E

WIPO/IP/CAI/1/03/9.A
ORIGINAL: English
DATE: February 2003

CAIRO UNIVERSITY

WORLD INTELLECTUAL
PROPERTY ORGANIZATION

WIPO NATIONAL SEMINAR ON INTELLECTUAL PROPERTY

organized by
the World Intellectual Property Organization (WIPO)

in cooperation with
the Cairo University, Arab Republic of Egypt

Cairo, February 17 to 19, 2003

INTELLECTUAL PROPERTY ON THE INTERNET

Lecture prepared by Professor Michael Blakeney, Director, Queen Mary Intellectual Property Research Institute, Center for Commercial Law Studies, University of London

1. THE INTERNET – LEGAL ISSUES

The Internet is a world wide link of computers and computer networks which use a common protocol for communicating with one another. The physical connection between computers on the Internet is typically effected through leased space on existing telephone networks. The information content on the Internet is held in computers, known as “servers” which are owned and operated by information providers, which may be universities, government instrumentalities, or commercial enterprises. Computers which make up the Internet may be “host” or “client’ computers. Host computers are connected to neighbouring Internet computers by a dedicated line through which messages are routed according to the Internet communication protocol. Client computers interface with host computers and provide the user with access to request and receive information from the Internet. Host computers are typically provided by commercial “Internet Service Providers (ISPs)”. Client computers may be directly connected to host computers through a local area network or may be connected to a host computer by a modem via the telephone network.

The establishment of the Internet has created significant commercial opportunities, with eCommerce developing at an exponential rate. These commercial applications of the Internet have been accompanied by a new catalogue of intellectual property problems. These can be analysed by looking at the typical commercial transaction. The first stage of a transaction is attracting consumer interest through on-line advertising. The process of domain name selection by traders has created problems in the trademarks area. The advertising of products has created problems in the copyright area. The content of products delivered by traders, particularly those comprising, text, music, film and data have also created copyright and related problems. Systems for the management of electronic commerce have generated new categories of digital intellectual property rights. The enforcement of commercial obligations generated by electronic commerce has presented obvious jurisdictional problems, where parties are in different countries, with different bodies of contract law and additionally, the Internet has created new categories of legal actor. In addition to the vendor and purchaser, there is also the question of the liability of the Internet service provider and the telecommunications carrier.

This paper will examine some of these issues, by focussing first on the question of domain names and then by surveying some of the digital technology laws.

2. EVOLUTION OF THE DOMAIN NAMES SYSTEM

The Internet grew out of research in the USA by the Department of Defense's Advanced Research Projects Agency (DARPA). The task of maintaining the list of names and addresses of host computers on the system was delegated to UCLA, where this work was undertaken by Dr John Postel. The list of addresses was made available to the network community through a sub-contractor, SRI International. Dr Postel continued to maintain the list after he had moved to the Information Sciences Institute at the university of Southern California. Dr Postel also published a list of technical parameters that had been assigned for use by developers of Internet communication protocols. These functions became collectively known as the Internet Assigned Numbers Authority (IANA).

Each host computer on the Internet has a unique IP number, IANA, directed, until his death in October 1998, by Dr Postel[i] allocates blocks of numerical addresses to regional IP registries (ARIN in North America, RIPE in Europe and APNIC in the Asia Pacific Region). Each Internet computer is allocated a Uniform Resource Locator (URL) address which comprises four groups of numbers. To simplify this system in 1984 the Domain Name Space (DNS) system was developed. This system converts the numeric URL address into the hierarchical format of letters. There are two types of Top Level Domains (TLD's), generic TLDs ("gTLDs") and country code TLDs ("ccTLDs").

The gTLDs are divided into the original set of gTLDs approved in the late 1990s (the "old gTLDs") and the new set of gTLDs approved in 2001 to meet the growing demand for domain names.

> The old gTLDs are: .com, .net, .org, .int, .mil, .gov, and .edu. The first three of these are open to all registrants, and the other are restricted.

The new gTLDs are: .aero (for aviation industry), .biz (for businesses), .name (for personal names), .coop (for cooperative organizations), .info (general), .pro, (for professionals), and .museum (for museums).

In addition to the gTLDs, there are country specific TLDs or country code TLDs ("ccTLDs"). Each country was assigned a code that corresponds to the Standard 3166 of the International Organization for Standardization (ISO 3166). There are more than 240 ccTLDs. Domain names in the ccTLDs are administered by private and governmental registries.

Examples of ccTLDs are: .au (Australia) .ca (Canada), .ch (Switzerland), .fr France), .tv (Tuvalu Islands).

To the left of the TLD is the second level domain. This is generally the identifier with the greatest value as an identifier or branding tool. In www.wipo.int, wipo is the second level domain.

Domain names have become an important feature of business branding strategy. At the same time, domain names have raised three significant legal issues. The first of these is how domain names will be used and owned, and what rights trademark owners have to block the use of trademarks as domain names. The second is what law will be applied to determine rights to domain names since the law of trademark is primarily defined by national laws. Finally, issues arise as to how rules relating to selection and use of domain names--whatever their source—will be enforced since the reach of the Internet is international rather than national and jurisdiction; enforcement cannot be dealt with as they would be in a trademark case.[1]

---

[1] For an discussion of the Internet and the changes it has wrought on IP, see "The Management of Internet Names and Addresses: Intellectual Property Issues, Report of the WIPO Internet Domain Name Process", http://wipo2.wipo.int, April 30, 1999 (hereinafter the "First Process Report").

3. ADMINISTRATION OF THE DOMAIN NAME SYSTEM

The allocation of domain names was originally undertaken in the USA, by the Internet Assigned Numbers Authority (IANA).[3] In 1991 the task of coordinating and funding the management of non-military aspects of the Internet was taken on by the National Science Foundation (NSF), a US statutory authority with responsibility for supporting scientific research in the USA, including the maintenance of computer networks to connect research and educational institutions. In 1992 NSF solicited competitive proposals to provide a variety of Internet infrastructure services, including the registration of domain names. On 31 December 1992, NSF entered into a competitive agreement with a Virginia-based, private corporation, Network Solutions, Inc (NSI), to supply some domain names registration services. NSI registered domain names in the generic top level domains, namely <.com>, <.org> and <.net>, on a first come, first served basis. This agreement expired on 30 September 1998. The IANA also allocated the right to administer country code TLDs to local Network Information Centres (NICs) or to local corporations. For example the <.co.uk>, <.ltd.uk>, <.plc.uk>, <.net.uk> and <.org.uk> domain names are administered by Nominet UK Limited (Nominet).

The US Department of Commerce established the National Telecommunications and Information Administration (NTIA) to oversee the US government's Internet policies. On 30 January 1998, the NTIA released a Green Paper: *A Proposal to Improve the Technical Management of Internet Names and Addresses*[4]. The green paper outlined the process by which the US Government will transfer management of the Domain Name System from the IANA to a private non-profit US based corporation: the Internet Corporation for Assigned Names and Numbers (ICANN). This corporation would: 1) set policy for and direct the allocation of IP number blocks; 2) oversee the operation of the Internet root server system; 3) oversee policy for determining the circumstances under which new top level domains would be added to the root system; and 4) coordinate the development of technical protocol parameters.

After receiving public comment, on 5 June 1998, the NTIA released its White Paper: *Management of Internet Names and Addresses*,[5] which suggested that the new corporation to take over from the IANA should require applicants for domain names to:

(i) pay registration fees at the time of registration or renewal and agree to submit infringing domain names to the authority of a court of law in the jurisdiction in which the registry, registry database, registrar, or the "A" root servers are located.

