EXPLANATORY MEMORANDUM TO

THE ELECTRONIC COMMERCE DIRECTIVE (TERRORISM ACT 2006) REGULATIONS 2007

2007 No. 1550

1. This explanatory memorandum has been prepared by the Department of Trade and Industry and is laid before Parliament by Command of Her Majesty.

2. Description

2.1 These Regulations implement Directive 2000/31/EC of the European Parliament and of the Council of 8th June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) ("the Directive") in so far as the Directive applies to the Terrorism Act 2006 ("the Terrorism Act"). In particular, the Regulations implement the 'country of origin' rules and the limitations of liability set out in the Directive.

3. Matters of special interest to the Joint Committee on Statutory Instruments

3.1 None

4. Legislative Background

4.1 The Directive was originally implemented by the Electronic Commerce (EC Directive) Regulations 2002[1] ("the E-Commerce Regulations"). However, the E-Commerce Regulations only apply in relation to Acts passed before the date on which the E-Commerce Regulations were made and in relation to "the exercise of a power to legislate" on or before that date[2]. So far as legislation that postdates the E-Commerce Regulations is concerned, the Directive needs to be implemented on a case-by-case basis.

4.2 The Directive is concerned with the regulation of "information society services" which are, broadly speaking, commercial services provided on the Internet. Section 1 of the Terrorism Act creates an offence of publishing a statement that is likely to be understood as encouraging terrorism and section 2 creates an offence relating to the dissemination of terrorist publications. The Directive applies to the Terrorism Act because, although the offences under sections 1 and 2 are more general in their application, it is possible to commit such offences by providing commercial services on the Internet.

4.3 Further, sections 3 and 4 of the Terrorism Act are specifically concerned with the application of sections 1 and 2 to Internet activity. Sections 3 and 4 establish a sort of Internet "notice and take-down regime" under which a constable can issue a notice requiring the removal from public view, or the amendment of, a statement, article or record which the constable considers to be "unlawfully terrorism-related" (as defined in section 3(7)). In addition, where a notice is given to a person, subsections (4) to (6) of section 3 mean that the person will be subject to certain limited obligations to remove from public view or amend any "repeat statements" (as defined

[1] SI 2002/2013.
[2] Regulation 3(2).

in subsection (4)) that are posted on the Internet. Non-compliance with a section 3 notice is not, of itself, a criminal offence. However, where a person fails to comply with such a notice he will be treated as endorsing the statement, article or record in question and therefore, if he is prosecuted for an offence under section 1 or 2, he will not be able to take advantage of the defence in section 1(6) or section 2(9)[3].

4.4 Article 3 of the Directive sets out 'country of origin' rules in relation to the regulation of information society services. Generally, these rules provide that, within the "coordinated field" (as defined in the Directive), information society services must be regulated by the law of the EEA state[4] in which the provider of the services is established, rather than the law of the EEA state in which the services are received. This means that, on one hand, where the United Kingdom ("the UK") regulates information society services within the co-ordinated field, such regulation must extend to information society services provided by persons established in the UK, even where such services are provided elsewhere in the EEA (Article 3(1)). On the other hand, the UK must not, for reasons falling within the "coordinated field", restrict the freedom of a person established in another EEA state to provide information society services in the UK (Article 3(2)). It is, however, permissible to derogate from this latter rule if the public interest conditions and procedural requirements in Article 3(4) are satisfied.

4.5 In the Department's view, sections 1 to 4 of the Terrorism Act fall within the "coordinated field" as defined in the Directive. It is therefore necessary for these provisions to comply with the country of origin rules in Article 3 the Directive. Section 17 of the Terrorism Act already goes some way towards achieving what is required by Article 3(1)[5]. Where section 17 does not operate, regulation 3 is intended to ensure compliance with Article 3(1). Paragraphs (4) to (6) of regulation 3 are to ensure compliance with the limitation relating to criminal penalties in paragraph 1(1)(d) of Schedule 2 to the European Communities Act 1972 on the power conferred by section 2(2) of that Act. Regulation 4 is intended to ensure compliance with paragraphs (2) and (4) of Article 3.

