BNA International

World Internet Law Report

International Information for International Businesses

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

Volume 5, Number 9 September 2004

Articles

Case Report

News

News

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: 29th Floor, Millbank Tower, 21-24 Millbank, London SW1P 4QP, England. Tel. (+44) (0)20 7559 4801; Fax (+44) (0)20 7559 4840; 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 £695; Eurozone €1150; U.S. and Canada U.S.$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.

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

In this September issue of *World Internet Law Report* we are pleased to include a collection of excellent commentaries: convergence; online licence agreements; the U.K. Computer Misuse Act; and the impact of the E-Commerce Directive are just some of the topics covered in *WILR* this month.

Our thanks go to Jolyon Barker, Head of Deloitte's TMT group, who writes in our Technology section on the current state and future implications of convergence across the Telecommunications, Media and Technology industries. Jolyon's article focuses on three key questions: the underlying trends driving continued convergence; how convergence will drive the evolution of the TMT sector; and the critical success factors for TMT companies in the future.

We are also pleased to include two excellent commentaries from Alessandro del Ninno and Giorgio Como, which focus on the impact of the E.U. E-Commerce Directive. Alessandro's article looks at how implementation of the Directive in some key E.U. Member States has impacted the rules for electronic contracts, while Giorgio discusses the liability under the Directive for intermediary service providers in Italy.

Paul Barton and Liz McSweeney of London City firm, Field Fisher Waterhouse, provide us with commentaries on the regulation of online licence agreements and the Computer Misuse Act, following developments this year in the United Kingdom.

Finally, we include a special report from Kate Ellis of Eversheds on the latest challenges for ICANN and Eva Wong of Coudert Brothers looks at the privacy implications of Google's Gmail.

Please forward comments and suggestions to nicholad@bna.com, or tel. (44) (0)207558 4807.

Nichola J. Dawson

We wish to thank the following for their contribution to this issue:
Jolyon Barker, Deloitte, London; *Paul Barton* and *Liz McSweeney,* Field Fisher Waterhouse, London; *Giorgio Corno,* Studio Corno Avvocati, Milan; *Kate Ellis,* Eversheds, Manchester; *Tomas Kucirek,* Deloitte & Touche, Prague; *Alessandro del Ninno,* Studio Legale Tonucci, Rome; *Don McAleese,* Matheson Ormsby Prentice, Dublin; *Ignacio Temiño Ceniceros,* Abril Abogados, Madrid; *Eva Wong,* Coudert Brothers, London.

E-Commerce

The Rules for E-Contracts in Selected Member States: The Implementation of Directive 2000/31/EC

By Avv. Alessandro del Ninno, Head of the Information & Communication Technology Department at Studio Legale Tonucci, Rome. The author may be contacted by e-mail at: adelninno@tonucci.it

Differences in national legislation and legal uncertainties as to which national rules applied were preventing the development of information society services and the smooth functioning of the internal market. In its Communication of April 1997, the E.U. Commission therefore announced the creation of a legal framework to promote e-commerce between the Member States. A Resolution was subsequently passed by the European Parliament in April 1998 in support of the Commission's recommendation.

Directive 2000/31/EC of June 8, 2000 "on certain legal aspects of information society services, in particular electronic commerce in the internal market" (hereinafter "the Directive") seeks to clarify some legal concepts and harmonise certain subject matters in order to enable information society services to fully benefit from the free movement of services within the internal market.

The following considerations are focused on the European Union and national rules related to electronic contracts, with the aim of creating an information society service as defined by the E.U. Directive on Electronic Commerce (which recalls the definition provided by E.U. Directives 98/34/EC and 98/48/EC). An *information society service* shall mean any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.

For the purposes of the above definition:

- *"at a distance"* means that the service is provided without the parties being simultaneously present;
- *"by electronic means"* means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means;
- *"at the individual request of a recipient of services"* means that the service is provided through the transmission of data on individual request.

(Specific rules for electronic contracts are provided by Directive 97/7/EC on the protection of consumers in respect of distance contracts. Directive 97/7/EC was implemented in the Member States by means of specific national rules; however, the compulsory requirements and fulfilments for electronic contracts with consumers set out in the Directive are not discussed here.)

A specific analysis on how the major E.U. Member States (Germany, France, the United Kingdom, Italy and Spain) have implemented the E.U. Directive rules related to electronic contracts follows below.

The National Rules on E- Contracts

Legal Recognition

The Directive requires Member States to remove any legal obstacles which could hamper the use of electronic contracts. This means that a contract cannot be deprived of legal validity on the ground that it has been made by electronic means.

The Directive lists categories of contracts which would not automatically be legally valid and whose electronic conclusion could be restricted. These categories relate to contracts:

- creating or transferring rights in real estate;
- requiring the involvement of courts or public authorities;
- of surety-ship and collateral securities supplied by people acting for non-business purposes;
- governed by family law or by the law of succession.

Further, Member States must allow electronic contracts to be concluded by electronic means and to be legally valid (except for the limited number of types of contract above).

France

In France, the Law on the Digital Economy (Article 25 of Law 575/2004) states that most contracts can be concluded electronically. Law 575/2004 also provides that the following contracts cannot be concluded electronically:

- contracts on family or succession law;
- contracts requiring the involvement of judicial authorities;
- surety contracts supplied by people acting for non-business purposes.

Germany

In Germany, according to the Act of June 22, 2001 adapting the rules on formal requirements to the needs of modern business, electronic contracts are in principle valid. There are no differences for the legal recognition of traditional and electronic contracts.

However, in some cases the law requires the use of a qualified electronic signature. The following contracts cannot be concluded electronically:

- contracts which must be concluded in written form (*e.g.*, donations, surety and credit agreements);
- contracts that need a notary's certification or public authentication (*e.g.*, contracts that create or transfer rights

in real estate, or contracts governed by family and succession law).

Italy

In Italy electronic contracts are fully valid in principle (according to Article 15.2 of Law of March 15, 1997, n. 59, to article 11 of Presidential Decree of December 28, 2000, n. 445, and to the Legislative Decree implementing the Electronic Commerce Directive no. 70 of April 9, 2003.

Thus, some contracts need to be in writing such as accommodation contracts or contracts that create a perpetual or life annuity. However, when the electronic contract is signed with an advanced electronic signature based on a qualified certificate and created by a secure-signature-creation device, the document must be recognised as having full evidentiary value. In other cases, the courts will be free to evaluate the evidentiary value of the contract.

The Legislative Decree of April 9, 2003 no. 70 implementing the Electronic Commerce Directive states that it does not apply to certain types of contracts such as those creating and transferring rights in real estate (except for rental rights), requiring the involvement of courts or public authorities or governed by family law or law of succession.

Spain

In Spain the Civil Code and Commercial Code recognises the principle of freedom of form, thus accepting all types of contracts regardless of form). Further, the same principle is provided by the Royal Decree 1906/1999 of December 17, 1999 on electronic contracts and by the Law on electronic commerce of June 27, 2002, no 34.

Contracts governed by family law or by the law of succession and contracts whose validity is dependent on the intervention of a third party (*e.g.*, notaries, registrars, courts) cannot be validly concluded in electronic form.

United Kingdom

In the United Kingdom the responsible ministers have been granted the powers to remove legal restrictions which prevent the use of electronic communications or storage for certain stated purposes. These include anything which must be done in writing, by post, using a personal signature or seal, a declaration under oath, maintenance of a document, publication of information and payment.

The U.K. Regulations on electronic commerce (the Electronic Communications Act 2000 and the Electronic Commerce (EC Directive) Regulations 2002) have not implemented the provision of the E.U. Directive that allows contracts to be concluded electronically.

The government believes that the great majority of relevant statutory requirements (*e.g.*, for writing or signature) are capable of being fulfilled electronically where the context in which they appear does not indicate to the contrary.

The Government has indicated that it does not envisage removing hardcopy requirements relating to the following categories of contracts:

- for England, Wales and Scotland: all contracts that create or transfer rights in real estate, except for rental rights;
- for the United Kingdom: all contracts relating to the imposition and operation of export controls of goods and technology insofar as the items controlled are not outside the scope of the Treaty.

The U.K. approach means that ministers can change individual pieces of legislation one at a time rather than stating that contracts in general can be concluded by electronic means subject to exceptions. Where existing legal requirements create obstacles to the use of electronic contracts, the Government has indicated that it will propose the necessary amendments on a case-by-case basis.

Information Requirements (for B2B Online Contracts)

The Electronic Commerce Directive stipulates that (except when otherwise agreed and except for contracts concluded exclusively by exchanging e-mail messages) the service provider must communicate a defined set of information on the process of concluding the contract before an order is placed.

The service provider must also provide the recipient with the contract terms and general conditions in a way that allows the recipient to store and reproduce them (*e.g.*, by e-mail).

The following minimum set of information must be provided by service providers "directly and permanently" to recipients of services and to the responsible authorities:

- name of the service provider;
- address at which the service provider is established;
- details of the service provider including e-mail address;
- the trade register in which the service provider is entered and registration number;
- for activities subject to an authorisation scheme: name and address of the authority delivering the authorisation;
- for regulated professions: the professional body with which the service provider is registered; professional title; Member State(s) where the service is provided and reference to professional rules in the Member State of establishment;
- VAT number (if any);
- price of information society service and tax and delivery costs (if any).

Please note that further information requirements are requested for online contracts and distance contracts with consumers, according to E.U. Directive 97/7/EC on the protection of consumers in respect of distance contracts. The following paragraph only points out the information requirements requested by the E.U. Directive on Electronic Commerce.

France

In France, according to Article L 441-6 of the Commercial Code, to Article 72 of Decree 84-406 of May 30, 1984 and to Article 19 of the Law 575/2004 on the Digital Economy, the general information to be provided by the information society service provider includes:

- name or corporate name for companies;
- address, e-mail and phone number;
- trade register and registration number (n° SIREN) on commercial documents, share capital and address of the registered office for companies;
- individual VAT identification number if relevant;

- if the activity is regulated, the name and address of the authority that has granted the authorisation;
- if relevant, the professional rules that bind the provider.

Prices stated must be clear and unambiguous, in particular on the inclusion of taxes and delivery costs. These requirements concern all sales or services offered to professionals. These measures are applicable to business-to-business as well as business-to-consumer transactions.

Germany

In Germany, according to sections 312c, 312d, 312e and 355, 356 of the Civil Code (BGB) and to the Ordinance on information requirements of November 26, 2001 the information requirements for the conclusion of electronic contracts between professional parties are in principle the same as those for business-to-consumer contracts.

Most of the information requirements can be waived by contract.

The service provider must always make the contract terms and standard contract terms available to the customer in a way that allows the latter to store and reproduce them. In the case of supply of goods, the terms must be available at the latest at the time of delivery.

These requirements are not applicable to contracts concluded exclusively by individual communication.

Italy

In Italy, according to the legislative decree 70/2003, the service provider must provide:

- all information relevant for the conclusion of the contract;
- specific indications concerning goods or service requirements;
- price;
- terms of delivery;
- terms of testing;
- terms of payment.

In addition, the service provider must ensure, except when otherwise agreed between professional parties, that at least the following information is given clearly, comprehensibly, unambiguously, and prior to the order being placed by the recipient of the service:

- the different technical steps to follow to conclude the contract;
- how the concluded contract will be filed by the service provider and how it will be accessible;
- the technical means for identifying and correcting input errors prior to the placing of the order;
- the languages offered, other than Italian, for the conclusion of the contract;
- any relevant procedure for dispute resolution, codes of conduct to which the service provider subscribes and information on how those codes can be consulted electronically.

These obligations do not apply to contracts concluded exclusively by exchange of electronic mail or by equivalent individual communications.

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

These information requirements are considered to be based on the general principle of "bona fide", valid for any kind of contract.

Spain

In Spain the general requirements for any type of contract apply (there must be valid consent, capacity to contract, *etc*.). The law on general contract terms partially apply if the contracts terms are general conditions as opposed to being individually negotiated.

There are currently no specific information requirements. The Law on electronic commerce 34/2002 contains the same information requirements as the Electronic Commerce Directive.

United Kingdom

In the United Kingdom, the U.K. Regulations contain the same information requirements as the Electronic Commerce Directive.

Steps to Conclude Electronic Contracts

Community legislation does not specify at what time an electronic contract is deemed to be concluded. This time is therefore determined by reference to Member States' laws. However, the Electronic Commerce Directive states that (except when otherwise agreed by professional parties and except for contracts concluded exclusively by an exchange of e-mail messages):

- the service provider must acknowledge receipt of an order electronically and without undue delay; and
- technical means must be made available to identify and correct input errors before an order is placed.

France

In France any electronic offer for the supply of goods and services has to indicate the terms and conditions (Article 25 of the Law 575/2004). Further, any electronic offer must mention:

- the different steps to conclude the contract;
- the technical ways to identify and correct any mistake;
- the languages proposed for the conclusion of the contract;
- the storage formalities and the electronic means to consult relevant professional codes of conduct.

Online merchants also have to indicate prices in a clear and unambiguous manner and to specify whether taxes and delivery expenses are included.

In order for the contract to be valid, the recipient must be able to check the details of his order and to correct errors before confirming his acceptance.

The merchant must acknowledge receipt of the order without unjustified delay and by electronic means.

A future decree will specify how the information and contracting requirements have to be complied with on mobile phones.

Germany

In Germany, the presentation of goods or services on the Internet is not a legally binding offer but a so-called *"invitatio ad offerendum"*, *i.e.*, a proposal to make an offer. Exceptionally, if

the supplier indicates his unconditional will to supply the goods or services to every person accessing his website, this will be considered as an offer.

The customer makes the offer by communicating to the supplier his intention to buy. The supplier has to confirm the reception of the order electronically and without undue delay. The supplier has to provide adequate technical measures to correct input errors. Within a short period of time, the supplier has to make available the contract terms and standard contract terms to the customer in a way that allows the latter to store and reproduce them – for the supply of goods at the latest time of delivery.

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 under normal circumstances (see Section 312e of the Civil Code – BGB).

Italy

In Italy the service provider must acknowledge the receipt of an order without undue delay and by electronic means. The receipt must contain a summary of the general and particular conditions applicable to the contract, the essential characteristics of the goods or service, price, means of payment, means of withdrawal, delivery cost and other taxes.

This rule does not apply to contracts concluded exclusively by electronic mail or equivalent individual communications or when professional parties agree otherwise.

