WORLD INTERNET LAW REPORT

Volume 4, Issue 5 May 2003

Monthly news and analysis on Internet law and regulation from around the world

BNA International Inc., London

INTERNATIONAL INFORMATION FOR INTERNATIONAL BUSINESS

WORLD INTERNET LAW REPORT is published monthly by BNA International Inc., a subsidiary of The Bureau of National Affairs, Inc., Washington, D.C., U.S.A. Administrative headquarters: Heron House, 10 Dean Farrar Street London SW1H 0DX, England. Tel. (+44) (0)20-7559 4801; Fax (+44) (0)20-7222-5550; E-mail marketing@bnai.com. In the U.S. call toll-free on: 1-800-727-3116.

Subscription price: U.K. and rest of world £595; Eurozone €975; U.S. and Canada U.S.$995. Web version (standard licence): £695/€1125/$1150. Additional copies of this publication are available to existing subscribers at half price when they are sent in the same envelope as a standard subscription. Reproduction of this publication by any means, including facsimile transmission, without the express permission of The Bureau of National Affairs, Inc. is prohibited except as follows:

1) Subscribers may reproduce, for local internal distribution only, the highlights, topical summary and table of contents pages unless those pages are sold separately;

2) Subscribers who have registered with the Copyright Clearance Center and who pay the $1.00 per page per copy fee may reproduce portions of this publication, but not entire issues. The Copyright Clearance Center is located at 222 Rosewood Drive, Danvers, Massachusetts (USA) 01923; tel. (508) 750-8400. Permission to reproduce BNA material otherwise may be obtained by calling (202) 452-4471; fax (202) 452-4084.

Website: *www.worldtaxandlaw.com*
ISSN 1468-4438

Welcome to the May issue of *World Internet Law Report*! Our first article this month examines the liability risks for U.K. ISPs from users who commit copyright infringements on file sharing networks. Mike Conradi of Baker & McKenzie provides an in-depth commentary, detailing the legal background and technologies involved to date, and offers some practical suggestions that service providers can take to avoid liability.

Gayle McFarlane of Eversheds also writes in the E-Commerce section of the journal this month, reporting on the recent investigations into website compliance in the United Kingdom by the Office of Fair Trading and the trading standards authorities.

With the recent implementation of the E.U. Copyright Directive into Italian Law, our article by Alessandro del Ninno looks at how changes to Italian copyright law have provided for the protection of authors' rights online. We also include a round-up of recent domain name dispute resolution rulings on page 17.

We are also pleased to include an article by Professor David Hricik, who writes for the first time in the journal this month. Professor Hricik provides an account of online ethics in the new technological society.

As part of an ongoing review process to assess the journal's relevance and currency, we are inviting subscribers to complete a short online survey. Many thanks to all those of have already participated. Subscribers who have not yet done so but would still like to take part, can access the survey at *www.worldtaxandlaw.com/Internet/*

If you would like to contact me directly, please telephone on +44 (0)20 7559 4807, or send an e-mail to: nicholad@bna.com

Nichola J. Dawson

We wish to thank the following for their contribution to this issue:

Maria O'Connell, Eversheds, Manchester, U.K.; *Mike Conradi,* Baker & McKenzie, London; *Prof. David Hricik,* Mercer University School of Law, Georgia, U.S.; *Christopher Kuner,* Hunton & Williams, Brussels; *Gayle McFarlane,* Eversheds; *Stephan Le Goueff,* Le_Goueff@vocats.com, Luxembourg; *Angelika Höbinger,* Dorda Brugger & Jordis, Vienna; *Alessandro del Ninno,* Studio Legale Tonucci, Rome; *Tanguy Van Overstraeten* and *Sylvie Rousseau,* Linklaters De Bandt, Brussels; *Heather Rowe,* Lovells, London; *Natalia Tobón,* Cavelier Abogados, Bogotá.

CONSUMER PROTECTION

Case Report

GERMANY

■ COURT RULES THAT WEB POP-UP WINDOWS ARE UNLAWFUL

T. v. Dr. R., LG Dusseldorf, No. 2a O 186/02

Dusseldorf Regional Court, March 26, 2003

A German court has ruled that exit pop-up windows are illegal under the law against unfair competition and as such can be enjoined by a cease and desist order.

The Dusseldorf regional court found that exit pop-up windows, which are triggered automatically on a user's Web browser, were illegal because they forced users to take notice of their advertisements, even though users were attempting to leave the site. The court compared the practice to unsolicited commercial e-mail.

The decision is of significance mostly for those e-commerce operators based in Germany whose websites have exit pop-up windows in never-ending chains – which is usually the case only with adult or gambling sites, according to plaintiff's attorney Daniel Raimer of Strömer Rechtsanwälte, Düsseldorf.

Those operators who do not use the chains of pop-up windows, or who are located outside the country, "probably have little to fear" from the ruling, Raimer said.

Burden To Consumer

Under Section 1 of the law against unfair competition, a party can demand that a competitor cease a certain practice if the activity is counter to proper public order. In the case at hand, the pop-ups constitute a nuisance and a burden to the consumer, the court said.

The case involved a chain of exit pop-up windows, which the user could only exit by exiting the browser entirely, or using the task manager feature. The court said that the appearance of further pop-up windows was against the express will of the user who was attempting to leave by clicking, and instead the user was forced to take further notice of the advertisements. It cannot be assumed that every user is so experienced as to know about the possibility of exiting the window chain via the task manager, it argued.

Whether the goods or services advertised in the exit pop-up windows are the same as those offered at the website being exited or not is immaterial, the court said. The fact that the plaintiff and other adult sites allegedly also use exit pop-up windows does not change the fact that the practice is counter to proper public order, the court stated. Under Section 1 of the law on unfair competition, it is not merely the competitors who warrant protection, but also consumers and the general public. In this case it is the consumer who warrants protection from the practice, it said.

User May Purchase in Order To Exit

The regional court said that it could not rule out the possibility that users might choose to purchase a service merely in order to exit the chain, or that users would agree to a service that they would not otherwise have purchased if it had not appeared on the screen.

The exit pop-up windows constitute a "burdensome or otherwise unwanted disturbance" for the user, due to the user's wasted time, frustration at the re-appearing windows, and costs of the connection for the period of the prolonged visit, it stated.

In response to the plaintiff's argument that forcing the user to take notice of advertisements via an unending chain of exit pop-up windows was equivalent to receiving unwanted e-mail messages, the court said that although both were counter to proper public order, there was a significant difference in that, in contrast to receiving unwanted e-mail, the Internet user voluntarily calls up the domain and establishes contact with the Web page in the first place.

The court said the plaintiff's warning notice over use of the exit pop-up windows was justified only insofar as the pop-ups concerned a disturbance to customers under the law against unfair competition, and not in any other aspects, such as trademark or name rights. Both parties in the case offer adult content on their respective websites.

ISP Liability and File Sharing Networks

By Mike Conradi, Baker & McKenzie, London; e-mail: michael.conradi@bakernet.com

The recent, and well-publicised *Easyinternetcafe* case appears part of a new trend on the behalf of copyright owners to take legal action against intermediaries. With this in mind, is there a risk that ISPs in the United Kingdom could find themselves liable for copyright infringements committed by their users on peer-to-peer (P2P) file sharing networks?[1]

Summary

End-users will have primary liability for their infringing activities and in many cases, this may even be so serious as to lead to criminal liability notwithstanding that it is not done for profit. The position of P2P software or service providers, such as Napster and now Kazaa, will depend on the extent of their ability to monitor and control end-users' activities, and on whether or not they can be said to be "authorising" infringement.

ISPs however, are in a considerably stronger position. In fact, the *Easyinternetcafe* case offers reassurance to them because it confirms that there is no primary liability for infringement on a party, such as an ISP, who has no ability to control the infringing action. More significantly, the "mere conduit" defence set out in the E-Commerce Regulations[2] should exempt an ISP from liability in respect of *transmissions* of infringing copies, or in respect of the act of giving *access* to a network on which such copies are available. This is in contrast to the U.S. position where no such broad defence exists.[3]

However, the defence would probably not apply to liability for *authorising* the making of infringing copies. The *Amstrad* cases show that merely facilitating unauthorised copying does not amount to authorisation but they also show that it is important, in order to avoid liability, to ensure that nothing is done or said, whether in marketing literature or otherwise, which could be taken to grant permission or to condone copyright infringement. It might be prudent, for example, for an ISP to adopt a prominent anti-infringement message such as Apple's *Don't Steal Music* slogan and to take reasonable measures (if any are possible) to limit use of file-sharing networks to legitimate purposes. It would also be advisable for an ISP to avoid sponsoring or advertising with any file sharing service.

Whether there is liability for copyright infringement or not, an ISP could however still be required to disclose the names of infringing users to copyright owners, and a court could still issue an injunction requiring an ISP to block access to file-sharing facilities.

This means that although ISPs would be able to muster some good arguments against claims, which might be brought against them by copyright owners, there can be no absolute guarantee that all such claims would fail. Most of the unilateral measures that an ISP could take to reduce the risk (such as strictly enforcing an acceptable use policy, or restricting access to file-sharing networks), could risk damaging the ISP commercially if end-users simply went to competitors. For this reason it might be worthwhile for the industry as a whole, perhaps through an industry-wide body such as ISPA,[4] to agree on a course of action – though, depending on the nature of what is proposed, this may require prior approval from the competition authorities.

Some practical advice for ISPs, given this legal background, is set out in the conclusion below.

This article focuses on the state of play, and on the peer-to-peer services as offered at the time of writing (April 2003). As technology evolves and new services become available, further challenging legal questions beyond the scope of this paper, will be generated. Microsoft, for example, is currently beta testing a product called "threedegrees" which amongst other things will allow users to form groups and listen to shared music remotely.

1. Background

1.1 The U.S. – Napster and Afterwards

Napster was the original file-sharing software. It worked by creating a central registry of files and then matching users who wanted a particular file with users who had that file available. It was this central registry that formed a key part of the case against it in the U.S. decision, *A&M Records v. Napster*.[5] In that case, Judge Beezer found that Napster had *contributory* liability where it knew of specific infringing files and failed to take action to prevent distribution, and it had *vicarious* liability since it had a direct financial interest in drawing users to its service.[6]

By contrast, newer file-sharing software such as Kazaa, does not work by means of a central registry. Instead, such software simply links users into a series of ad hoc networks, which they may then search for files they want to download. The software provider has no ability to monitor or control the files made available. The Recording Industry Association of America (RIAA) is pursuing a separate case against Kazaa, and it remains to be seen whether this inability to control or monitor files will be enough to allow it to escape liability in the United States.

1.2 End-Users

End-users in the United Kingdom of course, are primarily liable for copyright infringement where they copy or issue copies of copyright material. Under the Copyright, Designs and Patents Act 1988 (CDPA), s17 – copyright is infringed by *reproducing a work in any material form, including storing it by electronic means* and, by s18, copyright is infringed by issuing copies of a work to the public. Under s107(1) CDPA, it is also a *criminal* offence without the licence of the copyright owner to posses an infringing copy of a copyright work in the course of business or, under sub-para (e), to distribute an infringing copy other than in the course of business to such an extent as to affect prejudicially the owner of the copyright.

In two cases from 1991,[7] it was held that the informal swapping of computer games via an enthusiasts' network amounted to "distribution" under s107(1)(e). By analogy, it seems likely many end-users of file sharing services will be committing a criminal offence where they make files available for others to copy, even when they do not do so for personal gain.

1.3 P2P Service or Software Providers (*e.g.*, Napster, Kazaa)

Under s24(1) CDPA (secondary infringement), copyright in a work is infringed by a person who without licence makes, imports, possesses in the course of business or sells an article specifically designed for making copies "knowing or having reason to believe that it is to be used to make infringing copies". Moreover, under s107(2) it is a *criminal* offence to make or possess an article specifically designed or adapted for making copies knowing or having reason to believe that it will be used to make infringing copies for sale or hire, or for use in the course of business.

A person will not be liable under s24(1) or under s107(2), then, unless their actions are performed "knowing or have reason to believe" that infringing copies will be made as a result. It follows from the definition of "infringing copy" in s27(2) (as a copy whose making constituted an infringement of the copyright *in the work in question*) that the requisite knowledge for liability under either section is knowledge of the specific works that are being infringed, not just that there may be infringements committed in general.[8] The *Amstrad*[9] cases (decided under the 1956 Act which preceded the CDPA) indicate that the courts will be reluctant to find liability even where a person sells an article in the full knowledge that "millions of breaches of the law of copyright" will occur, if that person has no specific knowledge of which works are being infringed.

Assuming that software would constitute an "article" for the purpose of these sections,[10] then, Napster would probably have been found liable in the United Kingdom under s24(1) because, via the central database, it *did* have knowledge of *specific* copyright infringements. Kazaa, without Napster's ability to monitor use, might be able to escape liability on the basis that it has no such specific knowledge. Both would probably avoid criminal liability under s107(2) in respect of non-commercial copying by end-users because of the requirement that the infringing copies themselves be used in the course of business. There remains the possibility that they could be convicted of the criminal offence of "aiding and abetting" though, as the case-law indicates that this offence requires proof of a positive act of assistance done with intent to aid a crime, or when indifferent to a specific known illegality,[11] a conviction may be difficult as it would seem to require evidence of assistance in respect of a particular copyright infringement.

Software providers might also be liable for "authorising" an infringement under s16(2): see the discussion below.