4.6 Articles 12 to 14 of the Directive require the UK to limit, in specified circumstances, the liability of intermediary service providers who carry out certain activities essential for the operation of the Internet, namely those who act as "mere conduits" and those who "cache" or "host" information. These provisions were originally implemented by regulations 17 to 22 of the E-Commerce Directive. During the passage of the Terrorism Act through Parliament, the Government gave a commitment in Parliament "to bring forward a statutory instrument which will apply the protection against criminal liability currently enjoyed by mere conduits to the Terrorism Bill, as well as other provisions of the [E-Commerce Regulations]" (*Hansard*, 1 February 2006, Column 213). Regulations 5 to 7 of these Regulations create specific exceptions from liability for an offence under section 1 or 2 of the Terrorism Act for intermediary service providers when they provide mere conduit,

[3] Under sections 1(6) and 2(9) a person has a defence to the offences in sections 1 and 2 respectively if he can show, among other things, that a statement or publication did not express his views and did not have his endorsement.

[4] The Directive was incorporated into the EEA agreement by Decision 91/2000 of the EEA Joint Committee; the definitions of "EEA agreement" and "EEA state" inserted into Schedule 1 to the Interpretation Act 1978 by section 26 of the Legislative and Regulatory Reform Act 2006 are adopted in this memorandum.

[5] Section 17 extends the application of section 1 of the Terrorism Act to things done outside the UK, but only in so far as the offence relates to the encouragement of "Convention offences".

caching and hosting services, in the circumstances set out in the Directive and reflected in the E-Commerce Regulations.

4.7 These regulations also take into account Article 15 of the Directive which prohibits EEA states from imposing a general obligation on intermediary service providers to monitor the information which they transmit or store. The effect of the exceptions from liability in regulations 5 to 7 is that intermediary service providers could not be required to comply with any such general obligation arising from subsections (4) to (6) of section 3 of the Terrorism Act.

4.8 Where appropriate, the Regulations closely mirror relevant provisions in the Directive (in particular, Articles 12 to 14 of the Directive). However, as sections 1 to 4 of the Terrorism Act are concerned with criminal offences, it had been necessary to produce tailor-made provisions specifically to fit the Terrorism Act to ensure the precision required where criminal offences are involved[6].

4.9 A Transposition Note in respect of the Directive is set out in Annex A.

4.10 The scrutiny history of the Directive is set out in Annex B.

5. Extent

5.1 This instrument applies to all of the United Kingdom.

6. European Convention on Human Rights

6.1 As the instrument is subject to negative resolution procedure and does not amend primary legislation, no statement is required.

7. Policy background

7.1 The Directive seeks to contribute to the proper functioning of the Internal Market by ensuring the free movement of information society services within the EEA. One way in which it seeks to achieve this objective is through the country of origin rules described in paragraph 4.4. Similarly, the requirement to limit the liability of intermediary service providers described in paragraph 4.6 has been established because, as the Directive recognises, disparities in EEA states' legislation and case-law concerning the liability of service providers acting as intermediaries prevent the smooth functioning of the Internal Market, in particular by impairing the development of cross-border services and producing distortions of competition[7].

7.2 In the view of the Department of Trade and Industry and the Home Office this is an essentially technical measure to ensure that the Terrorism Act is consistent with the Directive. However, it is recognised that regulations 5 to 7, which create exceptions from liability for offences under sections 1 and 2 of the Terrorism Act, are considered by intermediary service providers to be of real significance. It is considered that the extension of sections 1 and 2 of the Terrorism Act in regulation 3

[6] A similar approach to implementing the Directive has been taken in the Tobacco Advertising and Promotion Act 2002 etc. (Amendment) Regulations 2006 (SI 2006/2369), see in particular regulation 9, and in new section 166A of the Criminal Justice and Public Order Act 1994 inserted by section 53 of the Violent Crime Reduction Act 2006.

[7] Recital (40).

to cover UK established service providers where they provide services in other EEA states will, in practice, cover only a small number of new cases. In many cases such providers will already be covered by sections 1 and 2, because, for example, they will be providing the services in question in the UK, as well as another EEA state. Further, it is expected that the public interest conditions in regulation 4 which limit the circumstances in which service providers established in EEA states other then the UK can be prosecuted for a section 1 or 2 offence or given a section 3 notice will, in practice, almost always be met. With regard to the exceptions from liability in regulations 5 to 7, the Home Office and the Department of Trade and Industry are of the view that, in any event, it is unlikely that intermediary service providers would be liable for offences under sections 1 or 2 due to the intent and recklessness tests in these sections 1 and 2[8]. However, regulations 5 to 7 now make clear the position regarding the liability of such providers.