(ii) agree at the time of registration or renewal, that in cases involving cyberpiracy or cybersquatting (as opposed to conflicts between legitimate competing rights holders), they would submit to and be bound by alternative dispute resolution systems identified by the new corporation for the purpose of resolving those conflicts; and

(iii) abide by decisions taken by the new corporation to exclude famous trade marks from being used as domain names (in one or more TLDs) except by the designated trademark holder.[6]

After some further consideration, on 20 October 1998, the Commerce Department has referred the corporate proposal back to the NTIA to consider a broadening of the membership of the ICANN and to create workable mechanisms to hold the new board accountable.[7] In its White Paper, the US Department of Commerce indicated that it would seek international support to call upon WIPO to initiate a "balanced and transparent process" to: 1) develop

recommendations for a uniform approach to resolving trade mark/domain name disputes involving cyberpiracy; 2) recommend a process for protecting famous trade marks in the generic top level domains; and 3) evaluate the effects, based on independent studies, of adding new gTLDs and dispute resolution procedures on trade mark and intellectual property holders. These proposals were placed before the first meeting of a new WIPO standing committee on trademarks, industrial designs on 13-17 July 1998.

In its reply of March 20, 1998 to the US White Paper, the EU sought to emphasise its concern that the future management of the Internet should reflect an international approach. It expressed its concern that the White Paper proposals "Contrary to such an international approach, the current US proposals would, in the name of the globalization and privatization of the Internet, risk consolidating permanent US jurisdiction over the Internet as a whole, including dispute resolution and trademarks used on the Internet." The EU proposed :

- balanced and equitable international private sector participation in Internet governance reflecting an equitable balance of interests and contributions; including adequate procedures for the representation and protection of consumer and user interests;
- ensuring an appropriate level of representation and participation for the responsible international organizations in the area of Internet governance in the context of a more general approach to the international consensus regarding the information and communication industries worldwide;
- implementation of the existing guidelines regarding the Domain Name System (DNS) adopted by the Bonn Conference (2), including the introduction of competition in the allocation of existing generic Top Level Domains and conformance with agreed intellectual property and dispute resolution procedures;
- application of the appropriate competition rules to ensure in particular that the transition to the new structures does not create or strengthen dominant positions of companies and organizations charged with the governance of the Internet nor that any agreements or practices amongst those companies and organizations prevent, restrict or distort competition;
- ensuring transparency and certainty of the DNS with a view of the orderly administration of taxation and the need to combat fraud;
- fair and transparent financing of Internet organizations including equitable allocation and utilization of the existing Internet Infrastructure Development Fund;
- in thecontext of the re -allocation of the DNS Root Servers, to attend to their management and operation and particularly how to improve operational security of the system in the event of partial failure, including which data should be distributed and replicated globally to this effect;
- periodic review and updating of the arrangements which are put in place.

The conclusion reached in the EU response to the White Paper was " to reach a balance of interests and responsibilities, so that the international character of the Internet is recognized" and recommended that "the US Administration limit its direct regulatory intervention in the Internet only to those relationships which fall clearly under existing contracts between the Agencies of the US Government and their contractors and that all other decisions be referred

to an appropriate internationally constituted and representative body."

ICANN's mandate included the creation of a system of registrars who would receive and process applications for domain names. WIPO was asked to study the issue of trademark protection and domain names and make recommendations for a uniform approach to resolving trademark/domain name disputes. In response to this request, and the request of its Member States, in 1998-1999 WIPO undertook a study of trademark issues, domain names and possible methods for resolving disputes related arising in the confluence of these two areas. WIPO's report was published on April 30, 1999.[2] The chief recommendations were certain "best practices" for registration authorities:

> Requiring that applicants for domain names provide contact information so as to avoid the problem of anonymous infringement of rights;
> Providing for exclusion from registration of famous and well-known marks;
> Requiring that applicants for a domain names agree to submit domain name disputes to jurisdiction and alternative dispute resolution procedures;
> Requiring acceptance of a Uniform Dispute Resolution Policy (the "UDRP") governing the procedures for resolving disputes over domain names.

The recommendations were for the gTLDs and did not apply to the ccTLDs.

4. DOMAIN NAME ALLOCATION

(a) Priority

The allocation of domain names on a 'first come, first served' basis has caused some trade mark proprietors to be excluded from the use of their trade marks as their domain names. For example, the word DELTA is registered as a trade mark in the United States in respect of both Delta Air Lines and deltaComm, an Internet Service Provider. However, the domain name <delta.com> is owned by the ISP, despite the fact that Delta Air Lines is the larger and better known company.J [reverse hi-jacking]

(b) Registration Categories

The priority which first applicants for domain names obtain, is exacerbated by the fewness of gTLDs, compared with the 42 classes of goods and services available for applicants for trade marks. A particular problem is the fact that there is only one gTLD available to companies, namely <.com>. In *Prince Plc v Prince Sports Group Inc*,Z Prince Plc, a UK computer company, registered the domain names <prince.com> and <prince.co.uk>. The Prince Sports Group Inc, a US maker of tennis products and the company with which the public would more commonly associate the word 'Prince', was unable to register the domain name. The Prince Sports Group demanded that the domain name should be handed over to it, as it asserted that Prince Plc's use of the domain name infringed the Group's trade marks. Prince Plc commenced proceedings against Prince Sports Group in the UK for unjustified threats to bring trade mark proceedings and sought, inter alia, a declaration that its use of the domain name in relation to information technology did not infringe the Group's trade marks for sporting goods. At the time of sending its letter, Prince Sports had not obtained any UK trade marks upon which to base a claim of infringement. Accordingly, Neuberger J held that the US company

---

[2] The First Process Report, note 2.

had made ‘unjustifiable threats’ in breach of the *Trade Marks Act* 1994 (UK).[ط]

Unlike trade mark registrations which have to satisfy the various criteria of registrability, such as distinctiveness, intention to use, domain names have not needed to satisfy equivalent tests. A fundamental principle of trade mark law is that registration ought not be granted for marks which might legitimately be used by persons acting in good faith in a particular trade. This principle, is applied in the general requirement that a mark be distinctive and non confusing and also in the refusal to protect marks which refer to the character or quality of products, or to geographic locations, or surnames. Similarly, trade mark protection is withheld from marks which have become generic. These principles are not applied in domain name registration, but in a recent case, the owner of the trade mark ‘CDS’ was held to be unable to assert its trade mark rights against the owner of the domain name <cds.com> because the term ‘cds’ was the generic term used by the public for ‘compact discs’.[ي] In other words, it may be possible that some trade mark principles may creep into domain name registration practice, through judicial intervention.

(c) Cybersquatting

A number of domain name disputes have arisen in the context of what has been called “Cybersquatting”, where individuals obtain domain name registrations which are likely to be sought by well known enterprises, with a view to selling them to those enterprises.[ك] For example, in *Harrods Limited v Network Services Limited*,[ل] the well known department store had been approached for payment to relinquish the <harrods.com.> domain name by its unauthorised registrant. Harrods commenced proceedings for infringement, passing off and conspiracy, applying for summary judgement when no defence was filed. The defendants were not represented at the hearing. The trial judge accepted that passing off and trade marks principles were applicable to domain names and ordered the defendants to relinquish the domain name and to desist from passing off.

