

# **A Response to the Consultation on The Electronic Commerce (EC Directive) Regulations 2002**

Submitted by: Mark Gracey, Legal Liaison Manager  
Thus plc  
E: Mark.Gracey@thus.net  
T: +44 (0)20 8492 7176

Clive Feather, Internet Expert  
Thus plc  
E: Clive.Feather@thus.net  
T: +44 (0)20 8371 1138

Date: 2<sup>nd</sup> May 2002

This response may be published on our web site and may be published in full by the Government.

## **Thus plc**

Thus plc is a leading provider of Internet, call centre, data and telecoms services in the United Kingdom. Our Internet services are principally offered under the 'Demon' brand both in the UK and the Netherlands.

## **Introduction**

We welcome this opportunity to respond to the DTI's consultation on the Regulations to implement the provisions of the E-Commerce Directive. We see the Directive as a great step forward in the development of a legal framework for E-commerce and a great opportunity for a new era of legal certainty for E-commerce and Communication Service Providers.

We have chosen to focus this response on our three main areas of concern. Specifically the "country of origin" principle (Regulation 7); commercial communications (Regulations 9 and 10); and the liability of intermediaries (Regulations 17, 18, 19, 20 and 21).

## **The "Country Of Origin" Principle (Regulation 7)**

We believe that it is important that a Service Provider should be governed by legislation laid down in its Member State, and not by any other Member State's laws, even if the recipient of the service is not in the same Member State.

The Directive attempts to confirm this by clarifying that Service Providers should be governed by the legislation of the Member State within which they are based. However, the draft Regulations do not appear to provide this clarity. There is no mention that Service Providers are only subject to UK law.

We should all be reminded of the Yahoo! Nazi Memorabilia case, in which a French law which prohibits any French person from buying or selling Nazi memorabilia was used against Yahoo!: they have been ordered to prevent any French users of the Internet from gaining access to particular parts of the Yahoo! Auction site, which sell such material. This order applies to all their services, including those operated in the United States and accessed by French customers of other ISPs.

We would not want to be in a position where laws in countries within which we do not operate could govern us.

Most Member States such as Austria and Germany have already implemented this part of the directive correctly and we urge the Government to do the same in the UK implementation.

## **Commercial Communications (Regulations 9 and 10)**

We receive, on average, 3000 complaints a month from our customers, complaining about unsolicited commercial communications that they have received. Although a proportion of the material they are complaining about may not originate within the EC, it highlights how large the issue really is for our customers.

Dealing with these complaints presents a clear resource issue for us, but the problem does not stop here. Unsolicited commercial communications constitute a major load on Internet Service Provider's (ISP's) systems at little or no benefit to the ISP and its customers

No amount of marking unsolicited communications "clearly and unambiguously identifiable" will solve this problem. In fact, it may indeed increase the problem as more Service Providers feel that they can use email to promote their products and services, resulting in clogged up customer mailboxes (with email they typically don't want or indeed read) and overloaded ISP networks.

Although the Directive does not impose the need to define what "clearly and unambiguously identifiable" may mean, we urge the Government to provide a definition so that ISP systems can automatically detect such communications. This could be easily achieved, by simply adding an extra header to the email (e.g. an SMTP "Unsolicited-Commercial: yes" header). This would allow automated processing and would retract from any argument that putting a marker in the subject of the message would restrict creativity by the author.

At this point we would like to raise again the point we made in our previous response to the consultation on the implementation of the Directive, about "opt-in" lists. We feel strongly that opt-in is the only solution, and we refer the Government back to our previous response:

“At this point it is a good idea to address the terms “opt-in” and “opt-out” and the confusion that sometimes arises between them. As far as we are concerned, “opt-in” includes any arrangement whereby the end user has taken some action *which they were aware* would add their address to a mailing list or equivalent. That is, either:

- at the time that they supplied their address, they explicitly asked to receive relevant communications;
- at the time that they supplied their address, they were offered the opportunity to not receive such communications and did not take it (sometimes known as “implicit opt-in” or “inertia opt-in”).

