

Draft Electronic Commerce (EC Directive) Regulations:

Response from The Internet Services Providers Association (ISPA) UK

Introduction

ISPA welcomes this opportunity to comment on the UK's implementation 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).

The Internet Services Providers' Association (ISPA) UK is the trade association for companies involved in the provision of Internet services in the UK. ISPA was founded in 1995, and seeks to actively represent and promote the interests of businesses involved in all aspects of the UK Internet industry. Its membership includes Internet service providers (ISPs), backbone providers, cable companies, web design and hosting companies and a variety of other organisations. ISPA currently has approximately 100 members, representing around 90% of the UK Internet access market. A list of members is attached at Annex 1.

Executive Summary

- ISPA urges the DTI to provide legal certainty to UK service providers and clarify that they are, in principle, only subject to the national laws and regulations of the UK i.e. the laws of their 'country of origin'. ISPA believes this principle, outlined in the Directive, is essential for the development of e-commerce in the UK.
- ISPA believes that, as currently drafted, the Regulations regarding the limitation of liability of intermediaries are unnecessarily complex. The insertion of the words '*in damages*', and the separate Regulation providing a defence in criminal proceedings, distinguishes between a service providers' civil and criminal liability. Regulation 21 also appears to lower the threshold of knowledge to one of *constructive* knowledge rather than *actual* knowledge. ISPA therefore urges the DTI to delete '*in damages*' from Regulations 17-19, and delete Regulation 21 in its entirety.
- ISPA believes the lack of a specific definition of actual knowledge gives rise to a number of problems, and therefore encourages the DTI to provide adequate guidance on what *doesn't* constitute actual knowledge. In addition, ISPA suggests that minimum requirements to be contained within a notice are also suggest in the Guidance for Business, providing clarification for all relevant parties.
- ISPA urges the DTI to include providers of hyperlinks and location tool services within the scope of the Regulations regarding the limitation of liability of intermediaries. In the absence of adequate legislation, conflicting case law across Europe will continue to cause legal uncertainty for providers of such services.
- ISPA urges the DTI to clarify within the Regulations that service providers have no general obligation to monitor material transmitted across or stored on their networks,

in order to avoid future misunderstandings and misconceptions regarding the role, status and capabilities of service providers.

- In order for the development of procedures dealing with the removal of illegal information to move forward, ISPA believes it is necessary for codes of conduct to be underpinned by statute. ISPA therefore urges the DTI to consider providing a horizontal legal framework upon which voluntary codes of conduct can be developed.

Country of Origin Principle – Regulation 7 (Article 3 of the Directive)

The E-Commerce Directive states that currently *‘legal uncertainty exists with regard to the extent to which Member States may control services originating from another Member State’*. The Directive therefore attempts to provide certainty by clarifying that service providers should be subject to the national laws and regulations of the Member State in which they are based, i.e. their ‘country of origin’. This approach provides legal security to service providers as to which law is applicable, thereby enabling the correct functioning of the Single Market in the area of e-commerce. This principle is essential for UK businesses, in particular SME’s, wishing to provide services across the European Union, and has been correctly implemented by other Member States including Austria, Germany and Luxembourg.

Whilst this is clearly the intention of the Directive, the UK’s draft regulations do not appear to adopt this approach. The current drafting implies that the UK has adopted a ‘country of destination’ approach, whereby service providers are subject to the laws of the Member State in which the service is *received*. As currently worded, the draft regulations do not give the required security to service providers.

The UK’s draft regulations state:

‘... an enforcement authority with responsibility in relation to any enactment or other legal requirement shall ensure that the information society services provided by a service provider from an establishment in the United Kingdom comply with that enactment or legal requirement which applies to an information society service and falls within the co-ordinated field irrespective of whether the service in question is provided in the United Kingdom’.

ISPA believes this Regulation is unnecessarily complex and also misinterprets the meaning of Article 3.1 of the Directive. The regulations refer to the *enforcement* of applicable law by UK authorities, but nowhere state that service providers are only subject to UK law *or* what the applicable law is. Consequently, service providers established in the UK are left with uncertainties regarding the applicability of foreign law, precisely the uncertainties that the Directive seeks to remove by making the applicable law the country of origin of the service provider.

ISPA believes that the UK’s interpretation of the Directive will cause substantial harm to the development of e-commerce in the UK. Whilst UK service providers will be subject to the laws of the UK and 14 other Member States, competitors based in those countries will be required, broadly, to comply merely with the laws of the country in which they are established. As a result, companies established in the UK will be placed at a competitive disadvantage to those in other Member States, as they will be confined practically to e-trading solely in a domestic market, while their European competitors trade across Europe, including the UK. At the same time, the UK will become a less attractive location for non-European companies seeking a base for their European operations. The knock on effects for the UK economy, and indeed the economy more widely, could be severe.