2. Liability of an ISP

2.1 ISPs – Primary Infringement

In a recent case,[12] Easyinternetcafe was found liable for copyright infringement where it offered to burn files from a private directory onto a CD for customers. This might seem a worrying precedent for ISPs that allow their end-users to access file-sharing services, but in fact the judge in that case actually drew a distinction with an ISP's activities on the basis that the ISP, but not Easyinternetcafe, is an "involuntary" copier. Although liability under sections 17 and 18 of the CDPA is strict (that is, absence of knowledge of the infringement is not a defence), this does not mean that it extends to *involuntary* actors, such as ISPs, that have no ability to control the infringing action in question.[13]

ISPs may find some additional relief from liability for primary infringement under the proposed changes to the CDPA to be brought about when the Copyright Directive is implemented.[14] Article 5(1) states that copyright will not be infringed by the making of a temporary copy which is an essential part of a process whose sole purpose is to enable transmission of a work between third parties, and which has no "independent economic significance". Although there is no guidance yet as to what is meant by the phrase, it is likely to mean independent significance *to the copyright owner.* In the case of a temporary copy made by an ISP, then the exemption will probably apply.

2.2 ISPs – Secondary Infringement

In addition to the provisions of the CDPA discussed above, there is a further section that may be relevant to the liability of an ISP for secondary infringement. Section 24(2) states that copyright in a work is infringed by a person who, without authorisation, *transmits* a work by means of a telecommunications system (otherwise than by broadcasting or inclusion in a cable programme service) knowing, or having reason to believe, that infringing copies of the work will thereby be made.

The *Shetland Times*[15] case indicates that transmission of material via the Internet could be considered a "cable programme service" and the judge in *Easyinternetcafe* agreed, albeit *obiter.* If upheld, this would mean that an ISP would not be liable under s24(2) because of the express exclusion of cable programme services from that section. It might also allow an ISP's end-users to claim the benefit of the defence under s70 (time-shifting)

which states that making a personal copy of a cable programme for the sole purpose of listening to it later is not an infringement. The change of definition from "cable programme" to "communication to the public of a [copyright] work", which is expected as part of the implementation of the Copyright Directive in the United Kingdom (discussed at paragraph 2.1 above), will make it more, rather than less, likely that ISPs and their end-users will be able to claim the benefit of these sections.

In any event, it seems likely that an ISP could escape liability by arguing that, as an "infringing copy" relates to a specific work, there can be no liability where there is no ability to know, in respect of any given transmission, whether or not copyright in a particular work is being infringed. The same argument would apply in relation to the question of any liability on an ISP for "aiding and abetting"(see paragraph 1.3 above).

2.3 The "Mere Conduit" Defence

Even if the arguments in favour of the ISP discussed above do not prevail, there is also a defence available as a result of the Electronic Commerce (EC Directive) Regulations 2002 (the E-Commerce Regulations).[16] Regulation 17 (mere conduit) says that

> "Where an information society service is provided which consists of the transmission… of information provided by a recipient of the service, or the provision of access to a communication network, then the service provider (if he otherwise would) shall not be liable for any damages or criminal offence where he:
>
> (a) did not initiate the transmission;
>
> (b) did not select the receiver of the transmission; and
>
> (c) did not select or modify the information".

This would seem to exempt from liability, ISPs that are engaging in either of two types of activity:

- transmitting information on behalf of end-users; or
- providing end-users with access to a communications network.

The DTI's (non-binding) guidance on the Regulations[17] (para 6.1) makes clear the government's view that condition (a) above is met even where a service provider automatically initiates a transmission at the request of a recipient and that condition (c) is met even where manipulations of a technical nature have taken place so long as they do not alter the integrity of the information. Regulation 17 would also seem to cover virtual ISPs, as well as "real" ISPs, since they too offer services of the type referred to.

Regulation 20 states that a party's right to apply for an injunction is not affected.[18] This means that, even though an ISP might escape *liability*, it might still be possible for content owners to obtain an injunction requiring the ISP to stop file-sharing activities, if they could persuade a court to make such an order. Moreover, Article 8(3) of the Copyright Directive, when implemented in the United Kingdom, will expressly require that rightholders be able to apply for an injunction against intermediaries whose services are used by third parties to infringe copyright.[19]

2.4 "Authorising" Infringement

The E-Commerce Regulations are relatively new, and there are not yet any reported cases on them. It seems likely, though, that Regulation 17 would only offer a defence where a *transmission*, or the act of giving *access* to a network, would otherwise create a liability. Thus it might not apply to liability for *authorisation*. This analysis is reinforced by Recital 44 of the E-Commerce Directive (implemented by the E-Commerce Regulations), which states that a service provider who "deliberately collaborates" with recipients of a service to undertake illegal acts goes beyond the activities of a "mere conduit".

Under s16(2) of the CDPA, then, copyright in a work is infringed by a person who, without the licence of the copyright owner, does or *authorises another* to do any restricted act. In the second Amstrad case,[20] it was held that "authorise" means:

> "to grant, or purport to grant, expressly or by implication, the right to do the act complained of".

Thus it will be very important to ensure that any literature or material published by the ISP could not be taken to condone or authorise illegal activity. In *Amstrad*, it was sufficient to avoid liability under the equivalent section of the 1956 Act simply to put appropriate warnings about copyright infringement in sales literature – even if that literature also stated that users could use the equipment to "copy [their] favourite cassettes". Nowadays, however and especially since file-sharing activity constitutes such a large share of an ISP's business, it is quite possible that the courts would take a less tolerant view. ISPs should adopt a prominent anti-infringement message and avoid sponsoring or advertising with any file sharing service.

In a 1976 Australian case,[21] it was held that a person authorises an infringement where they fail to take reasonable steps to limit use to legitimate purposes.[22] In *Amstrad*, it was not necessary for the court to rule on this point because there were no such steps that Amstrad could have taken. In the case of file-sharing software though, it would be open to the English courts to rule that an infringement has indeed been "authorised" if it is possible to limit use to legitimate purposes (as with Napster though not, arguably, with Kazaa) but this opportunity has not been taken. In relation to ISPs an allegation of "authorisation" may well hinge on what is, and is not, technically possible and commercially reasonable. For this reason, it will be important for an ISP to understand the technical background properly and thoroughly.

2.5 Disclosing the Names of Infringing Users

ISPs, even if not liable for any criminal or civil wrongdoing, could still be ordered by a court to disclose the names of subscribers who have infringed copyright. The recent U.S. case where Verizon was ordered to disclose the name of a subscriber who had been making infringing copies of music files[23] has highlighted this

issue, and the Danish courts appear to have made similar orders recently[24] against a number of ISPs at the request of the Danish Anti-Piracy Group.

The *Ashworth*[25] case shows that it is likely that an English court would be willing to make a similar order. The House of Lords in that case held that an order to disclose the identity of a third party could be given against a person who was "involved with" the wrongdoing, although they need not have committed any criminal or civil wrong themselves. It was not necessary, in that case, for the claimant to intend to bring legal proceedings against the third party – rather it was sufficient that they had some other "legitimate purpose" in seeking disclosure. The court noted that there was an "overwhelming likelihood" that a specific wrongdoing had been committed by an individual whose identity was unknown to the claimants. By analogy, it would seem reasonable to conclude that content-holders would have to show to a similar standard, that copyright in specific works had been infringed.[26] It is unlikely that a court would make a wide-ranging order for disclosure of the identity of all users who have, or might have, infringed copyright.

This means that an ISP in the United Kingdom could well be compelled by a court to disclose the name of a particular user who has infringed a particular copyright. In the absence of a court order, though, if an ISP were to disclose the identity of a user to a third party this would almost certainly be a breach of the Data Protection Act 1998 as well as of its contract with that user. This generates something of a "Catch-22"situation for ISPs – if they refuse a suitably particularised request then they risk the expense, hassle and adverse publicity of a court action which they would be likely to lose. If they agree to the request they will almost certainly be in breach of the Data Protection Act as well as with their contract with the user.

In the 2001 *Totalise*[27] case, two websites found themselves caught in this position. Comments relating to Totalise were posted on bulletin boards run by the popular financial sites, Motley Fool and Interactive Investor. Totalise alleged that the comments were defamatory and asked both Motley Fool and Interactive Investor to disclose the name of the author. Both of them refused on the basis that the Data Protection Act 1998 prevented them from doing so unless Totalise obtained a court order. Ultimately, the Court of Appeal granted the order requiring disclosure of the name of the author, but held that, if it were the case that a voluntary disclosure would have been in breach of a legal obligation, then it would normally be right that the party seeking the order should pay the costs of the other.

This indicates that the most sensible solution would seem to be for the ISP to respond to the copyright owner, explaining that the names of users will not be disclosed without a court order but (if the request is specific-enough) indicating no opposition to such an order.

3. Conclusion – Practical Advice for ISPs

- Take any reasonable steps available (if there are any) to limit use of the service to non-infringing applications. This will entail ensuring that there is a clear understanding of what is, and is not, technically possible.
- Ensure that no literature or marketing material contains anything that could be taken to condone or authorise illegal activity.
- Adopt a prominent anti-infringement message.
- Refrain from doing business with (for example, by sponsoring) any of the file sharing software or service providers such as Kazaa.
- Implement and enforce an appropriate acceptable use policy that allows for termination of the accounts of repeat infringers. In order to avoid the need to investigate and decide on the validity of complaints, this policy could require both the complainer (and, if they so wish, the end user) to submit a statement "under penalty of perjury" (sworn affidavits in the United Kingdom). The policy would then simply commit the ISP to act in accordance with any such statement and would require the complainer to take court action in the event of a dispute.[28]
- Ensure that there is a procedure in place to deal with and respond to allegations of *specific* copyright infringement by end-users.

Summary Table

Might the following persons incur liability in relation to copyright infringement on P2P networks?

	Primary Ss17-18 CDPA	**Secondary** S24 CDPA	**Criminal** S107 CDPA	**Authorising** S16 CDPA
End-User	✔	✘	✔	✘
File-Sharing Service Provider (*e.g.*, Napster)*	✘	✔ If knowledge of *specific* infringements	✘ (assuming non-commercial use of the copies)	✔
File-Sharing Software Provider (*e.g.*, Kazaa)*	✘	✘	✘ (assuming non-commercial use of the copies)	✔
ISP	✘	"mere conduit" defence	"mere conduit" defence	✔ unless attempts to limit use to legitimate purposes

* These categories are intended to distinguish a service such as Napster, which is actively involved in each and every instance of file-sharing (in that case by maintaining a central register) from a *software provider*, such as Kazaa, which, at least in theory, is no longer involved in the process beyond providing the initial software.

■ Refuse any request from a copyright owner for disclosure of the identity of a user in the absence of a court order. Such an order is unlikely to be forthcoming, and should be resisted, unless the request is specific as to the copyright and as to the user.

1 File sharing forms a very significant part of the traffic carried by ISPs. A senior manager at the ISP Tiscali, has recently been quoted to say *"In any given network, peer-to-peer traffic is between 30 (percent) and 60 percent of total traffic"*. See *http://zdnet.com.com/2100-1105-981281.html*

2 Electronic Commerce (EC Directive) Regulations 2002, SI 2002/2013.

3 The U.S. Digital Millennium Copyright Act of 1998 establishes some exemptions from liability for intermediaries but these are narrower than those which apply in the European Union and more conditions must be satisfied.

4 The Internet Service Providers' Association. *www.ispa.org.uk*

5 Full judgment at *www.nyls.edu/samuels/copyright/beyond/cases/napster.html*

6 He also found that Napster had *not* established that end-users were engaged in "fair use" of copyright material under U.S. law – which provides a significantly wider exemption than the U.K.'s "fair dealing" provisions.

7 *Irvine v Carson* (1991) 22 IPR 107 and *Irvine v Hanna-Rivero* (1991) 23 IPR 295.

8 See Laddie, Prescott & Vitoria *The Modern Law of Copyright* para 19.8, which states that the copyright owner must specifically identify the works alleged to have been infringed.

9 *Amstrad Consumer Electronics v British Phonographic Industry* [1986] FSR 159 and *CBS Songs Ltd v Amstrad Consumer Electronics* [1988] AC 1013.

10 It is at least arguable that software is *not* an "article" since the term implies some physical quality. In *St Albans CDC v ICL Ltd* [1996] 4 All ER 481, it was held that software, by itself, is not a "good".

11 For example, *National Coal Board v Gamble* [1959] 1 QB 11.

12 *Sony Music Entertainment (UK) Ltd & Others v Easyinternetcafe Ltd [2003] EWHC 62(Ch).*

13 See Laddie *The Modern Law of Copyright* 3rd edition, paras 4.13-4.14.

14 Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights (OJ L167/10). The deadline set for implementation was December 22, 2002 but this was put back in the United Kingdom to the end of March 2003 and, at time of writing (April 2003) has now been postponed again to "late spring".

15 *Shetland Times v Jonathan Wills* [1997] EMLR 277 – though only an interim injunction case.

16 *www.legislation.hmso.gov.uk/si/si2002/2002213.htm* – introduced to implement the E-Commerce Directive, 2000/31/EC.

17 *www.dti.gov.uk/cii/docs/ecommerce/businessguidance.pdf*

18 Presumably the grounds for the grant of such an injunction would be that there would have been a cause of action against the defendant but for Regulation 17. As this article illustrates, this may not be easy.

19 And on January 30, 2003 the European Commission issued a proposed new directive on the enforcement of intellectual property rights, which by Article 10(1) would allow *preliminary* injunctions against intermediaries to be granted. Full text: *www.europa.eu.int/comm/internal_market/en/indprop/piracy/com2003-46/com2003-46_en.pdf.*

20 *CBS Songs Ltd v Amstrad Consumer Electronics* [1988] AC 1013.

21 *Moorhouse v University of New South Wales* [1976] RPC 151.