We are aware that some people class the second situation as “opt-out”, but we do not; in our opinion, any subsequent communications were solicited. We would recommend that the transposition adopt wording similar to the following<sup>1</sup>:

Electronic mail and SMS shall only be used for the purpose of direct marketing where:

- (a) the recipient has given prior consent for this use; or
- (b) the recipient supplied their communication details in circumstances where they were provided with the opportunity to refuse consent for this use as part of the same transaction; or
- (c) the recipient is an existing customer of the person sending the communication, it is for the direct marketing of products or services supplied by the sender, and the recipient is given the opportunity in each such message to stop, free of charge and in an easy manner, any further such messages.

These three situations encompass the legitimate forms of “unsolicited”<sup>2</sup> commercial communications.”

We realise that the Directive does not address “opt-in” registers, so it is not surprising that the Regulations do not address them either. We will look forward to commenting on this matter further as part of the implementation of the Communications Data Protection Directive, but do feel that the Government could legislate in this area, as part of these Regulations.

It should also be noted that if “opt-out” is chosen as the way to legislate in this area, then marking unsolicited communications “clearly and unambiguously identifiable” is essential, so that the problem and inconvenience that such communications cause, can be managed as easily as possible.

## **Liability of Intermediate Service Providers (Regulations 17, 18, 19, 20 and 21)**

### ***Damages***

Regulations 17 to 19 state that a Service Provider shall “not be liable in damages”. The last two words do not relate to anything in the Directive, which provides an unrestricted limitation of liability.

---

<sup>1</sup> This is based on the European Parliament’s proposed Amendment 34 to COM(2000)385.

<sup>2</sup> We would, of course, argue that such communications are solicited, not unsolicited.

Indeed these words suggest that the limitations can only be used as a defence in some civil matters, with Regulation 21 covering criminal proceedings. Furthermore Regulation 21(2) excludes Regulation 19(a)(ii) applying in criminal proceedings. Given that Regulation 19(a)(ii) limits a Service Provider's liability if the Service Provider was "not aware of facts or circumstances from which it would have been apparent to the service provider that the activity or information was unlawful", legal uncertainty for the Service Provider remains in criminal proceedings. It effectively means that the Service Provider could still be held liable under some circumstances.

We therefore feel that the way in which damages are addressed in the Regulations is not in line with the spirit of the Directive, and that the words "in damages" should be removed from Regulations 17, 18 and 19.

Furthermore, Regulation 21(2) should also be removed.

### ***Exclusions***

In the previous consultation on these regulations, Thus plc raised the question of how the various exclusions interact with the limitations of liability. It is not possible for a Service Provider to determine, ahead of time, whether any particular transmission or information concerns a topic in the excluded area and therefore it seems unreasonable to restore liability depending on the material. We also believe that it was not the intention of the Directive to exclude these topics from the limitation of liability, since it would in practice negate the protection provided by the Directive. We therefore suggest that a further section is added to the Regulations which makes it clear that a Service Provider is not liable for content excluded by sections 3(1) and 4 of the Regulations.

### ***Protection of rights***

The interaction of the "no liability" regime and the power of a court to order actions and protect rights is also not completely clear. We believe that in the:

- A court should be able to act to protect rights (e.g. by requiring the removal of material).
- Nevertheless, the court cannot order a service provider to make a pro-active search.
- The court can order that material be removed immediately the service provider becomes aware of it.
- Nevertheless, the service provider is protected from liability until they become aware.
- Each specific communication or item, or related sets of communications or items, are treated separately (except where there is an obvious link between cases).

This would imply that the simple "notwithstanding regulations 17, 18 and 19" in section 20(2) is insufficient to fully address the situation. Furthermore, the regime should cover criminal as well as civil proceedings, so references to these regulations should also be included in regulation 21.