7.3 Intermediary service providers were consulted about the Terrorism Bill during its passage. At the time they expressed their concern to the Department of Trade and Industry and the Home Office that the Bill would erode the limitations of liability that are required to be provided by the Directive. In particular, they were concerned that it would be possible for mere conduits and those providing caching and hosting services to be liable for an offence under section 1 or 2 of the Terrorism Act if they failed to comply with a notice given to them under section 3, in circumstances where the protections from liability laid down by the Directive should apply.

7.4 These concerns were mentioned in debates on the Bill (for example, during the third reading of the Bill, *Hansard*, 1 February 2006, Columns 203 to 214). And, as mentioned in paragraph 4.6, the Government gave a commitment in Parliament to bring forward a statutory instrument to address these concerns.

7.5 On 17 November 2006 the Department of Trade and Industry sent a copy of a draft of the Regulations to the intermediary service providers' representative body, the UK Internet Service Providers' Association (ISPA), in order to give intermediary service providers an opportunity to comment on the draft Regulations. ISPA responded with a small number of comments from its members on 5 December 2006. Department of Trade and Industry officials met with the Secretary General of ISPA to discuss these comments and the draft Regulations more generally on 21 December 2006. ISPA members would have preferred the circumstances in which a host is taken to have "actual knowledge" that information is unlawfully terrorism-related under regulation 7 to be limited to the case where a host is given formal or informal notice that information is unlawfully terrorism-related by those responsible for giving notices under section 3 of the Terrorism Act. By contrast, they suggested a host should not be taken to have actual knowledge that information is unlawfully terrorism-related if alerted to it by any other person. However, having considered this suggestion, the Department of Trade and Industry and the Home Office have concluded that such a limitation is not required by the Directive and would unnecessarily limit the effect of sections 1 to 4 of the Terrorism Act.

7.6 Guidance on the Directive and the E-Commerce Regulations is available on the Department of Trade and Industry's website[9]. Guidance on sections 1 and 2 of

[8] The Government also expressed this view in Parliament - see *Hansard*, 1 February 2006, Column 213).
[9] DTI - The Electronic Commerce Directive (00/31/EC) and the Electronic Commerce (EC Directive) Regulations 2002 (SI 2002 No. 2013)

the Terrorism Act is set out in Home Office Circular 8/2006[10]. The Home Office has also issued Guidance on notices issued under section 3 of the Terrorism Act which is available on its security website[11].

8. Impact

8.1 The Regulatory Impact Assessment prepared for the E-Commerce Regulations (which originally implemented the Directive) remains relevant to these Regulations. A copy is at Annex C.

9. Contact

9.1 Adam Richards at the Department of Trade and Industry Tel: 020 7215 2956 or e-mail: adam.Richards@dti.gsi.gov.uk can answer any queries regarding the instrument.

[10] http://www.circulars.homeoffice.gov.uk/

[11] Home Office | Security | Guidance on notices issued under section 3 of the Terrorism Act 2006. A revised version of the guidance, taking into account the effect of these Regulations, will be posted on the security website when these Regulations come into force.

Annex A

TRANSPOSITION NOTE FOR THE ELECTRONIC COMMERCE DIRECTIVE (TERRORISM ACT 2006) REGULATIONS

Directive 2000/31/EC of the European Parliament and of the Council of 8th June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) ("the Directive")

These Regulations apply the Directive specifically in the context of the Terrorism Act 2006 ("the Terrorism Act"), ensuring the precision that is required where criminal offences are concerned.