The leading UK case on the subject of cybersquatting as trade mark infringement and on the related subject of the status of well known marks in the Internet domain names regime is the Court of Appeal decision in *Marks & Spencer and Others v One in a Million.*[م] The appellants had registered a number of domain names which incorporated the famous trade marks of the respective plaintiffs: Marks & Spencer Plc, Sainsbury Plc, Virgin Enterprises Ltd, British Telecommunications Plc, Telecom Securicor Cellular Radio Ltd and Ladbrokes Plc, with a view to selling those domain names to the respondents. The trial Judge, Mr Jonathan Sumption QC, sitting as Deputy Judge of the UK High Court, held that the mere registration of another's name as a domain name was not in itself actionable as passing off, stating that "The mere creation of an 'instrument of deception' without either using it for deception or putting it into the hands of someone else to do so, is not passing off. There is no such tort as going equipped for passing off. It follows that the mere registration of a deceptive company name or a deceptive Internet domain name is not passing off."[ن] However, his Honour ruled that the practice of the appellants in registering well known marks as domain names for the purpose of blocking their use by the proprietors of those marks, except upon the payment of money, was an infringing use of a trade mark in the course of trade within the meaning of s.10(3) of the *Trade Marks Act* 1994 (UK).[س]

The judgement of Lord Justice Aldous, with whom Lord Justices Stuart-Smith and Swinton Thomas agreed, considered in some detail the application of passing off principles to the

practice of cybersquatting. The conclusion which Lord Justice Aldous reached from an examination of the cases was that there could be discerned

> …a jurisdiction to grant injunctive relief where a defendant is equipped with or is intending to equip another with an instrument of fraud. Whether any name is an instrument of fraud will depend upon all the circumstances. A name which will, by reason of its similarity to the name of another, inherently lead to passing off is such an instrument…The court should consider the similarity of the names, the intention of the defendant, the type of the trade and all the surrounding circumstances.[ع]

Also, where a defendant has an intention to appropriate the goodwill of another, Aldous LJ could see no reason why the court should not infer that it will happen, even if there was a possibility that such an appropriation would not take place.

The basic facts of the case were not in dispute. The Court of Appeal accepted that the business of the appellants was dealing in Internet domain names. The appellants obtained the registration of prestigious names as domain names without the consent of the owners of the goodwill in those names with a view to selling those names to the owners of the goodwill. For example, the respondents offered to sell the domain name <bt.org> to British Telecommunications Plc for £4,700 plus VAT and the domain name <burgerking.co.uk> to Burger king for £25,000 plus VAT. Thus the Court of Appeal found that the purpose of the appellants' blocking registrations of these domain names was for the purpose of extracting money from the owners of the goodwill in those names. "Its ability to do so was in the main dependent upon the threat, expressed or implied, that the appellants would exploit the goodwill by either trading under the name or equipping another with the name so he could do so."[ف]

The Court of Appeal rejected the appellants' submission that mere registration did not amount to passing off. It ruled that the "placing of the register of a distinctive name…makes a representation to persons who consult the register that that the registrant is connected or associated with the name registered and thus the owner of the goodwill in the name".[ص] In the case of the appellants' domain names incorporating the name Marks & Spencer, the Court found that registration of the domain name would cause damage by eroding Marks & Spencer's exclusive goodwill in its name and that the domain names were instruments of fraud. Thus the trial judge was justified in granting injunctive relief to prevent them from being used for a fraudulent purpose and to prevent them from being transferred to others.

The appellants sought exoneration for their domain names which were not inherently distinctive, for example those which were surnames, such as "Sainsbury" and "Ladbroke", or which might be the initials of persons, such as "BT", or which were the names of a range of companies such as "Virgin". However, Aldous LJ was not prepared to accept this distinction as they "were well-known 'household names' denoting in ordinary usage the respective respondent".[ق] Concluding that

> The appellant registered them without any distinguishing word because of the goodwill in those names. It was the value of that goodwill, not the fact that they could perhaps be used in some way by a third party without deception which caused them to register the names. The motive of the appellants was to use that goodwill and threaten to sell it to another who might use it for passing off to obtain money from the respondents. The value of the names lay in the threat that they would be used in a

> fraudulent way. The registrations were made with the purpose of appropriating the respondents' property, their goodwill, and with an intention of threatening dishonest use of them by another. The registrations were instruments of fraud and injunctive relief was appropriate just as much as it was in those cases where persons registered company names for a similar purpose.[ر]

In light of their success on the passing off claim, the respondents did not press their trade mark infringement action. Counsel for the appellants had submitted that for there to be a trade mark infringement under s.10(3) of the Trade Marks Act, 1994, there had to be use of the trade mark: (a) as a trade mark; (b) for the purpose of denoting origin of goods; and (c) which was confusing. Aldous LJ indicated that he was not sure that s.10(3) required the use to be a trade mark use and that it had to be confusing. On the supposition that this was correct, he held these matters to be satisfied as the appellants had sought to sell domain names which were confusingly similar to registered trade marks; the purpose for which the domain names had been registered was to indicate origin and they were to be used in relation to the services provided by the registrant who traded in domain names.[ش]

Finally, counsel for the appellants submitted that it had not been established that the contemplated use would take unfair advantage of, or was detrimental to the distinctive character or reputation of the respondents' trade marks. This was rejected by the Court which observed that "the domain names were registered to take advantage of the distinctive character and reputation of the marks. That is unfair and detrimental".[ت]

In the USA, the practice of cybersquatting has been dealt with under the various state and Federal anti-dilution statutes. However, the state of the US law on this practice appears to resemble that in the UK prior to the Court of Appeal's decision in the *One in a Million Case,* in requiring something more than mere registration of another's trade mark as a domain name before finding trade mark infringement. A recent example of this position is *Panavision International LP v Toeppen*[ث] . Panavision was the owner of the trade marks *Panavision* and *Panaflex* in the USA in respect of movie camera equipment. In December 1995 it had attempted to establish a web site on the Internet with the domain name <Panavision>. It transpired that this domain name had already been registered by Mr Dennis Toeppen. In reply to a letter which he received from Panavision, informing him of the latter's trade mark rights, Mr Toeppen offered to exchange the domain name for a payment of $13,000. Mr Toeppen also offered on receipt of this payment not to register any other Internet address alleged by Panavision to be its property. Panavision refused this demand, whereupon Mr Toeppen registered the 'Panaflex' mark as a domain name. The Californian District Court ruled that Mr Toeppen's actions violated the Federal Trademark Dilution Act of 1995 and the Californian Anti-dilution statute.[خ] As he was located in Illinois, Toeppen objected to the Californian District Court exercising jurisdiction and submitted that as the registration of domain names was not a commercial use, the court had erred in finding trade mark dilution. On the issue of jurisdiction, the Ninth Circuit ruled that the District court had properly exercised its jurisdiction as Toeppen knew that his conduct would have the effect of injuring Panavision in California, which was its principal place of business and the centre of the movie industry. The court found that the attempt to sell the domain names was the requisite commercial activity which constituted dilution. Toeppen's conduct was considered to satisfy the requirement of detriment to the trade mark proprietor by diminishing "the capacity of the Panavision marks to identify and distinguish Panavision's goods and services on the Internet".[ذ]

Where a domain name which is the trade mark of another company is used in relation to similar goods in respect of which the trade mark is registered, then trading using the registered mark will be an infringement. Problems arise where the domain name is used in relation to unlike goods or services. For example, in *Interstellar Starship Services Limited v Tchou,*[ض] the defendant owned the domain name <epix.com> and used it to publicise the activities of a cabaret theatre group. This was held not to infringe the trade mark 'ERIX', owned by the plaintiff manufacturer of video imaging hardware and software, because the domain name was being used in connection with services sufficiently different from those of the plaintiff and there was no likelihood of consumer confusion.