We would therefore suggest amendments to Regulations 20(1) and 20(2) to read:

*20. (1) Subject to paragraph (2), nothing in regulations 17, 18, 19 and 21 shall –*

- (a) prevent a person agreeing different contractual terms;*

- (b) *affect the rights of any party to apply to a court for relief to prevent or stop infringement of any rights; or*
- (c) *affect any power of an administrative authority to prevent or stop infringement of any rights.*

*(2) Where a court or administrative authority acts in accordance with paragraph (1), it may require a service provider to take specific action on becoming aware of relevant facts or circumstances, but these regulations shall continue to apply to the service provider in respect of his actions prior to his becoming aware.*

### ***Liability of agents***

It is unclear whether the definition of “Service Provider” includes employees and agents when performing their duties. For the sake of clarity, the Regulations should include specific exemptions for employees or agents who are acting on behalf of the Service Provider.

### ***Mere conduit (Regulation 17)***

The “mere conduit” Regulations are very strict, requiring that the Service Provider not initiate the transmission, not select the receiver, and not select or modify the information. While these Regulations are correct in principle, they cause problems if interpreted too strictly.

Firstly, many Internet services involve some form of automated response or relay. That is, the user connects to the Service Provider’s equipment and that equipment then makes its own connection to a third party, or makes a delayed response, or in some other – automated – way “initiates” a connection. Such a connection is an extension of the original user’s will, but in a strictly technical sense it is a separate connection made by the Service Provider and therefore excluded by regulation 17(1)(a).

Secondly, there are many situations where the final destination of a message is determined by its contents. For example, an email may be forwarded to a mailing list whose membership is unknown to the sender. In a strict sense the Service Provider is selecting the recipient of the message, but in reality it is, again, the sender who makes the selection.

Thirdly, very few systems actually transmit data completely unchanged. Routers alter the “time to live” field of packets, email systems add “Received:” headers to provide an audit trail, data may be compressed to reduce bandwidth requirements or encrypted across an insecure link, various systems translate between character encodings, and so on. These changes are automatic and do not affect the meaning of the transmission; they are also well-known and there are overarching reasons to retain them. This also applies to caching.

Although these points are addressed in the *Guide for Business*, we believe that they should be laid out in the Regulations to allay any doubt.

### **Caching (Regulation 18)**

An essential element of caching is that it is automatic and requires no human intervention. Therefore it is vital that any conditions or rules binding on a Service Provider are also capable of being applied automatically. Similarly, it would be onerous – and impossible to handle in practice – if each Service Provider could use a different mechanism to specify these conditions; clearly it is vital that they follow industry standards.

We therefore suggest the renumbering of the existing text of regulation 18 as 18(1) and add a new paragraph 18(2):

*(2) In paragraphs (1)(b)(ii) and (1)(b)(iii) the conditions and rules shall be expressed, and in paragraph (1)(b)(iv) the technology shall operate, according to established industry standards and in a manner that can be processed automatically.*

and remove redundant wording from 18(1)(b):

*(iii) complies with any rules regarding the updating of the information;  
(iv) does not interfere with the lawful use of technology to obtain data on the use of the information; and*

### **Liability for hosting (Regulation 19)**

By far our biggest area of concern with the implementation of the Directive is with Regulation 19.

As we detailed in our response to the previous consultation, This has to deal with complaints about content held on our servers, almost on a daily basis. We have to decide whether or not to remove the material based on a complaint we have received. If we don't remove the material then we could face action under UK law; if we do remove the material then we could face reprisals from our customers for wrongful takedown. We have no way of knowing whether the complaint is malicious or not, and often whether the material complained about is indeed in breach of the law.

We believe that legislation is needed in this area to provide the clarity and legal certainty that a Service Provider requires. Although this is not something that the Directive specifically attempts to achieve, we believe that the implementation of the Directive into UK law provides a suitable time to introduce it, and an opportunity to enhance the standing of the UK as one of the best places to operate on-line business.

We recognise that it is impractical at this stage to provide complete legal certainty for Service Providers. However, we request that Government provide backing in the Regulations for a co-regulatory approach, involving a suite of industry codes of practice. These codes of practice will be made up of two elements:

First, a basic definition of what a “notice” should look like and the minimal details that would be required to put a Service Provider on notice and provide “actual knowledge”. This can be outlined in the Regulations.