Article	Objective	Implementation	Responsibility
3 Internal Market	Article 3 is intended to contribute to the smooth functioning of the Internal Market by promoting the free movement of information society services among EEA states[12]. It requires the regulation of information society services on a country of origin basis.	See below.	
3(1)	Paragraph (1) of Article 3 requires each EEA state to ensure that information society services provided by service providers established on its territory comply with the national provisions applicable in that EEA state which fall within the "coordinated field", even where the information society services are provided in another EEA state.	Regulation 3 extends the application of sections 1 and 2 (and consequently sections 3 and 4) of the Terrorism Act to UK established service providers when they provide services in EEA states other than the UK, in so far as the Terrorism Act does not already achieve this effect. Paragraphs (4) to (6) of regulation 3 take into account the limitation in paragraph 1(1)(d) of Schedule 2 to the European Communities Act 1972 on the power conferred by section 2(2) of that Act.	Secretary of State
3(2), (4) and (5)	Paragraph (2) of Article 3 provides that EEA states may not, for reasons falling within the "coordinated field", restrict the freedom to provide information society services from another EEA state. However, it is permissible to derogate from this rule if the conditions set out in paragraph (4) of Article 3 are satisfied. By virtue of this provision, EEA states may take measures to restrict the freedom to provide information society services from another EEA state where such measures are necessary for reasons including, public policy and public security. The measures must be taken in	Regulation 4 means that proceedings for an offence under section 1 or 2 of the Terrorism Act may not be brought against information society service providers who are established in an EEA state other than the UK, or a section 3 notice given to such providers, unless the conditions set out in paragraph (4) of Article 3 are satisfied, where required. There is no requirement to comply with the cooperation steps in Article 3(4)(b) (reflected in regulation 4(5)) before instituting proceedings for an offence under section 1 or 2 of the Terrorism Act, as instituting such proceedings falls within the	Secretary of State

[12] The Directive was incorporated into the EEA agreement by Decision 91/2000 of the EEA Joint Committee; the definitions of "EEA agreement" and "EEA state" inserted into Schedule 1 to the Interpretation Act 1978 by section 26 of the Legislative and Regulatory Reform Act 2006 are adopted in this note.

	relation to an information society service that prejudices, or presents a serious and grave risk of prejudice, to the above objectives and they must be proportionate to those objectives. Except where court proceedings and acts carried out in the framework of a criminal investigation are concerned, before taking restrictive measures an EEA state must take the steps mentioned in paragraph (4)(b) to ensure cooperation with the Commission and the EEA state in which the service provider in question is established. Paragraph (5) of Article 3 provides that the steps in paragraph (4)(b) may be dispensed with in urgent cases.	exception to Article 3(4)(b) for court proceedings and criminal investigations.	
12 to 15 Liability of intermediary service providers	Articles 12 to 15 are intended to promote the smooth functioning of the Internal Market by seeking to remove disparities in the liability of intermediary information society service providers.	See below.	
12	'Mere conduit' Paragraphs (1) and (2) of Article 12 require EEA states to ensure that intermediary service providers who merely transmit information provided by a recipient of a service or provide access to a communication network are not liable for the information transmitted provided certain conditions are satisfied. The conditions are that the service provider does not: (a) initiate the transmission, (b) select the recipient of the transmission, or (c) select or modify the information contained in the transmission.	Regulation 5 ensures that the intermediary service providers covered by Article 12 are not capable of being guilty of an offence under section 1 or 2 of the Terrorism Act provided conditions reflecting those set out in Article 12 are satisfied.	Secretary of State
13	'Caching' Article 13(1) requires EEA states to ensure that intermediary service providers who transmit information are not liable for the automatic and temporary storage of information supplied by a recipient of a service, where such storage is performed solely for the purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, provided certain conditions are	Regulation 6 ensures that the intermediary service providers covered by Article 13 are not capable of being guilty of an offence under section 1 or 2 of the Terrorism Act provided that they comply with conditions reflecting those set out in Article 13. A notice given under section 3 of the Terrorism Act is an example of an order by an administrative authority to remove or disable access to information as referred	Secretary of State