In the US this problem can be accommodated under the anti-dilution laws thus, the US Internet Service Provider 'America Online', which owned the domain name <aol.com>, obtained a cease and desist order against a German group which was operating an on-line casino at <aol-casino.com>.[غ]

(d) Well Known Marks

A number of disputes have arisen where companies with similar names, or manufacturing the same sorts of products have sought to adopt the same or similar domain names on the Internet. With the introduction in most countries of the protection of well-known marks, as an obligation enjoined by TRIPS,[ظ] reputed traders have successfully prevented the use of domain names by unauthorised third parties which are identical or substantially similar to well known marks.[أأ] A particular problem for trade marks protection is that trade marks registration can be obtained in respect of each of 42 classes of goods and services, whereas only a single domain name is available for commercial enterprises.

An example of cybersquatting, involving well-known marks is a Greek case which involved the domain names "Amazon.gr" and "Amazon.com.gr," where the Greek Provincial Hearing of Syros found that the small Greek firm holding these domain names intentionally misled consumers into believing that they were operated by Amazon.com.

The *One in a Million Case* is an illustration of the protection of domain names as well known marks. In the USA the Federal Trademark Dilution Act which came into force on 16 January 1996 provides protection for "famous" trade marks both registered and unregistered. During the debates on the law it was suggested that this legislation would assist trade mark owners to deal with unauthorised third party domain names.

(e) Confusing Use

There is an extensive corpus of US case law concerning trade mark infringement through domain name use. In the main these decisions follow the course of typical trade mark infringement cases. Confusing use is more likely to be found in those situations where the plaintiff and defendants are engaged in similar activities, whereas the courts have not as easily been prepared to find confusion where those activities are dissimilar. Thus, the vendor of computer software to law firms under the trade mark "JURIS", successfully enjoined the use of the domain name <juris.com> by a subsequent vendor of computer software and related services to legal, insurance and forensic businesses.[بب] Similarly, the proprietor and first user of the service mark "CARDSERVICE" which provided credit and debit card processing services was able to prevent the use of the domain name <cardservice.com> by a defendant

seeking to carry on the same business.[ככ] The court noted in this case that the effect of the domain name registration by the defendant barred access of the plaintiff to the Internet under this domain name with the result that consumers would be diverted from the plaintiff to the defendant.

As in trade mark law, the greater the repute of the plaintiff's marks, the more likely will confusing use be found in dissimilar areas of enterprise. Thus in *Planned Parent Federation of America, Inc v Bucci*[כד] the repute of the plaintiff's "PLANNED PARENTHOOD" trade mark under which it offered reproductive health care and birth control services, was the basis of the court's enjoining the use of the defendant's domain name <plannedparenthood.com> under which he promoted anti-abortion advocacy.

A more robust approach to the application of trade marks principles to the acquisition of domain names in the UK is suggested in *Avnet Inc v Isoact Ltd.*[כה] The plaintiff was a distributor of electronic components and computer software. It maintained a web site and published trade catalogues. It conducted its business by reference to its “Avnet” trade mark and had obtained a registration for this mark in the UK in class 35. This class covers “advertising and promotional services”. The defendant conducted an entirely different business as “Aviators Network”, an ISP with a particular focus on aviation matters. The defendants used the domain name “avnet.co.uk”. The plaintiffs, alleging an infringement of its class 35 trade mark, sought an order that the defendant assign to it the defendant’s domain name. The trial judge refused to make the order sought by the plaintiff as he did not consider the defendant to be engaged in any activity which infringed the plaintiff’s trade mark. He ruled that although persons might use the defendant’s web site for advertising purposes, this was not the essence of what the defendant did, but was incidental to its provision of a forum for the discussion of aviation matters.

The trial judge had expressed doubts as to whether any Internet users on accessing the defendants aviation web site, would have been confused into thinking that there was some association with an electronics components distributor.[כו] Contrasting domain names with trade marks, he noted that the former operated on words alone and not words connected with goods and services. Consequently, users of the Internet know that when a word is searched “even if a searcher is looking for the word in one context, he will, or may find web pages or data in a wholly different context”.[כז] Had the plaintiff succeeded in its application, a consequence would have been to use a UK-based proprietary right as a means of obtaining a domain name, conferring global exclusivity.

(e) Meta-tagging

Meta-tags are a component of HyperText Markup Language (HTML), which is the programming language of the World Wide Web. Meta-tags are used to provide keyword information to describe the contents of Web pages. A search engine, such as AltaVista, Yahoo or Lycos typically scans the keywords in a Web site's meta-tag to rate that site's relevancy to a search. These meta-tags are not visible to viewers of a Web site as they are embedded in the Web-site code. It is possible to manipulate the frequency with which a Web-site scores hits in a search engine's inquiry.

In *Playboy Enterprises v Calvin Designer Label*[כח], a US case, the plaintiff owned the registered trade marks *Playboy* and *Playmate.* The defendant used these marks as part of the domain names <playboyxxx.com> and ,playmatelive.com> which it embedded in the meta-

tags of its Web site. The court enjoined the defendant from using these trade marks "in buried codes or metatags on their home page". And from "disseminating, using, or distributing any Web site pages, advertising, or Internet code words or titles" whose appearance resembling those of the plaintiff so as to create a likelihood of confusion, mistake or deception.

The same trade marks embedded as meta-tags were the subject of litigation in *Playboy Enterprises Inc v AsiaFocus International Inc*[طط] and *Playboy Enterprises Inc v Welles.*[ي] In the former case the defendant used the plaintiffs trade marks as meta-tags in its Web sites which featured pictures of nude women. Additionally, the defendant incoporated these marks in its domain names <asian-playmates.com> and playmates-asian.com>.This Web site was offered as a facility for advertisers promoting the sale of playing cards, calendars and similar merchandise. The court took into account the willfulness of the defendant's conduct in awarding the plaintiff $3 million plus costs. The plaintiff failed in the latter case, which concerned the use of the plaintiff's trade marks in the meta-tags of a Web site established by Ms Terri Welles, 1981 "Playmate of the Year". The court found this use to be properly descriptive or an editorial use of the trade marks.

In *Oppendahl & Larson v. Advanced Concepts*[كك] a Colorado law firm which had established a Web site noted for its information on cyberlaw matters, objected to the use of its meta-tags by a web page design company. The plaintiff law firm obtained orders enjoining the defendant from using its common law trade marks as meta-tags in Web pages constructed by the defendant.

(f) Word Stuffing, Blacking and Cloaking

These practices involve the embedding of another's trade mark(s) in a Web site so that they are not visible to a reader, but can be acquired by a search engine. Thus, for example, a retailer of medium level fashion brands can embed multiple examples of well-known, high fashion brands in a web site in the same colour as the background of the retailer's Web site (eg white on white, or black on black). Similarly, a direct trade rival of the owner of a well-known brand can use the same technique to embed the well-known mark in the trade rival's Web site.
An interesting issue is whether this practice can be described as trade mark infringement, given that the embedded mark is not visible. This issue was canvassed in part in the US case, *Playboy Enterprises, Inc v Calvin Designer Label*[لل] . That case also involved meta-tagging and the incorporation of the plaintiff's trade marks in its visible domain names. The court had little difficulty in finding trade mark infringement, dilution and unfair competition.

(g) Spamming

"Spam" is unsolicited junk e-mail which is sent in multiple postings to Internet users as a form of direct mail, promoting sales of goods and services. Trade mark concerns are raised when spam mail is sent under return addresses comprising the domain names and trade marks of innocent third party traders. In *Hotmail Corp v Van$ Money Pie Inc*[مم] the defendants sent spam e-mail messages advertising pornographic material, utilising the plaintiff's domain name <hotmail.com> as a return address. The plaintiff was a provider of e-mail addresses under an agreement which forbade the sending of spam mail. The court enjoined the defendant from the use of the plaintiff's trade mark and domain name.