Second a suite of vertical sectoral codes of practice, which a Service Provider can rely on to provide guidance on how to deal with the various types of liability (e.g. there would be one for copyright infringement, one for defamation complaints, etc.).

Thus will be actively encouraging industry, Government and other interested parties to participate in the generation of these codes of practice. However, without legislative backing, these codes of practice will not be enough to provide the legal certainty that Service Providers require, and may not therefore offer sufficient incentive for Service Providers to participate. For this reason, we believe that the Regulations should specifically make reference to these codes, in the same way that codes of practice are endorsed by the Home Secretary, in the Anti-Terrorism, Crime and Security Act.

Without such a reference to codes of practice in the Regulations, there is a potential that complainants that do not wish to follow the codes in making their complaint, could attempt to side step them, and still seek damages against the Service Provider. Clearly the more legal certainty that can be provided in the endorsement of such codes, the greater the benefit to Service Providers and their customers.

In Appendix One we have put together some wording for the Regulations in this area. We urge the DTI to make use of this working in its implementation.

The notes in the appendix also attempt to address the issue of “put back”. This is where the content provider (the actual “author” of the material) says that the material complained of is not in breach of UK law and can be reinstated. This is clearly a difficult subject to tackle, with concerns that the rights of a complainant are balanced well with the rights of the content provider (the Service Provider’s customer). We feel strongly, that for any codes of practice to be fair and to succeed some form of “put back” process is required.

#### ***No Obligation to monitor***

The *Guide for Business* states that there is no need to implement Article 15 (“No general obligation to monitor”) of the Directive as no such obligations exist in current UK law.

We disagree with this. Recent cases (such as those involving Thompson & Venables) would imply that a court could order a Service Provider to carry out pro-active monitoring. Furthermore, if in the future a court was to declare a Service Provider as a publisher under certain circumstances, there would, by implication, be an obligation on the Service Provider to monitor material passing through or stored upon its systems.

Also, the article ought to be explicitly transposed in the interests of transparency.

However, we also note that under the Regulation of Investigatory Powers Act 2000, there is an obligation for certain Service Providers to monitor content.

With all these points in mind we suggest the introduction of an additional section 20(3) as follows:

*Notwithstanding paragraphs (1) and (2), no court or administrative authority shall require a service provider to monitor the information they transmit, provide access to, or store, nor to search for facts or circumstances indicating*

## **Summary**

Thus welcomes the opportunity to respond to the draft Regulations for the implementation of the E-Commerce Directive into UK law. We believe that the following areas should be addressed in the Regulations:

- Further clarity for the “country of origin” principle, so that it is clear that a UK based Service Provider will only be governed by legislation in the UK and not by laws in other member states.
- Definition of what marking unsolicited communications “clearly and unambiguously identifiable” means, so that such communications can be filtered automatically.
- Reference to and support for opt-in.
- Removal of “in damages” from Regulations 17 to 19.
- Exclusions to the Regulations should not apply to Regulations 17 to 19.
- Further clarity in the area of the powers of a court with respect to liability imposed on a Service Provider.
- Further clarity on the impact the Regulations have on employees and agents working on behalf of a Service Provider.
- Interpretation of the Regulations on mere conduit and caching.
- A need for codes of practice to be endorsed by the Regulations with details of the minimal requirements needed to provide a Service Provider with actual knowledge
- Implementation of Article 15 into the Regulations.

## **Appendix One**

The existing draft regulations do not make an attempt to address the questions of “actual knowledge”, “codes of practice”, or “notice and takedown”.

From the point of view of service providers there are a number of issues to consider. Firstly, there is no indication or guidance as to what level of certainty and diligence is required. According to one member of the Commission, the intention was for service providers to have to be convinced “beyond all reasonable doubt” that something was the case. This would be a very high test to meet. On the other hand, it has been suggested that a passing comment, brought to the attention of an employee of the service provider, would be sufficient to impart “actual knowledge”, even though the person making the comment has no standing in the matter and does not provide the specific details needed to investigate. If someone says “I think that Clive Feather’s web site contains a libellous statement”, is the service provider required to identify the web site in question and then read it all to attempt to identify the statement in question ? Where is the line drawn ?