	satisfied. The conditions are that the service provider: (a) does not modify the information, (b) complies with conditions on access to the information, (c) complies with rules regarding the updating of information, specified in a manner widely recognised and used by industry, (d) does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information, and (e) acts expeditiously to remove or disable access to the information stored upon obtaining actual knowledge of the fact that the information at the initial source of transmission has been removed or access to it has been disabled or a court or administrative authority has made an order to such effect.	to in paragraph (1)(e) of Article 13 (and reflected in regulation 6(3)(c)). Conditions (c) and (d) of Article 13(1) are not expressly reflected in regulation 6 as currently there are no readily identifiable industry standards of the kind referred to in those paragraphs.	
Article 14	'Hosting' Article 14 requires EEA states to ensure that intermediary service providers who provide a service consisting of the storage of information are not liable for information stored at the request of a recipient of the service as long as the service provider: (a) does not have actual knowledge of illegal activity or information, or (b) upon obtaining such knowledge or awareness, the service provider acts expeditiously to remove or disable access to the information. EEA states are not required to protect a service provider from liability where the recipient of the service is acting under the authority or control of the service provider.	Regulation 7 ensures that the intermediary service providers covered by Article 14 are not capable of being guilty of an offence under section 1 or 2 of the Terrorism Act provided that they did not know when the information was provided to them that it was unlawfully terrorism-related (as defined in the Terrorism Act) or, upon obtaining actual knowledge that the information was unlawfully terrorism-related, they expeditiously remove the information or disable access to it. Paragraph (3) ensures that the protection from liability does not apply if the recipient of the service is acting under the authority or control of the service provider.	Secretary of State
Article 15	Article 15 prohibits EEA states from imposing on intermediary service providers a general obligation to monitor the information they transmit or store or a general obligation actively to seek facts or circumstances indicating illegal activity.	The effect of the exceptions from liability in regulations 5 to 7 is that intermediary service providers cannot be required to comply with any general obligations to monitor information or activity arising from section 3 of the Terrorism Act.	Secretary of State

Annex B

Scrutiny History

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) ("the Directive")

DTI submitted explanatory memorandum 10644/99 on 20/9/1999 on an "Amended Proposal for a Directive of the European Parliament and of the Council on certain legal aspects of electronic commerce in the Internal Market". The Commons European Scrutiny Committee considered it politically and legally important and for debate (Report 28, Item 20423, Sess. 98/99). It was debated on 27/10/1999 in European Standing Committee C. The Lords Select Committee on the European Union cleared it from scrutiny (Progress of Scrutiny, 12/11/1999, Sess. 98/99).

DTI submitted an OTNA explanatory memorandum on 18/10/1999 on a "Presidency proposal for a Directive of the European Parliament and of the Council on certain legal aspects of Information Society Services, in particular, electronic commerce in the Internal Market". The Commons European Scrutiny Committee considered it politically important and for debate which was held on 27/10/1999 in European Standing Committee C (Report 2, Item 20529, Sess. 99/00). The Lords Select Committee on the European Union cleared it from Sub-Committee E by letter of 15/12/1999 (Progress of Scrutiny, 17/12/99, Sess. 99/00).

Finally, DTI submitted explanatory memorandum 5123/99 on 8/2/99 on a "Proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the Internal Market". The Commons European Scrutiny Committee considered it politically and legally important and for debate (Report 9, 19753, Sess. 98/99). This took place on 27/10/99 in European Standing Committee C on 27/10/99. The Lords Select Committee on the European Union did not report on it (Progress of Scrutiny, 11/6/99, Sess. 98/99).

REGULATORY IMPACT ASSESSMENT

1. Title of proposed measure

The Electronic Commerce (EC Directive) Regulations 2002[1]

2. The issue and objective

Issue: E-commerce provides the UK and the rest of the European Economic Area (EEA) with an opportunity to stimulate economic growth, industrial competitiveness and employment. To facilitate this, it is desirable to put in place an effective legal framework that would remove the chief obstacles to providing services electronically within the EEA. The Regulations will aim to do this and to meet legislative obligations in respect of the E-Commerce Directive. UK businesses will have to ensure that they are in compliance with the provisions of the Regulations.

Objective: The purpose of the Regulations is to create a framework within which UK business (particularly SMEs) and consumers will have the legal certainty needed to take full advantage of the opportunities offered by e-commerce. The main areas addressed are:

(a) identifying and clarifying rules so that both consumers and business have greater confidence about whose laws apply to an online transaction;

(b) ensuring transparency and consistency in the information to be provided by sellers to consumers about themselves, their offerings and how to conclude a contract online;

(c) ensuring consistency in aspects of online commercial communications, such as conditions for unsolicited emails; and

(d) limiting the liability of intermediaries who transfer or store information on behalf of others but are not aware of its content.

3. Risk assessment

The risks discussed below correspond to the four areas identified in the previous paragraph.