The Legislative Decree 70/2003 implementing the Electronic Commerce Directive states that the "ordinary" rules on the conclusion of contracts apply to the cases where the order is placed by electronic means. This means that Italian rules on contracting provided by the Italian Civil Code (in particular Articles 1326 and 1335) apply to determine the time at which a contract is deemed to be concluded. These state that a contract is concluded when the party becomes aware of the acceptance of his offer by the other party. The acceptance is known when it reaches the address of the other party.

Spain

In Spain the general contract principles provided by the Civil Code and by the Commercial Code apply to the conclusion of online contracts. In business-to-consumer contracts and business-to-business contracts, the contract is deemed to be concluded when the acceptant issues his/her acceptance to the offeror.

After conclusion of the contract, the vendor must acknowledge receipt of the acceptance within 24 hours from reception of the acceptance (except when otherwise agreed by professional parties and except for contracts concluded exclusively by exchange of e-mails).

On the place of the contract, the Spanish articles 27, 28 and 29 of the Law on electronic commerce 34/2002 establishes that the contract is deemed to be concluded:

- for business-to-business contracts, at the place where the Internet seller is established unless otherwise agreed by the trading parties;
- for business-to-consumer contracts, at the place where the consumer resides.

The Law also specifies that an electronic offer is deemed to be valid for the period specified by the vendor. If a period of time has been specified, the offer remains valid as long as it is accessible to the recipient of the service.

United Kingdom

In the United Kingdom, the Electronic Commerce (EC Directive) Regulations 2002 follow the provisions of the Directive.

There are no specific rules on the time of conclusion of an electronic contract. It is not clear how the traditional common law rules should be applied to electronic contracts. For instantaneous methods of communication such as telex and telephone, the general rule is that a contract is concluded when notification of acceptance is received by the offeror. However, for non-instantaneous methods of communication such as the post, the rule is that the contract is concluded at the time the letter is posted. Which of these rules would apply to electronic contracts has not yet been decided. This will depend upon whether the communication is considered to be instantaneous in which case the general rule would apply and if not the postal rule may be deemed to apply.

The Liability of Intermediary Service Providers in Italy: The Impact of Directive 2000/31/CE

By Giorgio Corno, Studio Corno – Avvocati. The author may be contacted at legale@studiocorno.it

Since the mid-1990s, the European Parliament and Council have adopted measures towards harmonisation of the regulations of certain legal aspects of information society services,[1] in order to improve the free movement of goods, people, services and capital,[2] within and outside[3] the internal market.

With regard to the measures adopted within the internal market, in November 1999 the European Parliament and Council decided to "put Europe on-line" and develop a so-called *eEurope*,[4] to help create jobs and make European industries more competitive as part of the European Union's continuing efforts to fulfil its obligation (enshrined in Article 2 of the Treaty on European Union) "to promote economic and social progress and a high level of employment".

The E-Commerce Regulation

Work at European level to promote the development of e-commerce started at an early stage with the Commission's 1997 Communication "A European Initiative in Electronic Commerce".[5]

On June 8, 2000 the European Parliament and the Council adopted Directive 2000/31/CE on certain aspects of

  WILR ISSN 1468-4438

information society services[6] (in particular, electronic commerce) in the Internal Market (the so-called Directive on electronic commerce, ("the Directive")).

The Directive, which seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between Member States (Article 1.1), does not apply to so-called indirect e-commerce activities[7] as well as to other sectors of law,[8] and disciplines only some aspects of e- commerce.[9]

Member States progressively adapted their statutes to the Directive by the approval of specific rules of law.[10] Italy complied by implementing Legislative Decree no.70 of April 9, 2003 (in force since May 13, 2003).[11]

This article focuses on the liabilities of online service providers acting as intermediaries for unlawful acts, according to the Directive, Decree 70/2003 and some of the recent rulings by Italian courts.

Internet Service Providers: Intermediary and Content Providers

Internet Service Providers (ISPs) may provide different information society services, as defined above. Specifically, they may provide:

- *Intermediary services*: where they are in no way involved with the information transmitted. These services include:
  - Transmission of a communication network provided by a recipient of the service (mere conduit), or the provision of access to a communication service (access provider). These services may include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, provided that the information is not stored for any period longer than is reasonably necessary for the transmission.
  - Transmission of a communication network provided by a recipient of the service, when the ISP's activity is limited to the automatic, intermediate and temporary storage of that information and is performed for the sole purpose of increasing the efficiency of the information's onward transmission to other recipients of the service upon their request (*caching*).[12]
  - Storage of information provided by a recipient of the service (*hosting*).
- *Website content or any of the services included therein*. When offering these services, providers are involved with the information transmitted through the Internet.

According to the distinction above, ISPs may be alternatively defined as Intermediate Service or Contents Providers.

Italian Case Law Prior to the Enforcement of Directive 2000/31/CE

Content providers are directly liable, either civilly or criminally, for unlawful activities directly performed, such as infringement of a trademark through the registration of a domain name[13] or a copyright; performance of unfair competition conducts; breach of the anti-pornography regulations; defamation and so on.

Intermediary Services Providers' liability for third parties unlawful activities has been examined in many proceedings. Specifically, prior to the enforcement of Directive 2000/31/CE, Member States' legislation and case-law concerning liability of service providers acting as intermediaries for third parties' unlawful activities differed considerably.

Italian Courts have discussed in particular, ISPs' liability for: (a) allowing, or contributing to third parties' unlawful activities; or for (b) lack of a prompt response to unlawful activities carried out by third parties as soon as these were known.

With regard to (a), courts of lower jurisdictions held ISP providing *hosting*[14] services liable for torts deriving from allowing or facilitating the unlawful behaviour of one of the recipients of their services;[15] or for the spread of a defamatory data within the website of the recipient of their services.[16] Other courts, however, exempted intermediary service providers such as *access* or *hosting providers*[17] from liability for third parties' unlawful activities, when they had neither knowledge or control over the information transmitted or stored.[18]

With regard to (b), courts held Intermediary Service Providers liable for torts consequent to the failure to take prompt action to prevent access to the contents of the services themselves; or for failing to inform the competent authorities, had they known the unlawful or prejudicial feature of the service contents to which they provided access, whenever required by the supervisory competent authority. In other words, ISPs who become acquainted with presumed unlawful activities or information regarding a recipient of their services, against competent authority request, were held bound to provide the required information to allow the identification of the parties of data storage agreements, in order to prevent unlawful activities. According to this rule, a court held an access provider liable for not having collected the information required to identify the recipient of its services.[19]

The Principles Contained in Directive 2000/31/CE

The interpretation of Intermediary Service Providers' liability differed within individual E.U. Member States.[20]

This situation prevented the smooth functioning of the internal market, in particular by impairing the development of cross-border services and producing distortions of competition.

Directive 2000/31/CE tries to develop rapid and reliable procedures for removing and disabling access to illegal information. As clearly stated in the E.U. Commission's "First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of June 8, 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)", which was issued on November 21, 2003[21]:

(a) "The provisions on the liability of intermediaries create legal certainty for intermediary service providers and thus help to ensure the provision of basic intermediary services on the internet;

(b) This Directive establishes precisely defined limitations on the liability of internet intermediaries providing services consisting of mere conduit, caching and hosting. The limitations on liability in the Directive apply to certain clearly delimited activities carried out by internet intermediaries, rather than to categories of service providers or types of information".[22]

The limitations on liability provided for by the Directive are established in a horizontal manner, meaning that they cover liability, both civil and criminal, for all types of illegal activities initiated by third parties.

The Directive does not affect:

(a) the liability of the person who is at the source of the content nor does it affect the liability of intermediaries in cases which are not covered by the limitations defined in the Directive;

(b) the possibility of a national court or administrative authority to require a service provider to terminate or prevent an infringement.[23] These questions are subject to the national law of the Member States";

(c) the liability of providers for hyperlinks and location tool services, "notice and take down" procedures and the attribution of liability following the taking down of content.

Legislative Decree no. 70/2003: Mere Conduit or Access Provider

Legislative Decree no. 70/2003, which adopted the Directive in Italy, introduces a differentiated system of liabilities, depending on the activity performed by the ISP, according to the provisions of Directive.

Specifically, according to Article 12 of Decree no. 70/2003[24]:

(a) the intermediary provider who performs a mere conduit or access provider activity, shall not be liable for the transmitted information, if they do not initiate the transmission; select the receiver of the transmission; select or modify the information contained in the transmission.[25]

(b) the act of transmission and of provision of access referred to above include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

The intermediary provider who performs a *mere conduit or access provider* activity shall, however, be bound: (a) by the obligations towards their clients arising from contractual provisions; (b) while processing personal data, by the existing regulations, concerning personal data and system security,[26] as well as by any other applicable regulation.

Courts or administrative authorities with supervisory functions,[27] may require the service provider (through the issuing of an interim order) to terminate or prevent an infringement.[28]

Legislative Decree no. 70/2003 (2): *Caching* Providers

Article 13 of Decree no.70, dated April 9, 2003 states that the intermediary provider who performs a *caching* activity shall not be liable for the information transmitted if they do not modify it; comply with conditions on access to the information; comply with rules regarding the updating of information, specified in a manner widely recognised and used by industry; do not interfere with the lawful use of technology used by industry to obtain data on the use of the information; act expeditiously to remove or disable access to the information they have stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled,[29] or that a court or an administrative authority has ordered such removal or disablement or the removal has been ordered.

As well as for *mere conduit* activities, courts or administrative authority, entitled to supervision functions, may require the service provider, through the issuing of an interim order, to terminate or prevent an infringement.

Legislative Decree no. 70/2003 (3): *Hosting* Providers

Article 14 of Decree no.70, dated April 9, 2003 states that the intermediary provider who performs *hosting* activity, shall not be liable for the stored information at the request of a recipient of the service, on the condition that:

- the ISP does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent;[30]
- upon obtaining such knowledge or awareness, the ISP acts expeditiously to remove or to disable access to the information.

Courts or competent administrative authority may require the service provider, also through the issuing of an *interim* order, to terminate or prevent an infringement action or to disconnect the access.

Legislative Decree no. 70/2003 (4): No General Obligation to Monitor

Article 17 of Decree no. 70/2003 does not impose on ISPs who provide the services mentioned above and within the limits of Articles 14–16 of the Directive, a general obligation:

- to monitor the information which they transmit or store;
- to actively seek facts or circumstances indicating illegal activity.

However, service providers shall inform without delay, the competent public authority of alleged illegal activities undertaken or information provided by recipients of their services or to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.[31]

Should an ISP breach this obligation, they will be held liable for the consequent damages.

Enforcement of the Directive in Europe

As expressly stated in the E.U. Commission's First Report on the application of Directive 2000/31/EC,

> "there is still very little practical experience on the application of Articles 12-14. In a few cases[32] national courts have already interpreted the Directive. However, in these cases, the national implementing measures of the Directive had not yet been adopted in the States concerned".

The Enforcement of the Directive in Italy: Recent Judgments

Two judgments were recently issued in Italy, by a civil and a criminal court of first instance, coherent with the provisions of decree no. 70 of 2003 described above.

The first judgment was rendered[33] in a civil action where the court had been asked to judge whether an ISP providing hosting services could be held liable for copyright infringement consequent to the publication on a website of a recipient of its services of the text of a book without the required author's authorisation. The ISP was unable to prove that publication of book was carried out following instructions by the recipient of the service. Therefore, the content of the website was considered as provided by the ISP, which was consequently qualified as a content provider. As the ISP could have been aware of the facts or circumstances under which the illegal activity occurred, the exemption of liability according to Article 16.2 of Decree 70/2003 was not applied to this case. Consequently, the ISP was held liable for copyright infringement.[34]

The second judgment was rendered[35] in a criminal action. The court had been asked to judge whether an ISP who owned and managed a website, which provided an automatically generated[36] list of other websites together with the links to those sites, could be held liable (under criminal laws governing pornography[37]) should one of the linked websites have displayed pornographic materials[18], prepared and realised by subjects different from the ISP.

No evidence of the ISP's involvement in creating the pornographic website was ascertained during the proceedings; no lien of any kind (economic or otherwise) with the owners of the pornographic website was discovered; no knowledge of illegal activity or information was attributable to the ISP. The ISP did not have a criminal intention (so-called *dolo*[39]) and, therefore, was not held criminally liable. The website owners were also exempt. The rule expressed in this judgment confirms that even in criminal proceedings, ISPs may be exempt from liability even if they fail to modify the information contained in the transmission (Articles 16 and 17).[40]

The case also refers to ISPs' liability for hyperlinking, which was not provided for in the Directive.[41] This is why this case, as well as those which have occurred in other jurisdictions where liability for hypertexts has already been disciplined, will be taken into account by the E.U. Commission (in accordance with Article 21.2 of the Directive) during the preparation of its bi-annual report concerning the enforcement and improvement of the e-commerce Directive.

1 According to Directive no.98/34/Ce of the European Parliament and of the Council dated June 22, 1998, as well as Directive no.98/84/Ce of the European Parliament and of the Council dated November 20, 1998, "information society services" are "any services provided against remuneration, at a distance, by electronic way, by elaborate electronic equipment (included the digital compression) and the data storage, and by individual request of a services receiver".

2 As provided by section no.14, point no.2 of the European Community constitutive Treaty.

3 These objective were shared with the major non-European areas. Among other initiatives, the Commission is involved in a number of bilateral regulatory dialogues on e-commerce related to information society issues, in order to promote the Directive's regulatory approach and to work towards consistency at international level. These bilateral dialogues include the E.U./U.S. Information Society Dialogue, the co-operation with Canada in the context of Canada-E.U. Trade and Investment Sub-Committee (TISC), including an e-commerce work plan in 1999; the E.U.-Japan dialogue; the E.U.-Mercosur regulatory dialogue; and the dialogue with the Mediterranean countries. On these and other initiatives, see the E.U. Commission's First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of June 8, 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), issued on November 21, 2003.

4 The European Commission put forward its "eEurope" initiative precisely to manage this transition, both within the Union and in the candidate countries of Central and Eastern Europe.

At the Lisbon Summit in March 2000, European heads of state and government recognised that Europe must also become a more digital economy. Indeed, they set a new goal for the European Union – to become the most competitive knowledge-based society in the world by 2010. The European Union's success in achieving this goal will help determine the quality of life of its citizens, the working conditions of its workers and the overall competitiveness of its industries and services.

There have, so far, been two action plans: (a) the Action Plan 2002 endorsed by the E.U. leaders at their Feira summit in June 2000; (b) the Action Plan 2005 approved by E.U. leaders in Seville in June 2002.