5. LIABILITY OF DOMAIN NAME ALLOCATION AUTHORITIES

In addition to trade mark infringement actions against registrants of domain names, litigants, particularly in the USA, have sought to join the domain name allocation authorities as being a contributory infringer. Where NSI has attempted to place a disputed domain name on hold, until the dispute can be resolved by court action, it has been sued for breach of contract. Finally, where the allocation authority has refused to grant a disputed domain name, it has run the risk of liability under antitrust law for preventing market entry, or under the Lanham Act for unfair competition.[ننن]

In an endeavour to deal with some of these problems, NSI promulgated a *Domain Dispute Resolution Policy Statement* on 28 July 1995, which has been modified on a number of occasions, most recently on 25 February 1998. Under this policy NSI requires undertakings from each domain name applicant that its use or registration of the domain name does not infringe any intellectual property right of a third party and that NSI will be indemnified for any claims of trade mark infringement arising out of the applicant's use or registration of the domain name. The NSI dispute resolution policy had been criticised both by representatives of trade mark owners[سسس] and domain name registrants[ففف]. On the trade mark owners' side, concern was expressed that domain name registration proceeds without a trade mark search and that the NSI requires a protested domain name to be identical to a registered trade mark before it is put on hold. Domain name registrants complain that domain names are put on hold by NSI merely upon the receipt of a complaint and regardless of whether the registrant has superior trade mark rights. Dissatisfaction with NSI's dispute resolution policy precipitated the current movement for reform of the administration of the Internet, described above.

6. DISPUTE RESOLUTION

(i) Administration

Domain names are perceived as a right granted to the domain registrant under contract between the registrant and the relevant domain name registration authority. The registrant of a domain name is merely given a contractual right to use the domain name. Thus, the registration of a domain name in and of itself does not confer intellectual property rights, such as trademark rights, to the registrant. Nevertheless, in certain cases, parties owning trademarks within the country where the dispute takes place can use trademark law to seek protection against cybersquatters.

> *ThegTLDs and 18 ccTLDs for which ICANN is responsible are governed by the Uniform Domain Name Dispute Resolution Policy ("UDRP"). This provides for the online arbitration of disputes through the WIPO's Arbitration and Mediation Center, or another approved provider. National domain name registries may offer dispute resolution services, or may rely on the courts to handle disputes. Some of the exceptions to this are Belgium, Greece and Italy.*

The UDRP sets forth a process for claims where a trademark owner alleges "bad faith, abusive registration of a domain name in violation of trademark rights." In such cases, an administrative panel receives the claim and response, and decides the matter in a brief, efficient on-line procedure requiring less than 50 days for resolution. The parties are obliged to participate in the administrative procedure by contract: when a party applies for a domain name, it must agree, as a condition to grant of the registration, to submit to the process. If the claim of bad faith registration is supported, the domain name is transferred to the claimant.

The parties are not, however, precluded from seeking redress from a court after the administrative process is complete.

ICANN recognizes three dispute resolution service providers including the WIPO Arbitration and Mediation Center.[3]

(b) Procedure

The WIPO procedure for handling domain name disputes is efficient and fast. Once a complaint is filed, the challenged registrant has 20 days to respond. Upon receipt of a response or default, the Center appoints a panel from its published list of international experts. The panel (generally a one person panel) submits a decision to the Center, which then transmits it to the parties, the registrar, and ICANN. The registrar implements the decision by leaving the domain name with the challenged registrant, or transferring the domain name to the claimant. However, if a losing registrant commences court proceedings within ten days, the process stops, no transfer occurs, and the court or parties resolve the matter. The entire process within the WIPO Center is completed in less than two months, involves no live testimony or appearances, and is conducted primarily on-line. All records are public and all decisions are posted on the WIPO Arbitration and Mediation Center web site.

(c) Policy

The UDRP Policy, which has been enunciated by ICANN, for the resolution of domain name disputes[فف] can be summarized as follows:

The Policy is limited to disputes involving deliberate, bad faith, abusive domain name registrations (often termed 'cybersquatting');

Parties may elect to litigate;

Remedies are restricted to the status of the domain name (i.e; no award of damages);

Registrars are exempt from the proceeding provided they have complied with the Policy.

Under the UDRP, to avail oneself of the Policy, a complainant must assert that three elements are present:

1. The domain name is identical or confusingly similar to a trademark;
2. The responding party does not have a legitimate interest in the domain name; and
3. The domain name is being used in bad faith.

Paragraph 4b. of the UDRP, identifies as indicative of bad faith:

The acquisition of a domain name principally for the purpose of sale;

registration to prevent a trademark holder from using it in a domain name;

registration is designed to disrupt the business of a competitor; or

use of a domain name which is intended to confuse the public or divert users

---

[3] See http://arbiter.wipo.int/center/index.html.

away from a trademark holder's web site.

(d) Cybersquatting Disputes

WIPO's Interim Report on the domain name process[صص] recommends the establishment of a centralized "exclusion list" of famous and well-known marks which could not be used as domain names by anyone other than the trademark owner. Trademark owners could apply to have their marks added to the list. The criteria for inclusion would be those developed by the WIPO Standing committee on Trademarks:

> the degree of knowledge or recognition of the mark in the relevant sector of the public;
>
> the duration, extent and geographical area of any use of the mark;
>
> the duration, extent and geographical area of any promotion of the mark;
>
> the duration and geographical area of any registrations or applications for registration, of the mark, to the extent that they reflect use or recognition of the mark;
>
> the record of successful enforcement of rights in the mark, in particular, the extent to which the mark was recognized as well-known by courts or other competent authorities;
>
> the value associated with the mark;
>
> Evidence of the mark being the subject of attempts by non-authorized third parties to register the same or confusingly similar names as domain names.

A problem with all of these recommendations is that there is currently no generally recognized list of famous and well-known marks.

(e) Celebrities

A number of domain name cases involve celebrities attempting to retrieve a domain name that uses all or part of their name. In *Julia Roberts v. Russell Boyd* the WIPO Arbitration panel ruled that the registration was in bad faith. Evidence was tendered that the Respondent had registered domain names of other celebrities and had place the domain name for auction on eBay.[قق] In *Kevin Spacey v. John Zuccarini*[رر] the domain name was similar, but not identical to that of the celebrity (i.e; 'kevinspacy.com'), but the Panelist awarded the domain name to the Complainant.

More recently, however, the Panelists in *Bruce Springsteen v. Jeff Burgar and Bruce Springsteen Club*http://elj.warwick.ac.uk/jilt/01-3/hancock.html - fn22#fn22[شش], the approach was to construe the UDRP more narrowly and leave complex questions of personality rights and common law trademarks for judicial consideration. In declining to transfer the domain name to the Complainant the Panel observed that:

> ... users of the internet do not expect all sites bearing the name of celebrities or famous historical figures or politicians, to be authorised or in some way connected with the figure themselves. The internet is an instrument for purveying information, comment, and opinion on a wide range of issues and topics. It is a valuable source of information in many fields, and any attempt to curtail its use should be strongly discouraged. Users fully expect domain names incorporating the names of well known figures in any walk of life to exist independently of any connection with the figure themselves, but having

been placed there by admirers or critics as the case may be.[تت]

(f) Denigrating domain names 'Dot-Sucks'

Persons seeking to reflect negatively on well known enterprises have sought to register domain names that encompass the identity or trademark of the enterprise, together with the suffix, 'sucks'. Most cases, however go beyond parody and involve some ulterior commercial interest. For example, in *Wal-Mart Stores v. MacLeod*[ثث] *t*he Respondent had registered the domain name 'Wal-Martsucks.com', but had not made any actual use of the site. The Respondent conceded that the registration was made in bad faith, acknowledging specifically that his sole purpose in registering the domain name was to sell it. On the other hand in *Lockheed Corporation v. Dan Parisi*[خخ] the majority of the Panelists allowed the parody site to remain as the Complainant could not establish confusion with its trademark.