ISPA notes that in its separate current consultation on the implementation of the E-Commerce Directive, HM Treasury favours an adoption of the country of origin principle. The consultation document states the following:

‘In implementing the E-Commerce Directive in Financial Services, the Government aims to bring the full benefits of country of origin regulation to businesses that provide information society services’.

In a third separate consultation, the Financial Services Authority also states:

‘It is, therefore, UK policy to enhance competition and innovation by supporting the transition to a Community-wide system in which a firm needs to comply only with the... requirements in force in the country from where the service is provided... - the country of origin approach.’

ISPA also wishes to draw the DTI’s attention to comments made by Patricia Hewitt, the then Minister for E-Commerce, during the Parliamentary Committee hearing on the Electronic Communications Bill (9.12.99), where she said:

‘At the Single Market Council on Tuesday, we finalised a common position on the electronic commerce directive based, crucially, on the principle of supplier’s country of origin. We are therefore making progress in the United Kingdom and Europe in creating the right conditions for electronic commerce.’

In July 2000, the eEnvoy’s Monthly Report to the Prime Minister, signed by Patricia Hewitt and Andrew Pinder, also stated:

‘On 4 May [2000] the European Parliament approved without an amendment the e-commerce Directive. This will ensure that e-commerce traders in the EU need comply only with the law in their home Member State.’

ISPA therefore urges the DTI to amend Regulation 7 in order to clarify that the objective of the UK government is to ensure that service providers established in the UK are subject to UK law, giving service providers the degree of certainty required to encourage the development of e-commerce in the UK.

ISPA suggests that wording similar to that contained in Luxembourg, Austria or Germany’s transposition is adopted:

(Luxembourg)

‘The legislation of the place of business of the information society service provider shall be applicable to providers and the services they provide, without prejudice to the freedom of the parties to choose the law applicable to their contract.’

(Austria)

‘In the co-ordinated field, the legal requirements for a service provider established in a Member State shall be determined in accordance with the law of such state’.

(Germany)

‘Service providers established in the Federal Republic of Germany and the teleservices thereof shall be subject to the requirements of German law even if the teleservices are offered or rendered commercially in another state’.

Amending draft Regulation 7 in this manner will provide clear and concise legal certainty to service providers, and will encourage foreign investment in the UK economy.

As a consequence of this amendment, ISPA also believes that Regulation 5 (Private international law) should be deleted. ISPA is concerned that, as currently drafted, Regulation 5 suggests that the law applicable to information society services will be determined according to private international law, and therefore gives legal weight to Article 1(4) of the E-Commerce Directive, which was not intended by the Directive. As the purpose of private international law is to deal with conflicts of applicable law, ISPA believes this Regulation is redundant because the Directive clearly prescribes the applicable law (the country of origin) with the exception only of the given derogations. ISPA therefore urges the DTI to delete the Regulation.

Limitation of liability of intermediaries – Regulations 17-19 (Articles 12-14 of the Directive)

ISPA broadly welcomes the clarification provided by both the Directive and the draft regulations regarding the liability of intermediaries. However, ISPA believes that the DTI has not adopted a straightforward approach when drafting the UK regulations and is particularly concerned about the precise wording of Regulations 17-19.

As currently drafted, Regulations 17-19 state:

‘Where an information society service is provided... the service provider (if he otherwise would) shall not be liable in damages’,

The insertion of the words ***‘in damages’*** in this way suggests that the limitations can only be used as a defence in *civil* proceedings, not in criminal proceedings. In order to address this, a separate regulation, which provides a defence for criminal proceedings, has been inserted (Regulation 21). However, this regulation appears to impose a *lower* threshold of knowledge to incur liability than the Directive intended, by stating that in criminal proceedings Regulation 19(a)(ii) shall not apply.

Regulation 19(a)(ii) limits a service providers’ liability ***‘if the service provider was not aware of the facts or circumstances from which it would have been apparent to the service provider that the activity or information was unlawful.’*** If this limitation does not apply in criminal proceedings, the knowledge threshold is lowered to one of one of *constructive knowledge*, rather than *actual knowledge*. This is quite clearly contrary to the provisions of the E-Commerce Directive, which applies a blanket actual knowledge test, rather than setting different thresholds for civil and criminal liability. ISPA believes this exclusion not only exposes service providers to legal uncertainty, but also sets a dangerous precedent, with damaging implications for UK e-business, as UK companies may find themselves liable for content which they *should* have known was illegal.