5 COM(97) 157 final, 16.4.1997.

6 Also included in such services are the numerous economic activities performed *online e.g.*, the offer of goods or services. The eighteenth "whereas" of the Directive no.2000/31/Ce states that "information society services are not solely restricted to services giving rise to online 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 online information or commercial communications, or those providing tools allowing for search, access and retrieval of data". Such services also include the transmission of information by a telecommunication network, supplying access to a communication network or the storage of information provided by a services receiver. The Directive does not regulate the use of e-mail or the use of other equal individual communication, for example, by natural persons who work out of their commercial, company or professional activity.

7 Directive 2000/31/CE lies down requirements applicable to information society service providers or information society services, regardless of whether they are of a general nature or specifically designed for them in respect of: (a) the requirements for setting up as an information society service, such as those concerning qualifications, authorisation or notification; (b) the pursuit of the activity of an information society service, such as requirements concerning the behaviour of the service provider, requirements regarding the quality or content of the service including those applicable to advertising and contracts, or requirements concerning the liability of the service provider. The Directive does not cover requirements applicable to goods as such; requirements applicable to the delivery of goods; requirements applicable to services not provided by electronic means.

8 According to Article 1.5, the Directive 2000/31/CE, shall not apply to the field of taxation; questions relating to information society

services covered by Directives 95/46/EC and 97/66/EC; questions relating to agreements or practices governed by cartel law; the activities of information society service of notaries or equivalent professions to the extent that they involve a direct and specific connection with the exercise of public authority; the representation of a client and defense of his interest before the courts; gambling activities which involve wagering a stake with monetary value in games of chance, including lotteries and betting transactions.

9 Specifically, following some general provisions (Articles 1–3), the Directive focuses on establishment and information requirements (Articles 4 and 5); specific rules for commercial communications (Articles 6, 7 and 8); contracts concluded by electronic means (Articles 9–11); liability of intermediary service providers (sections 14–17). The final provisions of the Decree are directed to promote the use of codes of conduct (Article 16); of out of court dispute settlements as well as court actions (Articles 17–18); co-operation between Member States for the implementation of the Directive (Article 19) and sanctions applicable to infringement of national provisions adopted pursuant to the Directive. (Article 20).

10 The E.U. Commission's First Report on the application of the Directive, issued on November 21, 2003 expressly states that: "The deadline for Member States to transpose the Directive into national law was 17 January 2002, 18 months after the entry into force of the Directive on 17 July 2000. The Council and the European Parliament accepted a relatively short transposition period having agreed that setting up a legal framework for e-commerce was a matter of priority.

There were, however, some delays in transposition, due mainly to the horizontal nature of the Directive, which affects a large variety of legal issues. So far 12 Member States have brought into force implementing legislation. In the remaining 3 Member States, work on the transposition of the Directive is well advanced".

11 The Decree was published in the Official Gazette of the Italian Republic, Supplemento ordinario no. 87, dated April 14, 2003. The text is available in Italian at *www.senato.it/parlam/leggi/deleghe/03070dl.htm*

12 This service provided, as an example, mailing lists or newsgroups organizers.

13 *Trib. Firenze* March 21, 2001, no. 3155.

14 Tribunale (court) of Naples order dated June 14, 2002, in *Corriere Giuridico* 2003 with regard to the unauthorised publication on a website of a copyright protected book and the (denied) liability of the host provider; Tribunale of Macerata, December 2, 1998; Court of Naples, order August 8, 1997, in *Giusizia Civile* 1998, I, 258 ss. With regard to the liability for unfair competition with the author of the unfair competition acts of two ISPs and, specifically, of one who owned the domain name of a website through which unfair competition conduct took place and who exclusively maintained the website; and of another who created and published webpages on behalf of the author.

15 Tribunale of Teramo, December 11, 1997; Tribunale of Naples, August 8, 1996, in Dir. inf e inf., 1997, 970. These courts qualified the ISP as a publisher (*editore*) and the Internet as a newspaper (*organo di stampa*). Consequently, they applied Italian law no. 47 of 1948 on publishing (*legge sulla stampa*) according to which the director and the publishing house are jointly liable, together with the author, for torts made by the author. Against this interpretation Franzoni, *La responsabilità del provider*, in AIDA 1997, 250 ss.

16 Court of Rome, order dated December 11, 1997; Criminal Prosecutor of Vicenza, decree dated June 23, 1998, in Dir. inf e inf., 1998, 821.

17 Court of Cuneo, orders June 23–27, 1997, in *Giur. piemontese* 1997, 493; and October 19, 1999, in *AIDA*, 2000, 809. The Court of Cuneo excluded an *access* and *hosting* ISP's joint liability, together with the one of the owner of a website, for a breach of copyright.

18 Court of Monza, Sez. Dist. Desio, Order May 14, 2001; Court of Rome, order dated March 22, 1999, in *Diritto Informatica*, 2000 an July 4, 1998, in *www.interlex.com,* with regard to the publication of a defamatory information in a newsgroup neither moderated nor controlled by the provider.

19 Court of Bologna, order dated November 26, 2001, in *www.ipsoa.it/ngonline.*

20 An overview on the different interpretations may be found in Sica, Le responsabilità civili, in Tosi (a cura di), Commercio elettronico e servizi della società dell'informazione. Le regole giuridiche del mercato interno e comunitario. Commento al D.Lgs. April 9, 2003, no. 70, Milano, 2004, s.267.

21 This Report was issued according to Article 21 of the Directive and may be found easily on the Internet in the E.U. commission website (*http://europa.eu.int*).

22 In particular, the limitation on liability for hosting in Article 14 covers different scenarios in which third party content is stored, apart from the hosting of websites, for example, also bulletin boards or "chat-rooms".

23 Nevertheless, a scenario in which large scale use is made of injunctions as part of a general policy to fight against illegal content rather than being used against a specific infringement, may raise certain concerns. For example, in 2002, the authorities of North Rhine-Westphalia ordered around 90 Internet access providers to block access to a number of specified sites.

24 See the Court of Cuneo order June 27, 1997, Court of Rome order dated May 17, 1998, quoted by A. Pierucci, "*La responsabilità extracontrattuale del fornitore di servizi telematici*", Padova, 2000.

25 The concept of "time reasonably necessary" may also be found in Directive 1997/66/CE and Directive 2002/58/CE concerning data protection in electronic communications.

26 Legislative Decree of June 30, 2003, no. 196, in force since January 1, 2004 (the so-called "code of personal data protection"), which disciplines personal data protection, harmonised all the existing regulations concerning personal data protection and, among them, the ones contained in law no. 675 of 1996, which enacted in Italy Directive no.95/46/CE dated October 24, 1995 concerning personal data processing. Articles 31–36 of the aforementioned code concerns personal data and system security On this topic see Sica, *Il sistema delle responsabilità*, in G.Comandè – S.Sica, *Il commercio elettronico. Profili giuridici,* Torino, 2001, 236.

27 From time to time and depending on the specific situation, Autorità di Garanzia per le Comunicazioni (administrative authority for communications) e Garante per la protezione dei dati personali (administrative authority for personal data protection) as well as Garante per la Concorrenza e il Mercato (administrative anti trust authority) may be entitled to these powers. See Sica, *Le responsabilità civili*, in Tosi (a cura di), *Commercio elettronico e servizi della società dell'informazione. Le regole giuridiche del mercato interno e comunitario. Commento al D.Lgs.* April 9, 2003, no. 70, Milano, 2003, 286.

28 ISPs who provide "mere conduit" activities are bound to the administrative or judicial authority only if they perform an activity of automatic, intermediate and temporary storage of the transmitted information, directed towards the transmission on the network with a communication and a duration not exceeding the time required.

29

The burden of proof therefore, lies with the provider who must also prove that they acted in accordance with business standards ("con diligenza professionale"), according to Article 1176, paragraph II, of the Italian Civil Code. See Ponzanelli, *Verso un diritto uniforme per la responsabilità degli Internet Service Providers*, in *Commercio elettronico e categorie civilistiche*, a cura di Stanzone e Sica, Milano, 2002.

30 Therefore, with regard to criminal actions, the hosting provider shall only be liable when they have actual knowledge of the illegality of activity; while; with regard to actions consequent to torts, ISPs shall be liable should they have an actual knowledge of the facts, which clearly show the existence of a tort. See Riccio, *La responsabilità civile degli internet providers,* Torino, 2002, 206. The burden of proof re. such knowledge lies with the claimant; while the ISP must prove that they acted according to business standards. See Sica, *Le responsabilità civili*, in Tosi (a cura di), *Commercio elettronico e servizi della società dell'informazione. Le regole giuridiche del mercato interno e comunitario. Commento al D.Lgs.* April 9, 2003, no. 70, Milano, 2003, 295.

31 For a thorough analysis, see Tosi, *Commercio elettronico e servizi della società dell'informazione*, in "Diritto delle Nuove Tecnologie", 2003, pp. 267–348.

  WILR ISSN 1468-4438

32 Cases *Deutsche Bahn v. XS4ALL*, judgment by Gerechtshof te Amsterdam (Court of Appeals), 762/02 SKG, of November 7, 2002, and *Deutsche Bahn v. Indymedia,* judgment by Rechtbank Amsterdam (District Court), KG 02/1073, of June 20, 2002, in the Netherlands (judgments available at *www.rechtspraak.nl*); and *Public Prosecutor v. Tele2 in the EEA-country Norway*, judgment by Borgarting Lagmannsrett (Court of Appeals), 02-02539 M/01, of June 27, 2003. Tele2 was acquitted when the public prosecutor dropped charges against it.

33 Court of Catania June 29, 2004, judgment no. 2286. The text of the judgment is available at *www.altalex.com/index.php?idnot=7548&print=true&idstr=61*.

34 Damages were awarded however, as the claimant did not provide proper evidence of the assumed damage, or of its value.

35 Court of Milan, section V, judgment March 18, 2004, no. 1993, available at *www.altalex.com/index.php?idnot=7076&print=true&idstr=61*.

36 The list was realised automatically, showing the most visited websites, and the party prosecuted did not have the capability to influence the content of the site.

37 Specifically, Articles 600 bis–600 septies of the Italian Criminal Code, introduced by the Law of August 3, 1998, no. 269, against the use of prostitution, pornography and sexual tourism against minors. With regard to Law 269/98 see Buonomo, *Le responsabilità penali*, in Tosi, *Commercio Elettronico e servizi della società dell'informazione*, Milano,, 2003, 343; Resta, *Pornografia minorile: l'anticipazione dell'intervento penale e il difficile bilanciamento tra interessi*, note to Cass. V pen. February 3, 2003, in *Dir. Inf. e Informatica* 2003, s.794.

38 No image or illegal material was published, but only a link to other websites.

39 "Eventual intention" (so-called: *dolo eventuale*).

40 No specific sanction, either criminal or administrative, was introduced by Decree 70/03 as a consequence of the violation of the provisions of Articles 12–15. This choice was made within the provision set forth by Article 20 of the Directive.

41 Some Member States and, specifically, Spain, Austria and EEA-State Liechtenstein and Portugal, already decided to provide for limitations on the liability of providers of hyperlinks and search engines. Spain and Portugal have opted for the model of Article 14 both for search engines and hyperlinks, whereas Austria and Liechtenstein have opted for the model of Article 12 for search engines and of Article 14 for hyperlinks. On this issue see the E.U. Commission's First Report on the application of Directive 2000/31/EC, issued on November 21, 2003.

News

CZECH REPUBLIC

E-Signature Law is Revised to Conform with the E.U. Directive

The purpose of an amendment effective as of July 26, 2004, and published under Act No. 440/2004 Coll,. is primarily to achieve compatibility with Directive No. 1999/93/EC of the European Parliament and the Council on Community Principles of Electronic Signatures.

The amendment introduces a qualified time stamp which shows when the data report existed in a specific time. If the time stamp is appended to the electronic signature, a public administration authority will be informed that the document was filed by electronic means at the time indicated on the stamp.

Another new possibility is the use of an electronic mark for which digital signature technology is used. As opposed to the electronic signature which signals a physical person, a legal entity or an organisational administrative state unit can also designate data with an electronic mark. The anticipated introduction of excerpts from public administration registers at post offices and birth and marriage registers is subject to the electronic marks.

The amendment also regulates the use of electronic registry offices by state administration bodies. An implementing ordinance regulating the activity of electronic registry offices is to be issued by the ministry in the near future.

By Deloitte & Touche, Prague, in association with Havel & Holasek, Prague. Contact Tomas Kucirek by E-mail at tkucirek@deloitteCE.com.

IRELAND

E-Commerce Regulations are Amended

On July 26, 2004 the Minister for Enterprise, Trade and Employment introduced regulations which amend the regulations that implement the Electronic Commerce Directive in Ireland.

The European Communities (Amendment of SI No. 68 of 2003) Regulations 2004 (SI No. 490 of 2004) amend Regulation 21 of the European Communities (Directive 2000/31/EC) Regulations 2003 (SI No. 68 of 2003) (the "Electronic Commerce Regulations").

The effect of the amendment is to clarify who the Director of Consumer Affairs may appoint as "authorised officers" under the Electronic Commerce Regulations. The amendment makes it clear that such "authorised officers" do not need to be from the Office of the Director of Consumer Affairs. Under the Electronic Commerce Regulations "authorised officers" are given wide-ranging powers for the purpose of ensuring compliance with the regulations and also in connection with the investigation of offences. These include the power to search premises; to require the production of information or records; to take copies of records and documents; and to require assistance in relation to the use of any related data equipment.

By Don McAleese, Partner and Head of Information Technology Law Group, Matheson Ormsby Prentice, Dublin.

Intellectual Property

The Regulation of Online Licence Agreements in the U.K.

Paul Barton from City firm Field Fisher Waterhouse examines the fast evolving world of online licences. The author may be contacted by e-mail at paul.barton@ffw.com.

The underlying goal of an online licence agreement is to protect and regulate the use of intellectual property rights ("IPR") in the online material or services being offered through the online medium. Online licences are used to prevent unlawful abuse of IPRs and create the conditions in which website owners can successfully exploit online content.

Background

Earlier this year, the British Phonographic Industry ("BPI") warned that it will sue people who illegally swap music and songs on the Internet. BPI's director general, Andrew Yeates, said that the BPI was hoping to encourage new, legitimate services which would, together with an increased awareness of the legal implications of file-sharing, help to stamp out unauthorised copying.

There has been a huge development in the last year of "legal" music and other media download websites. *Apple* has recently launched its European *iTunes Music Store* while *Napster* have moved from offering a free file-sharing service to one for which the customer must pay a small fee for every song they download.

As a result of a more aggressive stance by the music industry and increased litigation in the United States and throughout Europe, the number of infringing music files available on file-sharing networks fell to 700 million in June 2004 (down 30 percent from the June 2003 peak of one billion files).

