourage the development of electronic communication service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available electronic communications services, for example calling cards and facilities for payment by credit card. To the same end, Member States may ask the operators to offer their subscribers a different type of detailed bill in which a certain number of digits of the called number have been deleted.

(34) It is necessary, as regards calling line identification, to protect the right of the calling party to withhold the presentation of the identification of the line from which the call is being made and the right of the called party to reject calls from unidentified lines. There is justification for overriding the elimination of calling line identification presentation in specific cases. Certain subscribers, in particular help lines and similar organisations, have an interest in guaranteeing the anonymity of their callers. It is necessary, as regards connected line identification, to protect the right and the legitimate interest of the called party to withhold the presentation of the identification of the line to which the calling party is actually connected, in particular in the case of forwarded calls. The providers of publicly available electronic communications services should inform their subscribers of the existence of calling and connected line identification in the network and of all services which are offered on the basis of calling and connected line identification as well as the privacy options which are available. This will allow the subscribers to make an informed choice about the privacy facilities they may want to use. The privacy options which are offered on a per-line basis do not necessarily have to be available as an automatic network service but may be obtainable through a simple request to the provider of the publicly available electronic communications service.

(35) In digital mobile networks, location data giving the geographic position of the terminal equipment of the mobile user are processed to enable the transmission of communications. Such data are traffic data covered by Article 6 of this Directive. However, in addition, digital mobile networks may have the capacity to process location data which are more precise than is necessary for the transmission of communications and which are used for the provision of value added services such as services providing individualised traffic information and guidance to drivers. The processing of such data for value added services should only be allowed where subscribers have given their consent. Even in cases where subscribers have given their consent, they should have a simple means to temporarily deny the processing of location data, free of charge.

(36) Member States may restrict the users' and subscribers' rights to privacy with regard to calling line identification where this is necessary to trace nuisance calls and with regard to calling line identification and location data where this is necessary to allow emergency services to carry out their tasks as effectively as possible. For these

purposes, Member States may adopt specific provisions to entitle providers of electronic communications services to provide access to calling line identification and location data without the prior consent of the users or subscribers concerned.

(37) Safeguards should be provided for subscribers against the nuisance which may be caused by automatic call forwarding by others. Moreover, in such cases, it must be possible for subscribers to stop the forwarded calls being passed on to their terminals by simple request to the provider of the publicly available electronic communications service.

(38) Directories of subscribers to electronic communications services are widely distributed and public. The right to privacy of natural persons and the legitimate interest of legal persons require that subscribers are able to determine whether their personal data are published in a directory and if so, which. Providers of public directories should inform the subscribers to be included in such directories of the purposes of the directory and of any particular usage which may be made of electronic versions of public directories especially through search functions embedded in the software, such as reverse search functions enabling users of the directory to discover the name and address of the subscriber on the basis of a telephone number only.

(39) The obligation to inform subscribers of the purpose(s) of public directories in which their personal data are to be included should be imposed on the party collecting the data for such inclusion. Where the data may be transmitted to one or more third parties, the subscriber should be informed of this possibility and of the recipient or the categories of possible recipients. Any transmission should be subject to the condition that the data may not be used for other purposes than those for which they were collected. If the party collecting the data from the subscriber or any third party to whom the data have been transmitted wishes to use the data for an additional purpose, the renewed consent of the subscriber is to be obtained either by the initial party collecting the data or by the third party to whom the data have been transmitted.

(40) Safeguards should be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS messages. These forms of unsolicited commercial communications may on the one hand be relatively easy and cheap to send and on the other may impose a burden and/or cost on the recipient. Moreover, in some cases their volume may also cause difficulties for electronic communications networks and terminal equipment. For such forms of unsolicited communications for direct marketing, it is justified to require that prior explicit consent of the recipients is obtained before such communications are addressed to them. The single market requires a harmonised approach to ensure simple, Community-wide rules for businesses and users.

(41) Within the context of an existing customer relationship, it is reasonable to allow the use of electronic contact details for the offering of similar products or services, but only by the same company that has obtained the electronic contact details in accordance with Directive 95/46/EC. When electronic contact details are obtained, the customer should be informed about their further use for direct marketing in a clear and distinct manner, and be given the opportunity to refuse such usage. This opportunity should

continue to be offered with each subsequent direct marketing message, free of charge, except for any costs for the transmission of this refusal.

(42) Other forms of direct marketing that are more costly for the sender and impose no financial costs on subscribers and users, such as person-to-person voice telephony calls, may justify the maintenance of a system giving subscribers or users the possibility to indicate that they do not want to receive such calls. Nevertheless, in order not to decrease existing levels of privacy protection, Member States should be entitled to uphold national systems, only allowing such calls to subscribers and users who have given their prior consent.

(43) To facilitate effective enforcement of Community rules on unsolicited messages for direct marketing, it is necessary to prohibit the use of false identities or false return addresses or numbers while sending unsolicited messages for direct marketing purposes.

(44) Certain electronic mail systems allow subscribers to view the sender and subject line of an electronic mail, and also to delete the message, without having to download the rest of the electronic mail's content or any attachments, thereby reducing costs which could arise from downloading unsolicited electronic mails or attachments. These arrangements may continue to be useful in certain cases as an additional tool to the general obligations established in this Directive.

(45) This Directive is without prejudice to the arrangements which Member States make to protect the legitimate interests of legal persons with regard to unsolicited communications for direct marketing purposes. Where Member States establish an opt-out register for such communications to legal persons, mostly business users, the provisions of Article 7 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on electronic commerce)(6) are fully applicable.

(46) The functionalities for the provision of electronic communications services may be integrated in the network or in any part of the terminal equipment of the user, including the software. The protection of the personal data and the privacy of the user of publicly available electronic communications services should be independent of the configuration of the various components necessary to provide the service and of the distribution of the necessary functionalities between these components. Directive 95/46/EC covers any form of processing of personal data regardless of the technology used. The existence of specific rules for electronic communications services alongside general rules for other components necessary for the provision of such services may not facilitate the protection of personal data and privacy in a technologically neutral way. It may therefore be necessary to adopt measures requiring manufacturers of certain types of equipment used for electronic communications services to construct their product in such a way as to incorporate safeguards to ensure that the personal data and privacy of the user and subscriber are protected. The adoption of such measures in accordance with Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity(7) will ensure that the introduction of technical features

of electronic communication equipment including software for data protection purposes is harmonised in order to be compatible with the implementation of the internal market.

(47) Where the rights of the users and subscribers are not respected, national legislation should provide for judicial remedies. Penalties should be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive.

(48) It is useful, in the field of application of this Directive, to draw on the experience of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data composed of representatives of the supervisory authorities of the Member States, set up by Article 29 of Directive 95/46/EC.

(49) To facilitate compliance with the provisions of this Directive, certain specific arrangements are needed for processing of data already under way on the date that national implementing legislation pursuant to this Directive enters into force,

HAVE ADOPTED THIS DIRECTIVE:

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

Article 3

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.
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.

Article 4

Security

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.

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.

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.

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.

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.
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.
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.
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.

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 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.

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.

Article 13

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 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 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).

Article 15

Application of certain provisions of Directive 95/46/EC

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.

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.

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.

2003 No.

ELECTRONIC COMMUNICATIONS

**The Privacy and Electronic Communications (EC Directive)
Regulations 2003**

<i>Made - - - - -</i>	<i>2003</i>
<i>Laid before Parliament</i>	<i>2003</i>
<i>Coming into force - -</i>	<i>2003</i>

The Secretary of State, being a Minister designated(a) for the purposes of section 2(2) of the European Communities Act 1972(b) in respect of matters relating to electronic communications, in exercise of the powers conferred upon her by that section, hereby makes the following Regulations:

Citation and commencement

1. These Regulations may be cited as the Privacy and Electronic Communications (EC Directive) Regulations 2003 and shall come into force on **[enter date of coming into force]**.

Interpretation

2. —(1) In these Regulations –

“bill” includes an invoice, account, statement or other document of similar character and “billing” shall be construed accordingly;

“call” means a connection established by means of a telephone service available to the public allowing two-way communication in real time;

“communication” means any information exchanged or conveyed between a finite number of parties by means of a public electronic communications service, but does not include information conveyed as part of a programme service, except to the extent that such information can be related to the identifiable subscriber or user receiving the information.

“communications provider” has the meaning given by section [398] of the [Communications Act 2003](c);

“corporate subscriber” means a subscriber who is not an individual, that is to say a subscriber who is –

- (a) a company within the meaning of section 735(1) of the Companies Act 1985 (d);
- (b) a company incorporated in pursuance of a royal charter or letters patent;

(a) S.I. 2001/3495.
(b) 1972 c.68.
(c) [2003]
(d) 1985 c.6.

- (c) a partnership in Scotland;
- (d) a corporation sole; or
- (e) any other body corporate or other entity which is a legal person distinct from the individuals (if any) of which it is composed.

“the Directive” means Directive 2002/58/EC of the European Parliament and of the Council of the European Union **(a)**;

“electronic communications network” has the meaning given by section [29] of the [Communications Act 2003];

“electronic communications service” has the meaning given by section [29] of the [Communications Act 2003];

“electronic mail” means any text, voice, sound or image message sent over a public electronic communications network which can be stored in the network or in the recipient’s terminal equipment until it is collected by the recipient and includes messages sent using a short message service;

“individual” means a living individual and includes an unincorporated body of such individuals;

“the Information Commissioner” and “the Commissioner” both mean the Commissioner appointed under section 6 of the Data Protection Act 1998**(b)**;

“information society service” has the meaning given in the Electronic Commerce (EC Directive) Regulations 2002**(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 public electronic communications service, including data relating to the:

- (a) latitude, longitude or altitude of the terminal equipment;
- (b) direction of travel of the user; or
- (c) time the location information was recorded.

“OFCOM” means the Office of Communications;

“programme service” has the meaning given in section 201 of the Broadcasting Act 1990**(d)**;

“public communications provider” means a provider of a public electronic communications network or a public electronic communications service;

“public electronic communications service” has the meaning given in section [148] the [Communications Act 2003];

“public electronic communications network” has the meaning given in section [148] of the [Communications Act 2003];

“subscriber” means a person who is a party to a contract with a provider of public electronic communications services for the supply of such services;

“traffic data” means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing of that communication and includes data relating to the routing, duration or time of a communication;

(a) OJ No. L 201, 31.07.2002, p.37.

(b) 1998 c.29; section 6 was amended by the Freedom of Information Act 2000 (c.36), section 18.

(c) S.I. 2002/2013

(d) 1990 c.42; section 201 was amended by the Broadcasting Act 1996 (c.), section 148(1), Schedule 10, paragraph 11.

“user” means any individual using a public electronic communications service;

“value added service” means any service which requires the processing of traffic data or location data beyond that which is necessary for the transmission of a communication or the billing of that communication.

(2) Expressions used in these Regulations that are not defined in paragraph (1) and are defined in the Data Protection Act 1998 shall have the same meaning as in that Act.

(3) Terms defined in the Directive that are not defined in paragraph (1) or in the Data Protection Act 1998 have the same meaning as in the Directive.

(4) Any reference in these Regulations to a line shall, without prejudice to the effect of paragraph (3), be construed as including a reference to anything that performs the function of a line, and “connected”, in relation to a line, is to be construed accordingly.

(5) Any reference to direct marketing in these Regulations is a reference to the communication of any advertising or marketing material on a particular line.