(a) A substantial barrier to the more confident and widespread use of e-commerce within the EEA is the imposition of restrictions by any of the 18 different sets of national legislation. As the UK is a nation with a relatively high proportion of foreign trade, UK business is particularly exposed to any restrictions associated with doing online business abroad. Compliance with restrictions prevailing in the Member State in which the recipient of the service is located entails considerable expense for business wishing to provide electronic services across borders, in terms of both ensuring that activities are lawful and keeping abreast of any alterations to the legal framework. Moreover, the absence of a harmonised legal framework may create uncertainty for the recipient of the service. The Regulations are a first step to liberalising online services and implement a partial harmonisation of single market rules so as to reduce the cost and time burdens for businesses and create greater certainty for service recipients.

[1] Title of Regulations Transposing 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) (OJ L 178, 17.7.2000, p. 1). The text (PDF 106 KB) is at europa.eu.int/eur-lex/en/lif/dat/2000/en_300L0031.html.

(b) Without specific information, service recipients will not know where to complain if necessary and it will be difficult to ensure that the service in question is supervised at source. Information about the seller, the relevant authorities in the seller's home country, the products and services and their prices and what to do to order online needs to be clear. In particular, consumer take-up is also likely to be inhibited by a diversification of approaches.

(c) Similarly, unless service recipients have information about an online advertiser (or the person on whose behalf he is advertising), they will not be able to protect themselves effectively against unwanted or unsolicited advertising emails. Without requirements that advertising emails are flagged as such, users may be discouraged from entering into e-commerce by the potential costs and difficulties of managing their electronic in-boxes.

(d) Without some harmonisation of the conditions under which intermediary providers of access and storage services could limit their liability for illegal or harmful information and activities, disparities in treatment by national authorities may grow and competitiveness may suffer. If liability is imposed, service providers may become less willing to provide certain services or may be forced to impose conditions on access to their services.

There are also major risks associated with a failure to implement the provisions of the Directive correctly into UK law. This could lead to proceedings being brought by the European Commission in the European Court of Justice. Failure could also to lead to the Government being held liable for any losses suffered by those denied their rights under the Directive.

4. Identification of options

Two principal options have been identified:

- option 1—do nothing; and
- option 2—specific implementation of the provisions of the Directive, in general and in detail.

5. Issues of equity or fairness

The harmonisation resulting from the Regulations will reduce the exposure of the public to certain risks.

The Regulations will improve the confidence of actual and potential consumers to engage in e-commerce and promote a level playing field for SMEs.

The Regulations are intended to impact evenly across all sectors of online service provision.

Though the Regulations apply to large and small businesses alike, SMEs in general have less administrative capacity to ensure compliance. However, they stand to benefit disproportionately, through easier access to new markets. SMEs trade less abroad than large companies, but even those confined to the UK market stand to benefit from the Regulations as most of the information, advertising and other provisions apply also to domestic transactions.

6. Identification of the benefits

Option 1: This has the benefit that there would be, for the time being at least, no change to the current legal framework. There would be no immediate cost for Government or business and consumers would continue to benefit from current levels of protection.

Option 2: If implemented consistently across the EEA, this has the benefit of allowing UK providers of online services to comply with only one national legislation—that of the UK—to a much greater extent than is currently the case, irrespective of where they do business in the EEA, by removing the need to track and comply with restrictions in up to 18 different national legislations when providing services within the EEA. It will similarly lift restrictions on providers of online services into the UK. However, UK enforcement authorities and courts will be able to take proportionate measures against certain incoming services in certain circumstances, for example, where it is necessary to protect public policy or consumers. On the whole, the Regulations should increase competition between online service providers and create more choice for UK consumers. They also benefit business and consumer confidence by requiring the provision of information about the service provider and providing for limitations on the liability of service providers who may unwittingly transmit or store illegal information.

7. Quantifying and valuing the benefits

The Regulations implement a complex Directive, with implications across several major areas of national and European Community law. Only broad, qualified estimates of its financial impact could be made. It is possible, however, to give an indication of the costs which service providers operating in a number of EC states currently bear, and which the Regulations should remove or decrease substantially.