Although the music industry has been particularly active in recent years at tackling online piracy, interesting online licensing challenges lay ahead with the imminent arrival of "Internet Television". In the next year or so, we will become accustomed to services such as *TiVo TV* and *Microsoft*'s Internet Protocol Television ("*IPTV*") which, along with other services, will begin to offer a complete online multi-media service. *TiVo*, the pioneers in television services for digital video recorders, already has over 700,000 subscribers and its service and technology revenue for the fiscal year ended January 31, 2003 was over U.S.$60 million.

As audio-visual online service offerings become ever more sophisticated, the holders of the IPR in the products and services being offered over the Internet will want to be sure that their rights are not being abused. There is and will continue to be, the need for a strict regulatory regime in place to control the licensing of such online services.

This article looks at some of the rules that are specific to the licensing of services and products offered over the Internet.

Regulation

It is very important to those people who conduct business through the Internet that the material they make available online is protected. In Europe, the level of protection afforded works made available over the Internet and through e-commerce channels was enhanced and harmonised via the Copyright Directive.[1] In the United Kingdom, the Copyright Directive has been implemented into national law through the Copyright and Related Rights Regulations 2003, which came into force on October 31, 2003 and, through amendment to the Copyright, Designs and Patents Act 1988, has clarified the rights of originators of copyright material to control reproduction and communication to the public by electronic transmission of works.

In addition, any organisation that conducts business over the Internet will want to ensure that the licence agreements under which they offer services or products will adequately protect their IPR while at the same time allowing the user the freedom to get the best use of the website for their required purposes.

The website owner will need to consider the different kinds of content that will be used on the site, such as text, photographs, audio files, video files, software and other kinds of medium. The more interesting and varied the content, the more likely it is that people will visit the site. Each different item of multi-media employed in the website will benefits from different kinds of protection and is governed by different regulation. Below is a summary of the rules in the United Kingdom which apply to possible kinds of content that make up a website.

Text

Text will be protectable as a literary copyright work and possibly also in copyright as a database (section 3 Copyright, Designs and Patents Act 1988). Text may also be protected under EC Directive 96/9/EC on the legal protection of databases (as implemented in this country by the Copyright and Rights in Databases Regulations 1997) by the recognition of a database right. The strength of the database right was confirmed recently following a wide interpretation of the term "database" by Advocate General Stix-Hackl in her opinion in *BHB v. William Hill* (C-203/02). Any text that is distributed through the website will be protected in the same manner as any text appearing on the website as above.

Pictures and Graphics

Pictures and graphics will be protectable as artistic copyright works (section 4 Copyright, Designs and Patents Act 1988).

  WILR ISSN 1468-4438

Such a collection of pictures or graphics may also qualify for copyright protection as a database (section 3 Copyright, Designs and Patents Act 1988) and benefit from protection from the database right as above for text. Any pictures or graphics that are distributed through the website will be protected in the same manner as any that appear on the website as above.

Moving Images

Moving images will be protectable as a film (section 5 Copyright, Designs and Patents Act 1988) and, if comprising drawings (for example, a cartoon or other animation), as an artistic copyright work (section 4 Copyright, Designs and Patents Act 1988). A collection of moving images may also qualify for copyright protection as a database (section 3 Copyright, Designs and Patents Act 1988) and for the database right as above for text. Any moving images that are distributed through the website will be protected in the same manner as any that appear on the website as above.

Music

Musical content on a website is protectable as a musical copyright work (section 3 Copyright, Designs and Patents Act 1988). Lyrics are protectable as a literary copyright work and the recording of the music is protectable as a sound recording (section 5 Copyright, Designs and Patents Act 1988). A collection of pieces of music may also qualify for copyright protection as a database (section 3 Copyright, Designs and Patents Act 1988) and for the database right as above for text. Any music that is distributed through the website will be protected in the same manner as any music that appears on the website as above.

Trademarks and Logos

Any trademarks and logos may be protectable as artistic copyright works (section 4 Copyright, Designs and Patents Act 1988). They may also enjoy registered trademark protection (section 2 Trade Marks Act 1994). Unlawful use of such IPRs could also entitle the rights owner to sue in the tort of passing off.

Layout and Design

The layout and design (or look and feel) of a website may be protectable as an artistic copyright work (section 4 Copyright, Designs and Patents Act 1988). As above, it could potentially be protectable under the laws of passing off or qualify for patent protection (section 1 Patents Act 1977).

Software

Any software that is distributed through the website will be protectable as a literary copyright work (section 3 Copyright, Designs and Patents Act 1988). Such software may also qualify for patent protection (section 1 Patents Act 1977).

Key Components of Online Licence Agreements

The exact content of an agreement is largely determined by the needs and services or products that a website owner may wish to provide. The following is a non-exhaustive list of the types of clauses that website owners may wish to include in their agreement.

Grant of Licence

The website owner must decide what kind of licence they wish to give to the website user. They must consider if the licence needs to be exclusive or non-exclusive, the term of the licence, the scope of the licence and if there needs to be any limits on use.

It is common to see a "non-commercial use" clause in music download sites such as *iTunes* or *Napster*. The owners of these websites do not own the IPR in the music that they are selling online and thus they need to take such precautions. If a website owner wanted to sell a product in which they own all the rights then this clause may be drafted differently. *Microsoft*'s *IPTV* terms and conditions make it clear that the user may not re-distribute any of the services or products.

Parties' Responsibilities

The website owner will need to decide which responsibilities he or she wants to assume in relation to the website. Normally the website owner will be responsible for the accuracy and completeness of the website content. The customer is unlikely to want to take responsibility to review this content (including any user-generated content) for accuracy or to determine whether any of the content may result in any liability towards a third party.

Fee/Payment

The fee or payment structure will depend on the service or product being provided. For an online music provider such as *iTunes*, a one-off payment structure may be appropriate. However, some providers may offer unlimited monthly downloads in return for a monthly fee. Microsoft's *IPTV*, for example, offers a subscription service for its interactive entertainment network. The website owner will have to decide when he or she would like to be paid, how he or she would like to be paid and whether the fees expressed are to be inclusive or exclusive of VAT.

Warranties

In B2B licence arrangements, the licensor will probably have to provide warranty protection to the licensee relating to the content of the website. The user will want assurance that the website does not infringe the IPR of third parties, that its content does not violate any laws or regulation and that its content is not defamatory, obscene, pornographic or anti-competitive. Viruses are becoming increasingly sophisticated and so it is vital that the licence contains a warranty of some sort to cover (to the best of the licensor's knowledge) all viruses including Trojan Horses, worms, time bombs *etc*.

Intellectual Property Rights

This is clearly a very important clause and will require some thought. Much of the hard work will be taken care of with a careful definition of IPR in the definitions clause of the online licence agreement. As the IPR in the online content is likely to be owned or provided by different rights holders, the licence agreement will need to specify the terms on which users and licensees can access the constituent parts and their corresponding IPRs. The owner will also need to consider what happens to the rights in any content that is adapted (where permitted) by the user to suit his or her personal needs. In B2B licence arrangements, the licensee will usually request various

indemnities in relation to potential third party claims over the IPR.

Other Clauses

When constructing an online licence due consideration should be given to including clauses such as liability, term and termination, privacy/protection of personal information, confidentiality, notices, publicity, assignment, entire agreement, third party rights, variation, waiver and jurisdiction/governing law. Some providers will want to include age restrictions and, if relevant, parental consent provisions.

The Privacy and data protection issues always require careful attention and appropriate provisions need to be drafted so appropriate consents are obtained and uses of personal data are properly explained.

Looking Forward

Although the Internet has now been around for many years, it is only in the last few years that website and IPR owners have really started to think seriously about using appropriate legal protection. Perhaps as a result of increased litigation on behalf of the music industry, sites such as *Napster* have had to rethink their service offering and corresponding licence arrangements as they have moved into the "legal" and regulated domain.

However, as the technology becomes increasingly sophisticated, so must the legal framework through which services are offered via the Internet. As we look forward to the next generation of web-enabled content services, lawyers are already revising the necessary online licence agreements to best protect the interests of their client.

1 Directive 2001/29 EC of May 2001 on the harmonisation of certain aspects of copyright and related rights in the Information Society.

Case Report

SPAIN

Court Finds Online Music Platform Guilty of Exploiting IP Rights

Weblisten S.A. v. Emi Odeon S.A.

Provincial Court of Madrid, section eight, July 16, 2004.

Section Eight of the Provincial Court of Madrid has recently upheld the ruling made by the Court of First Instance No. 49 of Madrid against Weblisten, S.A., an online music platform based in Madrid, after the latter was sued by the record company Emi Odeon, S.A. for breach of its intellectual property rights.

The ruling orders Weblisten to compensate Emi Odeon, S.A. for unfair competition by payment of a sum of €16,884, to remove the songs issued by the aforementioned company from its website and to insert a banner on its homepage with the text "Weblisten found guilty of unfair competition".

The representatives of Weblisten appealed against the Court's ruling on the grounds that the Unfair Competition Act had not been breached, claiming that its activity consisted of acts of public communication of phonograms over the Internet, as undertaken by radio stations, and that it may not be understood accordingly that there is a distribution of copies, although copies may be obtained of the broadcast.

The Provincial Court ruled that Weblisten was proceeding unfairly and in breach of normal market procedure on the grounds that the replication of services of a third party is unfair when it involves an undue exploitation of another's efforts.

Weblisten is an Internet portal that allows users to listen to songs without payment of any kind. It also allows user to download tracks in MP3 format, with prior payment of a fee and/or purchase of a voucher.

The portal states that no permission is required from the holders of the copyright, as their songs are used in the public communication of the musical pieces and it is not therefore, liable for the subsequent actions of the users.

According to the Spanish Copyright Act of April 12, 1996, making music available for listening constitutes an act of public communication. Furthermore, if users accessing the website are allowed to download the music onto their hard drive, enabling it to be reproduced on their own computer (*i.e.*, the loading or storage of digitalised material on the computer's ROM) the right to reproduction is being exploited and thus requires the express permission of the holders of the aforementioned rights.

The lawfulness or unlawfulness of the activity of a software provider that enables music files to be made available to Internet users, and the effect that this may have on the authors, performers, agents and the record industry lies at the heart of the debate involving international legal doctrine.

So far, the French Government, record companies and Internet service providers (ISPs) have reached an agreement whereby access to the Internet may be withdrawn for all those users who download music by this means without due payment.

By Ignacio Temiño Ceniceros, Abril Abogados, Madrid.

  WILR ISSN 1468-4438

Legislation & Guidance

United Kingdom: The Computer Misuse Act 1990

As reported previously in World Internet Law Report, the report of the public inquiry held by the All Party Internet Group (APIG) into the Computer Misuse Act 1990 (CMA) – the United Kingdom's primary legislation dealing with "cybercrime" – was published in June 2004. Liz McSweeney of City law firm Field Fisher Waterhouse takes an in-depth look at APIG's recommendations concerning the CMA and provides a brief overview of other U.K. legislation that can and should be used in order to combat the ever increasing threat of so-called "cybercrime".

When APIG announced its intention to undertake a review of the CMA earlier this year, the news was greeted positively, if a little cautiously, by its critics. In their view the CMA, which had been passed in the days when the World Wide Web was only a scientist's project, was woefully inadequate in the face of modern on-line computer crime. It was argued for instance that the 1990's language of the CMA meant that it was difficult to apply it to modern technologies or to the increasingly ingenuous uses made of computer systems and networks in order to commit crime. In particular it was felt that a specific offence relating to "denial of service attacks" (DOS: the repeated and deliberate targeting of a computer network, for example a company's website, in order to overload it and cause it to crash, therefore preventing its use by legitimate users) should be incorporated into the CMA as arguably, such offences could not currently be prosecuted under the CMA. APIGs enquiry was the end-result of several years of relatively intense lobbying on such issues.

Its remit was to consider whether the CMA was broad enough to cover modern cybercrime; whether its generic definitions should be updated to address new technologies (*e.g.*, mobile phones, palmtops); whether there were any "loopholes" in the Act that needed plugging; whether the penalties under the CMA served as a sufficient deterrent to cyber-criminals, and whether the Act needed revision in order to meet international treaty obligations.

APIG's Recommendations

After considering both oral and written evidence submitted to it by U.K. businesses, those involved in IT security and representatives of the Government, the APIG delivered a comprehensive report containing sixteen separate recommendations. It advocated not only specific amendments to the CMA itself but also various other measures that the Government and other stakeholders, should be taking in its overall fight against cybercrime. The key recommendations are summarised as follows.

The CMA Should Retain its Technology Neutral Language

The language of the CMA has often been described as inappropriate. Terms such as "data" and even the word "computer" itself are left undefined. This has led to the criticism that modern, sophisticated devices such as mobile phones (and therefore the use of mobile phones to commit crime), are simply not covered by it. The APIG concluded, however, that there was no evidence that the CMA's definitions, or rather lack of definitions, in any way impeded the bringing of prosecutions under it. On the contrary, the APIG determined that the advantage in not defining key terms was that the CMA was able to "move with the times" and was not constrained by terminology that would inevitably become outmoded, possibly even obsolete. The APIG's recommendation was therefore, that the Government should resist calls to incorporate more specific definitions into the CMA. It should instead,

> "continue with a scheme whereby the terminology used in the CMA would be understood by the courts to have the appropriate contemporary meaning".

A Specific DOS Offence Should be Created

As noted, the critics of the CMA have repeatedly complained that the three basic categories of offence created by the CMA are not easily applied to modern cybercrime. Currently, the CMA imposes criminal sanctions for unauthorised "access to", or "modification of," computer material. Additional sanctions are imposed where such unauthorised access takes place as a preliminary to the commission of another crime (for example, blackmail).

Many have argued however that DOS attacks in particular fall outside the scope of these three basic offences. A DOS attack can be carried out by a variety of methods. It may for example, take the form of thousands and thousands of hits being simultaneously made on a website, which by overloading its systems, will eventually cause the site to crash. Arguably, this constitutes neither unauthorised access to, or unauthorised modification of computer material. Consequently, it has been claimed that the CMA fails to criminalise such attacks. Critics of the CMA have further sought to substantiate this claim by pointing to the fact that despite the ever-increasing number of DOS attacks (according to some studies there are now over 4000 separate attacks of varying levels of severity taking place each week), so far there has been only one DOS-related case brought under the CMA (*R v Caffrey*) – even then the defendant was acquitted.