Revocation of the Telecommunications (Data Protection and Privacy) Regulations 1999

3. The Telecommunications (Data Protection and Privacy) Regulations 1999^(a) and the Telecommunications (Data Protection and Privacy) (Amendment) Regulations 2000^(b) are revoked.

Security of public electronic communications services

4. —(1) Subject to paragraph (2), a provider of a public electronic communications service (“the service provider”) shall take appropriate technical and organisational measures to safeguard the security of that service.

(2) If necessary, the measures required by paragraph (1) may be taken by the service provider in conjunction with the provider of the electronic communications network by means of which the service is provided, and that network provider shall comply with any reasonable requests made by the service provider for these purposes.

(3) Where, notwithstanding the taking of measures as required by paragraph (1), there remains a significant risk to the security of the electronic communications service, the service provider shall inform the subscribers concerned of:

- (a) the nature of that risk;
- (b) any appropriate measures that the subscriber may take to safeguard against that risk; and
- (c) the likely costs to the subscriber involved in the taking of such measures.

(4) For the purposes of paragraph (1), a measure shall only be taken to be appropriate if having regard to -

- (a) the state of technological developments; and
- (b) the cost of implementing the measure,

^(a) S.I. 1999/2093

^(b) S.I. 2000/157

it is proportionate to the risks against which it would safeguard.

(5) Information provided for the purposes of paragraph (3) shall be provided to the subscriber free of any charge other than the cost incurred by the subscriber in respect of the receipt or collection of the information by him.

Confidentiality of communications

5. — (1) A person shall not use an electronic communications network to store information, or to gain access to information stored, in the terminal equipment of a subscriber or user, unless the requirements of paragraph (2) are met.

(2) The requirements are that the subscriber or user of that terminal equipment is:

- (a) provided with clear and comprehensive information about the purposes of the storage of, or access to, such information; and
- (b) given the opportunity to refuse the storage of or access to such information.

(3) Where an electronic communications network is used by the same person to store or access information in the terminal equipment of a subscriber or user on more than one occasion, it is sufficient for the purposes of this regulation that the requirements of paragraph (2) are met in respect of the initial use.

(4) Paragraph (1) shall not apply to the technical storage of, or access to, information:

- (a) for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network; or
- (b) where such storage or access is strictly necessary for the provision of an information society service requested by the subscriber or user.

Restrictions on the processing of certain traffic data

6. —(1) Subject to paragraphs (2) and (3) of this regulation, traffic data relating to subscribers or users which is processed and stored by a public communications provider shall, when no longer required for the purpose of the transmission of a communication, be -

- (a) erased;
- (b) in the case of an individual, modified so that it ceases to constitute personal data of that subscriber or user; or
- (c) in the case of a corporate subscriber, modified so that it ceases to be data that would be personal data if that subscriber was an individual.

(2) Traffic data held by a public communications provider for purposes connected with the payment of charges by a subscriber or in respect of interconnection payments may be processed and stored by that provider until the time specified in paragraph (5).

(3) Traffic data relating to a subscriber or user may be processed and stored by a provider of a public electronic communications service —

- (a) if such processing and storage is for the purpose of marketing electronic communications services or for the provision of value added services to that subscriber or user;

(b) the subscriber or user to whom the traffic data relates has given his consent to such processing or storage; and

(c) such processing and storage is undertaken only for the duration necessary for the purposes specified in subparagraph (a).

(4) Where a user or subscriber has given his consent in accordance with paragraph (3), he shall be able to withdraw it at any time.

(5) The time referred to in paragraph (2) shall be the end of the period during which legal proceedings may be brought in respect of payments due or alleged to be due or, where such proceedings are brought within that period, the time when those proceedings are finally determined.

(6) Legal proceedings shall not be taken to be finally determined -

(a) until the end of the ordinary time for an appeal by either party, if no appeal is brought within that time; or

(b) if an appeal is brought, until the conclusion of the appeal.

(7) References in paragraph (6) to an appeal include references to an application for leave to appeal.

Further provisions relating to the processing of traffic data under Regulation 6

7. —(1) Processing of traffic data in accordance with regulation 6(2) or (3) shall not be undertaken by a public communications provider unless the subscriber or user to whom the data relates has been provided with information regarding the types of traffic data which are to be processed and the duration of such processing and, in the case of processing in accordance with regulation 6(3), he has been provided with that information before his consent has been obtained.

(2) Processing of traffic data in accordance with regulation 6 shall be restricted to what is required for the purposes of one or more of the activities listed in paragraph (3) and shall be carried out only by the public communications provider or by a person acting under the authority of that provider.

(3) The activities referred to in paragraph (2) are activities relating to:

(a) the management of billing or traffic;

(b) customer enquiries;

(c) the prevention or detection of fraud;

(d) the marketing of electronic communications services; or

(e) the provision of a value added service.

(4) Nothing in these Regulations shall prevent the furnishing of traffic data to a person who is a competent authority for the purposes of any provision relating to the settling of disputes (by way of legal proceedings or otherwise), which is contained in, or made by virtue of, any enactment.

Itemised billing and privacy

8. —(1) At the request of a subscriber, a provider of a public electronic communications service shall provide that subscriber with bills that are not itemised.

(2) The Secretary of State and OFCOM shall each have a duty, when exercising their functions under Chapter 1 of Part 2 of the [Communications Act 2003], to have regard to the need to reconcile the rights of subscribers receiving itemised bills with the rights to privacy of calling users and called subscribers, including the need for sufficient alternative privacy-enhancing methods of communications or payments to be available to such users and subscribers.

Prevention of calling line identification – outgoing calls

9. —(1) This regulation applies, subject to regulations 14 and 15, to outgoing calls, where a facility enabling the presentation of calling line identification is available.

(2) The provider of a public electronic communications service shall provide users originating a call by means of that service with a simple means to prevent presentation of the identity of the calling line on the connected line as respects that call.

(3) The provider of a public electronic communications service shall provide subscribers to the service, as respects their line and all calls originating from that line, with a simple means of preventing presentation of the identity of that subscriber’s line on any connected line.

(4) The measures to be provided under paragraphs (2) and (3) shall be provided without charge.

Prevention of calling or connected line identification – incoming calls

10. —(1) This regulation applies to incoming calls.

(2) Where a facility enabling the presentation of calling line identification is available, the provider of a public electronic communications service shall provide the called subscriber with a simple means to prevent, without charge for reasonable use of the facility, presentation of the identity of the calling line on the connected line.

(3) Where a facility enabling the presentation of calling line identification prior to the call being established is available, the provider of a public electronic communications service shall provide the called subscriber with a simple means of rejecting incoming calls where the presentation of the calling line identification has been prevented by the calling user or subscriber.

(4) Where a facility enabling the presentation of connected line identification is available, the provider of a public electronic communications service shall provide the called subscriber with a simple means to prevent, without charge, presentation of the identity of the connected line on any calling line.

(5) In this regulation “called subscriber” means the subscriber receiving a call by means of the service in question whose line is the called line (whether or not it is also the connected line).

Publication of information for the purposes of Regulations 9 and 10

11. Where a provider of a public electronic communications service provides facilities for calling or connected line identification, he shall provide information to the public regarding the availability of such facilities, including information regarding the options to be made available for the purposes of regulations 9 and 10.

Co-operation of communications providers for the purposes of Regulations 9 and 10

12. For the purposes of regulations 9 and 10, a communications provider shall comply with any reasonable requests made by the provider of the public electronic communications service by means of which facilities for calling or connected line identification are provided.

Restrictions on the processing of location data

13. —(1) Location data relating to users or subscribers of public electronic communications networks or public electronic communications services may only be processed:

- (a) where the user or subscriber cannot be identified from such data; or
- (b) where necessary for the provision of a value added service, with the consent of the user or subscriber to whom the data relates.

(2) Prior to obtaining the consent of the user or subscriber under paragraph (1)(b), the public communications provider in question must provide the following information to the user or subscriber to whom the data relates:

- (a) the types of location data that will be processed;
- (b) the purposes and duration of the processing of that data; and
- (c) whether the data will be transmitted to a third party for the purpose of providing the value added service.

(3) A user or subscriber who has given his consent to the processing of data under paragraph (1)(b) shall, in respect of each connection to the public electronic communications network in question or each transmission of a communication, be given the opportunity to withdraw such consent, using a simple means and without charge.

(4) Processing of location data in accordance with this regulation shall —

- (a) only be carried out by —
 - (i) the public communications provider in question;
 - (ii) the third party providing the value added service in question; or
 - (iii) a person acting under the authority of a person falling within (i) or (ii); and
- (b) be restricted to what is necessary for the purposes of providing the value added service in question.

(5) This regulation shall not apply to the processing of traffic data.

Tracing of malicious or nuisance calls

14. —(1) A communications provider may override anything done to prevent the presentation of the identity of a calling line where —

- (a) a subscriber has requested the tracing of malicious or nuisance calls received on his line; and

(b) the provider is satisfied that such action is necessary and expedient for the purposes of tracing such calls.

(2) Any term of a contract for the provision of public electronic communications services which relates to such prevention shall have effect subject to the provisions of paragraph (1).

(3) Nothing in these Regulations shall prevent a communications provider, for the purposes of any action relating to the tracing of malicious or nuisance calls, from storing and making available to competent authorities data containing the identity of a calling subscriber which were obtained while paragraph (1) applied.

Emergency calls

15.—(1) For the purposes of these Regulations, “emergency calls” means calls to either the national emergency call number 999 or the single European emergency call number 112.

(2) In order to facilitate responses to emergency calls:

- (a) all such calls shall be excluded from the requirements of regulation 9;
- (b) no person shall be entitled to prevent the presentation on the connected line of the identity of the calling line; and
- (c) the restriction on the processing of location data under regulation 13(1) shall be disregarded.

Termination of automatic call forwarding

16. —(1) Where –

- (a) calls originally directed to another line are being automatically forwarded to a subscriber’s line as a result of action taken by a third party; and
- (b) the subscriber requests the provider of electronic communications services to him (“the subscriber’s provider) to stop the forwarding of those calls,

the subscriber’s provider shall ensure, without charge, that the forwarding is stopped without any avoidable delay.

(2) For the purposes of paragraph (1), every other communications provider shall comply with any reasonable requests made by the subscriber’s provider to assist in the prevention of the calls being forwarded.

Directories of subscribers

17. —(1) This regulation applies in relation to a directory of subscribers, whether in printed or electronic form, which is made available to members of the public or a section of the public, including by means of a directory enquiry service.

(2) The personal data of an individual subscriber shall not be included in a directory unless that subscriber has, without charge:

(a) been informed by the collector of the personal data of the purposes of the directory in which his personal data is to be included; and

(b) consented to the inclusion of such of his personal data in the directory as are considered relevant by the producer of the directory.

(3) Where personal data of an individual subscriber is to be included in a directory with facilities which enable users of that directory to obtain access to that data solely on the basis of a telephone number –

(a) the information to be provided under paragraph(2)(a) shall include information about that facility; and

(b) for the purposes of paragraph (2)(b), the express consent of the subscriber to the inclusion of his data in a directory with such facilities must be obtained.

(4) Data relating to a corporate subscriber shall not be included in a directory where that subscriber has advised the producer of the directory that he does not want his data to be included in that directory.