Secondly, it is often suggested that “codes of practice” or “notice and takedown” will protect service providers, and the consultation document suggests that voluntary schemes will suffice without legal backing. However, as the Rightswatch experience has shown, a service provider is not protected by these schemes. The problem is not with the scheme itself – there is general agreement that a notice sent and received via such a scheme is “actual knowledge” – but rather that there is nothing to require a complainant to go via such a scheme. If somebody chooses to ignore the code of

practice and simply send a vague comment (as described above), there is a real risk that the service provider loses the protections of regulations 18 and 19.

Overall the service provider is at risk in four ways:

1. liability to the complainant if they do not act on a “notification”;
2. liability to the content provider if they *do* act on a notification;
3. liability to the content provider if they do not act after the latter issues a “put-back” notice;
4. liability to the complainant if they restore material following such a notice.

For example, consider an E-commerce site which contains, somewhere within it, a sound recording that somebody makes a complaint (e.g. breach of copyright) about.

1. If the service provider does not act to get the recording removed, they could be liable for damages because anyone can download it free of charge.
2. If the only option the service provider has open to them (e.g. because the merchant’s offices are unmanned over a holiday) is to block access to the site, they could be liable for the losses when the site is unavailable.
3. If the merchant then states that the complaint is unfounded, the service provider is potentially liable until service is restored.
4. As soon as it is restored, the service provider is at risk of exacerbating the situation (and increasing the damages against them) if the complainant turns out to be in the right.

What can be seen is that a code of practice can *only* be made to work if it is backed by a law containing a “safe harbour” provision that both protects service providers who follow an appropriate code of practice, and provides penalties for wilful misuse of these codes. The following draft regulation attempts to provide the minimum legislative framework to this end. It

- (1) provides a framework for approving codes of practice, relying on the Secretary of State to ensure – after consultation – that the powers are used properly;
- (2) allows for either horizontal or vertical codes covering specific domains;
- (3) outlines the contents of a code;
- (4) provides a waiver of liability, for both action and inaction, where the code is followed; and
- (5) provides an enforcement power, for example to prevent vexatious or negligently-wrong notices or counter-notices.

### ***Codes of practice, notice, and takedown***

**22.** (1) *The Secretary of State may by order approve, and from time to time revise, one or more codes of practice which establish:*

- (a) *a form of notice sufficient to constitute actual knowledge that an activity or information is in breach of any law or otherwise unlawful (“notice”); and*
- (b) *the circumstances required for removal or disabling access to such material (“takedown”).*

(2) *Before approving a code under this regulation, 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 approved under this regulation (“an approved code”) may be restricted to a particular class of material, infringement, or liability and may be specified as applying to:*

- (a) those service providers stating (in the same manner as if the code was a set of professional rules as described in regulation 8(1)(f)(iii)) that they conform to the code;*
- (b) all service providers of a description specified in the code; or*
- (c) all service providers generally.*

*(4) An approved code may specify any or all of the following matters:*

- (a) the requirements for a notice to be valid;*
- (b) the actions necessary for takedown, and the timescales that are deemed expeditious for the purposes of regulations 18 and 19;*
- (c) the conditions necessary for any notice from a recipient of the service to restore material following takedown (“a counter-notice”); and*
- (d) any consequential duties and liabilities for any person affected by its provisions.*

*(5) A service provider (if he otherwise would) shall not be liable for any claim, and shall have a defence in proceedings for any offence, arising out of his actions where:*

- (a) he takes down material in accordance with an approved code following a valid notice;*
- (b) he restores material in accordance with an approved code following a valid counter-notice; or*
- (c) he fails to remove or restore material where an approved code applies to the circumstances, no valid notice or counter-notice has been received, and it would have been reasonable, in the circumstances, for such a notice or counter-notice to have been provided.*

*(6) The duties and liabilities in paragraph (4)(d) shall be enforceable, at the suit of any affected person, by an action for damages for breach of statutory duty, but only in those circumstances where an approved code states so.*