Understandably, the CMA's critics have tended to come from within the business community in the United Kingdom and from IT service providers, frustrated at the apparent lack of progress being made by the police and the courts in prosecuting DOS attacks. In contrast, the opinion

expressed by the Government, and by many lawyers specialising in computer-related crime has tended to be that the section 3 offence (unauthorised modification of computer material) is capable of being applied to DOS attacks, it being a question of the courts taking a common sense view in interpreting the existing legislation and applying it to such attacks.

In its report, APIG gave careful consideration to, and seemed for the main part to support the views put forward by the Government and other supporters of the CMA. It is noted for instance that the defendant in the Caffrey case was acquitted because the jury did not believe that he was responsible for launching the attack which had rendered the U.S. Port of Houston's computer systems temporarily inoperable, and that, significantly,

> "there does not seem to have been any attempt by the defence to have the case thrown out because the denial-of-service activity was not covered by the CMA".

Nevertheless, whilst accepting that the existing CMA offences already covered many forms of DOS attacks, APIG conceded that certain types of attack might not be caught. Therefore it concluded that overall there would be "significant value" in adding an explicit offence to the CMA to deal with such attacks, it being "undesirable to have the legality of an attack depend upon the exact mechanism used to launch it". APIG expressed serious reservations about how such an offence would in practice be drafted, not wishing to criminalise those behind instances of denial of service who are not motivated by criminal intent *per se* – such as "cyber-protesters". However, it was felt that the benefits of sending a clear message to the police, the CPS and the courts, as well as to cyber-criminals themselves, that such attacks were taken seriously, outweighed all other concerns.

Government Should Take Further Steps to Educate the General Public on the CMA

Despite recommending the inclusion of a specific DOS offence to deal with DOS attacks, APIG rejected calls for any further extension of the scope of the current CMA offences, stating that it already quite clearly covered "hacking" (unauthorised access) and the distribution of computer viruses (unauthorised modification of computer material), as well as arguably most forms of DOS attacks. It flatly rejected the view that the CMA failed to address modern cybercrime, stating that it "was not as ineffective and tightly drawn as some … seem to believe". Instead, APIG blamed the perceived failure of the CMA to deal with modern cybercrime on "widespread ignorance of current law". As a result it recommended that the Government take steps to provide guidance on the provisions of the CMA for the general public (for instance, by publishing educational material on the CMA on the Home Office website).

Other Relevant Criminal Legislation Should be Amended to Deal with Specific Cybercrimes

It was further recognised that the CMA should not be used to deal with all crime committed online or with the aid of a computer. For example, it was recommended that computer related crime involving fraud (such as "phishing", where website users are tricked into visiting a dummy version of a legitimate site and into disclosing security credentials) should be dealt with under separate legislation. The Law Commission's proposed Fraud Bill, (published in 2002 as part of its report on fraud law reform) contained, for instance, a specific offence of "false representation", which would "squarely address phishing". Again, noting the Government's recently announced consultation on fraud law reform, APIG recommended that it move quickly to bring a new Fraud Bill before Parliament, specifically covering fraud-related computer crime (which is only to an extent already dealt with under existing criminal law).

APIG also identified a potential "loophole" in the Theft Act 1968, relating to "theft of data" (for example stolen customer databases). Currently the Theft Act 1968 requires that there be a "permanent deprivation" of an article from its owner for a theft to occur. In the case of the theft of data held on a computer, such data would normally be copied, rather than "removed" from the computer altogether – as such, no "permanent deprivation" occurs. Ostensibly, the Act would not apply to such theft (although if the "access" to the material in itself was "unauthorised" it should be caught by the section 1 CMA offence of unauthorised access to computer material). In order to close this potential loophole however, APIG recommended that the Law Commission moved to produce a final report on its consultation paper on "Misuse of Trade Secrets" (which in APIG's view would cover such theft), thereby providing a "suitable framework" to adequately criminalise data theft.

"Best Practice" Procedures Needed for Monitoring Security of Customers' Machines

This recommendation was made in response to a number of proposals for the section 3 CMA offence (unauthorised modification) to be amended. One such suggestion proposed by Microsoft (UK) was that an exemption should be made to section 3 to allow a software vendor to alter an end-user's system, for security purposes, on the basis of "informed consent, albeit on an 'opt-out' basis." APIG swiftly dismissed this, wary of allowing software vendors "carte blanche" to alter end-user's systems, effectively without consent (an opt-out consent being a "negative" as opposed to express form of consent, in that in the absence of a person's specific objection to a proposed course of action, he or she is deemed to consent to it). Instead APIG consider that such an issue should be dealt with in the contract between the end-user and the software vendor; in which case the access and modification would be authorised; it was accordingly unnecessary to revise the provisions of section 3.

The BT Group also suggested that section 3 be amended to address the extent to which a system owner could take "active measures" to secure their systems. This was similarly dismissed on the grounds that such issues should be dealt with in the contract between the ISP and the end-user. The CMA would not be amended where other, more appropriate methods of obtaining the necessary consents were available.

APIG further rejected calls for the failure by an end-user itself to adequately protect its computer systems (on the basis that such failures put the entire online community at

risk) to be criminalised under the CMA. Seeing danger in introducing criminal liability into an already "complex technical area" of computer security, APIG concluded that many security breaches resulted from "systematic problems with computer software" rather than from computer owners "recklessly misconfiguring their machines". However, it being clear that many Internet users were (quite innocently) operating insecure systems, APIG saw considerable benefit from the proactive scanning of vulnerabilities by ISP's. Accordingly, it recommended that the ISP industry produce common guidance on how such proactive scanning could be carried out lawfully.

The Length of Sentences under the CMA Should be Increased

The current maximum sentences imposed by the CMA vary from six months imprisonment and/or a fine (for the section 1 offence of unauthorised access) to five years and/or an unlimited time for the remaining offences (which arguably deal with more serious criminality). APIG considered various arguments put forward by respondents to the enquiry as to why these sentences should be increased (including that it would make it easier to obtain a warrant and to extradite alleged offenders based outside the United Kingdom).

Whilst rejecting such arguments that sentences be increased effectively to improve the "expediency of the investigatory process", APIG did concede that the tariff for the section 1 offence should be increased to a maximum of two years imprisonment, bearing in mind the considerable financial loss that a company could suffer as the result of its computer systems being compromised.

APIG concluded that it was important to "send a clear message to society" that "hacking offences" were taken rather more seriously now than they were "in 1990". APIG did not recommend any increase in the section 2 and 3 tariffs. It is understood however that the Home Office is currently reviewing the tariffs for these offences, in order to determine whether they are in line with equivalent criminal offences in other legislation.

International Treaty Obligations: The Home Office Should Resist Calls to Criminalise "Hacking Tools"

The so-called Cybercrime Convention is the product of joint collaboration between the Council of Europe, the United States, Canada, South Africa and Japan. It aims to facilitate cross-border investigation and prosecution of international cybercrime by producing a common policy on the misuse of computer networks and data for illegal activity (including terrorism). The Convention has, to date, been signed by 38 countries but ratified by only five of those (Albania, Croatia, Estonia, Hungary and Lithuania). Meanwhile, it is reported that the U.K. Government hopes to be in a position, by fully incorporating the Convention into U.K. law, to ratify it by 2005.

In its report, APIG focused on Article 6 of the Convention (Misuse of Devices) which effectively imposes criminal liability on the production, use and supply of computer passwords, access codes or other such data which would enable the unauthorised access of a computer system by someone intent on committing a crime (essentially this covers the existing CMA offences). However, APIG expressed concern over the effect that imposing criminal sanctions on the use of "hacking tools" would have upon their legitimate users (*e.g.*, security professionals and systems administrators). How would the proposed office deal with the difference between such legitimate and illegitimate use?

With this in mind, and noticing the Home Office's intention to address the illegal use of such devices in its review of fraud law, APIG recommended that for the time being the Government continued to resist cause for the criminalisation of such tools under Article 6 of the Convention.

On the basis that its remit was to consider the desirability of amending the CMA and that most of the conventions' provisions were already incorporated into U.K. Law, APIG went no further in discussing the desirability of the U.K. Government ratifying the controversial Convention. However, it should be noted that the Convention has drawn criticism from civil rights campaigners on the basis that it may be used by repressive regimes to investigate the actions of individuals which are not considered crimes elsewhere in the world, and effectively to spy on select groups of people *e.g.*, ethnic minorities. The debate on the Conventions looks set to continue.

Analysis of the APIG Report

Overall APIG's conclusion was that the CMA is adequate and capable of being used to combat modern cybercrimes (or at least those involving unauthorised access to modification of computer material). It flatly rejected the view that the CMA is "past its sell by date" or that its broad and generic language needs updating. Instead the Courts should continue to adopt a commonsense view of the CMA in applying it to modern cybercrime.

Much of the report in fact focused on the view that the CMA is not "a one size fits all" piece of legislation. As with criminal law generally, theirs was a vast area of other legislation under which cyber-criminals could and should be prosecuted. As such, APIG supported current initiatives by the Home Office to review the law as fraud and theft in order to ensure that computer-related fraud and the theft of data were covered.

Reasons why the CMA appeared to its critics to be under performing in the Government's fight against cybercrime related to a lack of awareness of its provisions. Again, the lack of prosecutions under the Court were more to do with the inadequate resources of the police and CPS, and a general unwillingness to prioritise such crime. It was not because modern cybercrime could not be prosecuted successfully under the CMA.

The APIG's findings will obviously please some (the Government, for instance) and no doubt further frustrate its critics who have for so long firmly laid the failure of the police to prosecute cybercrime at the CMA's door. Whether the Government, the ISP industry and other stakeholders identified in the report will implement its recommendations remains to be seen. In the meantime those who would like to review APIG's report in more detail can find a copy of it on the APIG website at *www.apig.org.uk*.

Privacy

United Kingdom: The Legal Implications of Gmail

By Eva Wong, an Associate with Coudert Brothers. The author may be contacted on tel. +44 (0)20 7248 300 or by e-mail at wonge@coudert.com

When Google revealed plans on April 1, 2004 to launch its own free web-based e-mail service, a number of the proposed new services raised unprecedented legal challenges. Concerns relating to Gmail are generally relevant to all web-based e-mail providers, but the problems are exacerbated by the proposed scale and increased functionality of Gmail.

What is Gmail?

Gmail's service includes:

- Google search technology enabling a user to search their inbox in a way similar to using a Google search on the Internet for relevant key words.
- 1GB storage, enabling a user to create a permanent centralised archive of messages which is substantially more than other e-mail providers (for example, at the time that Gmail was announced, Hotmail only offered 2MB – this is soon to be increased).
- AdSense technology used in scanning e-mail text to create targeted banner adverts, similar to the banner ads which sometimes currently appear and are based on a text search on a webpage.

Relevant U.K. Legislation

The U.K. law on Internet-related privacy is derived from the European Union, and in considering Gmail, the following U.K. implementing legislation is applicable:

- The Data Protection Act 1998 ("DPA") – implementing Directive 95/46/EEC on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("the "Directive").
- Privacy and Electronic Communications (EC Directive) Regulations 2003 ("Privacy Regulations") – implementing Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector.

DPA

The DPA outlines Eight Data Protection Principles (the "Principles") with which a data controller (which Google would be in relation to U.K.-based Gmail users) must comply to ensure that its data processing is lawful. The Principles generally reflect the requirements of the Directive and there are similar requirements in other E.U. Member States. The Principles generally require that personal data must be collected fairly, for specified, explicit and legitimate purposes, and processed in a fair and lawful manner in accordance with those stated purposes. Processing must take place on one of the legitimate grounds such as consent, contract, legal necessity or on a balance of interest. The individual must be informed about any intended transfer of data to third parties and given the right to object to their data being used for direct marketing purposes, and have a right to access, rectify, erase or block the data related to them. This is usually done by providing an e-mail user with a privacy statement or including these terms as part of the contract.

Google will meet these requirements by obtaining the Gmail user's blanket consent, and informing the Gmail user of Google's policies as a precondition to use of the service. However, some aspects of Gmail may be seen as potentially threatening the protection granted in principle by the Directive. As the Directive was conceived before these latest technological developments, consent given by a Gmail user may not be sufficient where it undermines fundamental individual rights.

Privacy Regulations

The Privacy Regulations generally govern commercial communications and direct marketing to individual e-mail subscribers, and in particular, attempt to regulate unsolicited e-mail communications. In addition, there are also provisions relating to the use of cookies by website operators. Cookies are the small pieces of information transmitted along with a webpage that may be temporarily or persistently stored by the web browser, as used by many e-mail service providers. Depending on the "*path*" (typically the domain name, *e.g.*, ".google.com") of the cookie sent by the webserver software, the browser will send the cookie back to the webserver during subsequent browsing, thus identifying to the webserver software a particular user or browsing session. Google software can therefore collect information on every user, search term, IP address, unique cookie id number and time-date stamp.

The Privacy Regulations require that where cookies are used, certain information must be given to the individual. Google and Gmail comply with this requirement by providing information relating to their cookies in the Google and Gmail "Terms of Use", which also form part of the agreement with the user. In practice, a user does not have a realistic choice: if the user does not consent to the cookie, only a limited service would be available. The use of cookies by Google for Gmail also raises new privacy concerns which are described below.

Particular Issues

Security

The Seventh Principle of the DPA states that appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against unauthorised accidental loss or destruction of, or damage to, personal data (Sch 1, Pt I, para 7). The level of security to be offered depends on the nature of the data. As Gmail may contain personal data of a highly private and sensitive nature, the level of security to be provided by Google must be of a very high standard.

Google provides for the Gmail service a number of security protections, such as the use of encrypted access and encrypted password login. In addition, Gmail blocks the transmission of executable files which may contain viruses

or spyware, and does not load external images by default to prevent "web bugs". Further, when an individual clicks on advertisement links on a given webpage, certain "referrer" header information is sent to the linked website. Google promises to reduce the transfer of such "referrer" information in Gmail, preventing other websites from knowing that the individual was referred by clicking on a link in Gmail.

However, for every privacy enhancing and security strengthening measure which Google puts in place, there is an equal amount of technology capable of defeating such efforts. The MyDoom worm attack on Google as recently as July 24, 2004 shows that Google is not invulnerable from virus attacks. The ability for hackers to hijack high profile websites was demonstrated at the beginning of September 2004 when police in Germany arrested a 19-year old youth for hijacking the Ebay Germany website, and the youth admitted that Google was one of several other websites targeted.

Finally, human intervention is a risk that few companies can fully protect themselves against. A recent example is the theft of personal data from Acxiom, one of the world's largest database companies, by a spammer in Florida. The personal e-mails stored on Gmail are equally susceptible and the potential harm is exacerbated by the amount capable of being stored on Gmail.

Retention

The Fifth Data Protection Principle of the DPA requires that personal data should not be kept for longer than is necessary for the purposes for which the data was collected and further to which they are processed.