22 In *Moorhouse* this entailed a duty on a university to place appropriate notices next to library photocopiers.

23 *http://money.cnn.com/2003/01/21/technology/verizon_songswapper.reut/index.htm*

24 *www.theregister.co.uk/content/archive/28286.html*

25 *Ashworth Hospital Authority v MGN Ltd* [2002] 4 All ER 193.

26 In the Danish Anti-Piracy Group case mentioned previously the claimant seems to have been able to do this by means of Kazaa screenshots showing the filenames, which the unknown third party was making available.

27 *Totalise plc v Motley Fool and Interactive Investor* [2001] EWCA Civ 1897.

28 Microsoft's "copyright policy" adopts this approach. See *www.microsoft.com/info/cpyrtInfrg.htm.*

Website Compliance in the U.K: And The Survey Says…

By Gayle McFarlane, Solicitor, IT and E-Commerce Group, Eversheds LLP; www.eversheds.com. The author may be contacted by e-mail at: gaylemcfarlane@eversheds.com.

Website legal compliance has become more of an issue over the last few years with an increase in legislation specifically aimed at dealings using the Internet, particularly when consumers are involved. However, despite this continued interest in the way in which people carry out business online, evidence is emerging that until now, web traders have not given compliance serious attention, perhaps feeling that there is commercial merit in avoiding the costs of compliance due to the apparent reticence of the enforcing authorities to take action.

It would appear recently that this particular tide is on the turn, with two distinct bodies investigating website compliance. The Office of Fair Trading ("OFT"), together with local Trading Standards Offices, is the primary enforcer of much of the Internet-related legislation, as well as more general consumer protection legislation. Its authority is enshrined in the legislation itself, and it has the power ultimately to ask for the court's sanction of contempt of court should non-compliance continue. The Advertising Standards Authority ("ASA") on the other hand is a self-regulatory body, which largely relies on the adverse publicity generated when it makes a finding against an advertiser to discourage marketers from breaching its rules, although ultimately it can request intervention by the OFT in cases where its rules reflect the legislative position.

The OFT Investigation

In April 2003, the OFT and 55 local trading standards authorities carried out an investigation into websites in the travel industry sector to identify those making potentially misleading claims about travel deals.

The investigation was part of an international sweep, carried out in conjunction with 87 enforcement agencies in 24 countries, and discovering over 1,000 problem sites worldwide. Initial analysis of the results suggests that 40 per cent (54 out of 135) of U.K. websites investigated contained potentially misleading claims.

Specific travel claims were investigated to ensure their compliance with the Control of Misleading Advertising Regulations 1988 and the Package Travel, Package Holidays and Package Tours Regulations 1992, which con-

trol the sale and performance of packages sold or offered for sale in the United Kingdom by setting out the information be given to the consumer before the contract is concluded and before the package starts.

Examples of offending offers included "hot deals" advertised on the home page of a site which bear no resemblance to the prices actually on offer, and offers of "holidays from..." when in fact the cheapest price available was much higher. Under these Regulations, the OFT can apply to the High Court for a court injunction preventing the further publication of a misleading advertisement.

It is perhaps more worrying that more than 100 additional potential breaches of specific consumer protection legislation were identified. Commercial activity using the Internet is subject to existing "bricks and mortar" legislation as well as Internet specific legislation. Compliance issues uncovered by the OFT included breaches of:

- The Unfair Terms in Consumer Contracts Regulations 1999, which state that a consumer is not bound by a standard term in a contract with a seller or supplier if that term is unfair, for example, if it has not been negotiated and places a significant imbalance in the rights and obligations of those involved.
- The Consumer Protection (Distance Selling) Regulations 2000, which give consumers rights in the area of home shopping. Under the Regulations consumers shopping for goods and services over the Internet, as well as by other distance means have the right to clear information about the products and the supplier and, in some case, a cooling-off period.
- The Electronic Commerce (EC Directive) Regulations, which require online services providers to provide additional information to any recipient, consumer or otherwise, of their services. This includes specific information regarding the supplier and the steps that must be taken in order to complete a contract with that supplier.

All three sets of regulations can be enforced by qualifying bodies, such as the OFT, who can apply for a "Stop Now" order requiring the business to stop the behaviour immediately and not continue with those practices or anything similar. Failure to comply with a "Stop Now" order could result in proceedings for contempt of court. The OFT has confirmed that sites which have been identified as infringing are being pursued either by local trading standards or the OFT with a view to taking further action.

The ASA Investigation

The ASA has, perhaps not surprisingly, produced a more positive report on industry practice. It recently published the results of its Internet Banner and Pop-up Advertisements Survey 2002, which assessed a representative sample of 354 banner advertisements and 258 pop-up advertisements in paid-for-space between July 1, 2002 and December 31, 2002. It found that only 1 percent of Internet banner and pop-up advertisements fall foul of the British Codes of Advertising and Sales Promotion, now revised and in their 11th Edition.

However, 37 advertisements were labelled "questionable" by the ASA researchers. Reinforcing the message put out by the OFT above, these ads typically included price or other claims that would need to be supported with evidence, or appeared on inappropriate websites, for example advertisements for betting and gaming websites appearing on sites that could appeal to those under the age of 18. These questionable advertisements brought the level of compliance down to 94 percent, still a high percentage in comparison to the results found by the OFT.

A Common Approach

The investigation carried out by the OFT is the fifth "global sweep" it has participated in and shows the pro-active approach the OFT is willing to take to ensure website compliance. It also seems to show the OFT using the tried and tested tactics adopted by the ASA to ensure compliance by publishing the results of its survey, although has not yet gone as far as to "name and shame". It also suggests that it will be more willing to "use its teeth" in future, and web traders may find their local trading standard office, in conjunction with the OFT, increasingly likely to take action against those who do not comply with important consumer protection legislation.

The Information Commissioner has also indicated a desire to place website data protection compliance at the top of the agenda, and the Disability Rights Commission has recently carried out its own investigations. As many web traders only need to make small adjustments or additions to their websites in order to comply with the applicable legislation it would seem that now would be a good time to carry out a compliance review!

News

AUSTRLIA

New Anti-Spam Laws Proposed

Legislation banning unsolicited e-mail – or spam – has been proposed by a new report released by the Minister for Communications Information Technology and the Arts, Senator Alston.

A final report by the National Office for the Information Economy (NOIE) on countering the spam menace urges the Government to introduce legislation – including strong enforcement measures – prohibiting the sending of messages without the prior consent of the end user.

Senator Alston said the Government was committed to taking a strong stand on spam.

The sending of electronic junk mail has rocketed in recent years as e-mail usage has increased. The NOIE

report proposes a multi-level approach to tackling the problem, including:

- The introduction of national legislation banning the sending of commercial electronic messaging without the prior consent of end users unless there is an existing customer-business relationship (*i.e.*, an opt-in approach);
- The requirement for all commercial electronic messaging to contain accurate details of the sender's name and physical and electronic addresses;
- Collaboration with industry bodies to implement codes of practice to ensure the compliance of their members with national legislation;
- Requirement for ISPs to make available to clients filtering options from an approved schedule of spam filtering tools at reasonable cost, and evaluate and publicise spam filtering options and products;
- Australia working together with international organisations such as OECD and APEC to develop global guidelines and cooperative mechanisms to combat spam;
- The development of a major information campaign to raise awareness of the nature of spam, provide simple technical advice and a basic guide to anti-spam products.

The report, prepared by NOIE after extensive consultation with many sectors of industry and the online community, provides a blueprint for government and users alike to start making inroads against the problem. It makes it clear that there is no quick solution against spam, but there are many roles that all parties can play in dealing with the issue.

The report is available on the Noie website at *www.govonline.gov.au/publications/NOIE//spam/final_report/*

NOIE – The National Office for the Information Economy

BELGIUM

E-Commerce Directive Is Implemented at Last

The Belgian law implementing the E.U. E-commerce Directive has now come into force following publication in the *Belgian State Gazette*. The law follows a reasoned opinion published by the European Commission earlier in 2003 criticising Belgium's failure to implement the directive and requesting it take immediate action to do so.

It seems unclear why implementation was delayed, as the law closely follows the directive's provisions:

- The country of origin rule will generally be applied, whereby information society service providers are regulated by the law of the country in which they are established.
- E-tailers must clearly indicate their prices and provide users with certain information, including contact details and trade registration number. Additional information must be made available before an order can be placed online, including (i) the technical steps that must be followed, and (ii) general contract terms and conditions in a form that can be stored and reproduced.
- All types of advertisement must be clearly marked as such. The law creates an opt-in system for unsolicited commercial emails, going beyond the opt-out system of the directive.
- A contract concluded electronically will be treated as meeting any legal or regulatory requirements, provided that all functional aspects are satisfied. There are certain exceptions to this; for example, real estate transfers may not be concluded electronically.
- The law grants immunity from liability to certain intermediary service providers (*e.g.*, mere conduit, caching or hosting providers) and does not oblige them to monitor the information that they transmit and store. However, service providers must promptly inform the authorities of any suspected illegal activities undertaken by users of their services.
- The law sets out a warning procedure in case of breach of any of its provisions and allows for penalties of up to EUR250,000 for non-compliance.

By Tanguy Van Overstraeten and Sylvie Rousseau, Linklaters De Bandt, Brussels

COLOMBIA

Obligations for Enterprises Carrying out Electronic Transactions

Most owners of Internet sites in Colombia are unaware of the provision ordering all web and Internet sites of Colombian origin, whose economic activity is of a commercial, financial or service-rendering character, to register with the mercantile registry and to supply to the Directorate of Customs and Taxes (DIAN) the information on economic transactions under the terms said entity may require.

Such requirements, provided in Law 633 of 2000 and declared constitutional by the Colombian Constitutional Court in 2001,[1] have been largely ignored by most owners and go uncontrolled by the corresponding authorities.

Nevertheless, it is worth mentioning that for enforcement purposes, the DIAN must respect the following principles and limitations indicated by the Court:

- the right to privacy of persons performing electronic transactions;
- the principle of relevance which assumes in each specific case, that only information relating to the functions legally attributable to the entity requesting it may be required and disclosed; and
- the principle of ultimate purpose, in such manner that the information requested and revealed shall be strictly necessary for meeting the purposes of the administration in such concrete and specific case.

1 Constitutional Court, Judgment C-1147 of 2001 (October 31, 2001)

By Natalia Tobón, Cavelier Abogados, Bogotá, Colombia

EUROPEAN UNION

Commission Launches E-Business Legal Portal for SMEs

The Commission's Enterprise DG has launched a 12-language web portal containing information on the legal aspects of e-business, aimed specifically at small and medium sized enterprises (SMEs).

Having identified a general lack of legal knowledge among SMEs looking to do business online, Ebusinesslex.net was set up in order to facilitate cross-border electronic commerce within the E.U. single market.

The site contains information and resources on a range of relevant issues, including contractual aspects, online payments, privacy and data protection and intellectual property rights. Other features include a frequently asked questions section, an e-business legislation database, and references to self-regulatory initiatives.

Business associations and other e-business initiative participants are welcome to provide links to the Ebusinesslex.net portal.

Community R & D Information Service (CORDIS); http://dbs.cordis.lu/news/en/home.html

Increased Access to States' Public Sector Information Boosts E-Commerce

On March 27, 2003 E.U. telecommunications ministers reached political agreement on a proposal for a new Directive, which would establish rules for the re-use of public sector information. The aim of the proposal is to remove barriers to cross-border exploitation of public sector information across Europe, particularly on the Internet. Public sector information (*e.g.*, geographical and business information) can have important economic value, providing a source for new digital products, as well as key data input for trading online.

European Union Member States would not be compelled to allow the re-use of information. However, if they do allow such re-use they would have to abide by the rules in the Directive. These include rules about charging and the timely supply of documents, an obligation to make the information available "through electronic means where possible and appropriate", and an obligation to ensure that any applicable conditions for the commercial exploitation of the documents are non-discriminatory.

The rules would not apply, among other things, where a third party owns copyright in the document or where its exploitation would involve a breach of data protection rules.

The Proposal is available online at: *http://europa.eu.int/eurlex/en/com/pdf/2003/com2003_0119en01.pdf*

By Lovells, www.lovells.com/home.jsp. For further information, please contact Heather Rowe, a partner with the London office of the firm, at heather.rowe@lovells.com

How Electronic Piracy Is Threatening Competition

Protecting Europe's fast-growing electronic pay-services (paid for services provided via TV, radio and the Internet) against piracy will be an important contribution to making the European Union more competitive as 21st century knowledge-based economies are expected to rely increasingly on electronic pay services, according to a recent report published by the European Commission.

Piracy is far from a victimless crime: legitimate users end up paying higher prices, operators can go bankrupt and governments are deprived of tax revenue. The report assesses the implementation of the 1998 Directive on legal protection for electronic pay services and urges Member States to work together to fight piracy.

The report encourages providers to make more pay-TV services legitimately available across E.U. borders and that everything needs to be done to prevent piracy of electronic pay services, starting by fully implementing and enforcing existing E.U. law.

Aim of the Directive

The relevant E.U. law is contained in Directive 98/84/EC, which aims to provide a minimum level of legal protection for "conditional access" services – in other words services where access depends on the user having a "key", generally provided by the operator in return for payment. For pay-TV services, this key is usually in the form of a smart card on to which the necessary information is downloaded. For Internet-based services, it is usually in the form of a password authorised by the service operator. The Directive prohibits all commercial manufacturing, distribution and marketing activities related to pirate smart cards and other devices circumventing the access protection of pay-TV, radio and Internet services. It does not, however, make it illegal for individuals to possess such devices, though it is open to Member States to do so at national level.