(5) Where the data of an individual subscriber has been included in a directory, that subscriber shall, without charge, be able to verify, correct or withdraw that data at any time.

(6) Where a request has been made under paragraph (5) for data to be withdrawn from a directory, that request shall be treated as having no application in relation to an edition of a directory that was produced before the producer of the directory received the request.

(7) For the purposes of paragraph (6), an edition of a directory, which is revised after it was first produced, shall be treated as a new edition.

(8) In this regulation, “telephone number” has the same meaning as in [section 53(5)] of the [Communications Act 2003].

Use of automated calling systems for direct marketing purposes

18.—(1) A person shall not transmit, or instigate the transmission of, communications comprising recorded matter for direct marketing purposes by means of an automated calling system except in the circumstances referred to in paragraph (2).

(2) Those circumstances are where the called line is that of a subscriber who has previously notified the caller that for the time being he consents to such communications being sent by, or at the instigation of, the caller on that line.

(3) A subscriber shall not permit his line to be used in contravention of paragraph (1).

(4) For the purposes of this regulation, an automated calling system is a system which is capable of:

(a) automatically initiating a sequence of calls to more than one destination in accordance with instructions stored in that system; and

(b) transmitting sounds which are not live speech for reception by persons at some or all of the destinations so called.

Use of facsimile machines for direct marketing purposes

19.—(1) A person shall not transmit, or instigate the transmission of, unsolicited communications for direct marketing purposes by means of a facsimile machine where the called line is that of –

- (a) an individual subscriber, except in the circumstances referred to in paragraph (2);
- (b) a corporate subscriber who has previously notified the caller that such unsolicited communications should not be sent on that line; or
- (c) a corporate subscriber and the number allocated to that line is listed in the register kept under regulation 23.

(2) The circumstances referred to in paragraph (1)(a) are that the individual subscriber has previously advised the caller that he consents for the time being to such communications being sent by, or at the instigation of, that caller.

(3) For the purposes of paragraph (1), a communication on a subscriber's line shall not be treated as an unsolicited communication if that subscriber has notified the caller that he does not object to such communications being made by, or at the instigation of, the caller for direct marketing purposes on that line.

(4) A subscriber shall not permit his line to be used in contravention of paragraph (1).

(5) A person shall not be held to have contravened sub-paragraph (1)(c) where the number allocated to the called line has been listed on the register for less than 28 days preceding that on which the communication is made.

(6) The provisions of this regulation are without prejudice to the provisions of regulation 18.

Unsolicited calls for direct marketing purposes

20.—(1) A person shall not use, or instigate the use of, a public electronic communications service for the purposes of making unsolicited calls for direct marketing purposes where-

- (a) the called line is that of a subscriber who has previously notified the caller that such unsolicited calls should not for the time being be made on that line, or
- (b) the number allocated to a subscriber in respect of the called line is one listed in the register kept under regulation 23.

(2) A subscriber shall not permit his line to be used in contravention of paragraph (1).

(3) For the purposes of paragraph (1), a call on a subscriber's line shall not be treated as an unsolicited call if that subscriber has notified the caller that he does not object to calls being made by, or at the instigation of, the caller for direct marketing purposes on that line.

(4) A person shall not be held to have contravened sub-paragraph (1)(b), where the number allocated to the called line has been listed on the register for less than 28 days preceding that on which the call is made.

Use of electronic mail for direct marketing purposes

21. —(1) This regulation applies to the transmission of unsolicited communications by means of electronic mail to individual subscribers.

(2) Except in the circumstances referred to in paragraph (3), a person shall not transmit, or instigate the transmission of, unsolicited communications, for the purposes of direct marketing, by means of electronic mail, unless –

(a) the recipient of the electronic mail has previously notified the sender that he consents for the time being to such communications being sent by, or at the instigation of, the sender for direct marketing purposes; and

(b) the requirements of paragraph (4) are met.

(3) A person may send or instigate the sending of electronic mail for the purposes of direct marketing where –

(a) that person has obtained the contact details of the recipient of that electronic mail in the course of the sale or negotiations for the sale of a product or service to that recipient;

(b) the direct marketing is in respect of that person's products or services only and that person has taken reasonable steps to ensure that the recipient is aware of the nature of those products and services;

(c) the recipient has been given a simple means, without charge, of refusing the use of his contact details for the purposes of such direct marketing at the time that the details were initially collected, and where he did not initially refuse the use of the details, at the time of each subsequent communication; and

(d) the requirements of paragraph (4) are met.

(4) For the purposes of sub-paragraphs (2)(b) and (3)(d), the requirements are:

(a) the identity of the sender, or the person on whose behalf the communication is made, has not been disguised or concealed; and

(b) the recipient is provided with a valid address to which the recipient may send a request for such communications to cease.

(5) A subscriber shall not permit his line to be used in contravention of paragraph (2).

(6) For the purposes of this Regulation, a communication shall not be treated as an unsolicited communication if the recipient has notified the sender that he does not object to communications being sent, or at the instigation of, the sender for direct marketing purposes.

Information to be provided for the purposes of Regulations 18, 19 and 20

22. —(1) Where a public electronic communications service is used for the transmission of a communication for direct marketing purposes the person using, or instigating the use of, the services shall ensure that the following information is provided with that communication –

- (a) in relation to a communication to which regulations 18 (automated calling systems) and 19 (facsimile machines) apply, the particulars mentioned in paragraph (2)(a) and (b);
- (b) in relation to a communication to which regulation 20 (telephone calls) applies, the particulars mentioned in paragraph (2)(a), and, if the recipient of the call so requests, those mentioned in paragraph (2)(b).

(2) The particulars referred to in paragraph (1) are –

- (a) the name of the person;
- (b) either the address of the person or a telephone number on which he can be reached free of charge.

Records to be kept under Regulations 19 and 20

[Details of the register to be kept under regulations 19 and 20 are yet to be determined]

23.

Modification of contracts

24. To the extent that any term in a contract between –

- (a) a subscriber to and the provider of a public electronic communications service; or
 - (b) such a provider and the provider of an electronic communications network,
- would be inconsistent with a requirement of these Regulations, that term shall be void.

National security

25. —(1) Nothing in these Regulations shall require a communications provider to do, or refrain from doing, anything (including the processing of data) if exemption from the requirement in question is required for the purpose of safeguarding national security.

(2) Subject to paragraph (4), a certificate signed by a Minister of the Crown certifying that exemption from any requirement of these Regulations is or at any time was required for the purpose of safeguarding national security shall be conclusive evidence of that fact.

(3) A certificate under paragraph (2) may identify the circumstances in which it applies by means of a general description and may be expressed to have prospective effect.

(4) Any person directly affected by the issuing of a certificate under paragraph (2) may appeal to the Tribunal against the issuing of the certificate.

(5) If on an appeal under paragraph (4), the Tribunal finds that, applying the principles applied by a court on an application for judicial review, the Minister did not have reasonable grounds for issuing the certificate, the Tribunal may allow the appeal and quash the certificate.

(6) Where in any proceedings under or by virtue of these Regulations it is claimed by a communications provider that a certificate under paragraph (2) which identifies the circumstances in

which it applies by means of a general description applies in the circumstances in question, any other party to the proceedings may appeal to the Tribunal on the ground that the certificate does not apply in those circumstances and, subject to any determination under paragraph (7), the certificate shall be conclusively presumed so to apply.

(7) On any appeal under paragraph (6), the Tribunal may determine that the certificate does not so apply.

(8) In this regulation –

(a) "the Tribunal" means the Information Tribunal referred to in section 6 of the Data Protection Act 1998;

(b) Subsections (8), (9), (10) and (12) of section 28 and Schedule 6 of that Act apply for the purposes of this regulation as they apply for the purposes of section 28;

(c) section 58 of that Act shall apply for the purposes of this regulation as if the reference in that section to the functions of the Tribunal under that Act included a reference to the functions of the Tribunal under paragraphs (4) to (7) of this regulation; and

(d) subsections (1), (2) and (5)(f) of section 67 of that Act shall apply in respect of the making of rules relating to the functions of the Tribunal under this regulation.

Legal requirements, law enforcement etc.

26. —(1) Nothing in these Regulations shall require a communications provider to do, or refrain from doing, anything (including the processing of data) –

(a) if compliance with the requirement in question –

(i) would be inconsistent with any requirement imposed by or under an enactment or by a court order; or

(ii) would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders; or

(b) if exemption from the requirement in question -

(i) is required for the purposes of, or in connection with, any legal proceedings (including prospective legal proceedings);

(ii) is necessary for the purposes of obtaining legal advice; or

(iii) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

Compensation for failure to comply with requirements of Regulations

27. —(1) A person who suffers damage by reason of any contravention of any of the requirements of these Regulations by any other person shall be entitled to compensation from that other person for that damage.

(2) In proceedings brought against a person by virtue of this regulation it shall be a defence to prove that he had taken such care as in all the circumstances was reasonably required to comply with the relevant requirement.

Enforcement—extension of Part V of the Data Protection Act 1998

28. —(1) The provisions of Part V of the Data Protection Act 1998 and of Schedules 6 and 9 to that Act are extended for the purposes of these Regulations and, for those purposes, shall have effect subject to the omissions and other modifications set out in Schedule 1.

(2) In regulations 29 and 30, “enforcement functions” means the functions of the Information Commissioner under the provisions referred to in paragraph (1) as extended by that paragraph.

(3) The provisions of this regulation and those of regulation 27 are without prejudice to each other.

Request that Commissioner exercise his enforcement functions

29. Where it is alleged that there has been contravention of any of the requirements of these Regulations either OFCOM or a person aggrieved by the alleged contravention may request the Commissioner to exercise his enforcement functions in respect of that contravention, but those functions shall be exercisable by the Commissioner whether or not he has been so requested.

Technical advice to Commissioner

30. OFCOM shall comply with any reasonable request made by the Commissioner, in connection with his enforcement functions, for advice on technical and similar matters relating to electronic communications.

Amendment to section 11 of the Data Protection Act 1998

31. In section 11 of the Data Protection Act 1998 (rights to prevent processing for purposes of direct marketing), for subsection (2A) there shall be substituted —

“(2A) This section shall not apply in relation to the processing of traffic data (within the meaning of the Privacy and Electronic Communications (EC Directive) Regulations 2003) for the purposes mentioned in regulation 6(3) of those Regulations.”

Amendment to the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

32. —(1) In regulation 3 of the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000(a), for paragraph (3), there shall be substituted —

“(3) Conduct falling within paragraph (1)(a)(i) above is authorised only to the extent that Article 5 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector so permits.”

Transitional provisions

33. The provisions in Schedule 2 shall have effect.

(a) S.I. 2000/2699

SCHEDULE I

MODIFICATIONS TO PART V OF THE DATA PROTECTION ACT 1998 AND SCHEDULES 6
AND 9 TO THAT ACT AS EXTENDED BY REGULATION 28

Regulation 28

1

In section 40—

(a) in subsection (1), for the words “data controller” there shall be substituted the word “person”, for the words “data protection principles” there shall be substituted the words “requirements of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (in this Part referred to as “the relevant requirements”)” and for the words “principle or principles” there shall be substituted the words “requirement or requirements”;

(b) in subsection (2), the words “or distress” shall be omitted;

(c) subsections (3), (4), (5), (9) and (10) shall be omitted; and

(d) in subsection (6)(a), for the words “data protection principle or principles” there shall be substituted the words “relevant requirement or requirements”.