It is standard practice for e-mail providers to keep back-up copies in case there is a technical error or systems failure. However, privacy advocates are concerned because Gmail's increased storage size increases the risk of misuse. Retention of such a large amount of data should be more limited in time and no longer than necessary for the purpose bearing in mind the Seventh Principle of the DPA. Furthermore, concerns have been raised as to the retention of e-mails after deletion or the termination of a Gmail account. Gmail states that, "We will make reasonable efforts to remove deleted information from our systems as quickly as is practical". However, this does not set a clear time frame, and compliance with the Fifth Data Protection Principle would require that deletion of e-mail or termination of the e-mail account should be followed by removal from the system as soon as possible.

Interception of Communications

Privacy advocates have expressed concerns that certain technical aspects of Gmail may encourage greater encroachment on personal privacy by the state. Increased storage space and retention of large volumes of personnel data, application of content searching technology to e-mail, and collection of personal data through cookies have raised fears of possible direct governmental interference with Gmail accounts.

The DPA provides certain exemptions from full compliance with its requirements where it is necessary to safeguard national and public security, defence and investigation of criminal offences (s.28 and s.29). However, Gmail's Privacy Policy seems vague as to when it would make disclosures of personal e-mail to governments, and privacy advocates are concerned that Google will co-operate without sufficient challenge to governmental requests, thereby inhibiting the protection granted by national civil liberties laws.

Advertising

Google's extension of Adscan technology to Gmail to provide targeted banner advertisements has raised controversy. Adscan allows computers to scan the text on a given page, perform a mathematical analysis on it and match it to ads in Google's extensive database. This is an automated process in which no humans are involved. The adverts and links to related pages only appear alongside the message that they are targeted to and are only seen by the Gmail user each time they look at that particular message. There is no illegality in this process, as Gmail's processing in creating the targeted banners is made clear and apparent in Gmail's policies, with which the Gmail user has consented.

A complaint was made by Privacy International, a London-based privacy rights organisation, to the Information Commissioner's Office, the U.K. regulatory authority for data protection. This complaint does not challenge the legality of the type of advertising but expresses concern that Gmail may set a precedent which is,

> "likely to lead to a global trend to greater U.S.-based centralisation and storage of personal e-mails and a more comprehensive linkage between content and advertising".

The Information Commissioner's Office has informally states that provided Google makes it clear to Gmail users how their e-mail will be scanned, it would not be breaking any legislations but "until Gmail is up and running, though, we can't be certain".

Cookie Correlation

Part III of the DPA, and specifically the First and Sixth Data Protection Principles, create an expectation of informational self-determination to individuals in the United Kingdom. This includes the right to know what kind of information is kept about them, how it is used, who can see it, how it is protected, how it can be altered if incorrect, and that it will not be disclosed to third parties. There is some concern that these rights are threatened by the use of personal information collected by Google through cookies on the Google search engine and Gmail accounts.

In the case of Gmail whose domain is "gmail.google.com", cookies set by "www.google.com" with a path of ".google.com" are also sent to "gmail.google.com" and vice versa. The decision to have Gmail operating under the domain "gmail.google.com" is directly responsible for the technical possibility of correlating a user's search behaviour with their e-mail and personal data.

When an individual signs up to Gmail, they must submit their personal information. Gmail then assigns a cookie ID to the individual's e-mail address. Where the individual already uses Google, their cookie ID and IP address will already be known to Google, the creation of the Gmail account therefore provides the missing link between the individual's search history and their personal e-mail

address. There is no advertising or privacy legislation which would currently prevent Google from correlating such information, and Gmail has not denied that it does not intend to do so in future.

Comment

Google's proposed Gmail service has clearly raised a number of privacy and security issues. Privacy advocates have raised public awareness and submitted their opinions to the relevant authorities. Google has considered amending its privacy policy and terms of use, but the authorities have yet to make a formal response to this interesting and dynamic debate.

News

UNITED STATES

FTC Backs Anti-Spam "Bounty System" That Rewards "High-Value" Information

A federal programme that rewards individuals with "high-value" information about possible violations of the CAN-SPAM Act would be helpful to the Federal Trade Commission in its enforcement of the statute, the commission said in a report released on September 16, 2004.

The FTC was required under CAN-SPAM to conduct a study and report to Congress on the potential effectiveness of a "bounty system" for tracking down spammers.

The report concluded that the individuals most likely to provide the commission with the kind of information it needs are whistleblowers or insiders – those who are personal or business associates of spammers. The commission said the reward should be as high as $250,000, in some cases, to give such individuals a sufficient incentive to come forward.

The commission's report does not necessarily recommend the creation of an anti-spam bounty system, but it lets Congress know that such a programme has the potential to work, if designed properly.

Congressional Proposal Led to Study

"The Commission does not believe that the vast majority of consumers who are now forwarding 300,000 pieces of spam daily to the FTC spam database are likely to be a good source for such information", the report says. "Nor does it believe that persons with above-average skills and knowledge relating to Internet technology – the legions of so-called 'cybersleuths' that advocates of a bounty system envisioned – are likely to be a good source of such information."

Senator Jon Corzine (D-N.J.) is among those in Congress who support an anti-spam bounty system. Last year, Corzine introduced legislation that would create one. The provision in CAN-SPAM directing the FTC to study the issue was part of a deal worked out with him.

"There is no single magic bullet in the battle against spam, but we've made so little progress to date that we can't afford to leave any reasonable approach untried", Corzine said in a statement. "I'm hopeful that Congress now will authorize the FTC to move forward and at least see if providing monetary rewards can make a difference."

Corzine said the FTC's report includes "many helpful suggestions".

The commission's report notes that insiders or whistleblowers are more likely to know a spammer's identity and would be "best situated to possess information about the extent of the spammer's unlawful activities".

> "These persons can include current and former employees or associates with whom the spammer has a business relationship, or family and friends with whom the spammer has a personal relationship", the report says.

The commission noted that certain third parties, such as banks, payment processors, and Internet service providers, possess many of the critical pieces of information needed to help the government catch spammers, but such third parties would likely be unable or unwilling to provide this information to private citizens, such as cybersleuths, who have no subpoena power.

Powerful Disincentives

Such evidence is readily available to insiders, the commission said, and they would not need a compulsory process to obtain it. However, the report notes that insiders could be discouraged from coming forward by a number of "powerful disincentives", including:

- uncertainty over whether information submitted actually will be used by the government, and whether it will result in a successful legal proceeding;
- fear of losing a lucrative stream of income;
- fear of incurring personal legal liability; and
- fear of personal retaliation.

"The Commission is unable to establish with any degree of certainty the dollar amount that might be high enough to overcome these countervailing considerations, but believes that reward amounts in the range of $100,000, and in some cases as much as $250,000, are reasonable estimates", the report says.

Other Recommendations

Other guidelines provided by the FTC include:

- To discourage "disinformation," it should be specified that it is unlawful to provide false information in connection with the reward system.
- To dispel fear of exposure leading to loss of income or retribution, informants' identities should be protected, allowing them to remain anonymous, whenever testimony is not necessary for case prosecution.
- To prevent misunderstandings and "pointless haggling" with potential informants, it should be explicitly stated that the FTC cannot grant immunity.

"While including these elements may not guarantee that a reward system will achieve its purpose, the FTC believes that absent these elements, any reward system would likely fail", the report says.

A copy of the report is available at *www.ftc.gov/reports/rewardsys/040916rewardsysrpt.pdf*.

Security & Surveillance

EUROPEAN UNION

Cybercrime Experts to Start Work on E.U.-Wide Data Retention Standards

Cybercrime experts attending an international conference on September 15–17, heard that the 25-nation European Union will soon start work on E.U.-wide rules on controversial Internet data retention standards for the purpose of combating crime and terrorism.

Roger Holla, an official in the Information Society directorate of the European Commission – the European Union's executive arm – confirmed to *WILR* that national representatives will meet on September 27–28 to begin discussions on a draft published just before the union's summer legislative recess.

Ahead of the discussions, the directorate is holding a public consultation hearing in Brussels on September 21.

In a joint submission to the hearing, two campaigning groups, London-based Privacy International and the European Digital Rights initiative (EDRi), have criticised the draft as "invasive, illusory, illegal, and illegitimate."

The Legislative Draft, A Joint Initiative By France, Ireland, Sweden, And The United Kingdom, Has Been Framed As A Framework Decision, A Legislative Act By Which E.U. States Would Agree To Align Their Criminal Laws On Data Retention. The Elected European Parliament Would Be Consulted On The Draft, But The E.U. Council Of Ministers, Representing National Governments, Would Have The Last Word.

The legislation would require states to ensure that data is retained "for at least 12 months and not more than 36 months following its generation".

Thorny Subject

Andy Letherby, representing the U.K. National High Technology Crime Unit, told *WILR*, "This is a thorny subject. Some E.U. states require [Internet service providers] to retain transmission log files for a certain period. Others prohibit the practice outright. Yet others require ISPs to retain the logs, but stipulate that they can only be accessed with official authority, even by the ISPs themselves."

Work on the draft is being pushed ahead by the Dutch government, current holders of the rotating presidency of the Council of Ministers.

Taco Stein, a prosecutor in the Dutch National Prosecution Service, told *WILR*, "There's a widely held belief that E.U. law on the protection of personal data, Directive 2002/58, prohibits the retention of data except for the purposes of billing".

> "In fact, Article 15 (1) of the Directive permits retention for a limited period when this is considered 'a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (*i.e.*, state security), defense, public security, and the prevention, investigation, detection and prosecution of criminal offenses or of unauthorized use of the electronic communication system [...]'."
>
> "In the Netherlands, we adopted a graduated system under which investigators can obtain basic subscriber data for the purposes of identification in a routine criminal investigation. Traffic data can be sought in more serious, indictable offenses, and for the most serious crimes, access to content data can be sought on the authority of a judge."

The four states behind the E.U. initiative argue that many governments have used the Article 15 provisions to introduce divergent, national procedures, and that the differences are hampering cross-border investigations.

The proposed decision would apply to stored data generated by the full range of communication infrastructures, architectures, and protocols.

Plans Reported at Conference

The E.U. plans were reported at an international conference on cybercrime staged by Europe's other main international organisation, the 45-nation Council of Europe (CoE). The Strasbourg-based CoE brokered the 2001 European Cybercrime Convention – the world's first legally binding treaty on Internet crimes, which came into force on July 1, 2004.

In the conference discussions, 180 cybercrime specialists from 50 nations including the United States, reviewed progress with the Convention, a treaty that allows limited data retention.

To date, the convention has been signed by 32 nations and ratified by eight. Speakers predicted that the pace of ratifications will accelerate as CoE member states complete time-consuming procedures for amending national legislation.

Kevin McNulty, representing the U.K. Home Office (interior ministry), told *WILR* that British ratification of the convention would involve amending at least three laws covering police powers and the investigation of crime. The changes are the subject of an ongoing consultation procedure, and to date no parliamentary time has been set aside for the process, McNulty said.

The CoE envisions that the convention could be in force across 24 nations by the end of 2006.

Under the convention, states must criminalise computer-related crimes involving illegal access, fraud, forgery, child pornography, and infringements of copyright and related rights. Further provisions cover search and seizure, cross-border co-operation investigations, preservation and disclosure of data, and extradition. The treaty is silent on more recent problems such as spamming

and spyware, although CoE experts suggest that some of these techniques are covered by convention prohibitions on "illegal access."

After presidential elections, Congress plans to act on a recommendation by President Bush that the United States should ratify the treaty. The Senate Foreign Relations Committee June 17 examined the recommendation.

Ratification of the treaty by the Congress is supported by, among others, the Information Technology Association of America (ITAA). ITAA President Harris N. Miller argued in a recent statement that only through ratification of the treaty can an international approach to fighting cybercrime be effective. According to the ITAA, "Ratification of the Convention on Cybercrime would minimize obstacles to international cooperation that currently impede U.S. investigations and prosecutions of computer-related crimes".

A priority of the Cyber Security Industry Alliance, an industry group with members such as Symantec, is to pursue ratification of the treaty.

Meanwhile, the Electronic Privacy Information Center, a public interest group based in Washington, opposes ratification of the treaty, on grounds that it was drafted in secret and does not adequately safeguard privacy. "We object to the ratification ... because it threatens core legal protections, in the United States Constitution, for persons in the United States. The treaty would create invasive investigative techniques while failing to provide meaningful privacy and civil liberty safeguards", the group argued in a letter, dated June 17 to Senate Foreign Relations Committee members Richard G. Lugar (R-Ind.) and Joseph P. Biden (D-Del.).

Other States Sign

The convention, claimed to be the world's first legally binding treaty on cybercrime, has also been signed by non-European states including Canada, Japan, and South Africa.

CoE Director General of Legal Affairs, Guy de Vel hailed a decision in April by the attorneys general of the member states of the Organization of American States to recommend their governments to accede to the Convention. The Asia-Pacific Economic Cooperation (APEC) bloc already had recommended member states in 2002 to align their laws with the Convention, he said.

The CoE convention's limited provisions on an expedited preservation of stored computer data requires states to adopt procedures under which the preservation of data, including traffic data, can be ordered for up to 90 days, in order to identify the ISPs and the path through which the communication was transmitted. But Guy de Vel commented that it would be possible to amend the convention by a further protocol.

The CoE already has agreed to cover the issues of race hate and xenophobia on the Internet through a separate protocol, to allow the United States to ratify the main text without interfering with U.S. constitutional rights of free speech.

Dutch representative Prof. Henrik Kaspersen, who helped frame the CoE convention, pointed out that the highly controversial E.U. data retention proposals would apply only within the European Union. Non-E.U. states party to the convention would be free to maintain the lesser data retention rules laid down in the convention, or to adopt any future protocol aligned with the E.U. legislation.

Resistance to the E.U. proposal is expected in several European states.

Wolfgang Schreiber, an investigator from Germany's federal law agency (BKA), lamented that his government had declined to introduce data retention provisions in telecommunications legislation adopted over the summer.

More information about the CoE conference and the Cybercrime Convention is available at *www.coe.int*. The legislative draft by France, Ireland, Sweden, and the United Kingdom is available at *http://register.consilium.eu.int/pdf/en/04/st08/st08958.en04.pdf*. The EPIC letter to the Senate Foreign Relations Committee is available at *www.epic.org/privacy/intl/senateletter-061704.pdf*.

UNITED STATES

NIST Plans IT Security Checklists from Public and Private Organisations

The National Institute of Standards and Technology has issued a draft plan for developing security configuration checklists for information technology products aimed at helping federal agencies and others reduce cyber vulnerabilities.