The report also stressed that Member States, which have not properly implemented the Directive should do so immediately. The Commission decided in December 2001 and in March 2002 to initiate European Court of Justice proceedings against Belgium, Greece, Luxembourg and Spain (see *World Internet Law Report, February, 2003*). Since then, Greece and Luxembourg have taken steps to comply with the Directive. The Commission said that it is currently assessing these countries and will withdraw the infringement procedures against them if appropriate. In some other Member States, too, certain issues remain to be clarified before the Commission can pronounce with certainty that the Directive has been correctly implemented.

The Commission report also said that among the future Member States, there has been encouraging progress with the implementation of the Directive, although significant efforts still have to be made.

The full text of the report can be found at *http://europa.eu.int/comm/internal_market/en/media/condac/functioning/index.htm*

HUNGARY

ISPs Reach Accords on Internet Call Fees

BUDAPEST—After a heated dispute about how to reduce Internet usage fees, the Hungarian Ministry of Information Technology and Communications (IHM), the dominant telecommunications company Matáv Rt., and Internet service providers (ISPs) entered into agreements that aim to cut Internet access tariffs on subsidised packages by 25 percent.

The plan to reduce Internet usage fees was first announced by Prime Minister Péter Medgyessy, on February 11, 2003 as part of his modernisation programme to help prepare Hungary for accession to the European Union. The cost of Internet usage in Hungary is one of the highest among the member countries of the Paris-based Organisation for Economic Cooperation and Development.

As part of the deals, the IHM agreed with Matáv that the telecom giant would offer its subsidised access services to all ISPs at a wholesale price 25 percent lower than the retail price, as of March 1, 2003. As a result of an earlier agreement concluded in June 2002, the IHM pays fixed-line telephone operators HUF0.77 (U.S.$0.0033) per minute to reduce phone costs for dial-up Internet users, as of August 1, 2002.

Difficulties Over Billing

However, Matáv offered to provide its services to ISPs on a discounted basis only if they themselves billed and collected telephone charges related to Internet usage. Matáv and ISPs had been embroiled in a long dispute over billing for Internet usage, which was ended by an IHM decree on February 7, 2003. Under the decree, Matáv is required to bill for the charges and to refund the ISPs 13 percent of those revenues.

ISPs complained that they would not be able to cut their prices by 25 percent because the cost of handling billing would increase their expenses by some 12 percent.

Meanwhile Matáv, which is 60 percent owned by Germany's Deutsche Telekom, announced that it would lower its own Internet tariffs as of March 1, 2003 through its subsidiary Axelero Rt., which controls some 43 percent of Hungary's dial-up Internet market. Alternative ISPs accused the IHM of further strengthening Matáv's dominant position on the market.

Finally, the IHM agreed to pay ISPs outside the Matáv group 13 percent of their revenues if they lowered their prices by 6.5 percent. In addition, Matáv agreed to pay ISPs four percent compensation for taking over the risk of billing Internet-related call charges.

Matáv In Accords With ISPs

On March 4, 2003 Matáv entered into agreements with ISPs Vivendi Telecom Hungary Rt., GTS-Datanet Kft., EuroWeb Kft., and Freestart Kft. – which together with Axelero control some 80 percent of the Internet market – on the provision of wholesale Internet access packages at a 25 percent discount.

Under the accords, the ISPs agreed that they would take on billing and collection of Internet-related phone charges from their customers and reduce their fees.

In March 2002, the arbitration committee of Hungary's Communications Supervisory Authority issued a non-binding ruling favoring ISPs in their dispute with Matáv over billing for Internet-related phone charges.

Matáv Competitor In Deal With IHM

In a related development, Vivendi Telecom Hungary, the country's second-largest fixed-line telecom provider, agreed a contract with the IHM in March 2003, which enables it to offer a 25 percent wholesale discount to ISPs, similar to the agreement between Matáv and the IHM.

Vivendi had also complained that the IHM granted Matáv a competitive advantage by striking an exclusive deal with the company in mid-February 2003.

LUXEMBOURG

New Bill For Distance Selling

On March 13, 2003 the Bill (the "Bill") implementing Directive 97/7/EC of the European Parliament and of the Council of May 20, 1997 (the "Directive") on the protection of consumers in respect of distance contracts was adopted by the Chamber of Deputies.

The Bill, the purpose of which is mainly to regulate B2C relations, aims at reinforcing protection of consumers involved in distance selling and concerns all distance contracts concluded by mail, telephone, telefax, electronic means or any other telecommunication means.

The new text sets forth a general framework that integrates all specific consumer protection provisions currently stated in the Bill of August 14, 2000 relating to electronic commerce, including those related to the selling of financial services.

The main provisions ensuring protection of the consumer are, among others:

- the creation of a consumer prior information system;
- the creation of an acknowledgement of information system;
- the introduction of a right of withdrawal of seven days, including, except for some exceptions, for financial services; and
- the creation of a legal framework for opt-in and opt-out systems.

Finally, the Bill maintains the provisions of the Bill of August 14, 2000 concerning the protection of consumers where payment systems were fraudulently used.

For more information visit: *www.chd.lu/servlet/DisplayServlet?id=22082&path=/export/exped/sexpdata/Mag/005/002/024041.pdf*

By Stephan Le Goueff, Le_Goueff@vocats.com, Luxembourg.

TURKEY

New Legislation for Online Transactions In Line with E.U. Law

The first piece of legislation dealing directly with online transactions under Turkish law was finally adopted on March 6, 2003 and published in the Official Gazette of March 14, 2003. Law No. 4822 Amending Certain Provisions of the Consumer Protection Law No. 4077 ("Law No. 4822") has been enacted primarily as a result of the efforts towards harmonising Turkish Legislation with E.U. law. This amendment to the Turkish Consumer Protection Law has basically enlarged the definition of "goods" for the purpose of Turkish consumer law to cover electronic products, and added distance-selling contracts (concluded through electronic means) into the scope of the Consumer Protection Law.

By virtue of Article 3 of the Turkish Consumer Protection Law, the concept of goods in terms of the Turkish Consumer Protection Law also includes any non-material goods designed for use in an electronic environment, such as audiovisual products. In other words, all rights provided for consumers under the Consumer Protection Law will also apply to all online transactions effective from June 14, 2003; this provision of the Law being effective three months from the date of publication pursuant to Article 38 thereof.

The Turkish Consumer Protection Law as amended by Law No. 4822, is similar in many respects to its counterpart under E.U. law, namely the Distance Selling Directive 97/7/EC. For instance, Article 9/A of the Turkish Consumer Protection Law defines the distance selling contracts in the same way as Article 2 of the E.U. Distance Selling Directive. Both provisions define a distance selling contract as any contract concerning the delivery of goods or performance of services immediately or later, which are concluded in a written, audiovisual, telephonic and electronic environment or by using other communication means without physically meeting the customer.

Furthermore, both the recently added Article 9/A of the Turkish Consumer Protection Law and the E.U. Distance Selling Directive provide that before the conclusion of a distance selling contract, the consumer must be provided with certain information, and the contract may not be concluded before the consumer confirms in writing that he or she has received such information. Under Law No. 4822, the scope of such information will be determined in the Communiqués to be issued by the Ministry of Industry and Commerce. No such communiqué, however, has been issued thus far. Article 4 of the E.U. Distance Selling Directive sets out the information that the consumer must be provided with prior to the conclusion of the contract. As the amendments to the Turkish Consumer Protection Law are a result of the harmonisation efforts of Turkish law and the *Acquis Communautaire*, it is most likely that the Communiqués to be issued by the Ministry of Industry and Commerce regarding that prior information requirement will set forth very similar provisions to Article 4 of the E.U. Distance Selling Directive.

Pursuant to Paragraph 3 of Article 9/A of the Turkish Consumer Protection Law and Article 7 of the E.U. Distance Selling Directive, the supplier must execute the order within a maximum of 30 days from the day following that on which the consumer forwarded his order to the supplier. However, under the Turkish Consumer Protection Law, this duration may be extended for a maximum of ten days on the condition of previously notifying the consumer in writing.

There are also a number of differences between the distance selling provisions of the Turkish Consumer Protection Law and the E.U. Distance Selling Directive. For example, pursuant to Paragraph 4 of Article 9/A of the Consumer Protection Law, the vendor and supplier are obliged to prove that the delivery of the non-material goods or services to a consumer by electronic means has been made non-defectively. However, the question of defective goods is not separately regulated under the Distance Selling Directive. In European law, this issue is governed by the Product Liability Directive 85/374/EEC, pursuant to which the injured person must prove:

- actual damage;
- the defect in the product; and
- the causal relationship between damage and defect. In other words, the distance selling provisions of the Turkish Consumer Protection Law is favourable to the consumer compared to the E.U. Distance Selling and Product Liability Directives regarding the burden of proof.

Another amendment made by Law No. 4822 relates to the application of the provisions that govern the indoor sales as provided in the Consumer Protection Law to the distance selling contracts. Paragraph 5 of Article 9/A of the Consumer Protection Law, however, stipulates a number of exceptions for that application, *e.g.*, the provision pursuant to which any payment or document creating a debt for consumer may not be requested from the consumer in return of a good or service which is subject to the contract, during the duration of right for renunciation.

Paragraph 6 of Article 9/A also provides that the vendor or supplier is under obligation to return the paid price, letters of exchange, and any other documents which create a debt for the consumer due to this legal transaction within ten days from the date of reception of the withdrawal notice, and to take back the good within twenty days.

Moreover, under Article 6(2) of the Distance Selling Directive, where the consumer exercises the right of withdrawal, the supplier shall be obliged to reimburse the sums paid by the consumer and such reimbursement must be carried out as soon as possible and in any case within 30 days. Under the distance selling provisions of the Turkish Consumer Protection Law, however, a shorter period of time is provided; *i.e.*, the supplier must reimburse the sums paid within ten days from the date of reception of the withdrawal notice.

Having analysed the distance selling provisions under Turkish law at some length, it can be stated that the importance of such provisions stem from the fact that this is the very first piece of legislation directly governing electronic commerce. However, compared to its counterpart under E.U. law, much still remains to be done on the distance selling contracts under Turkish law. As stated in Law No. 4822 itself, the Ministry of Industry and Commerce will issue the necessary Communiqués to regulate the distance contracts in detail, and as a result of the approximation efforts of the Turkish legislation to E.U. law, it is likely that those Communiqués will closely follow their European counterparts.

By Gamze Cigdemtekin-Uysal and Cadgas Evrim Ergun, Cakmak Law Office, Ankara; e-mail: c.ergun@cakmak.gen.tr

INTELLECTUAL PROPERTY

Changes to Italian Copyright Law: Protecting Authors' Rights in the New Digital and Technological Markets

By Avv. Alessandro del Ninno, Information & Communication Technology Department, Studio Legale Tonucci; e-mail: adelninno@tonucci.it, web site: www.tonucci.it

Introduction

With the publication of the Legislative Decree of April 9, 2003 No. 68 (in the Italian Official Journal of April 14, 2003 No. 87) Italy has implemented E.U. Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society. The introduction of the new national rules (in force from April 29, 2003 with regard to works protected at the date of December 22, 2002 have been realised by amending the Italian Copyright Law, the legal framework of which has been extended with supplementary provisions. The new rules have clear implications on how works can be reproduced or distributed by means of the new technologies widely used in the Information Society (*i.e.*: Internet, UMTS or WI-FI technologies, etc).

A brief analysis of some of the main changes is provided in the following paragraphs:

Author's Exclusive Rights

The first modification introduced by Legislative Decree 68/2003 regards the "right of reproduction". The exclusive right to reproduce means that the holder can multiply the work in its entirety or in part, temporarily or permanently, in any means or form, by hand, print, lithography, engraving, photography, phonography, cinematography or any other means of reproduction (especially the latest statement, referring to "any other means of reproduction", let the author/holder use any technology to exercise his right to reproduce the work).

Another important amendment introduced by the Legislative Decree 68/2003 is related to the "*right to communicate to the public*", which has been updated taking new technologies and means for transmission into consideration. In fact, the amended text of Article 16 provides the exclusive right to communicate a work to the public by wire or wireless means, using one of the means of long-distance dissemination, such as telegraphs, telephone, radio and TV broadcasting means and other similar devices (including Internet connections) and includes communication to the public via satellite and retransmission by cable, as well as communication with the public codified with specific access restrictions. It also includes making the work available to the public in such a way that everyone may have access from a singular chosen place and moment (the exclusive right to communicate to the public cannot be extinguished by any act of communication to the public, including acts of making available the work to the public).

Another exclusive right that has been changed considerably by the implementation of the Legislative Decree 68/2003, is the author's right to control the distribution of a copyrighted work. The amended Article 17 of the Italian Copyright Law now provides that the exclusive right of distribution is aimed at marketing, circulating or making available to the public by any means and by any right of the original work, or copies of the original, and also includes the exclusive right to introduce copies made in non-Member States of the European Union for distribution in E.U. Member States.

Before Legislative Decree 68/2003 entered into force, the Italian Copyright Law contained specific provisions about the author's rights with regard to "works registered on mechanical devices". Due to technological developments, the related articles (61, 62 and 63) have been properly amended to include any kind of technology used by the author to exercise the rights provided in those articles (right to adapt, to record, to reproduce, to distribute, to rent, to lend, to publicly use and communicate the work, regardless of the technology used).

Exceptions and Limitations to the Author's rights

A key part of the Italian Copyright Law is represented by Chapter V of the Copyright Act, containing

rules about "Free utilisation of copyrighted works". The related rules provide cases, terms and conditions according to which it is possible for interested subjects to freely use copyrighted works, regardless of whether prior consent or authorisation has been given by the IPR holder. The previous rules did not in fact, take into consideration the reproduction of works through digital and technological means, but only paper copies (where the works were reproduced) and radio-casting devices.