ISPA does not believe that this was the intention of the DTI, and therefore calls on the DTI to delete the words ***‘in damages’*** from Regulations 17-19 and delete Regulation 21 in its entirety, thus limiting the liability of service providers in both civil and criminal proceedings. Not only does this avoid overly complex detail, but it also brings the regulations back in line with the Directive.

Definition of ‘Actual Knowledge’

The Regulations and the Directive limit the liability of a service provider on the condition that it does not possess ‘actual knowledge’ of illegal activity or information. However, as noted in the Guidance for Business, the Regulations do not specify how actual knowledge is obtained.

The lack of a specific definition of actual knowledge or awareness gives rise to a number of problems. Does a service provider acquire actual knowledge once the illegality of the material in question is confirmed? Or is knowledge acquired much earlier, for instance as soon as a customer makes a complaint, regardless of the level of detail of the complaint? And who can provide such knowledge?

The definition of actual knowledge is very much open to interpretation, and it is particularly difficult for a service provider to predict how this may be interpreted by a court of law. Moreover, there are likely to be discrepancies between what a service provider and a customer consider to be actual knowledge. In practice, a service provider is currently required to investigate any complaint it receives about potentially illegal content, no matter what level of information is provided by the complainant. In extreme situations, service providers find themselves the subject of hoax complaints, which may have been submitted anonymously with very little information about the content or its location. In the current climate of legal uncertainty on this issue, a service provider must always assume that it has obtained actual knowledge, regardless of the level or validity of information provided in a complaint.

The Guidance for Business states that the burden of proof should rest with the complainant, but ISPA is concerned this burden of proof has been placed without adequate guidance to service providers on the interpretation of this term, in order that they can make a reasonable legal assessment. ISPA believes that the DTI must provide more adequate guidance for all relevant parties (service providers, complainants, enforcement bodies) in order that procedures for the removal of infringing material can be clear and efficient. ISPA therefore suggests that the first sentence of paragraphs 6.6 and 6.8 of the Guidance for Business are replaced with the following:

‘Obtaining ‘actual knowledge’ means, at least, that a service provider has factual knowledge of both the activity and its illegality. The mere fact that the content appears on a website hosted by the service provider in question should not constitute ‘actual knowledge’. It should not be deemed sufficient that the service provider could have known or should have known of the activity and its illegality.’

Following on from this, ISPA would like the Guidance for Business to clarify that a service provider would not be considered to have actual knowledge unless certain basic requirements are contained within a notice, in order to assist service providers when considering potentially infringing material.

‘A notice should at least;

- (1) Be made in writing***
- (2) Be addressed to a designated agent of the service provider (e.g. individual or department)***
- (3) Clearly identify the subject of the complaint***
- (4) Establish the right of the complainant to make his/her claim***
- (5) Give details of the nature of the claim, and***
- (6) Provide reasonable evidence to allow the service provider to assess the validity of the claim.’***

A statement regarding the minimum requirements would not only provide clarity for service providers; it would provide guidance for genuine complainants and would enable service

providers to recognise and respond to complaints in a quick and efficient manner. This would promote one of the principle aims of the Directive, which involves constituting '***the appropriate basis for the development of rapid and reliable procedures for removing and disabling access to illegal information***'. The requirements would also have the effect of deterring vexatious complaints, which in turn would help protect service providers against the risks of wrongful removal.

Providers of Hyperlinks and Location Tool Services

ISPA is also concerned that the regulations fail to address the liability of providers of hyperlinks and location tool services. There is a great deal of conflicting case law across Europe surrounding this issue, which has created confusion and legal uncertainty for providers of such services. In the absence of adequate legislation, this uncertainty is likely to increase with the rise in the number of disputes, threatening the growth of e-commerce in the UK. In particular, companies providing such services may be encouraged to locate their businesses elsewhere, in a Member State with a more favourable regulatory climate.

Whilst the Directive will review this issue in 2003, ISPA believes that the conflicting case law across Europe necessitates that the issue is given urgent attention by the DTI. The Directive does not prevent Member States from dealing with this issue, and indeed, Member States such as Austria, Spain and Portugal have addressed it already in their transpositions of the Directive. ISPA therefore urges the DTI to follow suit, as a failure to address the issue in the UK regulations will only add to the existing uncertainties, and may act as a disincentive or deterrent for companies to provide these services.