2

In section 41, for the words “data protection principle or principles”, in both places where they occur, there shall be substituted the words “relevant requirement or requirements”.

3

Section 42 shall be omitted.

4

In section 43—

(a) for subsections (1) and (2) there shall be substituted the following provisions—

“(1) If the Commissioner reasonably requires any information for the purpose of determining whether a person has complied or is complying with the relevant requirements, he may serve that person with a notice (in this Act referred to as “an information notice”) requiring him, within such time as is specified in the notice, to furnish the Commissioner, in such form as may be so specified, with such information relating to compliance with the relevant requirements as is so specified.

(2) An information notice must contain a statement that the Commissioner regards the specified information as relevant for the purpose of determining whether the person has complied, or is complying, with the relevant requirements and his reason for regarding it as relevant for that purpose.”;

(b) in subsection (6)(a), after the word “under” there shall be inserted the words “the Privacy and Electronic Communications (EC Directive) Regulations 2003 or”;

(c) in subsection (6)(b), after the words “arising out of” there shall be inserted the words “the said Regulations or”;

(d) subsection (10) shall be omitted.

5

Sections 44, 45 and 46 shall be omitted.

6

In section 47(1) and (2), for the words “an information notice or a special information notice”, in both places where they occur, there shall be substituted the words “or an information notice”.

7

In section 48—

(a) in subsections (1) and (3), for the words “an information notice or a special information notice”, in both places where they occur, there shall be substituted the words “or an information notice”;

(b) in subsection (3) for the words “43(5) or 44(6)” there shall be substituted the words “or 43(5)”;

(c) subsection (4) shall be omitted.

8

In section 49, subsection (5) shall be omitted.

9

In paragraph 4(1) of Schedule 6, for the words “(2) or (4)” there shall be substituted the words “or (2)”.

10

In paragraph 1 of Schedule 9—

(a) for sub-paragraph (1)(a) there shall be substituted the following provision—

“(a) that a person has contravened or is contravening any of the requirements of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (in this Schedule referred to as “the 2003 Regulations”), or”,

and

(b) sub-paragraph (2) shall be omitted.

11

In paragraph 9 of Schedule 9—

(a) in sub-paragraph (1)(a), after the words “rights under” there shall be inserted the words “the 2003 Regulations or”, and

(b) in sub-paragraph (1)(b), after the words “arising out of” there shall be inserted the words “the 2003 Regulations or”.

SCHEDULE 2
TRANSITIONAL PROVISIONS

Regulation 33

Interpretation

1

In this Schedule “the 1999 Regulations” means the Telecommunications (Data Protection and Privacy) Regulations 1999 and “caller” has the same meaning as in regulation 21 of the 1999 Regulations.

Directories

2

(1) Regulation 17 shall not apply in relation to editions of directories first published before **[enter date that regulation is to come into force]**.

(2) Where the personal data of a subscriber has been included in a directory in accordance with Part IV of the 1999 Regulations, the personal data of that subscriber may remain included in that directory provided that the subscriber —

- (a) has been provided with information in accordance with regulation 17 of these Regulations; and
- (b) has not requested that his data be withdrawn from that directory.

(3) Where a request has been made under paragraph 1(2) for data to be withdrawn from a directory, that request shall be treated as having no application in relation to an edition of a directory that was produced before the producer of the directory received the request.

(4) For the purposes of paragraph 1(3), an edition of a directory, which is revised after it was first produced, shall be treated as a new edition.

Notifications

3

(1) A notification of consent given to a caller by a subscriber for the purposes of regulation 22(2) of the 1999 Regulations is to have effect on and after the **[enter date that regulation is to come into force]** as a notification given by that subscriber for the purposes of regulation 18(2) of these Regulations.

(2) A notification given to a caller by a corporate subscriber for the purposes of regulation 23(2)(a) of the 1999 Regulations is to have effect on and after the **[enter date that regulation is to come into force]** as a notification given by that subscriber for the purposes of regulation 19(1)(b) of these Regulations.

- (3) A notification of consent given to a caller by an individual subscriber for the purposes of regulation 24(2) of the 1999 Regulations is to have effect on and after the **[enter date that regulation is to come into force]** as a notification given by that subscriber for the purposes of regulation 19(2) of these Regulations.
- (4) A notification given to a caller by a subscriber for the purposes of regulation 23(3) of the 1999 Regulations is to have effect on and after the **[enter date that regulation is to come into force]** as a notification given by that subscriber for the purposes of regulation 19(3) of these Regulations.
- (5) A notification given to a caller by an individual subscriber for the purposes of regulation 25(2)(a) of the 1999 Regulations is to have effect on and after the **[enter date that regulation is to come into force]** as a notification given by that subscriber for the purposes of regulation 20(1) of these Regulations.
- (6) A notification given to a caller by an individual subscriber for the purposes of regulation 25(3) of the 1999 Regulations is to have effect and after the **[enter date that regulation is to come into force]** as a notification given by that subscriber for the purposes of regulation 20(3) of these Regulations.

Register kept for the purposes of regulation 23

4

[It will be necessary to include transitional provisions regarding the register kept under the 1999 Regulations once the final details of the register to be kept under regulation 23 have been determined.]

Data Protection Act 1998
Legal advice

Telecoms Guidance

CONTENTS

1. Background
2. Definitions
3. Traffic and Billing Data
4. Calling or Connected Line Identification
5. Directories of Subscribers
6. Direct Marketing
7. Security
8. Legal Requirements
9. Compensation and Enforcement

1. BACKGROUND

- 1.1** Directive 97/66/EC (which was originally known as the ISDN Directive) concerning the processing of personal data and the protection of privacy in the telecommunications sector was adopted on 15 December 1997.
- 1.2** It supplements Directive 95/46/EC (the “Directive”) which covers “the rights and freedoms of natural persons with regard to the processing of personal data”, the provisions of which are implemented in UK law by the Data Protection Act 1998 (the “Act”).
- 1.3** The main aims of Directive 97/66/EC (the “Telecoms Directive”) are to ensure the “protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the telecommunications sector and to ensure the free movement of such data and of telecommunications services in the Community”^a and to work towards technical standardisation between Member States in the field of telecommunications equipment.^b
- 1.4** The Telecommunications (Data Protection and Privacy) Regulations 1999 (the “Regulations”) came into force on 1 March 2000, the same day as the Act. They revoke the Telecommunications (Data Protection and Privacy) (Direct Marketing) Regulations 1998 (the “Direct Marketing Regulations”), which came into force on 1 May 1999 and which had already implemented part of the Telecoms Directive. The Direct Marketing Regulations had been implemented in advance of the Regulations to deal with what was regarded as the most pressing consumer concerns, namely, the sending of marketing faxes and the making of unsolicited direct marketing calls.^c
- 1.5** The Regulations repeat the provisions about direct marketing contained in the Direct Marketing Regulations and they also deal with limitations on the processing of traffic and billing data, calling or connected line identification and directories of subscribers, all of which will be dealt with in this guidance.
- 1.6** Enforcement of the Regulations will be by the Data Protection Commissioner either on her own initiative, or at the request of the Director General of Telecommunications or a person aggrieved by the alleged contravention.^d

a Article 1
b Article 13
c Article 12
d Regulations 36 & 37

- 1.7** The Telecoms Directive indicates that the Regulations are particularly designed to cover the Integrated Services Digital Network (ISDN), the public digital mobile networks, video on demand and interactive television. Whether the Regulations cover e-mail, however, has been the subject of much debate.

Although there is ambiguity in the Regulations, the Commissioner is of the view that e-mail is covered. The proposed changes to the Telecoms Directive and other developments in this context in the EU are likely to remove any doubt as to the fact that e-mail is covered.

E-mail is, of course, still caught by the Act in cases where there is processing of personal data. In addition, the Distance Selling Directive, (97/7/EU) (the “DSD”) which is to be implemented by Statutory Instrument to be made under the European Community Act 1972 applies to contracts between consumers and suppliers where there is no face to face contact between the parties up to and including the moment at which the contract has been concluded. It does not apply to financial services (which are to be dealt with in separate Regulations). One form of distance selling is e-mail and the Distance Selling Directive applies to this. It is also designed to cover unsolicited communications by way of telephone, fax, mail and e-mail.

- 1.8** The Regulations have not implemented Article 5 of the Telecoms Directive which is covered by the Regulation of Investigatory Powers Bill.
- 1.9** An Introduction to the Act was published by the Office of the Data Protection Registrar (now the Data Protection Commissioner) in October 1998 and this may be referred to in relation to any provisions of the Act to which reference is made in this guidance.

2. DEFINITIONS

The basic interpretative provisions in section 1 of the Act are incorporated into the Regulations but there are also specific definitions contained in the Regulations. In particular, it is worth noting the wide definition of the term “processing” in the Act given that some of the provisions in the Regulations are dependent upon the processing of personal data.

Throughout this guidance, there is also reference, from time to time, to the concept of “consent”. For a more detailed analysis of the meaning of consent please refer to Chapter 3 of the Introduction to the Act at paragraph 1.6.

2.1 Individual and Corporate Subscriber

An “individual” means a living individual and includes an unincorporated body of such individuals and a “corporate subscriber” is a subscriber who is not an individual but a body corporate or other entity which is a legal person distinct from the persons of which it is composed. The applicability of certain Regulations will depend upon whether the subscriber is an individual or a corporate entity. The Regulations provide different degrees of protection depending upon whether they are a corporate or individual subscriber. The Act, however, relates to data subjects namely, an individual who is the subject of personal data.

2.1.1 Subscriber and User

The Regulations draw a distinction between a “subscriber”, who is a “party to a contract with a telecommunications service provider for the supply of publicly available telecommunications services”, and a “user”, who is “an individual using a publicly available telecommunications service (whether or not he is a subscriber)”. This distinction is particularly relevant in the context of the Regulations relating to calling or connected line identification.

2.1.2 Caller

The expression “caller” is also used. Compliance with the Regulations relating to direct marketing centres on the “caller” who is defined as “a person using publicly available telecommunications services for direct marketing purposes, except that where such services are so used at the instigation of some other person “caller” means that other person”.

So, for example, in the case of a self-employed canvasser ringing from home to arrange appointments for a double glazing company, in that case the caller is the double glazing company.

Another example might be a tele-sales agency acting for more than one company. In that case, the caller is the company paying the tele-sales agency to make the call in question.

2.2 Line

Where signals are conveyed to telecommunications equipment wholly or partly otherwise than by line, reference to a line in the Regulations is construed as including a reference to what, in that case, functionally corresponds to a line and “connected” in relation to a line, shall be construed accordingly.

This therefore extends the application of the Regulations to mobile phones where no lines are involved.

2.3 Public Telecommunications Network and Telecommunications Services

The Regulations apply to the providers and users of public telecommunications networks and telecommunications services.

“Public telecommunications network” means any transmission system, and any associated switching equipment and other resources which:-

- (a) permit the conveyance of signals between defined termination points by wire, by radio, by optical or by other electro-magnetic means, and
- (b) are used, in whole or in part, for the provision of publicly available telecommunications services”.

Therefore, it applies to any transmission system used for the provision of publicly available telecommunications services. This means that a private telephone system will fall outside the ambit of the Regulations but will still be subject to the provisions of the Act to the extent that personal data are processed.