According to the amended version of Article 65 of the Italian Copyright Law, news articles of an economic, political or religious nature, published in reviews or in newspapers, or diffused by radio or other means available to the public, and other materials of the same nature can be freely reproduced or communicated to the public in other reviews or journals, including the Radio-TV ones, if the reproduction or the use has not been expressly restricted, as long as they indicate the work's source, date and author's name (if it is provided).

Further, the reproduction or communication to the public of copyrighted works on the occasion of journalistic reports is allowed, as long as they indicate the work's source (if available) and author's name (if provided).

Other kinds of works and materials subject to free utilisation as provided by the Italian Copyright Law are: speeches of a political or administrative nature given in public meeting or otherwise publicly communicated, as well as extracts from conferences open to the public, as long as they indicate the source of the work, the date and author's name, the date and the place where the speeches were held.

Other limitations for free utilisation of copyrighted works are those set forth in the amended Article 68 of the Italian Copyright Law. The rule provides – amongst others – that it is permissible to reproduce single works or any part thereof for personal use by hand or by means of reproduction not used for the purpose of public dissemination.

An interesting link between the rules provided by the Legislative Decree 68/2003 and the Italian rules implementing E.U. Directive 2000/31/EC on E-Commerce (introduced by means of the Legislative decree of April 9, 2003 No. 70) is represented by a new provision contained in Article 68-bis of the Italian Copyright Law. This new rule in fact, provides that except for what is provided in the order for the liability of intermediaries/providers of Information Society services in the area of electronic commerce, acts of temporary and accessory reproduction:

- without economic gain;
- being an integral and essential part of a technological process;
- exercised for the sole purpose of permitting the online transmission among third parties with the intervention of an intermediary or the legitimate use of a work or other materials,

are exempt from the exclusive right of reproduction.

Private Reproduction of Copyrighted Works for Personal Use

According to the E.U. Directive 2001/29/EC provisions, new rules have been added to the Italian Copyright Law with respect to the discipline of private reproduction of copyrighted works for personal use and the related exceptions and limitations.

The main principles can be summarised as follows:

(a) it is permitted to privately reproduce audio and visual materials on any equipment/support, carried out by a person for exclusive personal use, as long as there is no economic or commercial purpose, either indirect or direct and in compliance with the technological protection measures set up by the right's holders to protect his or her IPR (see art. 102-*quater* and 102-*quinquies* about the new regulation of technological protection measures and the electronic copyright-management information about the IPR);

(b) private reproduction for personal use cannot be effected by third parties. It is strictly prohibited to provide services aimed towards private reproduction if it is performed for economic or direct or indirect commercial gain;

(c) private reproduction rules mentioned above shall not apply to protected works or materials made available to the public in a way that anyone can have access to the place at any given moment, when IPR holders protect their work by means of technological protection measures or when the access is permitted on the basis of contractual clauses;

(d) with the exception of what is provided under letter (c) above, rights holders are obliged to permit that, notwithstanding the application of the technological protection measures, the physical person who had acquired the legitimate possession of the copies of the protected work or materials, or who had legitimate access, may make a private copy for personal use.

Authors and audio producers, as well as original producers of audio and visual works, and their assignees, have the right to compensation for the private reproduction of audio and video works. This compensation is comprised of a share of the price to the re-seller or of a fixed amount for audio and video recording and recording on computer systems. For audio and video recording equipment, such as analogue, digital, fixed or transferable memory, compensation amounts to a sum commensurate with the capacity of registration of the equipment.

The compensation shall be determined by a Decree of the Ministry for Cultural Affairs and must be paid to the Italian Society of Authors and Publishers (S.I.A.E.), which is responsible for distributing the monies to rightholders. In any case it is fixed, until the release of the Decree and in any event until December 31, 2005 to the extent of:

- analogical audio supports/equipment: EUR 0.23 for every hour of recording;
- dedicated audio digital supports/equipment, such as mini-discs, audio CD-roms and CD-RW audio: EUR 0.29 per hour of recording. Compensation shall be increased proportionally for equipment of a longer duration;
- non-dedicated digital supports/equipments capable of recording phonograms, such as data CD-R and CD-RW data: EUR 0.23 per 650 megabytes;
- digital audio dedicated memories, fixed or transferable, such as flash memories and cartridges for MP3 readers and similar type equipment: EUR 0.36 per 64 mega-byte;
- video analogical supports/equipments: EUR 0.29 for each hour of recording;
- dedicated digital video supports/equipments, such as DVHS, DVD-R video and DVD-RW video: EUR 0.29 per hour, equivalent to EUR 0.87 for supports/equipments with a storing capacity of 180 minutes. Compensation shall be increased proportionally for equipment of a longer duration;
- digital supports/equipments capable of audio and video recording, such as DVD Ram, DVD-R and DVD-RW: EUR 0.87 for 4,7 gigabyte. Compensation shall be increased proportionally for equipment of a longer duration;
- analogical or digital audio and video for exclusively recording aims devices: three percent of the price applied to the reseller.

Technological Measures for IPR Protection and E-Copyright-Management Information

According to Directive 2001/29/EC, a new set of rules has been added to the Italian Copyright Law to discipline the utilisation by the IPRs holder of technological measures aimed at technically protecting such IPRs. Holders of copyrights and related rights and the so-called "constitutor" of a databank (*i.e.*, the subject who employs the relevant financial resources and time aimed at building, setting up, presenting or verifying a databank: see Article 102-*bis* paragraph 3 of the Italian Copyright Law) can attach technical measures for effective protection to the protected works or materials. Such measures include any technology, devices or components that, in the average course of their functioning, are destined to impede or limit unauthorised acts from rights holders.

Technical protection measures shall be considered efficient in the event that the use of the protected work or material is controlled by rights holders by applying an access device or a protection procedure, such as encoding, distortion, or any other transformation of the protected material or work, however it is restricted by a control mechanism of copies that realise the protection objective.

Further, the new rules prohibit to evade or remove technical protection measures, which gives rise to an abusive use of the creative work or the protected materials.

It must be noted that the new rules about the technological protection measures do not affect the existing provisions of the Italian Copyright Law related to the protection of software. So, the rules added in 1992 to implement E.U. Directive 91/250/EC on the protection of software shall continue to be applied.

Other important provisions added by Legislative Decree No. 68/2003 regard electronic copyright-management information. Electronic copyright-management information can be included by owners of copyright and related rights as well as by the "constitutor of a databank" on protected works or materials. Such information can also be made to appear in any act of communication to the public of the protected works or materials. The electronic information identifies the protected work or material, as well as the author or any other rights' holders; it may also contain indications of the terms or the conditions or use of the works or the materials, as well as a number or code representing the information itself or other element of identification.

Rights holders who have fixed their technical restrictions according to the above rules are in any case obliged to remove them to allow – amongst others –the use of the protected works or materials upon request of a competent authority, for the purpose of public security or to ensure the proper functioning of an administrative, parliamentary or judicial procedure.

The breach of the rules analysed in this paragraph and regarding the technological measures for IPR protection and electronic copyright-management information is sanctioned with imprisonment or with economic penalties.

It must be noted that another Italian law has recently introduced harsher punishments for the breach of copyright in the field of the conditional access services. In fact, Law No. 22 of February 7, 2003 by amending the previous Legislative Decree of November 15, 2000 No. 373 "Implementation of the Directive 98/84/EC on the protection of conditional access services", now provides criminal and administrative sanctions. These apply to:

- whoever manufactures, distributes, sells, or advertises for commercial purpose, illicit equipments or softwares created or adapted with the aim of making conditional access service possible without the authorisation of the service provider; and
- those who use or simply hold for private purpose such illicit equipments or software (*i.e*, pirate decoders for cable TV).

In conclusion, the recent amendments to the Italian Copyright act update the related legal framework with a set of new rules specifically aimed at protecting authors' copyright in new markets (the technological and digital ones) and in a fast changing Information Society.

Domain Name Dispute Resolution Reports

In this column, the *World Internet Law Report* provides details of recent domain name dispute resolution rulings by ICANN-accredited institutions. The information on the reports is provided by Riccardo Roversi, Studio Legale Abbatescianni, Milan & Rome, with contributions from Judith Paine and Yee Mun Loh. Mr. Roversi may be contacted by e-mail at roversi@sla.it; tel. (+39-25) 413-1722; fax: (+39-25) 501-4830; Web: *www.sla.it*

MRA Holdings, LLC v. Alexander Boris Niche Profit Ltd

Domain name: girlsgoneswild.com

Dispute resolution provider: NAF (Case No. FA301000140623)

Panel: John J. Upchurch

Identical or confusing similarity: Domain name virtually identical to registered trademark.

Rights or legitimate interests: Failure to respond to Complaint; inference of no rights or legitimate interests.

Registration and use in bad faith: Registration of domain name that differed in one character created likelihood of confusion regarding affiliation or endorsement by Complainant.

Result: The domain name was ordered to be transferred.

Decision date: February 21, 2003

Broadcom Corporation v. Smoking Domains and Michelle Lehman

Domain name: broadcommunications.com

Dispute resolution provider: NAF (Case No. FA021200037037)

Panel: The Honorable Charles K. McCotter, Jr. (Ret)

Identical or confusing similarity: Domain name not confusingly similar to registered trademark, as overall impression of domain name was not confusingly similar to registered trademark.

Result: Domain name registration remains with Respondent.

Decision date: February 11, 2003

Bloomberg L.P. v. Future Movie Name

Domain name: bloonberg.com

Dispute resolution provider: NAF (Case No. FA0212000139664)

Panel: James A. Carmody

Identical or confusing similarity: Domain name incorporated a common typographical error into Complainant's domain name and registered trademarks.

Rights or legitimate interests: Pattern of infringing behaviour of registering domain names incorporating a typographical error of famous trademarks in order to confuse Internet users; "Typosquatting".

Registration and use in bad faith: Registration of infringing domain name in knowledge of Complainant's well-known rights.

Result: The domain name was ordered to be transferred.

Decision date: February 8, 2003

Twentieth Century Fox Film Corporation v. Michele Dinola

Domain name: foxmoviechannel.com

Dispute resolution provider: NAF (Case No. FA0212000135643)

Panel: Richard DiSalle, James P Buchele, Clive Elliot

Identical or confusing similarity: Domain name identical to Respondent's trademark registrations.

Rights or legitimate interests: Use of domain name to re-direct Internet traffic to revenue-generating search engine.

Registration and use in bad faith: Use of domain name resulted in consumer confusion as to Complainant's affiliation; registration was to trade off goodwill associated with famous trademark.

Result: The domain name was ordered to be transferred.

Decision date: February 3, 2003

Empressa Municipal Promocion Madrid S.A v. Easylink Services Corporation

Domain name: Madrid.com

Dispute resolution provider: WIPO (Case No. D2002-1110)

Panel: Ross Carson, Paz Solar Masota, Geert Glas

Identical or confusing similarity: No evidence filed of use of geographic indication of MADRID as a registered trademark; in absence of substantial proof of acquired distinctiveness or secondary meaning displacing the significance of the geographical indication, a geographical indicator does not serve as a trademark or service mark.

Rights or legitimate interests: Establishment of various legitimate interests under the Policy.

Result: Panel declined to order the transfer of the domain name.

Decision date: January 26, 2003

Daddy's Junky Music Stores, Inc. v. Amjad Kausar

Domain name: daddysjunkiemusic.com

Dispute resolution provider: NAF (Case No. FA0301000140598)

Panel: Tyrus R. Atkinson Jr.

Identical or confusing similarity: Domain name was virtually identical to Complainant's trademark incorporating Complainant's entire mark, but merely removed the apostrophe and spaces between the words with the addition of top-level domain.

Rights or legitimate interests: Domain name used to divert Internet users to Respondent's Website is no bona fide offering of goods or services.

Registration and use in bad faith: Inference of profit making by diverting Internet users to Respondent's Website.

Result: Domain name to be transferred.

Decision date: February 11, 2003.

Case Report

AUSTRIA

■ DEEP LINKING: COPYRIGHT NOTE ALLOWS DISPLAY OF FOREIGN CONTENTS ON WEBSITE

Meteodata vs. Bernegger Bau

Austrian Supreme Court, December 17, 2002

Background and Facts

The claimant is a company providing online weather forecasts. The company has marketed its services via the Internet since 1997 and has informed potential customers about its services via its website. The homepage of the company is displayed on the Internet under the domain name "meteodata.com" and contains several links to other websites. The site of the claimant shows *inter alia*, current weather charts for every European country and its regions, as well as weather profiles of major cities throughout the world. The following copyright note is placed directly below the accessible weather charts: "source: c METEO-data METEO-data". Each copyright note is configured as a link and leads directly to the homepage of the claimant.

The defendant conducts business in the building industry and registered its website under the domain name "b*****.at" in December 2000. The defendant's website is designed by using framing technology. Thereby, a website is divided into frames and different documents (from its own site or those of foreign websites) can be displayed simultaneously in each frame. Until December 2001, the defendant's website showed relevant factual information in a frame which could be accessed via the menu bar. The menu bar contains search terms, which are configured as links. If a search term is activated by the user, several subordinated search terms are made available, which enable access to information from several sub-pages within the frame. When activating the search term "building weather" in the menu bar, a subdivision of names of the Austrian Provinces – also being configured as links – becomes visible. If the user activates one of those names, the site of the claimant is accessed via framing technology as follows: the frame of the defendant's website shows the map of the specific Province including a description of the actual weather and a forecast for the next day together with an explicit and clearly visible copyright note "source: c METEO-data METEO-data" being configured as a link to the claimant's homepage. In the address field, the browser only shows the domain name of the defendant. Thus, when looking at the address field only, the user does not know that access to information of the claimant's website is given.