ISPA therefore believes that the regulations covering the liability of intermediary service providers should be augmented to include providers of hyperlinks and location tool services. A model provision based on Articles 12-14 of the Directive could be used:

'Where an information society service is provided which consists of the creation and provision of hyperlink, location tool or content aggregation services, the service provider (if he otherwise would) shall not be liable as a result of provision of that service where-

- a. the service provider-***
 - i. does not have actual knowledge that an activity or information was in breach of any law; and***
 - ii. is not aware of facts or circumstances from which it would have been apparent to the service provider that the activity or information was unlawful; or***
- b. upon obtaining such knowledge or awareness the service provider acts expeditiously to remove or disable access to the information, and***
- c. the recipient of the service was not acting under the authority or the control of the service provider.***

Alternatively, the definition of what constitutes 'hosting' (Regulation 19) could be amended, either in the Regulations themselves or in the Guidance for Business, in order to take account of such services. Under the draft Regulations, hosting is defined as the storage of information provided by a *recipient* of a service. It is equally usual for hosted material to be sourced by the service provider itself for inclusion in an online directory, without any actual knowledge of the legality or otherwise of the hosted material, therefore providers of such services could be categorised as providing hosting services.

No General Obligation to Monitor (Directive Article 15)

Article 15 of the E-Commerce Directive, which clarifies that service providers have no general obligation to monitor, has not been transposed into the UK's draft Regulations. Whilst ISPA welcomes the clarification provided by the Guidance for Business that no such obligations exist under UK law, and that their introduction would be incompatible with the E-Commerce Directive, it believes that its inclusion is necessary in order to further clarify the role and status of a service provider.

Article 15 provides a welcome clarification to service providers of their monitoring obligations, and is based on logical reasoning that it would not be possible – practically or economically – to force service providers to monitor content which is stored or transmitted across their networks.

Recent High Court Injunctions, and their subsequent interpretation and application by some quarters of the legal profession, have demonstrated a widespread misunderstanding about the role and capabilities of service providers, despite the prior publication of the E-Commerce Directive. On such an occasion, a High Court Injunction attempted to clarify the position of ISPs by stating that service providers would not be in breach of the Injunction unless they **'failed to take all reasonable steps to prevent the publication'**. It was not clear whether 'reasonable steps' included pro-active monitoring. What constituted 'reasonable steps' was not clarified by the Attorney General. Similarly, on another occasion, ISPA members received a solicitor's letter advising:

'We are serving this injunction as a matter of course on all members of the Internet Services Providers Association. We do not believe that you currently feature any information on any of your websites about this child. However, we are putting you on notice, that should you be approached in the future, you should refrain from featuring any information which relates to proceedings involving this child.'

ISPA was concerned about the ambiguity of the above wording, believing it to imply that service providers were expected to monitor content or act prior to the existence of any such information on its servers, which is quite clearly incompatible with the E-Commerce Directive. ISPA believes that clarification on this point would avoid the occurrence of such misunderstandings.

Other Member States have seen fit to include such an article in their transposition, such as Austria, where the Regulations state:

'... the service providers... shall not be obliged generally to monitor the information stored or transmitted by them or to seek out circumstances indicating illegal activities'.

ISPA therefore recommends that the DTI include a new Regulation which states:

'Nothing in these Regulations shall impose either a general obligation on service providers, when providing such services, to monitor the information which they transmit or store, or a general obligation to seek facts or circumstances indicating illegal activity. Monitoring obligations in specific cases shall be strictly limited and specified in law.'

Code of Practice for Notice and Take Down

Neither the E-Commerce Directive nor the draft Regulations specifically address procedures for removing or disabling access to illegal information. However, the Directive is clear in its recommendation that Member States should encourage the development and adoption of such procedures, perhaps in the form of codes of conduct.

ISPA believes that it is vital to develop such procedures and therefore looks forward to participating in the developments of any codes. 'Notice and takedown' is the procedure currently recognised by service providers for dealing with illegal material; a service provider is put on 'notice' that illegal or infringing exists on its servers, which it then removes or blocks access to, making the material unavailable via the Internet.

At present, this procedure is only formally recognised by an agreement between ISPs and the Internet Watch Foundation, an organisation established to combat criminal material on the Internet, such as child pornography. The procedure is successful because there are clear guidelines on what constitutes criminal material, and specially trained staff assess the legality of material according to these guidelines.

However, difficulties arise when this procedure is applied to other types of illegal content that may be defamatory or infringe copyright. Passing judgement on the legality of such material is extremely difficult and the risks for service providers associated with such decisions are great. On the one hand, a service provider may doubt the validity of a complaint or consider the material to be legal, and may therefore choose not to 'takedown' the content, risking legal action from the complainant. On the other hand, if the material is taken down, but subsequently proved to be legal, the service provider risks legal action from the content owner. Posed with these decisions, it is difficult for a service provider to act *expeditiously* to remove the material, as the Directive and draft regulations expect.