“Telecommunications services” means “services the provision of which consists, in whole or in part, of the transmission and routing of signals on telecommunications networks, not being services by way of radio or television broadcasting”.

The Regulations therefore specifically exclude radio or television broadcasting from the provisions.

2.3.1 Telecommunications Network Provider

This is a person who provides a public telecommunications network (whether or not he is also a telecommunications service provider).

2.3.2 Telecommunications Service Provider

This is a person who provides publicly available telecommunications services (whether or not he is also a telecommunications network provider).

The Regulations therefore separate the infrastructure of the network from the services which make use of that infrastructure and they are also important in pinpointing who is to comply with the Regulations, namely, the telecommunications network, or service, provider.

2.4 Telephone Preference Service Limited and Fax Preference Service Limited

The Telephone Preference Service Limited (the “telephone preference service”) and the Fax Preference Service Limited (the “fax preference service”) are wholly owned subsidiaries of the Direct Marketing Association, which were appointed by OFTEL to maintain separate lists of those who object to the receipt of unsolicited direct marketing telephone calls and faxes respectively, on behalf of the Director General of Telecommunications. The telephone and fax preference services are responsible for logging complaints from registered subscribers, making preliminary enquiries of the callers or senders of the faxes and producing a brief report of their findings which they supply to the Data Protection Commissioner on a regular basis.

2.5 Traffic and Billing Data

2.5.1 Traffic data is defined as data which:-

- “(a) are in respect of traffic handled by a telecommunications network provider or a telecommunications service provider;
- (b) are processed to secure the connection of a call and held by the provider concerned; and
- (c) constitute personal data whereof the data subject is a subscriber to, or user of, any publicly available telecommunications service or, in the case of a corporate subscriber, would constitute such personal data if that subscriber were an individual”.

a For further information see 6.6 to 6.9 below

2.5.2 Billing data

Billing data is defined as follows:

- “(a) the number or other identification of the subscriber’s station;
- (b) the subscriber’s address and the type of the station;
- (c) the total number of units of use by reference to which the sum payable in respect of an accounting period is calculated;
- (d) the type, starting time and duration of calls and the volume of data transmissions in respect of which sums are payable by the subscriber and the numbers or other identification of the stations to which they were made;
- (e) the date of the provision of any service not falling within subparagraph (d); and
- (f) other matters concerning payments including, in particular, advance payments, payments by instalments, reminders and disconnections.”

Billing data may be any one or all of the above.

3. TRAFFIC AND BILLING DATA

3.1 Traffic Data

Because data processed to establish calls (known as traffic data) could potentially contain personal information which should therefore only be stored for limited purposes and retention periods, the Regulations provide for the protection of individual and corporate subscribers with regard to the processing of such data. **a**

Traffic data must be erased or dealt with in such a way that they cease to be personal data on the termination of the call in question.

3.2 Billing Data^b

Certain data are required by the telecommunications network or service provider for the purpose of calculating the subscriber’s bill or for interconnection charges. The period for which such data may be retained is limited to the end of the period during which the bill may lawfully be

a Regulation 6(1)
b Schedule 2

challenged or payment pursued.^a In terms of contractual law, this would normally mean that a limitation period of six years plus appeals applied. However, the Commissioner's view is that this provision merely permits retention of such data where circumstances require it, for example, where a challenge is made to the bill during the time a telecommunications network or service provider would normally retain the data for their own billing purposes. It does not permit the wholesale retention of billing data in every case. Regard must also be had to the fifth data protection principle in Schedule 1 of the Act which provides that personal data shall not be kept for longer than is necessary for the purpose for which they are processed.

3.3 Consent and the Right to Prevent Processing for Purposes of Direct Marketing

Section 11 of the Act provides that an individual has an absolute right to request a data controller to cease or not to begin processing personal data of which he is the data subject for the purposes of direct marketing (the scope of which term is very wide (see 6.1 below)). In relation to the processing of billing data, the Regulations substitute a stricter rule than that provided by Section 11^b. Under the Regulations, in the case of the marketing of telecommunications services which are provided by that telecommunications service provider, before such marketing can even take place the data controller has to obtain the consent of the subscriber. The subscriber would need to have a broad appreciation of how the data were going to be used and the consequences of giving consent to such use.^c This is to be compared to the position under Section 11 of the Act where the data controller may process personal data for the purpose of direct marketing unless he or she receives a notice in writing from the data subject requiring the data controller to cease, or not to begin, processing personal data for the purposes of direct marketing.

3.4 Marketing Telecommunications Services

A telecommunications service provider is permitted to process billing data (as defined) for the purposes of marketing its own telecommunications services if the subscriber concerned has given his consent.^d This marketing need not necessarily be carried out over the telephone and might include, by way of an example, an analysis of a subscriber's calling patterns to provide that subscriber with the best tariff available.

a Regulation 7

b Schedule 1, paragraph 3

c See Chapter 3 of the Introduction to the Act at paragraph 1.6

d Regulation 8

In the case of a corporate subscriber, a person holding himself out as capable of making decisions on the part of the company is likely to be able to give consent.

3.5 Transitional Provisions

In the context of the marketing of telecommunications services, there are transitional provisions relating to billing data where such data are eligible data. Data are eligible data at any time if they are subject to processing which was already under way immediately before 1 March 2000^a.

The transitional provisions only apply where notice has been given to the subscriber of the existing processing and of the effect of these provisions and if, within 2 months of receipt of the notice, the subscriber indicates his dissent by written notice, then the processing must cease.

The Regulations then provide that without prejudice to the above provisions, where a notified subscriber is deemed to have given his consent, the consent may be withdrawn by him as though it were a consent actually given.

^a For an explanation of the meaning of “processing already under way” see chapter 6 of the Introduction

3.6 General Provisions Relating to the Processing of Traffic and Billing Data

The Regulations^a allow traffic and billing data to be processed by a telecommunications network, or service provider in the course of its business for the following purposes:

- the management of billing or traffic data;
- customer enquiries;
- the prevention or detection of fraud; and
- the marketing of telecommunications services.

The processing of such data is to be restricted to what is necessary for these activities and by persons acting under proper authority. This implies, therefore, that the relevant telecommunications providers should train staff properly to use data responsibly. There will inevitably be some overlap in activities and it is probably unrealistic to expect individuals or groups of individuals to be solely responsible for each of the purposes mentioned above.

3.7 Customer Enquiries

There is no definition of customer enquiries which is commonly taken to mean enquiries by a subscriber regarding his own account.

3.8 Disputes^b

Nothing is to prevent the furnishing of billing or traffic data to a person who has been given statutory authority to resolve disputes. At present, this would be the Director General of Telecommunications.

3.9 Itemised Bills^c

A subscriber is entitled, upon request, to receive bills which are not itemised, in recognition of the fact that such bills may jeopardise the privacy of users even though they are also useful for subscribers to verify the amount of the bill. Both the Secretary of State and the Director General of Telecommunications have a duty under the Telecommunications Act 1984 to reconcile the rights of subscribers receiving itemised bills with the rights to privacy of calling users and called

a Regulation 9
b Regulation 10
c Regulation 29 & 30

subscribers, for example, by ensuring that sufficient alternative means for the making of calls or methods of paying for calls are available to such users and subscribers to facilitate anonymous calls in particular. The Telecoms Directive suggests that this may be achieved by the provision of pre-paid telephone cards and pay phones.

4. CALLING OR CONNECTED LINE IDENTIFICATION (“CLI”)

The Regulations address the prevention and restriction of calling or connected line identification (“CLI”) for both incoming and outgoing calls.^a Although the system has many advantages it also raises privacy issues.

4.1 The Regulations cover Call Return and Call Display facilities i.e. the display on certain telephone equipment which alerts the subscriber to the identity of the caller before the connection is made. The CLI Services are governed by an OFTEL published code entitled the “Code of Practice for Network Operators in relation to Customer Line Identification Display Services and Other Related Services”. The Commissioner’s view is that adherence to the Code will assist with compliance with the Regulations.

4.2 The facilities referred to below are available separately to a subscriber in relation to each line if that subscriber has more than one line. Each line may, therefore, be treated differently.^b

4.3 Outgoing Calls

The onus is on the telecommunications service provider to ensure that:-

- a user originating a call, has, in relation to that call, a simple means to prevent, at no charge to him, presentation of the identity of the calling line on the connected line;
- a subscriber has, as respects his line and all calls originating from that line, a simple means to prevent, at no charge to him, presentation of the identity of his line on any connected line.^c

The distinction between the user and the subscriber is to be noted here as the user only has the right to block his identity in relation to a particular call, whereas a subscriber has the right to block his identity as respects his line and all calls originating from that line. In either case, the user or subscriber is not to be charged for this facility.

4.4 Calls to Emergency Services

CLI cannot be excluded from all outgoing calls using the national emergency call number 999 or the single European emergency call number 112. This is to facilitate the dealing with such calls by the emergency services to enable easier identification of the caller’s location.

a Part III
b Regulation 16(2)
c Regulation 11

4.5 Incoming Calls - Preserving Anonymity of Callers

In the case of incoming calls the telecommunications service provider is obliged to ensure that the called subscriber has a simple means to prevent presentation of the identity of a calling line on the connected line. In this instance, there is to be no charge for reasonable use of the facility.

This Regulation which allows the subscriber being called to permit the anonymity of the caller, is particularly likely to be used for cases in which the caller's anonymity is guaranteed, namely, various help-lines such as the Samaritans, Alcoholics Anonymous or Police information lines.

4.6 Incoming Calls - Preserving Anonymity of Called Line

This preserves the privacy of an individual to whose line a call is forwarded where the connected line has a different number from the number called. This is a facility used by many businesses and medical practices, for example, a call to a doctor's surgery after hours where the call may be forwarded to the number of an individual doctor or locum service. This facility will enable the number of the line to which the call is forwarded to remain private.

Under the Regulations the relevant telecommunications service provider is under an obligation to ensure that the subscriber to whose line a call is forwarded has a simple means to prevent, without charge, presentation of the identity of the connected line on any calling line.

4.7 Termination of Unwanted Call Forwarding

If calls are being forwarded as outlined in 4.6.1 above, the subscriber has the right to request of the relevant telecommunications service provider, that such forwarding shall cease without unavoidable delay and that any other network or service provider shall comply with all reasonable requests in this connection.

4.8 Incoming Calls - Call Rejection

Where a caller has eliminated the presentation on the connected line of the identity of the calling line the called subscriber must be provided with a simple means to reject the calls in question. There is no mention of any charge for the provision of this facility. However at the present time the

a Regulation 12(2)
b Regulation 12(3)
c Regulation 31
d Regulation 12(4)

Commissioner is aware that there are technical problems associated with offering this to all subscribers.

The current technical standards do not distinguish between a situation where CLI has been deliberately withheld and where CLI is unavailable, for example, in relation to incoming international calls. Therefore, a subscriber who chooses not to receive calls with CLI withheld will also not receive international calls.

There is an additional problem in relation to subscribers to mobile phone services. For most mobile subscribers the only way to reject a call made with CLI withheld is not to answer or to press "line busy". On some networks this will result in the call being transferred to the subscriber's voice mail. This may not be sufficient to fulfil the requirements of the Telecoms Directive or the Regulations but it would appear to be a Europe-wide problem and it is the Commissioner's understanding that this is a matter which may be resolved through European industry groups.