The defendant had no contractual authorisation to use the information provided by the claimant's website. As soon as the claimant found out about the procedure described above, the claimant charged a usage fee for weather services from December 1, 2000 to November 13, 2001. The defendant refused payment but removed all links under the search term "building weather" leading to the website of the claimant on December 14, 2001. Since then, no connection between the websites of the parties is given.

To ensure appropriate omission of use, the claimant demanded an interim injunction against the defendant to omit the use of weather charts of the Austrian Provinces or any other weather charts being displayed on the claimant's website within its own Internet appearance, and to omit enabling public access to the claimant's weather charts, especially by using framing technology, without the claimant's consent. The claimant argued that the defendant did not use hyperlink technology, where a complete change to the other website is effected, but displayed the contents of the claimants website via framing technology on its own homepage. The claimant argued that it is not visible to the user that the information being displayed had been taken from a foreign website. Thus, the false impression is given that the whole information package displayed derives from the website being accessed at that particular moment. Therefore, the claimant argued, that Section 1 UWG (Austrian Act against Unfair Competition) had been breached. Furthermore, the weather charts of the claimant are protected under Section 40 UrhG (Austrian Copyright Act). According to the claimant, the defendant infringes the rights of publication and the copyright of the claimant and contributes to illegal change and editing of a foreign work.

The defendant emphasised that the security claim is too indefinite and goes too far. In particular, not every link via framing technology is illegal. The defendant noted that according to Austrian law, copyrights or competition rights are not infringed if the contents of a foreign website are displayed via a link in a new window or on the whole page of a foreign website. The defendants also argued that there is no competition between the parties and that the copyright note shows clearly and unmistakably that the defendant does not offer these services himself. The defendant also expressed that in his view, use of the claimant's website is even encouraged as the copyright note leads directly to the claimant's homepage. Therefore, hits on the claimant's website are likely to be increased. Finally, the defendant noted that a weather chart is not a scientific or instructive work and thus is not protected by the UrhG.

First Instance and Appeal

The case of First Instance prohibited the defendant's use of the weather charts of the Austrian Provinces or any other weather charts which are displayed on the claimant's website within the scope of its appearance on the World Wide Web by hyperlinks without a claimant's consent, if it is not clearly visible that the connection is made by a hyperlink to the website of the claimant. The additional demand from the claimant, calling for a

prohibition against using the weather charts of the Provinces or any other weather charts being displayed at the claimant's website within its appearance on the Internet without consent of the claimant, especially by using frame technology, was dismissed. The Court stated that such a general ban to connect to foreign websites would undermine the character of the Internet. Linking to other websites is according to law, if the connection is made in such a way that access to a foreign website is recognisable and it is obvious to which sites access is given. In the present case however, the design of the web page is to be judged as an unscrupulous use of foreign achievements in the sense of Section 1 UWG. The Court argued that the copyright note did not change the situation at all, because it was not visible to the user that a connection to another website was made. The Court of Appeal confirmed this decision.

Decision of the Supreme Court

Austrian Copyright Act (UrhG)

As ruled in former decisions, the Supreme Court stated that the use of a work or photograph on the Internet is reserved to the author. However, the Supreme Court did not discuss the question whether digital use is to be included under copyright and spreading or under communication to the public. The Supreme Court argued that if the weather charts which were provided are held to be a work under Section 1 UrhG, and if the author has granted the claimant unrestricted rights of use, the defendants have to ensure that the users of their website are being helped to access the contents of the claimant's website. If such access is connected with a fugitive copy operation (in the internal memory of the computer) or an accompanying copy procedure (by staging in a proxy server), in most cases a copyright for one's own use under Section 42 para 1 UrhG is given. Copies for one's own use are legal and do not infringe copyrights, even if made for business reasons. The Supreme Court added that an interpretation of Section 42 para 1 UrhG according to European law does not change this result. The Supreme Court noted that an excess of permitted free usage of work would only be given if the defendant knowingly encouraged the infringement of intellectual property law by third persons. This was neither claimed nor proved by the claimant.

Moreover, the design of the claimant's website (vertical menu bar, advertising banner) is only an ordinary achievement which does not have any individual elements. Therefore, the claimant's website is not a work under Section 1 UrhG. The visualisation of parts of the claimant's website by links to the site of the defendant is therefore not an illegal manipulation of a work.

Austrian Act Against Unfair Competition (UWG)

The Supreme Court ruled that the defendant did not overtake an accomplishment of the claimant, but only enabled the users of its website a simplified access to the contents of the claimant's website. Thus, no unethical takeover of a foreign achievement occurred and Section 1 UWG was not breached. The Supreme Court stated further that no foreign work was obtained surreptitiously or by breach of faith, nor was it copied in order to encumber the claimant.

Moreover, the Court ruled that infringement of competition law is not given by avoidable deception of origin or by exploitation of ones standing. The defendant's website does not cause a risk of confusion as a clearly visible copyright note under each weather chart clarifies the origin of the chart. The standing of the claimant is neither exploited in an unethical way, nor are the claimant's benefits of the work endangered because even the claimant could take advantage of the copyright notice. As the note is designed as a link to the claimant's homepage, the claimant's work can be found on the Internet more easily. Although the claimant might loose advertising revenue because the user is directed past the claimant's homepage, the link only attempts to enable the user to access the information sort quickly and clearly. A loss of advertising revenue is only an unintended side effect.

The Supreme Court concluded that neither the claimant's competition rights nor its copyrights had been infringed.

By Angelika Höbinger, an associate with Dorda Brugger & Jordis. The author may be contacted at angelika.hoebinger@dbj.at

News

EUROPE

Further Relaxation of Rules for Registration of Top Level Domains

There has been further relaxation of the restrictions on companies registering country code top level domains (ccTLDs). Restrictions have now also been relaxed in Sweden and the Netherlands. Deregulation is being welcomed by companies as an unmissable opportunity to establish a presence in other countries and develop trade in their local markets.

Sweden – .se registrations were opened up to businesses not based in Sweden on April 2, 2003. Deregulation not only means that registration is no longer restricted to Swedish entities but also that the domain name no longer needs to correspond to the name of the registrant. There is also now no restriction on the number of .se domains that can be registered to a single entity.

Netherlands – From January 29, 2003 companies without a presence in the Netherlands have been allowed to register .nl domains. The registry operator (SIDN) still requires the registrant to provide a local contact, however, this is often a facility offered by service providers and so in practice does not pose any real difficulties to

companies wanting to register .nl domains who have no physical presence in the Netherlands.

Liberalisation of the ccTLD restrictions undoubtedly offer a great opportunity for companies to widen their commercial presence, however, the corporate world should be alert to the resulting danger of an increase in cybersquatting. Consequently, companies are advised to register the relevant ccTLDs for countries in which they trade as a means of protection against infringement of their intellectual property. The cost of registering a domain name is minimal, especially when compared with the cost of funding litigation when the name has been registered by a cybersquatter.

By Maria O'Connell, Eversheds, Manchester; tel: 0161 831 8280; mariaoconnell@eversheds.com

INTERNATIONAL

OECD Publishes Comparative Study on Domain Names

The Secretary-General of the OECD has published on its website a report drafted in December 2002 by the Directorate for Science, Technology and Industry entitled "Comparing domain name administration in OECD countries".

This report provides comparative information on the administration of domain names across the OECD area. It is available at: *www.oecd.org/pdf/M00040000/M00040342.pdf*

By Chris Kuner, Hunton & Williams, Brussels

LEGISLATION & GUIDANCE

News

EUROPEAN UNION

Judicial Network Goes Online

Members of the public and lawyers are now able to obtain information from the European Commission website about civil, family and commercial law systems in all E.U. Member States.

Welcoming the launch of the website Baroness Scotland, Parliamentary Secretary at the U.K. Lord Chancellor's Department, said:

> "It will be a valuable tool that will help improve access to justice for citizens across the European Union."

The website (*http://europa.eu.int/comm/justice_home/ejn/*) provides information on a number of legal topics covering the procedures and systems in each Member State, the European Union and international agreements. It is available in all official E.U. languages.

The first topics covered by the website include how to apply for legal aid and how to start civil court proceedings in each Member State. Information about the court structure in each Member State is also covered. In the coming months more topics will be added in areas including divorce, child maintenance and parental responsibility.

The website is one of the first initiatives of the European Judicial Network in Civil and Commercial Matters which was formally established on December 1, 2002 to facilitate judicial and legal co-operation between Member States.

U.K. Lord Chancellor's Department; www.lcd.gov.uk

FRANCE

Internet Rights Forum Issues New Guidance on Government Data

PARIS—France should compile all existing public sector information into a single database accessible to citizens and companies alike, according to a new series of recommendations published on April 14, 2003 by the country's leading authority on the establishment of rules for online activity.

In its new Recommendation, "What Policies for the Diffusion of Public Information", the Internet Rights Forum urges the government to create a new database of all digitised or non-digitised data produced by the state, regional or local government, and public authorities, and to make the information available online.

The Forum – a public-private sector body created in May 2001 to advise the government on Internet policy issues – suggests that the database should include all legal texts issued to date, as well as regularly updated data on listed and non-listed companies, government-generated maps, and statistical studies such as census information.

The Forum "recommends that the state diffuse immediately all the public data needed to allow citizens to fully exercise their rights", and suggests that the government also publish an online "directory" offering a road map to readily-available public information.

Personal information should be protected in any new government-led publishing endeavour, the Forum said, but its new Recommendation left open the door for non-nominative, or anonymous, publication of a wide array of data on individual citizens, whether culled from property and tax registries, public education and health files, or other sources.

While the information diffusion recommendations issued by the Forum – more than 100 private sector firms and public sector entities, as well as associations and groups from across the spectre of Internet activities – are non-binding, the group said its guidelines should offer greater direction to government officials and private sector firms seeking to balance the ever-greater information flow created by the uptake of information technology in government offices with the need to protect privacy.

The issue has taken on a higher profile in recent years in France as Internet use grows and citizens become more adept at seeking public information online, the Forum said.

In recognition of the changing realities, the Forum's new Recommendation includes calls for government to draft specific regulation for the "information industry", a generic term used by the Forum to describe database operators and other information collection and retrieval services.

The proposed rules should include a new obligation for transparency and full access to government-held information, alongside the right for citizens to oppose communication of any information for commercial use that may violate personal privacy, with a proposed public body, the Commission on Access and Diffusion of Public Data, which would be responsible for implementation of the new data diffusion policies.

The Forum calls on government to recognise that public information is of value to intermediaries and end-users alike, and seeks creation of new, transparent price structures for the sale of public data. "The diffusion of data can not be undertaken for free", the Forum said, proposing that prices be fixed as a function of distribution and intellectual property costs.

Free information will be limited to data deemed of interest to "citizens, or that which is necessary to allow citizens to exercise their rights", the Forum said.

The new recommendations are the result of nearly a year's consultations under the Forum umbrella between government officials, French Internet law experts, technological specialists, citizen groups, and representatives of industry.

The Recommendation has been forwarded to State Secretary for Administrative Reform Henri Plagnol, who is expected to include public data distribution in a wide-ranging modernisation of government, as well as to the European Commission, which is preparing a new E.U.-wide directive on public sector information distribution.

The Forum's public sector data diffusion recommendations, "*Quelle Politique de Diffusion des Donnees Publiques*?" may be consulted, in French, at: *www.foruminternet.org.*

PRIVACY

Case Report

UNITED STATES

ISP WINS $16.4 MILLION JUDGMENT AGAINST SPAMMER

EarthLink Inc. v. Carmack, N.D. Ga., No. 1:02-CV-3041, 5/7/03

U.S. District Court for the Northern District of Georgia, May 7, 2003

Internet service provider EarthLink Inc. won an important ruling in U.S. District Court for the Northern District of Georgia on May 7, 2003 when a federal judge levied a $16.4 million judgment against a spammer who had inundated EarthLink subscribers with unwanted junk e-mail for a year, the Atlanta-based company said EarthLink's assistant general counsel called the court order by U.S. District Court Judge Thomas W. Thrash Jr. "a victory against spam", adding that Thrash's order would allow private individuals and other ISP's to bring new legal action against the defendant in the case, Howard Carmack of Buffalo, N.Y., as third-party beneficiaries of the injunction, should Carmack begin spamming again.

Carmack sent over 825 million e-mail messages to EarthLink subscribers in the past year, the company said, using 343 EarthLink accounts. In his order, Judge Thrash estimated the company's actual damages at more than $2.7 million. The court trebled those damages after granting EarthLink's state and federal racketeering claims, and then doubled it again to $16.4 million in total damages to "serve as a clear warning to Carmack". Thrash also said the judgment will not be dischargeable in bankruptcy.

Largest Judgment to Date

In court papers, EarthLink alleged that Carmack

> "used stolen credit cards, identity theft, banking fraud and other illegal activities to fraudulently purchase hundreds of Internet accounts and began sending spam that included advertisements for computer virus scripts, work-at-home get rich

quick schemes, bulk e-mail software, and lists to be used by other spammers", as well as cable TV descramblers.

It is the third big victory against spammers for EarthLink, which in 1997 obtained an injunction against Sanford Wallace and a $2 million judgment against his company, Cyber Promotions, a year later. In 2002, the company obtained a $25 million judgment against a spammer named K.C. Smith who had generated more than 1 billion unwanted e-mails. It is the largest judgment to date against a spammer.

In his order, Thrash said that in the event another ISP files a lawsuit against Carmack the liquidated damages will be $25,000 or $2 per 1,000 e-mails sent, whichever is greater, as well as lost profit damages, attorney's fees, expenses and costs. Individual or end-user claims will be $1,000 per e-mail sent, as well as legal fees, expenses and costs.