7. ELECTRONIC COMMERCE

7.1 The European Situation

In Europe a Communication of the European Commission (EC) dated 16 April 1997, entitled "A European Initiative in Electronic Commerce" stated that the policy of the European Union was to establish a "common European position to achieve global consensus" and to make the Single Market framework, which "has proved its worth for traditional forms of business…work for electronic commerce".[ذذ] To this end on 8 June 2000, the European Parliament adopted a directive "on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)"[ضض]

In the recitals to the Directive, the European Parliament explained that the development of electronic commerce within the information society offered "significant employment opportunities in the Community, particularly in small and medium-sized enterprises, and would stimulate economic growth and investment in innovation by European companies, thereby enhancing the competitiveness of European industry. The Directive had the purpose of "ensuring a high level of Community legal integration in order to establish a real area without internal borders for information society services."[غغ]

The European Parliament had been concerned that the development of information society services within the EU was hampered by a number of legal obstacles to the proper functioning of the internal market which arose from divergences in legislation and from the uncertainty as to which national rules applied to such services. The European Parliament explained that in order to allow the unhampered development of electronic commerce, the legal framework must be "clear and simple, predictable and consistent with the rules applicable at international level so that it does not adversely affect the competitiveness of European industry or impede innovation in that sector."[ظظ]

It is acknowledged that if the market is actually to operate by electronic means in the context of globalisation, the European Union and the major non-European areas need to consult each other with a view to making laws and procedures compatible and that cooperation with third countries should be strengthened; in particular with applicant countries, the developing countries and the European Union's other trading partners.

In a regional association of diverse cultures, such as the EU, it is important to preserve

cultural diversity, consequently, the European Parliament required that the adoption of the Directive should not prevent the Member States from taking into account the various social, societal and cultural implications which are inherent in the advent of the information society. In particular it should not hinder measures which Member States might adopt in conformity with Community law to achieve social, cultural and democratic goals taking into account their linguistic diversity, national and regional specificities as well as their cultural heritage, and to ensure and maintain public access to the widest possible range of information society services; in any case, the development of the information society is to ensure that Community citizens can have access to the cultural European heritage provided in the digital environment.

The European approach to e-commerce regulation can be contrasted with that of the USA, which has sought to minimise the intervention of the national government in this activity. Thus at the same time of the EC Communication, the then President's senior adviser for Internet development stated that "the digital age moves too quickly for government action" and that "the private sector should lead" to avoid overtaxing and over-regulation".[iii] The US Government's *Framework for Global Electronic Commerce*, published in July 1997, established a "road map for international discussions and agreements to facilitate growth of commerce on the Internet", which highlighted the lead role of the private sector and the importance of a simple legal environment.

7.2 Information Society Services

The definition of information society services, adopted in this Directive was that which had been laid down in an earlier Directive which had promulgated technical standards and regulations in this field.[iv] This definition covers any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service. Excluded from this definition are those services which do not imply data processing and storage.

Information society services span a wide range of economic activities which take place on-line; these activities can, in particular, consist of selling goods on-line. These services are not restricted to on-line activities giving rise to on-line contracting but also, in so far as they represent an economic activity, extend to services which are not remunerated by those who receive them, such as those offering on-line information or commercial communications, or those providing tools allowing for search, access and retrieval of data. Information society services also include the transmission of information via a communication network, in providing access to a communication network or in hosting information provided by a recipient of the service. Generally speaking, radio and television broadcasting are not information society services because they are not provided at individual request. On the other hand, services which are transmitted point to point, such as video-on-demand or the provision of commercial communications by electronic mail are information society services.

The Directive excludes from the definition of information society service, the use of electronic mail or equivalent individual communications for instance by natural persons acting outside their trade, business or profession including their use for the conclusion of contracts between such persons.

The Directive in Article 5 requires that each Member States shall ensure that the service provider shall render easily, directly and permanently accessible to the recipients of the

service and competent authorities, at least the following information:
(a) the name of the service provider;
(b) the geographic address at which the service provider is established;
(c) the details of the service provider, including his electronic mail address, which allow him to be contacted rapidly and communicated with in a direct and effective manner;

7.3 On-line Contracts

Each Member State is required by the Directive to amend its legislation containing requirements as to form, which are likely to curb the use of contracts by electronic means.The result of this amendment should be to make contracts concluded electronically workable. The legal effect of electronic signatures is dealt with by a separate Directive on a Community framework for electronic signatures.[ccc] The acknowledgement of receipt by a service provider may take the form of the on-line provision of the service paid for. The electronic commerce Directive is expressed as not affecting Member States' general or specific legal requirements for contracts which can be fulfilled by electronic means, in particular requirements concerning secure electronic signatures.

Member States are permitted to maintain restrictions for the use of electronic contracts with regard to contracts requiring by law the involvement of courts, public authorities, or professions exercising public authority; this possibility also covers contracts which require the involvement of courts, public authorities, or professions exercising public authority in order to have an effect with regard to third parties as well as contracts requiring by law certification or attestation by a notary.

Member States' obligation to remove obstacles to the use of electronic contracts concerns only obstacles resulting from legal requirements and not practical obstacles resulting from the impossibility of using electronic means in certain cases.

This Directive does not affect the law applicable to contractual obligations relating to consumer contracts. Thus the Directive preserves the consumer of the protection afforded to him by the mandatory rules relating to contractual obligations of the law of the Member State in which he has his habitual residence. As regards the derogation contained in this Directive regarding contractual obligations concerning contracts concluded by consumers, those obligations are to be interpreted as including information on the essential elements of the content of the contract, including consumer rights, which have a determining influence on the decision to contract.

7.4 Contract Formation

Article 10 requires that Member States shall ensure, except when otherwise agreed by parties who are not consumers, that at least the following information is given by the service provider clearly, comprehensibly and unambiguously and prior to the order being placed by the recipient of the service:

(i) the different technical steps to follow to conclude the contract;
(ii) whether or not the concluded contract will be filed by the service provider and whether it will be accessible;
(iii) the technical means for identifying and correcting input errors prior to the placing of the order;
(iv) the languages offered for the conclusion of the contract.

Contract terms and general conditions provided to the recipient must be made available in a way that allows him to store and reproduce them.

Article 11 requires that Member States shall ensure, except when otherwise agreed by parties who are not consumers, that in cases where the recipient of the service places his order through technological means;

- the service provider has to acknowledge the receipt of the recipient's order without undue delay and by electronic means,
- the order and the acknowledgement of receipt are deemed to be received when the parties to whom they are addressed are able to access them.

Also this Article requires that, except in the case of contracts concluded by email, Member States shall ensure that, except when otherwise agreed by parties who are not consumers, the service provider makes available to the recipient of the service appropriate, effective and accessible technical means allowing him to identify and correct input errors, prior to the placing of the order.