These issues have hindered self-regulatory developments so far, and it has become obvious that for developments to move forward, provisions for a 'safe harbour' for service providers (i.e. protection from suit if they remove content in good faith following a complaint) need to be addressed. ISPA believes that the only way to address this issue is to underpin any code of conduct governing the removal of illegal material by statute. Service providers that followed the procedures outlined in any such code could then be protected from liability for claims following the removal of material.

ISPA therefore advocates the inclusion of another regulation, giving the Secretary of State powers to approve industry and/or professional codes of practice. Not only will this provide an incentive to all parties involved in the provision of information society services to develop balanced and effective procedures; it will also provide some form of protection to service providers who take steps to ensure that material is removed expeditiously. ISPA believes that a code of conduct underpinned by statute would be of useful assistance to judges in cases where disputes regarding the removal of illegal or infringing material went to court, and would provide intermediaries, content providers, users and other stakeholders with legal security.

ISPA therefore proposes that the following additional horizontal Regulation be included, providing a framework for the development of voluntary codes of conduct for the removal of illegal material:

'(1) The Secretary of State may by order approve, and from time to time seek revision of one or more industry or professional codes of practice which establish:

- (a) a form of notice sufficient to constitute actual knowledge of the presence of infringing or otherwise illegal material on a relevant service or site ("Notice"),***
- (b) the circumstances required for removal or disabling of access to such material ("Takedown") and***
- (c) the basis upon which the content provider may object to or prevent a Takedown or cause a reinstatement of material.***

- (2) *Before approving or issuing an Approved Code, the Secretary of State shall consult with those persons to whom the Code will apply (and may do so by consulting with one or more persons who, it appears to him, represent those persons).*
- (3) *A code of practice under (1) above ("an Approved Code") may be restricted to a particular class of material, infringement or liability.*
- (4) *An Approved Code may apply:*
- (a) *to service providers bound by or subscribing to a specific set of professional rules;*
 - (b) *to all service providers of a description specified in the Code; or*
 - (c) *to all service providers generally.*
- (5) *An Approved Code shall specify the following matters:*
- (a) *The requirements for a valid Notice;*
 - (b) *The actions necessary for Takedown, and what response time may be deemed expeditious for the purposes of Regulations 18(b)(v) and 19(b);*
 - (c) *The conditions necessary for any counter-notice, and its expiry;*
 - (d) *Any other consequential duties or liabilities, howsoever incurred and*
 - (e) *any procedure(s) which may be required for the resolution of disputes.*
- (6) *Where a service provider arranges for Takedown or reinstatement of any material in compliance with either R 18(b)(v) or R19(b), and a relevant Approved Code, he shall be protected from any liability to any person for claims based on his having removed, disabled access to or reinstated the material.*

Further Information

For further information, please contact:

Stephanie Harris
Public Affairs Manager

Tel: (020) 7233 7234

Email: secretariat@ispa.org.uk

ANNEX 1

List of ISPA Members

AbbTel
Ad-Libs
Adweb
Aggregated Telecom
Altohiway
AOL UK
ATLAS Internet
BiblioTech
BMC Software
Brightview
BT
Business Serve
Cable & Wireless
Centralnic
City Netgates
Community Internet
Demon Internet/Thus
DIALnet
Drakken
EasyEverything
Easynet
Eircom NI
Energis
Entanet
e-xentric
Fastnet International
Freechariot
Freeserve
Global Crossing
Internet Services
GreenNet Educational
Trust
GTS Netcom
ICL
iDesk
Intel Corporation
Intensive Networks
Interalpha
Internet Central
Internet Computer
Bureau
Internet UK
Ision Internet
Keycom

Kingston
Communications
Level 3
Communications
Microsoft
Mill House Internet
Services
Mirror Image Internet
Nameplanet
Names.Co Internet
Net CIB (Computers
in Business)
Netcetera
Netkonect
Communications
Netscalibur
Nettec
NewNet
Nextra
Nokia Internet
Communications
Nominet
NTL Internet
OA5
Paradigm ICT
Pipex Internet
PlugIn.co.uk
POPTel
Power Internet
Prestel On-Line
PSINet
Research Machines
SAA Consultants
Sprintlink
Star Internet
Sun Microsystems
Supanet
Synergie
The Internexus Group
Tiscali
Totalise
Via NetWorks
Video Networks
Vizzavi

Web Leicester
Which? Online
Wichity Corporation
WorldCom
Xchangepoint
Yahoo! UK