News

DENMARK

Court Fines Company for Sending Unsolicited Messages

COPENHAGEN—The Danish Maritime and Commercial Court on May 1, 2003 fined a Danish software and publishing company DKK 15,000 (about $2,300) for sending unsolicited commercial electronic mail and facsimiles to Danish companies and individuals in violation of Danish marketing law (M-1-02 Anklagemyndigheden mod Fonn Danmark ApS, 5/1/03).

It is the first time a European Union nation fined a company for sending unsolicited commercial e-mail, or spam, National Consumer Agency Deputy Head of Division Peter Fogh Knudsen told *WILR*.

The convicted company, Lyngby-based Fonn Danmark ApS, could appeal the verdict to a regional court but instead will pay its fine, according to Fonn Danmark lawyer, Christian Levin Nielsen.

The firm sent about two million e-mails and faxes to businesses and individuals over a period of two years, but the court based its decision and fine on 156 formal complaints introduced during court proceedings in April this year, Levin Nielsen said.

Legal Issues

Fonn Danmark's defence rested on a number of arguments. First, the company claimed it possessed consent to send the advertisements from e-mail and fax recipients who received its messages before the Danish law went into effect. By not telling the company to stop sending the messages, the firm argued the recipients had given "silent consent" to receiving the messages, Knudsen said.

The firm also claimed to believe concepts embodied in Norwegian law, where companies can contact other companies but not individuals by e-mail, would be part of Danish law because both countries are governed by E.U. standards, including E.U. directive 2002/58, the directive on privacy and electronic communications, Levin Nielsen said.

But Danish law meets and exceeds those E.U. standards, something Levin Nielsen said his clients belatedly discovered. Fonn Danmark had past business experience in Norway, Levin Nielsen said. Knudsen said another argument offered by the company was that the server sending the e-mail was located in Norway.

The court, in its ruling, ruled against the Fonn Danmark and imposed the fine.

Law Prohibits Ads Without Prior Consent

The government charged Fonn Danmark – a relatively small, private limited liability company selling software, software manuals, and related products – with violating The Danish Marketing Practices Act (699/2000, as amended by 428/2002). Penalties under the law include fines but not imprisonment.

The law prohibits commercial enterprises from sending out advertisements by e-mail, facsimile, or SMS without the advertisement recipient's prior consent. The section of the law prohibiting unsolicited e-mail entered into force on July 1, 2000.

After the Consumer Agency received complaints about Fonn Danmark by e-mail and postal mail in the Spring of 2001, the agency sent the firm three letters requesting it halt its allegedly illegal activities, apparently with little effect.

The Maritime and Commercial Court possesses jurisdiction over specialised civil cases. Appeals to its rulings are heard by one of two Danish regional courts, which are superior to a series of district courts but subordinate to the Supreme Court, Denmark's highest judicial body.

Peter Fogh Knudsen prosecuted the case for the National Consumer Agency. Christian Levin Nielsen of Zacco Law Firm represented Fonn Denmark ApS.

UNITED KINGDOM

New Rules on Unsolicited E-mail Expected To Be in Force by October

LONDON—New rules to stamp out unsolicited e-mail should be in force by the end of October 2003, according to government minister, Lord David Sainsbury.

Lord Sainsbury, a junior minister with the Department of Trade and Industry, told the House of Lords that the government would implement strict new rules about how personal e-mail details are used. He said that by "the end of October" the U.K. government would implement a European Union privacy directive to

outlaw the transmission of unsolicited e-mails across Member States.

The Directive on Privacy and Electronic Communications Directive (2002/58/EC) will go into effect on July 31, 2003. It applies to anyone processing personal data on any publicly available communications services, including the Internet and mobile text messaging services.

The DTI is currently discussing the implementing legislation with industry representatives. Its own consultation period on the issue, which began at the end of March, is scheduled to end on June 12.

Sainsbury acknowledged that the new European directive does not address spam arriving from outside the European Union. A DTI spokeswoman conceded that the anti-spam battle is unlikely to be won solely through the new legal framework. "This is not a single solution and it is not going to be the end of spam", she said.

Under the directive, unsolicited e-mails may be sent only to individuals for direct marketing purposes, "with their prior consent", or where there is an existing customer relationship.

Spam accounts for as much as 40 percent of all e-mail traffic and is costing business billions in lost productivity, the DTI said. "I can't think that it helps anyone in any activity, including voting, to have their computers flooded with some of this quite distasteful material", Sainsbury told the House of Lords.

Taking a Bite out of Cookies

The directive requires that cookies – small data files that a website sends to a user's hard disk – and other tracking devices on web pages be clearly marked to give people a chance to choose whether they want their activities monitored online. Cookies are necessary to remember web surfer details during the visit to the site or for the surfer's subsequent return.

The privacy concern regarding cookies is that they may store data without the user's explicit approval. An amendment to the directive states that cookies

> "may seriously intrude on the privacy of users. The use of such devices should therefore be prohibited unless the explicit, well-informed and freely given consent of the users concerned has been obtained".

The regulations do not require that this information is given before the cookie is sent to the user's computer, which means that the rules would not dramatically alter the operation of websites – a link to a page describing use of cookies would suffice. A draft of the directive would have required prior notice, but this requirement was removed before it passed.

The directive also recommends that websites allow individuals to decide if they wish to be included in subscriber directories. Clear information about the directory must also be given such as whether further contact details can be obtained from just a telephone number or a name and address.

Mobile operators and their partners will be allowed to provide customers with value added services, such as traffic and weather updates, where consent has been given. The DTI said the law will clear things up for companies using e-mail for legitimate marketing purposes and also give Internet service providers, businesses and individuals an effective weapon against spammers.

Implements E.U. Directive

The United Kingdom's draft Privacy and Electronic Communications (EC Directive) Regulations of 2003 will implement the E.U. directive. The regulations will also revoke the Telecommunications Regulations of 1999.

The prior consent requirement for e-mail also reflects the recently introduced CAP Code, which sets out the rules administered by the United Kingdom's Advertising Standards Authority, which administers the rules covering non-broadcast advertising in the United Kingdom. The voluntary code also covers online banner ads and pop-up ads on the Internet.

The new U.K. regulations have been opposed by the U.K. arm of the Interactive Advertising Bureau, which also lobbied against the privacy directive. IAB argued that the economic benefit of Internet cookies outweighs privacy concerns.

IAB said the law would affect the websites of nearly every business in the United Kingdom. It estimated that a spam ban would cost British companies £187 million ($300 million). An IAB spokesman said it was particularly concerned that persistent spammers could potentially face large fines under the new regulations.

The full text of the E.U. Directive on Privacy and Electronic Communications may be viewed at http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

UNITED STATES

Pornographic Spam Has Potential to Create Hostile Work Environment

Employers who fail to address the issue of employees receiving pornographic spam at work could face potential liability for a hostile work environment, according to some attorneys and security experts. From electronic offers for various devices and drugs, as well as pornographic images that pop up when an e-mail is opened, spam not only clogs employees' electronic inboxes but can make any number of them uncomfortable.

Attorneys say the issue of what employee-to-employee behaviour counts toward creating a sexually hostile work environment has been settled. For example, a worker who forwards pornographic e-mail to a co-worker contributes to a hostile work environment, as does an employee who makes lewd oral comments to a co-worker. The employer, if it knows or should have known about the behaviour, is obligated to stop it. A less clear but emerging issue is to what extent, if at all, the employer has liability for a hostile work environment

created by pornographic spam sent from outside the company.

To the extent that employees have complained about receiving pornographic spam at work, said Vic Schachter, who represents employers for Fenwick & West, Palo Alto, California, "then there is a serious issue", and the company needs to take steps to limit the flow of the offending e-mail – and limit potential liability.

If the remedy entails the extraordinary cost of revamping an entire e-mail or information technology system, then the employer is not obligated to do more than help the employee eliminate the spam, according to Schachter, perhaps by limiting how much the employee has to do with e-mail.

Spam as Grounds for a Claim?

Eugene Volokh, a University of California Los Angeles law professor who has written about the Internet and e-mail as possible grounds for hostile workplace claims, argued that a case can be made that cautious employers would do well to operate as if porn spam does create a hostile work environment.

> "For the [common] variety pornography, I think there's a plausible argument [that] if an employer does not filter out porn, it is creating a hostile work environment," Volokh said.

The California Fair Employment and Housing Act and Title VII of the Civil Rights Act of 1964 generally prohibit racially or sexually hostile work environments, he noted. Such laws "have been interpreted by the courts as mandating that employers stop their employees from, say, posting pornography and sometimes telling sexually explicit jokes" or accessing porn in the workplace, he said.

The Equal Employment Opportunity Commission "has specifically said, and courts have agreed, the company is responsible for any speech and any conduct that it has control over, not just speech or conduct of its employees", he said.

> "So the company, for example, is supposed to prevent creation of a hostile work environment by contractors, by clients, by delivery people, and even, one would argue, [by] total strangers who obtain access" via the Internet, Volokh opined.

Level of Injury

According to Volokh, courts and juries have found that offensive speech that people heard every couple of weeks in the workplace was pervasive enough to be actionable. Others have found liability from a dozen incidents over 20 months, only four of which were uttered in the plaintiff's presence, but all of which the plaintiff eventually learned of, Volokh said.

"If I were a risk-adverse lawyer, I would say that if indeed every day someone is complaining [about receiving pornographic spam] ... then it's possible that a jury would find it's pervasive. That's the difficulty of a vague rule," he added.

"The reason that these complaints are plausible is that they're very similar to complaints that we've seen before," he said, pointing to the fact that there have already been lawsuits brought over sexually explicit jokes or pornography in the workplace.

"The only question is, 'Would they file a complaint about porn and spam e-mail?' " Volokh said. Employers have an obligation to filter with an eye to the reasonable person, even though it can be difficult to discern what is reasonable, he added. In any case, whenever there is a new spate of racial, religious, or sexual spam, "the employer should try to get that blocked," Volokh said.

Beyond Employers' Control?

Rebecca Hastings, operations manager for the Society for Human Resource Management's Information Center, said pornographic e-mails and other spam "have become so widespread in workplaces and homes that both legislators and technical companies are hard at work to resolve it".

"Interestingly enough, the overkill spamming causes means the shock value may be somewhat minimised as people come to routinely open up their e-mail box and delete the undesirable messages", Hastings said.

> "Employers should remain diligent, however, in tackling this issue to the best of their ability and should be careful to respond to any and all employee concerns as best they can," she said

Ernest Haffner, senior attorney advisor in the EEOC's Office of Legal Counsel, Washington, said the agency has no specific spam recommendations in its guidelines on sexual harassment or hostile work environment, which are posted on the agency's website at *www.eeoc.gov.*

"This would be handled basically as any other hostile work environment claim", Haffner said. The sexual harassment guidelines discuss harassment by non-employees, "and the liability standard there is basically the same standard if you were harassed by a co-worker as by a supervisor", he said.

"The thing about spam porn is it's probably going to be an issue of control, because when you're dealing with a non-employee", the employer's control is a consideration in determining whether the employer's action is appropriate, said Haffner

Haffner said he has never received spam porn at work, "so I don't know if an employer would have to assume an employee would receive spam porn at work. ... It's something that clearly is covered in the sense it could create a hostile work environment. The employer has the responsibility to do something about it. It's unclear as to what sort of actions are going to be reasonable because the technology may not be there" for the employer to address the issue, Haffner said.

Bill Tamayo, regional attorney for the EEOC in San Francisco, agreed that employers looking to the agency are not likely to find guidance.

"The employer would be liable if the employer knew or should have known about it and failed to take corrective action", Tamayo said. "The question is, what could the employer have done?"

If the employer knew or should have known, they are required to "take prompt and corrective action. If they know an employee is bringing porn to the workplace and putting it where people are present, the employer is going to face liability. It is a little different" when porn spam is sent externally into the workplace, outside the employer's control, Tamayo said.

Employer Obligation

Cindy Cohn, legal director for the online civil rights group Electronic Frontier Foundation, argued that placing "an affirmative duty on a corporation to filter e-mail into the system is pretty hard. We don't do that with regular mail, and I think that would really be a bit of a stretch to happen in a corporate environment" for e-mail

> "When the Supreme Court can't figure out what [pornography] is, placing an affirmative duty on every employer so that no employee would ever be exposed to it would be a real stretch legally and technologically from where we are now", Cohn said.

Ira Rothken, a Marin County, California, attorney who has tried employment and spam cases in California, said he is unconvinced that an employer would be obliged to do something about offensive spam.

"I'd have a hard time believing that an employer could be held liable for the 'noise' of the Internet", – a reference to offensive spam – "unless the employer is the one sending the spam or somehow promoting the sending of that spam", Rothken said.

Create a Policy

Spam can create a hostile work environment for employees and is a headache for IT, according to Brian Tretick, principal with Ernst & Young for privacy assurance and advisory services who advises companies on privacy issues and is a member of the American Institute of Certified Public Accountants Privacy Task Force.

We're concerned that inbound pornographic adult-content e-mail coming in to your workplace may create, unintended by your company, a hostile work environment", as well as clog the e-mail system, Tretick told an audience of security professionals at the RSA Security conference April 14. "So companies will need to create policies and, more than policies, controls on that issue", Tretick said.

Inviting Spam

If employees visit pornographic websites on company computers, those visits can create a trail and invite spam from those sites that will have obtained the corporation's IP address. Firms can use off-the-shelf software to identify where, when, and by whom prohibited materials were accessed. However, pornographic spam often is sent to employees who have never visited pornographic websites.