Developed under the Cyber Security Research and Development Act 2002, the NIST security configuration checklists programme will cover a wide array of IT products, including operating systems, database systems, web servers, e-mail servers, firewalls, routers, intrusion detection systems, virtual private networks, biometric devices, smart cards, mobile devices, telecommunication switching devices, and web browsers.

Under the proposal, government agencies such as National Security Agency as well as NIST-approved IT vendors and checklist authors will submit to NIST checklists that offer instructions for securing IT hardware or software in different settings. NIST notes that computers used in financial institutions that handle highly confidential information would need a higher security configuration than those used at homes.

NIST has produced draft checklists for the Microsoft Windows 2000 and XP Professional operating systems and expects to post more checklists, beginning this winter at *http://checklists.nist.gov*.

NIST released the draft checklists document on August 12, 2004. Comments are due by September 30, 2004 and may be sent to checklists@nist.gov.

The text of the draft plan is available at *http://checklists.nist.gov/SP800-70-DRAFT.pdf*.

Review

Governing the Internet: Recent Challenges for ICANN

By Kate Ellis, an Associate in the Manchester office of Eversheds LLP. The author may be contacted at: kateellis@eversheds.com

Since its incorporation in 1998, the organisation appointed by the U.S. government to have responsibility for the management of key aspects of the Internet, the Internet Corporation for Assigned Names and Numbers (ICANN), has faced intense scrutiny from the Internet community. During 2002, in the face of substantial criticism about its role, accountability and responsiveness to Internet stakeholders, a debate took place about ICANN's future. Its performance was debated in several circles: the Internet community, the U.S. Senate and within ICANN itself. The debate resulted in ICANN's "Blueprint for Reform" in which ICANN identified significant areas of reform. Around the same time, the U.S. government narrowed the scope of ICANN's role.

Whilst ICANN has taken steps to reform since 2002, it has been hampered in its efforts due to the long-standing argument that it derives its authority from the U.S. government. Critics assert that this is not a legitimate basis from which ICANN can be responsible for the global management of the Internet. At the inaugural conference in December 2003 of the World Summit of the Information Society (WSIS), the key debate was the governance of the Internet and many participating countries supported the creation of a new, more international management of the Internet. At the conference, a UN group was set up to consider possible new ways of running the Internet. This group is due to report to the WSIS in 2005.

ICANN has sought to improve its performance by enhancing the participation of key stakeholders and by putting in place mechanisms to improve its transparency and accountability. However, more recently, the role and legitimacy of ICANN has again been placed in the public spotlight due to litigation in the United States brought against it by Verisign (the operator of the .com and .net generic top level domains (gTLDs)). The litigation has, again, threatened ICANN's role in the governance of the Internet.

Verisign

In 2001, Verisign entered into an agreement with ICANN under which Verisign undertook to operate the .com and .net registries. The agreement is due to expire in November 2007. The agreement placed Verisign in a commanding position within the Internet community and has also proved to be extremely lucrative for it. However, whilst Verisign has proved to be a commercial success, it has also attracted many critics who consider that Verisign abuses its dominant position to the detriment of its competitors.

In accordance with the agreement, Verisign pays fees to ICANN and, in return, Verisign provides "Registry Services" or core services relating to the management of the .com/.net registries. The agreement also obliges ICANN to:

- establish and maintain independent review policies for Verisign if it is adversely affected by ICANN's standards, policies, procedures or practices; and
- to take all reasonable steps, and make substantial progress, towards entering into similar agreements with other registries which compete with the .com gTLD.

Site Finder

On September 15, 2003, Verisign launched a new service, "Site Finder". Prior to its introduction, when a user mistyped a .com web address, the user would typically receive a message (a "404 error message") that the website could not be found. Site Finder, when an incorrect address was typed into a browser, brought up a screen which stated that the web address could not be found and provided links to alternative web addresses, search engines and popular categories of websites. Through advertising, Verisign anticipated that it would be able to generate in the region of $12.75 million in 2004 from Site Finder.

Following the launch of Site Finder, Verisign was severely criticised by various sectors of the Internet community. The main thrust of the criticism was that Verisign, for its own commercial benefit, had introduced a service which undermined the security and stability of the Internet. Critics said Verisign was trying to make millions from its management of what was, essentially, a public resource by trying to make money from Internet users' typos through advertising. Critics also claimed that Site Finder undermined some spam filters and prevented rival search services from functioning properly.

ICANN stepped into the debate and on October 3, 2003 it demanded that Verisign suspend Site Finder. ICANN alleged that the service was a core service that affected the management of the .com gTLD and that, as such, it had the right to restrict or prohibit the service. In its "Suspension Ultimatum", ICANN threatened to take legal action to prevent Verisign from offering Site Finder. Subsequently, in the face of staunch criticism, Verisign suspended Site Finder and agreed to enter into discussions with ICANN to try and resolve the dispute. ICANN also appointed its Security and Stability Advisory Committee (SSAC) to investigate Site Finder's effects on the stability of the Internet.

Litigation

Discussions between ICANN and Verisign stalled and on February 26, 2004 Verisign issued proceedings against ICANN in the U.S. federal court. Verisign's allegations were wide-ranging and re-ignited the debate about whether ICANN had a legitimate basis from which to control the governance of the Internet. Verisign's lawsuit followed the launch of a string of controversial services which Verisign wanted to provide to users in addition to its management of the .com and .net gTLDs, including Site Finder. Verisign alleged that ICANN's wrongful actions had deprived consumers of beneficial services and deprived it of revenues it would have generated from such services. Verisign asserted that because ICANN had blocked, delayed and restricted the "value added" services Verisign had sought to offer its customers, it was at a competitive

disadvantage as other gTLD registries had introduced similar services without restriction or delay.

In its complaint, Verisign alleged that the conduct of ICANN constituted a violation of federal anti-trust laws and breached its agreement with ICANN. It also alleged that ICANN's demand for Site Finder to be shut down was a "..brazen attempt by ICANN to assume regulatory power over Verisign's business…" which was "….a serious abuse of ICANN's technical co-ordination function". Verisign asserted that its agreement with ICANN did not authorise ICANN to prohibit, regulate or restrict its provision of services, the prices at which it could offer services or its marketing methods. Verisign argued that Site Finder provided users with helpful information and, to preserve its competitive position, it was entitled to provide new, innovative, value-added services to its customers to enhance the attractiveness of .com domain names. To support its complaint, Verisign referred to other gTLD registries which competed with it, including the .museum Registry. Verisign said that, notwithstanding a similar agreement between the .museum Registry and ICANN, .museum provided a similar service to Site Finder and had been assisted by ICANN in the launch of this service.

The most wide-ranging attack on ICANN was Verisign's allegation that there had been a conspiracy to restrain competition. ICANN is an unusual organisation which has numerous "constituencies" that acknowledge that they have commercial interests which may conflict with the interests of other constituents. Indeed, one of ICANN's objectives is to promote a coherent policy that accommodates the differing objectives of competing interests within the Internet community. ICANN comprises a Board of Directors and advisory bodies, called "supporting organisations". Each of the supporting organisations has primary responsibility for developing and recommending policy in its area of expertise and reports to the Board of Directors. Verisign alleged that a number of organisations and individuals within the SSAC had conspired to control ICANN and that members of the SSAC had "captured and controlled [ICANN's] processes". Verisign claimed that no evidence had been found that Site Finder affected the security or stability of the domain name system or the infrastructure of the Internet.

In May 2004, the federal court dismissed Verisign's main anti-trust claim. However, the judge allowed Verisign to reinstate the proceedings if it could provide more evidence.

In June 2004, Verisign filed an amended complaint. In relation to the conspiracy allegations, Verisign asserted that ICANN was controlled by economic competitors who had conspired to control supporting organisations that report to ICANN's ultimate decision maker, the Board of Directors.

On July 9, 2004 SSAC published its long-awaited report on Site Finder. The report found that "Verisign's actions did not have network-shattering effects but did violate fundamental architectural principles and well-established codes of conduct and good practice intended to ensure stability. Users' decisions and controls were preempted and users were potentially subjected to violations of their privacy". The report put forward a number of recommendations including a recommendation that synthesised responses should not be introduced into TLDs and that any changes in registry services should only take place after a substantial period of notice and consultation.

On August 5, Verisign criticised SSAC's report in a 95-page response. It said that SSAC's report contained "no evidence that the introduction of Site Finder destabilised the naming and address allocation system or the Internet" and claimed that SSAC's recommendations were:

> "inappropriate, unsubstantiated, and themselves contrary to longstanding written standards and specifications for the operation of the DNS and Internet".

Back in court, on August 26, Verisign's amended anti-trust complaint was dismissed. In the judgment, the judge noted that,

> "[T]here is nothing inherently conspiratorial about a "bottom-up" policy development process that considers or even solicits input from an advisory group" and that "participation is not enough to give rise to anti-trust liability; *control* is required".

The judge found that Verisign could not allege that the co-conspirators comprised a majority of the ICANN Board of Directors. As the court dismissed Verisign's anti-trust claim (which was the only claim which would be considered under federal law), it declined to exercise its jurisdiction over the remaining 'state law' claims, namely the breach of contract and interference with contractual relations claims. The decision was the second set back for Verisign in its attempt to prove that ICANN overstepped its role as the Internet's technical co-ordinating body.

On August 27, 2004, Verisign wasted no time re-filing a lawsuit against ICANN. It filed a pared down complaint in the state court of California claiming that ICANN was in breach of its agreement with Verisign.

Whilst the new proceedings will cause inconvenience and expense to both parties, the contractual dispute is unlikely to be of the same degree of concern to ICANN as the proceedings which had been brought by Verisign in the federal court. Critics of Verisign saw Verisign's anti-trust lawsuit as a device to ensure that ICANN's authority to regulate key aspects of the Internet was debated in the public spotlight in court. Even some of ICANN's staunchest critics suggested that Verisign's anti-trust allegations were unfounded. As the claim is now a contractual dispute in a state court, it is unlikely that it will settle questions such as the power which ICANN has to regulate the domain name industry and how much power Verisign has to introduce new services which critics (and competitors) assert are potentially damaging and anti-competitive. An anti-trust judgment against ICANN could have had a far greater reach and impact on the entire governance of the Internet.

Conclusion

Whilst the battle between Verisign and ICANN rumbles on, ICANN should ensure that the litigation does not detract it from continuing on its reforming path. Both ICANN and Verisign can be criticised for their respective roles in the debacle which has surrounded Site Finder. However, ICANN needs to ensure that it continues to focus on its mission which is to co-ordinate domain name and address functions by bottom-up consensus. This will ensure that decision making in relation to the governance of the Internet is de-centralised to preserve diversity and promote competition. Over the years, to greater and lesser degrees of success, ICANN has provided a consensus based, non-governmental management of issues which are critical to the management of the world wide web. With a high degree of reliability, the Internet has become a stable mechanism: domain names resolve with an astonishing degree of success. ICANN must continue to allow the natural evolution of the Internet and, with WSIS due to report in 2005 on the governance of the Internet, the pressure on ICANN to perform will undoubtedly continue, unabated.

Convergence is Dead: Long Live Convergence!

By Jolyon Barker, Head of the Technology, Telecommunications and Media Group at Deloitte.

This article examines the current state and likely future implications of convergence across the Telecommunications, Media and Technology industries and addresses three key questions:

- What are the underlying trends driving continued convergence?
- How will convergence drive the evolution of the TMT sector?
- What are the critical success factors for TMT companies for the future?

In the late 1990s, convergence in the Technology, Media and Telecommunications (TMT) sectors was *the* hot topic.

The world wide web and the growth of high-speed digital networks gave us instant access and transmission of information. We were presented with the vision of a brave new world of multi-media products and limitless content, all united by invisible connectivity.

The pace was frantic as TMT companies jostled for position in a rapidly evolving market. But the ensuing series of inter-sector marriages, takeovers and frenzied entry into new markets cost the three sectors billions in lost revenue.

In 2004, the picture appears markedly different. The original promise of some high-profile marriages remains unfulfilled. Many of the overtly technology-led services have flopped. Markets are still struggling to recover from corrections in value.

But despite the failure of many grand visions of recent years, the promise of a converging world is still with us and the transformational effects of digital technology continue to advance relentlessly. Still, few companies are betting the bank: investment is measured and incremental, and progress is slow and steady. Put simply, we are in a more mature and cautious era where developments are rooted in evolving, but financially robust, business models.

The question is, how is convergence developing in this more cautious era? And how should TMT companies position themselves to succeed in this converged world?

The Early Hype of TMT Convergence

Goldrush in the Late 90s

In the late 1990s, the application of new technologies started to blur traditional content and channel boundaries. Media companies, service providers and advertisers saw opportunities to reach their customers in new and more valuable ways, and offer a variety of new products and services. The seemingly imminent convergence of television, PC and mobile phone platforms held out the promise of highly profitable, multi-dimensional customer relationships.

This holy grail of converged service offerings drove a frenzy of inter-sector mergers and acquisitions within the TMT sector, as companies jockeyed for position. They gambled mighty sums on M&A: Vivendi and Seat Pagine Gialle spent €64bn between them. The pinnacle of the spending boom was the U.S.$250bn AOL Time Warner merger in 2001, bringing together the United States' largest Internet service provider with a major media and cable conglomerate.

The market bristled with new media companies and dotcom launches, with heavy investment in new technologies and online services. Company valuations were increasingly based on fuzzy metrics. The markets were dominated by day trading and short term positions rather than financial fundamentals and long term prospects. New Economy pundits predicted the end of bricks and mortar.

The Fallout

The inevitable swing from boom to bust has left a three-year "hangover" in the TMT space. TMT companies were the biggest casualties as stock markets started to fall. Poor business propositions were found out. Ricochet, the U.S.-based high-speed data service provider invested more than $1bn but filed for bankruptcy in August 2001. Video Network's HomeChoice service in the United Kingdom, was forced to scale back its ambitions as the costs of building and running its services failed to fall as originally anticipated. Technology-driven WAP services flopped embarrassingly amid much hype. And recent accounting write-downs suggest that some mobile operators, especially in the United Kingdom and Germany, substantially overpaid for their 3G licences.

Whilst the dotcom collapse reflected the extent of the market's over-valuation and widespread lack of financial discipline, a combination of culture clash and huge operational challenges also frustrated some of the most ambitious mergers: Vivendi Universal has started to divest a number of media and technology related businesses; AOL Time Warner posted the largest ever annual loss in corporate history (U.S.$100 billion) in January 2003 and has since dropped the "AOL" from its corporate name.