The explanatory memorandum accompanying the original proposal for a Directive cites several examples of the costs associated with compliance with multiple sets of legislation, following a survey carried out by the Commission. In order to ensure compliance with different legislation, respondents indicated that they require considerable legal advice: examples were 50 days of legal advice to set up an appropriate system; 3-4 days of advice per month; and half an hour per month to maintain the system. One German estimate was DM70,000 per year. Another operator estimated that a review of the regulatory framework for online services in the UK alone had cost 60,000 ECUs. Assuming comparable review costs for each Member State, dependence on regulatory control in the state of destination might cost a company over €1m were it to cover all of the EEA, with ongoing costs of around €35,000 a year thereafter. Given the requirements of the applicant states to implement the directive on or before accession, these costs can be roughly increased by two-thirds again in respect of pan-single market operation in the medium term. This compares to costs of regulatory control in the country of origin, which might for such a business be £40,000 initially, with minor recurrent costs thereafter. These are very general indicative illustrations. The simple calculation below takes much lower figures as its basis.

There were 3.7 million businesses in the UK at the start of 1999. Only 7,000 were large i.e. over 250 employees; and 24,000 were medium i.e. 50-249 employees. Small businesses (those with less than 50 employees) made up 38% of all turnover and most were micro i.e.1-9 employees. 2.3 million businesses were sole traders or those without employees. The UK Online Annual Report 2000 indicated that 450,000 SMEs were actually trading online, and seven out of ten entrepreneurs were pursuing e-commerce opportunities. Over 81% of all British businesses are now online (and over half of micro-businesses)

Assuming the benefits of doing without one-off review costs are on average £15,000 and yearly costs thereafter are £5,000 for the 31,000 large and medium companies (who are assumed to want or need to trade online widely in the single market), and respectively £3,000 and £1,000 for say 200,000 SMEs likely to trade online in Europe, this produces one-off benefits for the UK of about £1 billion and yearly savings of about £350 million.

This calculation leaves out sole traders, and businesses not yet online. It disregards the likelihood that many businesses will either have already done a one-off review, or would still want to do a substantial periodic review of legal conditions for trading across borders in Europe.

Whilst this example is only illustrative, it does suggest the order of magnitude of the savings that may accrue to businesses—and ultimately to the consumer—through Regulations implementing option 2. The calculation is also sensitive to the precise scope of implementation in the different Member States. Option 1 would not yield these benefits but would avoid the costs associated with transposition, implementation and enforcement of the Directive.

8. Compliance costs for business, charities and voluntary organisations

(i) Business sectors affected

The Regulations affect everyone providing online services within the internal market, given the definition of "information society services" as any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. It follows that the Regulations affect a large number of businesses, charities and voluntary organisations now, and their numbers should increase as the attractiveness of e-commerce grows.

(ii) Compliance costs for a "typical" business

The following costs are for option 2; option 1 imposes no immediate direct additional costs on business.

There will be costs relating to ensuring that the provision of services complies with all the relevant national legislation. In some cases, there may be a cost of changing to compliance with UK legislation instead of that of particular markets in the EEA. If these costs are greater than those that businesses bear at the moment, however, it is likely to be because of compliance with other instruments (covering advertising, licensing etc.) since the present Regulations will merely require compliance with home-state controls in such areas.

There will be some additional expenses involved in ensuring that certain information is provided on a website or other means of promoting the service. However, the type of information required is not expensive to procure, the majority of responsible businesses would aim to provide such information anyway and the costs and effort concerned would probably be integrated with the burden of meeting the interrelated information requirements of the Consumer Protection (Distance Selling) Regulations 2000.

There may also be some costs for certain businesses (e.g. those standing to benefit from the sending of unsolicited commercial communications) from the requirement for information provision, though much of this is already undertaken by advertisers in accordance with industry standard practice.

Intermediary providers of access and storage services may face some expenses if they are to benefit from the limitation of liability provisions of the Regulations. One respondent to the public consultation on draft Regulations who engages in such activities estimated that it would incur the following costs per annum to operate an effective notice and takedown regime in the 13 Member States in which it currently operates:

- £60-90,000 in legal costs;
- £80-120,000 in engineering and technical costs.

The Regulations may result in some one-off expenses for affected organisations. These would result from any necessary alterations to the systems in place and would vary according to the organisation. They are very hard to estimate with any degree of accuracy. None of the 100 respondents was able to give an estimate of any of these costs in the DTI's consultation exercise on the draft Directive in 1999, and only one respondent felt able to suggest the areas in which costs would be reduced or increased, despite a specific question about this. Similarly, only one of the almost 100 respondents to DTI's consultation in 2001 on its approach to implementation provided an estimate of compliance costs, and this was predicated on assumptions that are not reflected in the Regulations.