A properly drafted employer policy can specifically prohibit downloading or circulating offending materials and make voluntary viewing of pornographic websites at work a disciplinary offence, management attorney Schachter said.

In addition, the employer has other options if an employee goes out onto the Internet accessing porn on the company network, Schachter said. "We have actually gone into criminal prosecutions where child pornography is the issue" because such material violated federal and state statutes, he said.

"It's really taking potshots at a much larger problem," Schachter said, adding that ad hoc efforts may be the best course of action until broader regulation and control of spam exists.

Technological Spam Fixes?

According to EFF's Cohn, today's technology to prevent spam is not very effective.

Filtering technologies can block needed messages, she added, and the technologies ultimately rely on a personal definition of what is offensive, which can be imprecise. "One person's porn is another person's art", she said. "The problem is there aren't any parameters you can encode. It's not a binary decision. You can have the best technology in the world, but this won't tell you whether Cindy Cohn will think it's over the line or not."

Rothken argued against the notion of employer liability when workers receive offensive e-mail in the workplace from third parties, even if the employer generally knew of the e-mail.

> "Otherwise, a company would be in a situation where they'd have to filter the e-mails for the most sensitive employee, and that would have to be their policy. And I don't think the law would require such a draconian" action, he said.

Employers are using spam filtering or engaging in monitoring of their networks to address sexual harassment issues in employee-to-employee harassment, according to Chris Hoofnagle, deputy counsel for the Electronic Privacy Information Center, Washington.

Spam filtering, he said, does not have to be invasive. "You can allow the employee to control it", such as using a desktop spam control system, Hoofnagle said.

Employees still have expectations of privacy in the workplace, whether from custom or contract, according to Hoofnagle. "But it's a separate issue whether an employer is allowing a sexual hostile work environment", he said.

GENERAL

In the New Digital World, Old-World Ethics Still Apply

By David Hricik, Mercer University School of Law, Georgia, U.S.; www.Hricik.com

Overview

Although the dawn of the digital age has made practice easier in many ways, it has not lessened the need for lawyers to focus on legal ethics. As always, lawyers must be concerned about confidentiality, conflicts and competency. Though not changing these fundamentals, the vast increase in electronic document storage capacity, the lightning-quick speed of communications and the availability of performance-enhancing technology has affected each of these duties.

Foremost, digitalisation means that breach of a duty of confidentiality can have far greater consequences. More information can now be stored in smaller spaces than ever before. Where once it would have needed a truck to steal an important but voluminous file, today it can be accomplished by the palming of a memory stick, the taking of a CD, or the theft of a laptop computer. While in the years before digital, a lawyer had to be concerned that his brief case and its important folder of papers might be stolen or misplaced, lawyers must now recognise that a file room full of documents is at risk, if a lap top or even a single CD is lost or misappropriated. The issue is the same: the consequences different – and the opportunities for avoiding harm new and uncertain.

The ability for lightning-quick communications means that conflicts of interest can arise more easily and frequently. Just as in the long dark days before Al Gore invented the Internet, lawyers in the new digital world must be concerned about becoming disqualified by a person who in good faith discloses information to the lawyer in seeking to hire him. But unsolicited e-mail creates unique opportunities for such disqualification to occur, and perhaps requires different means to resolve. The analogue solution to this problem may not work in the digital world.

Competency is also affected by technology. Is a lawyer required to acquire expensive new technologies when to do so enhances his ability to provide legal services? If a lawyer is working on a case where the amount of paper involved could be better managed by digital technologies, which he does not have, and using those technologies would be cheaper for his client, must he use them? May he charge his client for their cost?

Courts and bar associations have as yet given little official binding guidance to lawyers on these and other issues. This article describes the impact of technology on certain confidentiality conflicts and competency issues that arise in the digital world.

Authorised Third-Party Access to Digitally Stored Client Confidences

You may allow third parties to have physical or virtual access to your computer systems, including client information stored on those systems. This is usually a necessary and important part of maintaining computer systems.

The problem is that those third parties are strangers to the attorney-client relationship between you and your client, and they (absent some unusual aspect of the law in your jurisdiction) do not owe a duty of confidentiality to your clients. Yet, you are giving them access to your client's information – some of it probably very sensitive. Under U.S. Law, Model Rule 5.3 and its state counterparts require lawyers to ensure that non-lawyer assistants act compatibly with the lawyer's obligations. Among those obligations of course, is a lawyer's obligation to protect client confidences under Model Rule 1.6 and its state counterparts (as well as the law of agency, for that matter).

The American Bar Association and others have stated that it is ethical for lawyers to permit third party vendors to have access to computer systems in order to maintain files and systems, but that confidentiality agreements should be obtained. The American Bar Association's opinion on the subject of third-party access to law firm computer systems advises:

> "A lawyer who gives a computer maintenance company access to information in client files must make reasonable efforts to ensure that the company has in place, or will establish, reasonable procedures to protect the confidentiality of client information. Should a significant breach of confidentiality occur, the lawyer might be obligated to disclose it to the client".[1]

The ABA stated that:

"a lawyer might be well-advised to secure from the service provider in writing ... a written statement of the service provider's assurance of confidentiality".[2]

The non-high tech analogies confirm the wisdom of obtaining a written agreement to respect the confidentiality of the information. For example, the bar opinions appear to uniformly hold that lawyers who store client files outside the firm with offsite storage facilities, must ensure that the storage company has a confidentiality obligation and reasonable security measures. Permitting third parties access is not an ethical violation, according to these opinions, so long as the obligation of confidentiality is maintained.[3]

Those who have given your or your firm's permission to computer consultants and the like should determine whether you need to augment their agreement with you to make their confidentiality obligations compatible with your own – particularly because digitalisation makes it easier for theft to occur, and to occur without warning and with greater consequences. Greater care needs to be given to the duties of non-lawyers who have access to digitised client confidences.

Unauthorised Access to Client Confidences

The Legal and Practical Importance of Passwords

The importance of using password protection cannot be overstated. The courts which have addressed e-mail and website security have both pointed to the presence of password protection as a key fact.[4] The courts view the use of passwords as a sign that the owner of the information intended to keep the information confidential. Passwords should play an important part in computer security, and indeed may have a constitutional import.

Information stored on laptops can be password protected. If a laptop is stolen, the thief may be more interested in the hardware than its contents, and the use of even a simple password protection scheme could dissuade the thief from doing anything but turning around and pawning the system.

Passwords can also be used within a firm's computer system, enabling employees working on a shared office network to password protect individual files and directories. Thus, if someone gains unauthorised access to your firm's network, your files may be inaccessible to the hacker.

Thus, passwords play important parts in protecting information at various levels. Yet, employees often write passwords down, taping the note to their monitors. Or, their logon name is their last name, and their password their first. Worse, some computers or software are left with its vendor-supplied defaults as the password. These are invitations to disaster.

Those with a computer containing confidential information should be aware of the importance the law gives to passwords – and the importance that they have as a practical matter. In a perfect world, passwords should be at least seven letters long or longer; should not be names; should contain letters *and* numbers or characters (@, *, and so on); and should never be written down near the computer.

Stolen Laptops and Personal Information Devices

Laptop theft is not rare and today's machines are capable of storing what just a few years ago, was unimaginable amounts of client data. As a result, a written policy regarding laptop usage – including the need to password protect files and limiting or prohibiting storage of critical client information such as critically important trade secrets or other valuable proprietary information – may be in order in large firms. Client consent, or at least disclosure of the practice of storing information on laptops may be wise.

There are also services that are designed to locate stolen laptops. For example, Absolute Software sells a program called CompuTrace. It installs a tracking agent that automatically, regularly, and silently calls into the CompuTrace website and reports its serial number and the phone number it is calling from (or, presumably, its IP address). Apparently, CompuTrace can even activate an "erase" feature on the computer and surreptitiously erase its data. Other similar programs are offered by pcphonehome.com and, no doubt, several other enterprises. Macphonehome is available for Apple users.

Other services are designed to recover lost, not stolen, items. For example, some companies sell tags that can be put onto laptops or other personal information devices. If it is lost, and someone reads the tag (and notes that it promises a reward) and calls the 800 number, then the company arranges for FedEx to pick it up and send it to the owner. Putting a sticker on your laptop with your phone number and an offer of a reward may do the same thing, and at no cost.

Conflicts in the Digital World

Suppose you or your firm is representing A, who is about to sue B. B knows he may be sued by A, but does not know your firm represents A. B goes to your firm's website, clicks the link that says "e-mail me if you have a problem" and discloses confidential information that is pertinent to the A versus B dispute. Are you or your firm disqualified?

In the analogue world, the answer is probably yes. Where a party in good faith discloses information to a lawyer in order to hire the lawyer, the lawyer (and perhaps his firm) are disqualified from being adverse to the party in a matter where that information could be used against the person. Entire firms have been disqualified from being adverse to a party who in good faith disclosed information while trying to hire a firm.

Having an e-mail is an invitation to transmission of such disqualifying information. A firm, which does not consider the impact of e-mail on this conflict of interest issue, may find itself more readily disqualified. As yet, only one bar opinion has addressed this issue, and its members split on whether e-mail is the same as analogue information.[5] It is difficult to see the difference in today's world between sending a fax, mailing an envelope or sending an e-mail. No doubt, courts and bar associations will agree.

It is important therefore, to try and resolve this conflict issue. In designing a website, consider several options. Some firms use disclaimers on the site. These purport to avoid creating an attorney-client relationship with a person, and advise the person not to send confidential information. These vary from a buried link to Vinson & Elkins' approach. If you go to its site,

www.velaw.com and click on a lawyer's e-mail address link, you are taken first to this page:

> "*Please Read Before Sending E-Mail* – There can be no guarantee that Internet mail is fully secure or private. Please do not transmit confidential information. Transmission of information is not intended to and does not create an attorney-client relationship. Therefore, please do not assume that your communications sent using electronic mail are privileged or confidential. Please do not send Vinson & Elkins any confidential information via the Internet without previously consulting with one of our attorneys".
>
> If you wish to discuss legal representation, you may request a consultation by e-mail or call one of our offices".

At the bottom of the page is the link where you can click to actually send the e-mail.

It remains to be seen whether these disclaimers are enforceable, but V&E's approach appears to be the strongest, since the disclaimer is not merely buried on a link on a page, but must be read before e-mail can be sent to the firm.

Word your legend carefully, however. Some firms state that nothing sent to them will be held in confidence unless the sender is already a client. That sort of language may prevent clients from claiming privilege over information sent to firms prior to formation of the attorney-client relationship.

Competency

No court or bar association has, as yet, opined on whether a lawyer can breach a duty of competency by failing to acquire new technology. If a reasonable lawyer would use scanned, word-searchable documents in a case, for example, is it incompetent for a lawyer to proceed without the technology? If it is less expensive to use that technology than billing hourly, may the lawyer charge the client for the cost of acquiring the equipment to do so?

There is little guidance on these issues. ABA Model Rule 1.6 touches upon the issue in a comment, noting that

> "major litigation and complex transactions ordinarily require more elaborate treatment than matters of lesser importance".

Lawyers should, as a result, consult with clients regarding the options, and obtain the client's informed consent if the lawyer believes that he does not have access to technology that a reasonable lawyer would use under the facts and circumstances of the case. A lawyer who has advised the client of the potential costs of using each approach, and potential benefits, will likely avoid violating the duty of competency, particularly where there is little to guide lawyers in the digital age.

Conclusion

The ways in which confidentiality can be breached, conflicts created, or incompetency manifested have changed. More than anything, the fact that these issues will arise in new contexts means that courts and bar associations will lag behind; digital pioneers tread where no lawyers have gone before, and in places which have not been examined by the authorities. This has a dual impact.

First, lawyers may not spot the issues. A lawyer who uses an application service provider, for example, may not consider the confidentiality issues that arise where information is stored with a third party. Lawyers using cutting edge technologies must consider the context carefully.

Secondly, there may be little to guide these electronic pioneers. Bar associations, whose opinions are often merely advisory, have issued only a few opinions dealing with digital ethical issues, and the analogies to pre-existing fact patterns may not always hold true. Further, bar associations may not fully understand the technical issues involved, and may issue opinions that condone risky behaviour, or prohibit behaviour the propriety of which outside the digital context is commonplace and unquestioned. Finally, courts and juries have only just begun to address malpractice and discipline in the digital age.

There will, no doubt, be many unhappy pioneers who discover potholes and detours along the information superhighway. With luck, this article has alerted you to at least a few of them, and provided some practical guidance to your practice.

1 ABA Comm. on Ethics and Prof. Responsibility, Formal Op. 95-398 (1995), p. 1.

2 ABA Comm. on Ethics and Prof. Responsibility, Formal Op. 95-398 (1995), p. 2.

3 *See* N.C. Eth. Op. 209 (Jan.12, 1996) ("[A] lawyer should store a client's file in a secure location where client confidentiality can be maintained."); N.Y. Eth. Op. 643 (Feb. 16, 1993) ("We also see no ethical impropriety in storing closed files . . . so long as client confidences . . . are protected from unauthorized disclosure. The files should be stored in a secure location and should be available only to the client, the client's present or former lawyer, or another with the client's informed consent.") (citation omitted); Mich. Eth. OP. RI-100 (Sept. 30, 1991) (lawyer may "[s]tore client representation files and other law firm files which are not to be destroyed in a facility which protects client confidences and secrets, safekeeps property, and complies with record-keeping requirements").

4 See *United States v. Maxwell,* 43 Fed. R. Evid. Serv. (Callaghan) 24 (U.S.A.F. Ct. Crim. App. 1995) (e-mail stored on AOL was covered by Fourth Amendment from unreasonable search and seizure where it was protected by log-on name and password).

5 Ariz. Op. 02-04 (Dec. 2002).