4.9 Charges

Where there is no mention in the Regulations that a charge may be made for a service, the Regulations permit that where a person is required to provide, or ensure the provision of, a facility, a reasonable charge may be made unless there is an indication to the contrary.^a

4.10 Duty of a Telecommunications Service Provider to advise that CLI is available

A telecommunications service provider who offers CLI facilities is obliged to take all reasonable steps to publicise that he does so and also to explain the consequences of the Regulations in relation to CLI.^b

4.11 Malicious or Nuisance Calls^c

There are provisions to assist with the tracing of malicious or nuisance calls where the relevant telecommunications service provider has been notified by a subscriber that he or she requires the tracing of such calls on his or her line.

In this situation, the telecommunications service or network provider as appropriate may override anything done to prevent the presentation of the identity of the calling line, to calls in relation to which the subscriber's line is the called line, so far as it appears to the provider in question to be necessary or expedient for the purposes of such action.

In relation to such calls, the relevant telecommunications service or network provider as appropriate may hold and make available to a person with a "legitimate interest" in this information, data containing the identification of a calling subscriber obtained pursuant to these provisions. The "data containing the identification of a calling subscriber" may not actually reveal the identity of the person making the call but merely the location from which the calls were made.

It is important to distinguish a person with a "legitimate interest" under the Regulations, from the reference to "legitimate interests" referred to in paragraph 6 of Schedule 2 of the Act. Under the Act, the expression "legitimate interests" has been given a relatively wide interpretation by the Commissioner. It relates to the "legitimate interests" pursued by the data controller or by the third party ... to whom the data are disclosed". In the Regulations the expression "a person with a legitimate interest" is not defined but it probably includes the police or other law enforcement body and even the subscriber himself. Further, given that telecommunications

a Regulation 4
b Regulation 15
c Regulation 14

service, and network, providers are obliged under the Regulations^a to comply with any reasonable requests made by any other provider, which includes the provisions relating to malicious or nuisance calls, any other provider must be included within the scope of persons with a “legitimate interest”.

a Regulation 16

5. DIRECTORIES OF SUBSCRIBERS

The Regulations contain provisions relating to directories of subscribers to publicly available telecommunications services, which are made available to the public or to a section of the public (“directory”). The provisions do not apply to an edition of a directory first published before 1 March 2000. The directory may be of telephone numbers (including mobile telephone numbers), but also of fax numbers and e-mail addresses. The Regulations make it clear that such directories may be in printed or electronic form or may be those relied upon by a directory enquiry service.

5.1 Individual Subscribers^a

In the case of an individual, except to the extent that the subscriber has consented otherwise, a directory entry cannot contain any personal data of that subscriber other than data which are necessary to identify the subscriber and his or her allocated number. Accordingly, the directory entry might be modified as follows:

- no entry at all relating to a specified number;
- no entry containing a reference which might reveal his or her sex;
- the deletion of such part of his or her address as may be specified.

An individual could, therefore, have a modified entry whereby he or she is only referred to by another name by which he or she may be known e.g. a nickname, maiden name or a pseudonym and all or part of his or her address is excluded. This could arguably satisfy the requirement that the entry should contain such data as are necessary to identify the subscriber and his or her allocated number.

The Commissioner recognises that, to avoid too many misdirected calls, there is merit in directory entries being as meaningful as possible.

There is no charge for this facility.

This represents a change in the normal practice of telephone directory entries where a subscriber is either ex-directory or a full address (minus the post code) appears. The Regulations will permit a directory entry with partial omission of the address in the case of individual subscribers, the idea being that fewer subscribers may choose to go ex-directory once they have the option of putting in part only of their address.

5.2 Corporate Subscribers^b

a Regulation 18
b Regulation 19

A corporate subscriber may request that their number be excluded from the directory. There is no provision for a modified entry as for individual subscribers nor is there any provision preventing additional information being included as in the case of individual subscribers.

5.3 Third Parties

In relation to both individual and corporate subscribers, where a third party has in his possession a record of a request by a subscriber to the producer of a directory relating to his entry that person is obliged to send a copy to the producer of the directory who shall treat the request in question as if it had been made direct.

5.4 Directory Enquiry Services

Where there is no entry relating to a subscriber or no entry relating to his or her number there is nothing in the Regulations to prevent the enquirer being told the reason or the possible reason why there is no such entry. This means that rather than merely advise the enquirer that a number is not listed, the enquirer can be told that the subscriber has requested that a number be excluded from the directory.^a This reflects what happened before i.e. if someone was ex-directory you would be told that was the case.

6. DIRECT MARKETING

The Regulations deal with the use of publicly available telecommunications services for direct marketing purposes.

6.1 Direct Marketing

Definition

There is no definition of direct marketing in the Regulations and the only assistance in interpretation provides that a reference to direct marketing “is a reference to the communication of any advertising or marketing material on a particular line”^b; “advertising” or “marketing” are not defined. The only other part of the Regulations which refers to marketing is in relation to traffic and billing data^c (see paragraphs 3.3 to 3.4 above) which provides for “the marketing of any telecommunications services” provided by “the telecommunications service provider concerned” which can be distinguished from the marketing with which we are concerned here.

The Act defines “direct marketing”^d as “the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals”. There is no further analysis of what “advertising” or “marketing” may mean but the Commissioner regards the term “direct

a Regulation 20
b Regulation 21(2)
c Regulation 8
d section 11

marketing” as covering a wide range of activities. The Commissioner is supported in this view by the following:

- In Recommendation no. R85(20) of the Council of Europe on “the protection of personal data used for the purpose of direct marketing” the following definition is adopted:-
 - Direct marketing “comprises all activities which make it possible to offer goods or services or to transmit other messages to a segment of the population by post, telephone or other direct means aimed at informing or soliciting a response from the data subject as well as any service ancillary thereto”.
- The Distance Selling Directive 97/7/EC states that the term advertising “is to be taken to include all forms of direct marketing communication, including any sales promotion or fund raising whether or not it contains an offer or an invitation to treat”.
- The Federation of European Direct Marketing, which represents the direct marketing sector at a European level, stated in a paper issued in 1998 that, “Direct marketing is a series of marketing strategies, using various delivery techniques designed to provide the receiver (consumers and companies) with information at a distance. Direct Marketing is not a homogeneous marketing discipline but rather a series of different strategies using different means of approach (e.g. broadcasting, printed press, mail, telephone, on-line services). It is used to sell products, to deliver information, public announcements, and for sales after service, customer care services, charity and political appeals.”

The Commissioner’s view, therefore, is that direct marketing, as defined in the Regulations, will apply not just to the offer for sale of goods or services, but also the promotion of an organisation’s aims and ideals. This would include a charity or a political party making an appeal for funds or support and, for example, an organisation whose campaign is designed to encourage individuals to write to their MP on a particular matter or to attend a public meeting or rally.

6.2 Automated Calling Systems^a

6.2.1 Individual and corporate subscribers

a Regulation 22

The use of automated calling systems for direct marketing purposes to an individual or corporate subscriber is prohibited unless the subscriber concerned has previously notified the caller that he consents to such calls.

An automated calling system is described as one which, when activated, operates to make calls without human intervention. This definition is not without difficulty. Article 12 of the Telecoms Directive refers to “the use of automated calling systems without human intervention” but does not clarify whether there can be human intervention in that the called party speaks to a live person when the connection is made.

On the assumption that the mischief that the Regulations are designed to address is a system where the subscriber does not speak to a live person, that is to say they receive a recorded message or some pre-determined voice-activated response, and cannot, therefore, obtain any information from the caller, the Commissioner intends, for the time being to interpret an automated calling system this way.

If it covers an automated system which delivers a pre-recorded message to the subscriber, then this Regulation is unlikely to affect many organisations. If, however, it means an automated dialling system, where it is the machine which does the dialling but where the called party does in fact speak to an individual then the implications are more significant. Such systems are used by organisations for reasons of efficiency.

The subscriber must have previously notified the caller that he or she consents to receiving calls via an automated calling system. So, where a network operator sends text messages to mobile telephones, the subscriber must have previously consented to this. Consent could be obtained by way of a term in the contract signed when the telephone is purchased. However, the subscriber would need to have a broad appreciation of the nature of the text messaging and the consequences of agreeing to the receipt of such messages. Organisations would need to be aware of their obligations under the Unfair Contract Terms Act 1977, and the Unfair Terms in Consumer Contracts Regulations 1994.

Generally, in the Regulations, where the expression “previously notified” is used, it must mean that a positive act is required to signify the intention of the subscriber.

6.3 Unsolicited and Solicited Communications

6.3.1 Unsolicited Communications

This part of the Regulations makes reference to “unsolicited” communications but this term is not defined and the Commissioner takes the view that it has its ordinary natural meaning of “uninvited”.

The Commissioner's view is that it is clear from the Regulations that, a call should not be treated as being unsolicited if a subscriber has indicated by way of notification to the caller that he does not object to receiving such calls, (See also 6.4 and 6.5)

In practice, therefore, where a subscriber has notified a caller that he does not object to receiving direct marketing calls, the caller may rely on this until it is specifically revoked, usually by the caller being directly advised otherwise. The fact that the subscriber subsequently registers with the telephone preference service will not automatically override a notification of non-objection because calls or faxes to numbers of subscribers who have notified non-objection are not to be treated as unsolicited.

6.3.2 Solicited Communications

The Commissioner's view is that the Regulations do not apply to genuinely solicited or invited calls on a particular number for marketing purposes whether the invitation is given by the subscriber or not.

So, if the subscriber or another individual having access to the subscriber's station has, for example, filled in and returned a coupon asking for further information about a particular product or service and has provided a fax or telephone number on the coupon, it may be considered that a call or a fax to that number to provide the information in question is not uninvited.

6.4 Use of Fax for Direct Marketing Purposes

6.4.1 Individual or Corporate Subscribers^a - Unsolicited Communications

The use of fax for direct marketing purposes by way of unsolicited communications on the lines of individual or corporate subscribers is prohibited where:

- the called subscriber has previously notified the caller that such unsolicited communications should not be sent; or
- the called subscriber's number is listed with the fax preference service.

The communication is not to be treated as unsolicited where the called line is that of a subscriber who has notified the caller that he or she does not for the time being object to receiving such communications. The use of the

a Regulation 23

words “for the time being” is in recognition of the fact that the subscriber could change his or her mind in the future.

Those involved in business to business marketing might find practical difficulty in distinguishing, in a list of businesses, between those which belong to sole traders or partnerships (and which, therefore, enjoy the rights given to individuals under the Regulations) and corporate subscribers. It is for this reason that **any subscriber** may choose to have his number listed with the fax preference service.

Furthermore, the Commissioner strongly encourages any sole trader or partnership which does not wish to receive unsolicited marketing material by fax to register their number with the fax preference service. The Commissioner will have regard, when investigating any complaint about the receipt of marketing material by an individual, as to whether:

- the direct marketer checked with the fax preference service and;
- whether there was a genuine intention to contact businesses as opposed to individuals.

6.4.2 Individual Subscribers

Individual subscribers also have the benefit of provisions which prohibit the sending of faxes (whether solicited or not) unless the subscriber has previously indicated to the caller that he consents for the time being to receiving such faxes.^a There is nothing to suggest that this notification has to be in writing.

6.5 Calls for Direct Marketing Purposes Individual Subscribers - Unsolicited Communications

The use of calls to individuals for unsolicited direct marketing (other than by fax as to which see 6.4 above) is prohibited where:

- the called subscriber has previously notified the caller that such unsolicited communications should not be made; or
- the called subscriber’s number is listed with the telephone preference service.