(iii) Total compliance costs

The costs of compliance with these Regulations will depend on the size of the organisation, its current level of involvement in e-commerce, the extent of the changes required to comply with the Directive, the level of systems change required and the extent to which alterations resulting from this Directive are made as part of the process of updating and upgrading required to provide an effective online service.

9. Consultation with small business: "the litmus test"

Small businesses have not provided figures for compliance costs. We expect there will be some impact on small business, although it should not be significant given that most small businesses involved in e-commerce should already comply with the majority of the requirements anyway. In principle, costs for small businesses would in themselves be lower (but greater in proportion to revenues), and benefits higher, than for larger businesses.

10. Identification of any other costs

Option 1: The absence of specific implementation of the Directive is likely to cause uncertainty that will inhibit the growth of e-commerce and therefore potentially impose costs on the UK (e.g. resulting from reduced competitiveness, lower employment and less economic growth).

Option 2: Implementation of the Directive by legislative and non-legislative means and enforcement of the Regulations will entail additional costs for Government and other organisations as set out below.

There will be enforcement costs for UK enforcement authorities (e.g. the Director General of Fair Trading, Trading Standards Departments etc.) acting on behalf of consumers in other Member States and encouraging other Member States' authorities to act on behalf of UK consumers. Implementation of the Directive will place a resource demand on local authorities in England, Wales and Scotland to effectively ensure compliance with the Regulations. The publicity surrounding implementation may give rise to an initial increase in demand for consumer and business advice and there may be an expectation on local enforcement

authorities to undertake promotional and educational work for consumers and businesses on the new legislation.

Additional administrative functions also flow from Articles 16, 17, 19 and 21 of the Directive, which are not directly implemented by the Regulations. Activities that will need to be resourced include:

- implementing and monitoring the Regulations and other obligations under the Directive;
- encouraging the development of codes of conduct and means of alternative dispute resolution;
- establishing and acting as contact points for the provision of advice and assistance to business and consumers;
- forwarding information to the Commission on developments in the UK, attending discussions on the implementation of the Directive and participating in the review of the Directive in 2003 and every two years thereafter;
- providing information and assistance when sought by other Member States and cooperating with their requests for regulatory enforcement action and the search for acceptable solutions to cross-border problems before Community legal action is invoked; and
- the operation of the procedures associated with the exercise of derogations from the requirement not to restrict the cross-border provision of information society services, whether invoked by the UK or by other Member States in respect of services originating in the UK.

11. Results of consultation

DTI consulted generally on the draft Directive in 1999 and on its approach to implementation in 2001. It received some 100 contributions from businesses, consumers, their representative organisations and others on each occasion. It consulted on draft Regulations and accompanying guidance for business between March and May 2002. In the course of discussions with interested parties, a number of other unquantifiable points about the costs and benefits of the Directive have emerged. These are additional to points dealt with above and might be summarised as follows:

- Regulations that genuinely facilitate the use of e-commerce are likely to reduce business costs by encouraging the use of cost-effective delivery mechanisms that are able to reach the maximum number of consumers; and
- SMEs will be particularly handicapped by inconsistent implementation of the Directive since they are less likely to be able to afford sound legal advice and will therefore be discouraged from exploiting the opportunities afforded by the internal market and investing in the European development of their businesses.

12. Summary and recommendation

Option 1 is not attractive since it foregoes substantial likely net benefits and would be in breach of the UK's Community obligations.

Option 2 will bring some costs in the form of business-systems changes required to ensure compliance with the Directive. However, these should, on the whole, be relatively small and may not apply to those entering the electronic market in the future (although, clearly, they will need to comply from day one). It will also bring costs with regard to transposition and enforcement. Offsetting these are commensurate benefits to consumer and business confidence and the fact that business opportunities will be increased considerably through the removal of restrictions on the cross-border provision of information society services. The DTI's assessment is that the benefits of the Regulations outweigh the costs and justify option 2.

13. Enforcement, sanctions, monitoring and review

See section 7, above.

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 Minister .....Alan Johnson...

(Minister of State for Employment Relations, Industry and Regions)

Date 30.7.02

Contact: Mary Tait
BRCII2 International Communications,
Department of Trade and Industry
Room 206
151 Buckingham Palace Road
London, SW1W 9SS
tel: (020) 7215 1807
fax: (020) 7215 4161
email: Mary.Tait@dti.gsi.gov.uk