7.5 Applicable Law

Of critical importance in establishing a legal framework for the conduct of electronic commerce is establishing which law will govern transactions. The Directive adopts the law of "the place at which a service provider is established". This is the place where an information society service provider carries out "an economic activity through a fixed establishment for an indefinite period". The place of establishment of a company providing services via an Internet website is not considered to be the place at which the technology supporting its website is located or the place at which its website is accessible but the place where it pursues its economic activity. In cases where it is difficult to determine from which of several places of establishment a given service is provided, the Directive selects the place where the provider has the centre of his activities relating to the relevant service.

The European Court of Justice has consistently held that a Member State retains the right to take measures against a service provider that is established in another Member State but directs all or most of his activity to the territory of the first Member State if the choice of establishment was made with a view to evading the legislation that would have applied to the provider had he been established on the territory of the first Member State.

7.6 Commercial Communications

Article 6 of the Directive requires Member States to ensure that commercial communications which are part of, or constitute, an information society service comply at least with the following conditions:

(i) the commercial communication shall be clearly identifiable as such;
(ii) the natural or legal person on whose behalf the commercial communication is made shall be clearly identifiable;
(iii) promotional offers, such as discounts, premiums and gifts, where permitted in the Member State where the service provider is established, shall be clearly identifiable as such, and the conditions which are to be met to qualify for them

shall be easily accessible and be presented clearly and unambiguously;

(iv) promotional competitions or games, where permitted in the Member State where the service provider is established, shall be clearly identifiable as such, and the conditions for participation shall be easily accessible and be presented clearly and unambiguously.

7.7 Unsolicited Commercial Communications

The Directive also deals with the sending of unsolicited commercial communications by electronic mail. It requires in Article 7 that unsolicited commercial communities should be clearly identifiable as such in order to improve transparency and to facilitate the functioning of industry self-regulation initiatives. It also requires that unsolicited commercial communications by electronic mail should not result in additional communication costs for the recipient.

Member States which allow the sending of unsolicited commercial communications by electronic mail without prior consent of the recipient by service providers established in their territory are required by the Directive to ensure that the service providers consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves.

7.8 Liability of Internet Service Providers

The Electronic Commerce directive seeks to limit the liability of Internet service providers when acting as intermediaries. It confers exemptions from liability in cases where the activity of the service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient. This activity is perceived to be of a mere technical, automatic and passive nature, which implies that the service provider has neither knowledge of nor control over the information which is transmitted or stored.

A service provider can benefit from the exemptions for "mere conduit" and for "caching" when not involved with the information transmitted. This requires among other things that there is no modification of the information that is transmitted, other than manipulations of a technical nature which take place in the course of the transmission, which do not alter the integrity of the information contained in the transmission. On the other hand, where a service provider deliberately collaborates with one of the recipients of his service in order to undertake illegal act, they cannot benefit from the liability exemptions established for these activites.

In order to benefit from a limitation of liability, the provider of an information society service, consisting of the storage of information, upon obtaining actual knowledge or awareness of illegal activities has to act expeditiously to remove or to disable access to the information concerned. This removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level.

The limitations of the liability of intermediary service providers established in the Directive do not affect the possibility of injunctions, for example orders requiring the termination or

prevention of any infringement, including the removal of illegal information or the disabling of access to it.

Also, the Directive does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities.

The Directive encourages Member States to draw up of voluntary codes of conduct.

7.9 Dispute Resolution

The Directive seeks to guarantee victims effective access to means of settling dispute and the Directive requests Member States to ensure that appropriate court actions are available and that the need to provide access to judicial procedures by appropriate electronic means, should be examined.

7.10 Implementation of the Electronic Commerce Directive

The Member States of the EU are obliged to implement the Electronic Commerce Directive as part of their domestic legislation. By way of example, the UK has issued draft regulations under its European Community Act 1972, which seek to implement the Directive. These regulations amplify a number of the provisions which are considered to be rather too vague in the Directive.

The UK regulations are addressed to commercial communications. These are defined as “any form of communication designed to promote, directly or indirectly, the goods, services or image of any person pursuing a commercial, industrial or craft activity or exercising a regulated profession, other than a communication” which notifies the electronic address of a person. This definition spans a wide range of online forms of communication, including websites and emails, which may be free of charge to the recipient and whose essential purpose is one of advertising. Included among those things that do not fall within the definition are domain names and email addresses themselves, independent audits, statutory reports or reports compiled by an independent regulator. The UK Department of Industry’s guide to the Regulations, excludes from the definition “mobile text “welcome” messages (routinely sent by mobile operators to roaming customers to introduce them to the local network and set out useful contact numbers) or electronic greeting cards”.[ddd]

The UK Regulations define “information society services” as covering any service normally provided for remuneration at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service).”[eee] The requirement for an information society service to be “normally provided for remuneration” does not restrict its scope to services giving rise to online contracting (i.e. buying and selling). It also extends to services (insofar as they represent an economic activity) that are not directly remunerated by those who receive them, such as those offering online information or commercial communications (e.g. adverts) or providing tools allowing for search, access and retrieval of data. Excluded from the concept of “services provided at a distance” are provided in the physical presence of the provider and the recipient, even if they involve the use of electronic devices, such as:

- medical examinations or treatment at a doctor's surgery using electronic equipment where the patient is physically present;
  consultation of an electronic catalogue in a shop with a customer on site;
- plane-ticket reservation at a travel agency in the physical presence of the customer by means of a computer network; and
- electronic games made available in a video arcade where the customer is physically present.'''

Regulation 7(3) excludes from the operation of the regulations:

(i) copyright, neighbouring rights, rights referred to in the Semiconductor Topographies Directive 87/54/EEC and the Databases Directive 96/9/EC and industrial property rights;

(ii) the freedom of the parties to a contract to choose the applicable law;

(iii) - contractual obligations concerning consumer contracts.

8. EC DIRECTIVE ON COPYRIGHT AND RELATED RIGHTS IN THE INFORMATION SOCIETY

The EC Directive on Copyright and Related Rights in the Information Society, was adopted on 9 April 2001 and is required to be implemented by the Members of the European Union by 22 December 2002.

The aim of the Directive is to extend copyright protection to the on-line environment and to implement the international obligations arising from the WIPO Copyright Treaty and the WIPO Performance and Phonograms Treaty.

It harmonises for European countries the rights of reproduction, communication to the public and distribution and provides for protection for anti-copying devices and electronic rights-management systems.

8.1 Reproduction Right

The Directive requires Member States to give copyright owners the exclusive right to authorise or prohibit copies of their works. This reproduction right includes direct or indirect, temporary or permanent reproduction of the works by any means and in any form, in whole or in part. This right is conferred on authors and other related right owners, such as performers, producers of films or sound recordings and broadcasters.

8.2 The Right of Communication to the Public

Member States must ensure their laws give authors the exclusive right to authorise or prohibit any communication of their works to the public. This encompasses communication by the broadcast media, or on the Internet. It also includes interactive on-demand services.

8.3 The Distribution Right

Member States must give authors the exclusive right to authorise or prohibit the distribution of their work, or any copy of it, to the public.

8.4 Exceptions

The Directive contains a long list of exceptions to the exclusive rights. There is one compulsory exception (Art. 5.1). To fall within this exception the copy must :

- be transient or incidental;
- be an integral and essential part of a technological process;
- have the sole purpose of enabling a transmission of the work over a network between third parties or some other lawful use; and
- have no independent economic significance.

This covers, for example, copies made by an Internet Service Provider on the Internet or technical copies made when browsing a website.

The other optional exceptions deal with matters such as photocopying, copying for private use, reproduction for teaching or scientific research or for criticism and review.