A call is not taken to be unsolicited if the subscriber has notified the caller that he does not object to receiving such calls.

a Regulation 24

6.6 Telephone and Fax Preference Service

The Regulations impose an obligation on the Director General of Telecommunications (“Director”) to maintain a record of telephone numbers of subscribers who have registered an objection to receiving unsolicited direct marketing faxes in the case of both individual and corporate subscribers or calls in the case of individual subscribers.^a

Due to the definition of “corporate subscriber” and “individual” in the Regulations, as stated above, an individual will also include a partnership which will, therefore, be able to take full advantage of the benefits of the Regulations in respect of the fax and telephone preference service as well as the right not to receive automated direct marketing calls.

The Regulations provide that appropriate fees may be charged for making available information from the record, such fees being equal to the costs incurred in maintaining the record. A number will be removed from the list if there is reason to believe that the number is no longer that of the listed subscriber.

The Commissioner has recommended that the mechanism set up should be as flexible and cost efficient as possible lending itself to easy use by both large scale telemarketing companies on the one hand and small groups wishing to solicit funds or support for a particular cause on the other. The Commissioner has also urged that, to the extent practicable, the most privacy friendly approach should be adopted. The operation of the telephone and fax preference service, including the charging arrangements, will be subject to formal review on a quarterly basis by OFTEL which should reveal whether the system is providing an adequate level of consumer protection.

6.7 28 Day Time Delay

It is acknowledged that there is a practical difficulty in providing up-to-date information about subscribers for a list which is constantly being added to or amended. Accordingly, the Regulations provide that a caller shall not be regarded as being in contravention of the relevant provisions by the making or the instigation of the making of a call and, likewise a subscriber shall not be regarded as being in contravention of the relevant provisions by permitting his line to be used for the making of a call if the number was not listed at any time in the preceding 28 days.^b Subscribers wishing to register with the fax preference service should call 0845 070 0702 and individual subscribers wishing to register on the telephone preference service should call 0845 070 0707. Those wishing to enquire

^a Regulations 23 & 25
^b Regulation 27(4)

about the lists with a view to making direct marketing faxes and/or calls should call 01932 414161.

6.8 Numbers Listed Before 1 May 1999

6.8.1 Individual Subscribers

Provision is also made for cases where individual subscribers may have advised:

- a telecommunications service provider;
- the producer of a directory; or
- where the producer of a directory is provided with information by another person, that other person,

of their requirement to have a number listed on the telephone or fax preference service prior to 1 May 1999. In such situations, they are deemed to have notified the Director in person and that number may be withdrawn at any time as if it were notified direct to the Director.^a

6.9 Telephone and Fax Preference Service - notification to specified persons^b

Where any one of the following:-

- a telecommunications service provider;
- the producer of a directory; or
- where the producer of a directory is provided with information by another person, that other person.

receives a request that a number be included in the telephone preference service or the fax preference service, that person is under an obligation, without delay, to submit a copy of that notification to the Director and it is to be treated as having been provided direct to the Director.

6.10 Duties of a Caller

Where a caller communicates direct marketing material by fax or by way of an automated calling system, the caller must:

a Schedule 1, Part I

b Regulation 26. Notification under the Regulations is not to be confused with the notification requirements under the Act.

- identify him or herself; and
- provide an address or a freephone telephone number on which he or she can be reached.

Where the call is otherwise than by fax or by way of an automated calling system, the caller must:

- identify him or herself and, if requested to by the recipient of the call;
- provide an address or a freephone telephone number on which he or she can be reached. **a**

The information given in either case must not be misleading and must be sufficient to enable the recipient of the call to trace the caller.

6.11 Directory

A producer of an edition of a directory of subscribers which is published after 1 March 2000 is obliged to ensure it contains a statement drawing attention to the provisions relating to the use of automated calling systems, calls and faxes for direct marketing purposes.

7. SECURITY

7.1 Security of Telecommunications Services^b

A telecommunications service provider must take appropriate technological and organisational measures to safeguard the security of its services, if necessary in conjunction with the provider of the network, and inform subscribers of any special risks of a breach of the security of the network.

Such security is not to be regarded as being at risk by reason of:

- a disclosure made in connection with the prevention or detection of crime;
- a disclosure made for the purpose of criminal proceedings;
- an order made by the Secretary of State to intercept any communications as may be specified in a warrant; or

a Regulation 27
b Regulation 28

- any disclosure made in the interests of national security or in pursuance of a court order.^a

This provision in the Regulations may be compared with the obligations on a data controller under the Seventh Data Protection Principle as to which see the Introduction to the Act at Chapter 3 paragraph 7.

7.2 National Security

A telecommunications service, or network, provider is not required to carry out or refrain from carrying out an act (including the processing of data) if exemption from the requirement in question is required for the purpose of safeguarding national security. A certificate signed by a Minister of the Crown certifying the same shall be conclusive evidence of that fact. Any person directly affected by the issuing of a certificate may apply to the Data Protection Tribunal against the certificate.^b

a Telecommunications Act 1984 as amended by the Interception of Communications Act 1985

b This provision has been amended by the Telecommunications (Data Protection and Privacy) Regulations 2000 SI 2000/157 to bring it into line with the Act

8. LEGAL REQUIREMENTS

A telecommunications service, or network, provider is not required to do, or refrain from doing, anything

1) if compliance would be inconsistent with any requirement:

- imposed by any enactment;
- imposed by any rule of law;
- imposed by court order; or
- which would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders; or

2) if exemption from the requirement in question:

- is necessary for the purposes of obtaining legal advice; or
- is required in connection with legal proceedings (including prospective legal proceedings); or
- is otherwise necessary for the purposes of establishing, exercising or defending legal rights,^a

9. COMPENSATION AND ENFORCEMENT

9.1 Any person who suffers damage by reason of any contravention of any of the requirements of the Regulations by any other person, is entitled to compensation from the other person for that damage. It is a defence for that other person to prove that he or she has taken such care as in all the circumstances was reasonably required to comply with the requirement concerned.

The Data Protection Commissioner has power to enforce the Regulations by virtue of the powers given to her under the Act, as amended by the Regulations. Action may be taken against any person regardless of whether or not they fall within the definition of a data controller under the Act. The Commissioner may seek advice on technical and similar matters relating to telecommunications from the Director to assist her with her enforcement functions.

a Regulation 33

Enforcement of the Regulations may be exercised by the Commissioner either on her own initiative, at the request of the Director or by a person aggrieved by the alleged contravention.

Enforcement of breaches of the Direct Marketing Regulations may also be exercised by the Commissioner by virtue of the Regulations.

For further information on the powers and duties of the Commissioner, please refer to Chapter 7 of the Introduction to the Act.

**PARTIAL REGULATORY IMPACT ASSESSMENT
DRAFT**

**THE PRIVACY AND ELECTRONIC COMMUNICATIONS (EC DIRECTIVE)
REGULATIONS 2003**

PARTIAL REGULATORY IMPACT ASSESSMENT ON THE PRIVACY AND ELECTRONIC COMMUNICATIONS (EC DIRECTIVE) REGULATIONS 2003

1. TITLE OF PROPOSAL

This Regulatory Impact Assessment has been prepared on the Privacy and Electronic Communications (EC Directive) Regulations 2003, which implement provisions arising from an EC Directive on data protection in the communications sector (Directive 2002/58/EC).

2. PURPOSE AND INTENDED EFFECT OF THE MEASURE

(i) Objective

Key new provisions:

- Regulation 5 - **cookies and similar internet tracking devices**: The Regulations require that anyone who uses **cookies** (whether they process personal data or not) and similar tracking devices must provide information and a chance to refuse to subscribers or users who are not content to accept them. This rule does not apply where the cookie or similar device is used only to enable the transmission of website or other online content or where it is an integral part of an online service which cannot be provided without it
- Regulation 6 - **value added services based on traffic and location data**: the Regulations allow for the provision of **value added services** based on traffic or location data, either by network operators on their own or in conjunction with third parties. There is no restriction on the type of services that may be provided as long as subscribers give their consent and are informed of the data processing implications
- Regulation 17 - **subscriber directories**: the Regulations give subscribers a right to decide whether they want to be listed in **subscriber directories** or not. Subscribers must be given clear information about the directories in question, including any reverse search-type functions
- Regulation 20 – **the Telephone Preference Service**: the Regulations give corporate subscribers the right to opt-out of unsolicited direct marketing phone calls by registering on the TPS (individual subscribers already have this right)
- Regulation 21 - **unsolicited commercial e-mail and SMS**: the Regulations require that **unsolicited commercial e-mail (UCE) and SMS** to individual subscribers is subject to a prior consent requirement, so that these may only be sent if the recipient has agreed in advance, except in the context of an existing

customer relationship, where companies may continue to market their own products by on an “opt-out” basis

(ii) Background

The Regulations are needed to implement an EC Directive, the Directive on Privacy and Electronic Communications (2002/58/EC). The Directive on Privacy and Electronic Communications is part of the new European regulatory framework for electronic communications networks and services. This Directive updates the current Telecoms Data Protection Directive (Directive 97/66/EC) in the light of new technologies and in particular ensures that the privacy rules which apply to phone and fax services also apply to e-mail and use of the internet. Directive 97/66/EC was implemented in the UK via the Telecommunications (Data Protection and Privacy) Regulations 1999 the Regulation of Investigatory Powers Act 2000, and the Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000. The new Regulations carry over those elements of the Telecommunications (Data Protection and Privacy) Regulations 1999 which still apply under the new regime.

The Regulations guarantee the confidentiality of communications, set conditions on the use of traffic, location and subscriber data, and subscriber directories, and regulate the use of communications networks for unsolicited direct marketing by e-mail and SMS. The Directive is implemented through the form of a Statutory Instrument to be made under the European Communities Act 1972. It will affect a wide range of organisations operating in the electronic communications and direct marketing sectors (not merely holders of licences issued under the Telecommunications Act 1984) including: phone/internet users, communications network and service providers, website and online content businesses, subscriber directory providers and anyone who direct markets by phone, fax, SMS or e-mail.

(iii) Risk Assessment

The United Kingdom is required by Community law to implement the Directive in UK law. A failure to do so could lead to proceedings being brought by the EC Commission in the European Court. A failure to implement could also lead to HMG being liable in the UK courts for losses suffered by those denied their rights under the Directive as a result.

3. Options

Two options have been identified:

Option 1 - do nothing on the grounds that the UK is already largely in compliance with the broad principles of the Directive through the implementing legislation for

the Telecoms Data Protection Directive (including the Regulation of Investigatory Powers Act, the Lawful Business Practice Regulations), other relevant legislation, including the Data Protection Act 1998, and current business practice, including industry codes of practice on e-mail marketing.

Option 2 - legislate through regulations made under Section 2(2) of the European Communities Act 1972.

4. Benefits

The following assessment can be made:

Option 1 - although, as indicated above, the United Kingdom is already largely in compliance with the Directive, the extent to which it is not is sufficient for there to be a risk of action in the ECJ, and of damages being awarded against the Government in the UK courts. The only provision to which this risk does not apply is the extension of the right to register on the TPS to corporate subscribers, which is allowed, but not required by the Directive. There is no benefit associated with Option 1.