Evolution, Not Revolution

Whilst convergence activity has in the past thrown up high profile failures, wildly inaccurate industry predictions and a frenzy of overspend, many convergence initiatives are quietly succeeding. The industry may have been over-ambitious about the timescales to achieve its aspirations, but the reality is that convergence is very much still alive. It is simply progressing at a different pace than predicted in the 90s: this is not to be a revolution after all, but an evolution.

Deloitte defines convergence as "the combination of the previously discrete sectors of Technology, Media and Telecoms to provide rich, multimedia products and services to consumers and businesses".

Where is Convergence Now?

There is evidence of convergence happening at three different levels:

- *Product/service convergence*: that is, the combination of formerly discrete products or services into a single product, driven by advances in technology, changes in consumer behaviour and the quest for new ways to increase revenues through new channels to market. Clear illustrations include the success of SMS voting in

response to television shows (10.7m text votes sent during U.K. reality TV show, "Big Brother 3", on Channel 4). In fact SMS-based entertainment is now a $1bn-plus worldwide market. The U.K. ring tone market was worth £60m in 2003, and is growing rapidly. Other growth areas include games on mobile phones, MMS (picture messaging) and video clips and video conferencing on 3G. For the first time in the United Kingdom, live terrestrial TV footage delivered to users' mobile handsets was recently available during Channel 4's "Shattered" though it's too early to understand its success. In the business to business market, Information and Communications Technology (ICT) is attracting attention from telecoms, technology and other players alike.

- *Platform convergence*: that is, both the reduction in the number of platforms as a critical mass is reached within a sector and the combination of platforms across previously discrete sectors. The key challenge for technology companies is to become the platform of choice. The issue is not a new one and is similar to the market tug-of-war between VHS and Betamax in the 1980s.

  The continued evolution of technology and development of universal standards will also help bring platforms together on one device. For example, Sky's success in the United Kingdom's digital TV market has allowed it to set the relevant standards: their technology covers video, Internet and interactive advertising. Playstation and X-Box consoles both now combine computer game and DVD capability in the one device. The latest 2.5G and 3G phones combine telephone, camera, e-mail, calendar, radio, Internet, audio and video capabilities.

  Digital storage and processing are on the increase in more and more devices, with the range of functions they can perform growing ever wider and the speed of evolution advancing all the time. In digital communication, the success of Internet Protocol (IP) in connecting millions of computers around the world has now spread to printers, cameras, set top boxes, mobile phones, cars, VCRs and even fridges. Anything that can collect or use digital information is a target: any device employing digital technology can be IP enabled, and the cost gets smaller every day.

- *Corporate/structural convergence*: the combination, whether through M&A, partnering, or any other method, of formerly separate TMT companies. In the late 1990s there was a high degree of integration across the three TMT sectors achieved primarily through mergers and acquisitions. Today, there is more intra-sector integration and consolidation – a trend that is consistent with platform convergence and the drive to focus on core competencies. The recent merger activity among record labels is a clear illustration of this, as is the consolidation in business application software – PeopleSoft have recently acquired JD Edwards and have since been fighting a takeover bid from Oracle.

  Integration activity across TMT sectors is now being achieved primarily through partnering arrangements, which enable businesses to collaborate on individual projects, extend beyond their core skills, and share the risks and rewards without having to deal with the more permanent integration issues facing a merger. A good example of this approach is the BT/Yahoo! collaboration, where BT is providing the connectivity and customer access, whilst Yahoo! provides the content around broadband services.

Other Developments

There has been an increase in focus on developing communities, as media companies coalesce around common areas of interest and target specific audiences rather than just the mainstream. Examples are The History Channel, CNN, and MTV. The BBC has been in the vanguard, delivering content across a range of platforms – in particular through BBCi. And despite the promise of new entrants using new technologies, big platform owners like Sky and BT remain key gatekeepers to customers, although they are subject to ongoing regulatory scrutiny.

Emerging Trends

How are companies within the TMT sector positioning themselves to exploit current and future opportunities?

Telecoms & Technology lead the way; Media has more to win and lose; and as ever before timing is crucial

Technology and telecoms companies have gained from convergence, with peer-to-peer file swapping driving broadband connections and PC sales, and music downloads selling iPods and other digital audio players. Telecoms companies are now trying new formulas to maximise the use of their bandwidth. For example, BT's broadband alliance with Yahoo! is already up and running, and further promises include music distribution and TV over broadband. France Telecom and TPS have joined forces in France to provide a TV service over the phone line. In addition, 3 is leading the way in 3G multi-media services, albeit at a massive cost (current estimates put the total investment at €20bn). Far from standing still, technology firms are getting directly involved with media delivery. Microsoft is supporting a number of technology media investments, including MSNBC and MSTV. Sony now has a large media business, with Playstation becoming a focal point around which the company is developing new converged services.

In contrast, content companies have generally suffered as a result of convergence. Newspapers have seen sales fall whilst giving away their content on websites (which in some cases have required significant investment); music companies have seen sales fall whilst their content is exchanged, mainly illegally, across the net; movie studios are likely to be the next victims of piracy. Whilst they have been less damaged by the general TMT fallout, media companies have still been affected by the recent general market and advertising depression. Of greater concern, is the fact that many content companies face the erosion of their traditional distribution channels and are seeing traditional revenue streams fading – the music industry, for example, experienced a 30 percent decrease in the sale of singles during 2003. They do have the opportunity to take advantage of an increasing number of alternative channels to market and the associated revenue streams – polyphonic tones being a good example. Some online newspapers are also starting to charge for their content (ft.com, wsj.com and Guardian Unlimited) or allow resellers to charge on their behalf, such as compactnews.com which sells Dow Jones content. However the issue is that due to the infancy of the many new

channels, the route to gaining a reasonable return is not always clear.

Knowing when to act to take advantage of new products and channels is crucial. Being first into an emerging market does not always create an advantage. Smaller organisations are often responsible for creating new products and stimulating customer demand, but they lack the ability to secure dominant positions once a market starts to establish. Larger enterprises will tend to enter the market once an idea is proven, and use their scale and scope to win – either buying out the competition, collaborating with them, or competing head to head. Good examples of this are Sky with their Sky+ box out-manoeuvring TiVo in the United Kingdom, and Nintendo and Sega, who are being nudged out of their home markets by Sony. In online music, following iTunes's sales of 10 million songs within four months in 2003, multiple parties including Dell, Sony, Roxio and Virgin have all entered the market.

Of course, this is not necessarily a bad thing: a small start-up company's definition of success may well be to break a market and then exit through a buy-out. A good current example in telephony is the U.S.-based, Vonage, whose Voice over Internet Protocol (VoIP) service gives users a massive discount on long distance calls over the Internet. Vonage seem content to remain small, but this is a business idea with enormous potential and with their core revenue under threat, telecoms and other companies will be invading soon. iTunes and a revamped HomeChoice may find themselves in the same situation as TiVo when their markets grow and more players enter. Few companies are betting the bank: activity is incremental, based on realistic, profit-based business models.

TMT has been unpopular with investors recently. Capital, particularly for large scale M&A, has been limited; markets are sceptical and more focused on profits and cash generation. We are now witnessing a period of exploratory behaviour rather than furious growth and market development; measured investment is the name of the game. Start-ups have to follow a normal business cycle and must prove their viability before ramping up investment. For example, following the success of iMode in Japan, similar offerings like Vodafone Live!, Orange World, 02 Active and TZones have appeared. And following the success of SMS voting associated with television shows like Big Brother, other television programmes and media companies are following suit with the five U.K. terrestrial channels now generating over £1m revenue every week from phone and SMS interactivity. In broadband, the successful partnership between SBC and Yahoo! was followed by MSN-Verizon, MSN-Qwest, BellSouth Earth Link and BT/Yahoo!.

Throughout this process, staged investment cycles permit controlled expansion. HomeChoice in the United Kingdom has promised to broaden its service offering whilst continuing to press for wholesale broadband price changes to allow it to start making profits. When iTunes started it was only available on Apple Macintosh in the United States. Once the concept was proved, it was made available on Windows and will eventually be available worldwide.

However, there are some exceptions to this more measured approach, notably:

- Hutchison's 3 is still pressing ahead; most of the other companies who bought 3G licences (in some cases for vast sums) are holding back their investment and waiting to see how 3 fares, how the new technology works and how the market starts to shape.
- Microsoft is spreading its bets, investing and sometimes losing large sums in console and online gaming, TV, music and video.
- Sony is gambling the future of its PC and console business on the acceptance of convergent, multimedia devices.

Partnering Strategies are Critical

Deloitte research in 2002 showed that 79 percent of infrastructure and 82 percent of content businesses said they were planning to increase their activity in broadband by strategic alliances. Only 30 percent said they were looking for merger opportunities; partnerships were the way forward. There are few examples of going solo in a convergent play and winning. Success more typically requires a combination of skills from a number of companies and partnering arrangements are now more popular than straight M&A. Compare the difficulties of the AOL Time Warner merger with the successful SBC-Yahoo! and Sony-Ericsson collaborations.

Under this kind of partnering arrangement, individual parties can focus on what they are good at, and still maintain their flexibility to adapt to the market and their ability to adopt new technologies. Collaborations have their own challenges, of course, in particular the management of increasingly complex relationships and risk; companies still need to be able to align their interests to succeed. But time and again this path is proving successful, for example, Pixar partnering with Disney for distribution; Nokia's collaboration with Electronic Arts who are developing games for their new n-Gage platform; and Sony, which is providing the console and broadband connector for online gaming and leaving the customer relationship and games hosting to the telecoms companies and game publishers.

There is also a strategic angle to collaboration. With distribution channels increasingly becoming fragmented, players are concerned about retaining power and influence over elements of the service not directly within their remit. They are also concerned with being heard in the marketplace – is their brand strong enough to reach its intended audience, or does it get drowned out by other brand "noise"? One way to be heard is by becoming a gatekeeper and so maintaining a direct relationship with a large customer base which over time can be monetised. Becoming a gatekeeper, or a hub of activity, usually requires the business to have some relationship with its customers – billing, for example. But this is not all: it also requires the ability to understand and assemble the right mix of skills to deliver what customers want to keep them happy. Equally, as services are delivered via multiple parties, it is important that clear business models are articulated and managed for all members throughout the value chain: controllers of the chain should remember that all participants will expect a fair share of the rewards.

Market Growth and Development

New technologies, formats and distribution channels tend to grow overall markets. Mobile telephony has enjoyed a compound annual growth rate of 60 percent without a significant impact on fixed line telephony's revenues. Videos and DVDs now account for close to 70 percent of a movie title's revenues. The European mobile gaming market is forecast to grow from just under $800m in 2002 to just below $7bn in 2006 without impacting PC or console gaming. The (ICT) solutions market has been a significant area of growth for telecoms and technology companies, with the U.K. market alone expected to grow to in excess of £90 billion by 2007.

Technology typically provides the springboard and opportunity to do new things that create value. Broadband enables online gaming, video networks and music downloads.

Mobile telephony leads to SMS, MMS and location based services. Music and video compression enable DVD and video on demand. But the development of new markets cannot be pushed by technology alone; it must be business-led, with the market potential clearly understood and the technology proven and reliable. Otherwise, the risk is embarrassing service failures and the consequent alienation of customers: witness WAP's failure, TiVo's retreat from the U.K. market or Hutchison's current struggle to offer handsets for its 3 service.

Technology cannot be ignored. Companies should recognise how it is changing their market and take actions to allow them to evolve and control it. Failure to do so can have disastrous results; for example, IBM's near decline before its successful transformation into a leading ICT solutions provider.

Incumbents can also recognise the potential but be resistant to change to protect existing revenue streams. BT, for example, until 2002, maintained a high price for broadband connections to protect significant ISDN revenues. In the music and film world, cannibalisation worries with electronic formats and the piracy concerns of sharing digital copies are now seriously threatening existing business models.

Regulation is also changing to reflect a converged world, with the 2003 Communications Act reforming the regulatory framework of the communications sector, transferring the majority of the responsibility to the U.K. Office of Communications (Ofcom). Competition no longer simply works within distinct industry markets differentiated along technology lines: it now reaches across markets at every level. The regulatory challenge for Ofcom will be to maintain and promote competition, both within and across traditional sectors, as the boundaries continue to blur.

The Future for TMT Companies

All the evidence points to a more considered approach to convergence in the future, based on solid building blocks and business models. Instead of the major players creating media and telecom convergence through acquisitions, more complex partnerships will develop, therefore offering opportunities to advance the next stages of both product and platform convergence. But in this environment, what are the criteria for success? Companies should:

- use robust but evolving business models;
- focus on their strengths and partner to meet market needs;
- be flexible and move quickly; and
- consolidate and maintain their position.

Robust but Evolving Business Models

New business ventures are going back to basics and starting with sound business and financial models. The market opportunities must be fully understood in terms of demand and acceptable pricing. Managing the risk profile whilst allowing business models to evolve is crucial.

Technology is creating new revenue streams from products and services like VoIP, PPV, VOD and PVRs, but opportunities should be confined to proven technologies with a clear route to profitability. The technology driven "push" has to be balanced against consumer "pull" considerations relating to preferences and enthusiasm for new products and services.

Focusing on Strengths and Partnering to Meet Market Needs

The TMT fallout drove companies to hive off non-core operations and activities. There will be a continued drive for companies to concentrate on what they do best, understand how they add value and leverage these skills into the market, and use strategic partnerships to fill the skill gaps. The increasing complexity of these technology-driven alliances will make the ability to manage partners and the underlying risks over their lifecycle critical.

Flexibility and Direct Action

The market for converged services will continue to change rapidly. It will be vital to maintain flexibility and speed to market, in particular monitoring new opportunities enabled by technology, spotting trends in the market and being able to deliver in the marketplace. Successful larger companies in this space will be excellent fast followers and will clean up the first mover "minnows". Smart movers will be able to take the good ideas from failing ventures and make them work (compare iTunes' success with Liquid Audio's failure). Success will be determined by being lean enough to react quickly and effectively and capitalise on new developments in the market, and using size to win.

Maintaining Market Position

Companies need to develop strong, lasting relationships with their customers and must therefore strive to understand customer needs and develop meaningful relationships with them, as well as displaying the necessary leadership, power and influence to attract the key partners required to provide the products and services. It will always be necessary to ensure reasonable financial returns are visible to the key organisations involved in service delivery to guarantee their loyalty and co-operation. Companies must also be alert to managing risk, returns and operations.

For many media companies this will not be attractive, let alone feasible. Content players should pursue the increasing number of channels to market to allow them to maximise the value of their assets, aligning themselves within distribution networks that make financial sense.