8.5 Copy Protection Devices

Member States must provide adequate legal protection against the deliberate circumvention of anti- copying technology used to protect copyright works. This covers not only those devices which are marketed as circumvention devices, but also those which have other uses. This would embrace, for example, websites with instructions on how to circumvent encryption technologies.

8.6 Electronic Rights Management

Where information is provided by a rights holder to identify a work and its author, and gives details of the terms and conditions of its use, Member States are required to protect against the deliberate removal or alteration of electronic rights management information, together with subsequent dealings in works from which such information has been removed.

9. DIGITAL SIGNATURES PROPOSAL

On May 13, 1998 an EC proposal was tabled to harmonsise the law relating to digital signatures in Europe. An electronic signature is defined as a signature in digital form in, or attached to, or logically associated with, data which is used by the signatory to indicate approval of the content of that data and which is:

- uniquely linked to the signatory;
- capable of identifying the signatory;
- created using means that the signatory can maintain under his sole control;
- linked to the data to which it relates in such a manner that it is revealed if the data is subsequently altered.

The proposal lays down a framework for certification service providers (CSPs) to issue qualified certificates which authenticate an electronic signature.

Member states must ensure that there is no barrier to electronic signatures having legal effect solely on the grounds that they are in electronic form.

10. DATA PROTECTION DIRECTIVE

Probably the most controversial piece of EU regulation is the Data Protection Directive, which requires Member States to implement data protection laws by October 24, 1998. Most European nations already have some form of data protection law, but a new provision for most is the requirement that data cannot be transferred from the EU to a third country without "adequate protection", unless the data subject unambiguously consents to the transfer.

[End of document]

أ For a short obituary on Dr Jon Postel see 'The death of an icon' *The Economist*, Oct.24-30, 1998, 101, see also http://wipo2.wipo.int/process/eng/html.

ب See <http://www.isoc.org:what-is-isoc.html>.

ج <http://www.ntia.doc.gov/ntiahome/domainname/domainname130.htm>.

د <http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm>.

ه *Ibid*., see also Klein, S & Lupo, A, ''White Paper' Leaves Some Domain Gray', National Law Journal, 29 June 1998 <: http://www.ljx.com/internet/0629whitedomain.html.>; Moskin, 'Board the Moving Bus: Trademark Owners Beware of Proposals to Improve Management of Internet Names and Addresses' (1998) 88 TMR 213.

و See *The Economist*, October 24-30, 1998, 101.

ز See Handler, 'Internet Domain Names and Trade Mark Law' [1998] *Digital Technology Law Jnl* (in print) para. 21.

ح Unreported, UK High Court, Lightman J, 31 July 1997, cited in Osborne, n.5 supra,at 646..

ط Abel, S, 'Trademark Issues in Cyberspace: The Brave New Frontier' 15 May 1998, rev 10.6 <http://www.fenwick.com/pub/cyber.html>.

ي *CD Solutions Inc v CDS Networks Inc*, unreported, Civil No 97-793-HA (D.Or, 22 April 1998) <http://www.perkinscoie.com/resource/ecomm/netcase/Cases-08.htm>, cited *ibid*., para.34.

ك See Meyer, 'Intellectual Property Rights on the Internet', (1998) 14 *Computer Law & security Report* 14 at 17.

ل Unreported, discussed in Osborne, 'Domain Names Registration & Recent Resolution and Recent UK cases', [1997] 11 *EIPR* 644 at 646.

م Unreported, 23 July 1998 reported at http://nic.uk/news/oiam-appeal-judgement.html.

ن [1998] FSR 265 at 271.

س *Ibid.* at 273.

ع N.26 at 14.

ف *Ibid* at 21.

ص *Ibid.*

ق *Ibid.*, 19.

ر *Ibid.*

ش *Ibid.*, 20.

ت *Ibid.*

[Endnote continued on next page]

[Endnote continued from previous page]

ث Unreported, April 17, 1998, 9th Circuit Court of Appeals, noted in [1998] EIPR N-139.

خ *Panavision International LP v Toeppen* 945 F. Supp. 1296 (CD Cal 1996).

ذ Quoted in [1998] EIPR at N-140.

ض Unreported, 983 F Supp 1331 (D. Or, 20 November 1997) [Internet] URL: http://www.perkinscoie.com/resource/ecomm/netcase/Cases-08.htm.

غ *America Online v AOL Casino* (unreported, filed 24 June 1998) [Internet] URL: http://www.perkinscoie.com/resource/ecomm/netcase/Cases-08.htm.

ظ See Blakeney, 'Well Known Marks', [1994] *EIPR* 481.

أأ Eg *Roadrunner Computer Systems, Inc v Network Solutions Inc*

بب *The Comp Examiner Agency, Inc v Juris, Inc* (CD Cal, 26 April, 1996).

جج *Cardservice International v McGee* 950 F. Supp 737 (ED Va 1997).

دد 42 USPQ 2d 1430 (SDNY 1997).

هـ [1998] FSR 16.

وو See Hurdle, 'Domain Names – The Scope of a Trade Mark Proprietor's Monopoly Avnet Inc v Isoact Ltd', [1998] 2 *EIPR* 74.

زز *Ibid.*

حح 985 F.Supp. 1220 (ND Cal. 1997).

طط (E.D. Va 10 Apr. 1998) discussed in Sommers and Hieber, 'Internet Trademark, Trade Dress and Domain Name Dispute Developments in the United States' Institute of Trade Mark agents Annual conference, October 8-9, 1998, Disneyland, Paris, 22-23.

ي (SD Cal 22 Apr. 1998), discussed, *ibid*, 26-27.

ك Discussed in Chong, 'Internet Meta-tags and Trade Mark Issues' [1998] EIPR 275.

لل 985 F. Supp 1220 (ND Cal. 1997).

مم (ND Cal Apr 16, 1998) discussed in Sommers and Hieber, n.47 *supra* at 47.

نن Eg see *Juno Online Services LP v Juno Lighting Inc* 979 F. Supp 684 (ND Ill 1997).

س Eg see International Trademark Association, *Internet Domain Name White Paper*, www.inta.org/wpwhole.htm.; Oppendahl, *Analysis and Suggestions Regarding NSI Domain Name Trademark Dispute Policy* (Sept. 1996) http://www.patents.com/nsi/iip.sht.

ع See authorities referred to in Sismilich, *Resolution of Internet Domain Name Disputes*, 21 Nov.1997, http://www.magpage.com/~sismilch/adrpaper.htm.

ف Uniform Domain-Name Dispute-Resolution Policy, <http://www.icann.org/udrp/udrp-policy-24oct99.htm>.

ص Interim Report of the Second WIPO Internet Domain Name Process, para. 150. See: <http://wipo2.wipo.int>.

ق WIPO Case No D2000-0120.

ر WIPO Case No D2000-0235.

ش WIPO Case No D2000-1532.

ت *Ibid.*, at 7.

ث WIPO Case No D2000-0062.

خ WIPO Case No D2000-1015.

ذ Com (97) 157, 16 April, 1997.

ض Directive 2000/31/EC.

غ *Ibid.*, recital 3.

ظ *Ibid.*, recital 60.

أأ Quoted in P. Rees, 'EU and US Regulation of Electronic Commerce: Converging Approaches in a Converging World", [1999] *International Commercial and Company Law Review* 176.

[Endnote continued on next page]

[Endnote continued from previous page]

ببب Directive 98/34/EC of 22 June 1998.

ججج Directive 1999/93/EC of 13 December 1999.

ددد Department of Trade and Industry, A Guide For Business to the Electronic Commerce (EC Directive) Regulations 2002, March 2002. 7.

ههه *Ibid*., para.2.13.

وو *Ibid*., para 2.15.