Option 2 - the expected benefit is the avoidance of action in the ECJ, and of damages awarded against the Government in the UK courts for non-implementation of the Directive by users and operators granted rights under it.

There would also be a benefit to subscribers who are given rights under the Directive.

In more detail, the expected benefits for **option 2** are:

- Clarification of the regulation of electronic communications networks in the light of new technologies, so that subscribers can be more confident that their privacy will be respected when they use electronic networks and services, and that network and service providers are given more certainty about the rules under which they must operate;
- A clearer legal framework for network operators wishing to provide value added services based on traffic or location data. An accompanying benefit to subscribers who will only receive these services if they have given their consent to them and are informed of the data processing implications;
- Protection of subscribers' privacy regarding unsolicited commercial e-mail and SMS and use of the internet including for direct marketing purposes;
- Increased transparency for subscribers or users regarding cookies and similar tracking devices;
- Enhanced protection of subscribers' privacy regarding listing in subscriber directories.

Business sectors affected

The Regulations will affect any organisation which is a phone or internet user, uses websites or other online services, is a communications network or service provider, is subject to entry in a subscriber directory, or is subject to direct marketing by SMS or e-mail.

Issues of equity or fairness

The United Kingdom is required by Community law to implement the Directive in UK law. A failure to do so could lead to proceedings being brought by the EC Commission in the European Court.

5. Costs

(i) Business sectors affected

A wide range of organisations operating in the communications and direct marketing sectors (not merely holders of licences issued under the Telecommunications Act) including: phone/internet users, communications network and service providers, website and online content businesses, subscriber directory providers and anyone who direct markets by phone, fax, SMS or e-mail will be affected. For direct marketing purposes this will also include charities and voluntary organisations.

(ii) Compliance costs

The following assessment can be made. The following costs are for option 2. Option 1 imposes no costs on business. The main compliance costs to business are likely to arise from the provisions on: traffic and location data; unsolicited commercial e-mail and SMS; cookies and similar tracking devices; and subscriber directories, as follows:

- **Value added services based on traffic and location data:** The costs to business wishing to provide value added services based on traffic or location data, would be those of gaining consent from subscribers and informing them of the data processing implications
- **Corporate subscribers – right to register on the Telephone Preference Service:** businesses who wish to direct market by phone to corporate subscribers will need to check the Telephone Preference Service to ensure that they are not registered. Many businesses already fall within the definition of individual subscriber (sole traders, for instance, and partnerships except in Scotland), and therefore already have the right to register on the TPS. There are various payment options for consulting the TPS depending on the size of the direct marketer and the number of phone numbers that they need to check. See Annex A for further details.

- **Unsolicited commercial e-mail (UCE) and SMS:** The costs to business wishing to send UCE and SMS will be that of gaining prior recipient consent (except in the context of an existing customer relationship, where companies may continue to direct market their own products on an “opt-out” basis
- **Cookies and similar internet tracking devices:** The costs to businesses wishing to use cookies or similar tracking devices will be that of providing information and a chance to refuse to subscribers or users who are not content to accept them
- **Subscriber directories:** The costs to business wishing to list subscribers in directories will be that of giving clear information about the directories in question, including any reverse search-type functions.

Question:

1. Please give indications of the recurring and non-recurring costs that the provisions on traffic and location data; unsolicited commercial e-mail and SMS; corporate TPS registration; cookies and similar tracking devices; and subscriber directories would entail to your business as follows:

	traffic and location data	unsolicited commercial e-mail	Corporate TPS registration	cookies	subscriber directories
Recurring costs £					
Non recurring costs £					

Other Costs

Under option 2 there may be some loss of revenue to network operators, service providers and direct marketers if fewer direct marketing text messages and emails are sent. There will also be a cost to Government of preparing the implementing legislation and enforcing the regulations.

Costs for a typical business

A wide range of organisations operating in the communications and direct marketing sectors including: phone/internet users, communications network and service providers, website and online content businesses, subscriber directory providers and anyone who direct markets by phone, fax, SMS or e-mail will be affected.

6. Consultation with Small Business: the Small Firms' Impact Test

14. The Regulations will impact on small firms to the same extent as to any other firms in the sector. The areas in which costs are anticipated are those of obtaining customer consent and it is thought that these are unlikely to have a significantly differing impact on different sizes of firms. The impact on small business in terms of cost (in comparison to differing sizes of firms) is therefore expected to be small. It should be noted, however, that small firms will also benefit in some of the areas in which they may also incur costs. It may be expected that these benefits would be disproportionate to those gained by larger firms, particularly in relation to the protection against unsolicited direct marketing calls which can be a particular problem for small firms.

7. Competition Assessment

A wide range of organisations operating in the communications and direct marketing sectors will be affected by the Regulations including: phone/internet users, communications network and service providers, website and online content businesses, subscriber directory providers and anyone who direct markets by SMS or e-mail. The Regulations will apply across the board to all organisations operating in these sectors both in the UK and throughout the EU.

It is anticipated that the Regulations are likely to have little or no effect on competition. The factors taken into account in making this assessment are:

- The wide variety of types of organisations and markets, and market shares covered by the Regulations which make competition concerns unlikely;
- The areas in which costs are anticipated are unlikely to have a significantly differing impact on different sizes of firms;
- The Regulations are unlikely to make a change to market structure as they do not impose costs on only certain firms within a market, nor do they favour/penalise new firms entering the market – they apply across the board;
- It is not anticipated that the regulations will restrict innovation, however they may place restrictions on businesses providing some products or services that they may otherwise have provided if they are not able to gain the necessary customer consent.

8. Enforcement and sanctions

The regulations will be enforced by the Information Commissioner. The Information Commissioner's office have powers to investigate and issue enforcement notices to individuals or companies which breach the Regulations.

Breach of an enforcement notice is a criminal offence liable to a fixed fine of £5,000 in a trial without a jury, or an unlimited fine if the trial is in front of a jury. In addition, anyone who has suffered damages because the Regulations have been breached has the right to sue the person responsible for compensation.

9. Monitoring and Review

Member States's implementation of the Directive will be reviewed by the European Commission during 2006.

10. Consultation

(i) Within government

Government departments and regulatory authorities consulted by the DTI over the course of negotiations on the Directive and preparation of the Regulations include:

Cabinet Office
Department for Culture Media and Sport
HM Customs and Excise
Independent Television Commission
Information Commissioner's Office
Foreign and Commonwealth Office
Home Office
Lord Chancellor's Department
National Assembly for Wales
Northern Ireland Executive
Office of the E-Envoy
Office of Fair Trading
Office of Telecommunications (Of tel)
Radio Authority
Radiocommunications Agency
Scottish Executive

(ii) Public consultation

The Directive on Privacy and Electronic Communications is one of the six Directives forming the new regulatory framework for electronic communications networks and services, known as the 1999 Communications Review. The Department and Of tel (the Office of Telecommunications) liaised closely with industry and consumer representatives and other interested stakeholders throughout the Review. In particular, the Department held two public workshops on the Review, in conjunction with Of tel, to which organisations including representatives of small businesses were invited

In addition, the Department began a consultation specifically on the Directive in April 2001, during the detailed negotiations on the draft of the Directive. The views of the Department's contact list on the Directive were sought – the list numbered approximately 900 interested parties at that time, and included UK electronic communications operators and service providers, trade associations, small firms organisations, consumer bodies, bodies in the charity and voluntary sector, direct marketing organisations, directory publishers, individual subscribers and a number of small businesses. Other interested parties were also invited to comment through the Department's website.

We received more than seventy representations from interested parties during the negotiations on the draft Directive. The draft Regulations will be sent to the individuals and organisations currently registered on our circulation list (this includes over 1,100 addresses).

11. Summary and Recommendation

On the basis of the analysis identified below, option 2 is the recommended option.

	<u>Option 2</u> Expected costs	<u>Option 2</u> Expected benefits
Business	Provisions on: traffic and location data; UCE and SMS; cookies; subscriber directories	Clarification of the legal framework, in particular regarding unsolicited SMS, and provision of value added services Protection of firms' privacy, and avoidance of unwanted direct marketing text messages and emails (for individual subscribers); Avoidance of unwanted direct marketing phone calls (for corporate and individual subscribers)
Citizens		(aa) Protection of subscribers' privacy, and avoidance of unwanted direct marketing text messages and emails;
Government	Cost of preparing implementing regulations and	Avoidance of ECJ action Avoidance of damages awarded against the

guidance Government in the UK
Cost of enforcing the courts for non-
regulations implementation

12. Declaration

I have read the Regulatory Impact Assessment and I am satisfied that the balance between cost and benefit is the right one in the circumstances.

Signed by the responsible Minister.....(This remains blank until the legislation is to be sent to Parliament).

Date.....

Contact point:

Mary Tait, European Communications Policy Team, Department of Trade and Industry 0207 215 1807

Date: March 2003

TPS Consultation Costs

TPS Annual Fees (copy supplied every 28 days or annual access to web download)

Complete data file	£7500 + VAT
Subset of data file (up to 50% of the numbers)	£5625 + VAT
Subset of data file (up to 25% of the numbers)	£3000 + VAT
Subset of data file (up to 5% of the numbers)	£1125 + VAT
Subset of data file (up to 1% of the numbers)	£750 + VAT

TPS One Off Ad Hoc Fees (single copies of the file)

Complete data file	£1000 + VAT
Subset of data file (up to 50% of the numbers)	£750 + VAT
Subset of data file (up to 25% of the numbers)	£400 + VAT
Subset of data file (up to 5% of the numbers)	£150 + VAT
Subset of data file (up to 1% of the numbers)	£100 + VAT

The TPS also offers three checking services for smaller companies. These include an internet interrogation service where for a minimum of £50 a month they can check up to 500 numbers, extra numbers cost 10p per look up; a call barring service whereby a company can arrange that their sales calls go through a filter system whereby calls to TPS numbers are stopped, and a premium rate number checking service. The call barring service and the premium rate service are both charged at a comparable rate to the internet interrogation service.

THE CONSULTATION CRITERIA

1. Timing of consultation should be built into the planning process for a policy (including legislation) or service from the start, so that it has the best prospect of improving the proposals concerned, and so that sufficient time is left for it at each stage.
2. It should be clear who is being consulted, about what questions, in what timescale and for what purpose.
3. A consultation document should be as simple and concise as possible. It should include a summary, in two pages at most, of the main questions it seeks views on. It should make it as easy as possible for readers to respond, make contact or complain.
4. Documents should be made widely available, with the fullest use of electronic means (though not to the exclusion of others) and effectively drawn to the attention of all interested groups and individuals.
5. Sufficient time should be allowed for considered responses from all groups with an interest. Twelve weeks should be the standard minimum period for a consultation
6. Responses should be carefully and open-mindedly analysed, and the results made widely available, with an account of the views expressed, and the reasons for decisions finally taken.
7. Departments should monitor and evaluate consultations, designating a consultation co-ordinator who will ensure the lessons are disseminated. The complete code is available on the Cabinet Office's web site, address <http://www.cabinet-office.gov.uk/servicefirst/index/consultation.htm>.

Comments or complaints

If you wish to comment on the conduct of this consultation or make a complaint about the way this consultation has been conducted, please write to Philip Martin, DTI Consultation Co-ordinator, Room 725, 1 Victoria Street, London SW1H 0ET or telephone him on 020 7215 6206 or mail to: Philip.Martin@dti.gsi.gov.uk