Volume 15, No. 1, 2000
Pages 1-40

The Computer Law Association Bulletin

CLA Website: HTTP://CLA.ORG

Editor
Esther C. Roditti
P.O. Box 2066
New York NY 10021 USA
Tel: 212-879-3322; Fax -4496
ecroditti@aol.com

U.S. Developments Editor
Randall M. Whitmeyer
Hutchison & Mason PLLC
3110 Edwards Mill Road (100)
Raleigh NC 27612 USA
Tel: 919-829-9600; Fax -9696
rmw@hutchlaw.com

International Editors
Ashley Winton
Osborne Clarke
Hillgate House, 26 Old Bailey
London EC4M 7HS England
Tel: 44-171-809-1268; Fax: -1269
ashley.winton@osborneclarke.com

Hilary E. Pearson
Bird & Bird
90 Fetter Lane
London EC4A 1JP England
Tel: 44-171-415-6000; Fax -6111
hilary.pearson@twobirds.com

Chair, Publications Committee
Diana J.P. McKenzie
Gordon & Glickson P.C.
444 North Michigan, Suite 3600
Chicago, IL 60611 USA
Tel: 312-321-7671; Fax -9324
djpmckenzie@ggtech.com

CLA Executive Director
Barbara Fieser
Computer Law Association
3028 Javier Road, Suite 402
Fairfax VA 22031 USA
Tel: 703-560-7747; Fax 207-7028
clanet@aol.com

News and Announcements 2
Coming Events
President's Letter

Russian Legislative Framework for IT and E-Commerce 4
By: Oxana Iatsyk,
Toronto, Canada

Congress Aims Its Cannons at Domain Name Pirates 9
By: Joel Voelzke,
Los Angeles, California

Insurance for Internet and E-Commerce Liabilities 14
By: David B. Goodwin and Rene L. Siemens,
San Francisco, California

United States Law Updates 20

International Law Updates 26

Editor's Report 37
Websites for Government and Related Reports

Inserts
CLA Welcomes New Members
Member Address Changes
Order Form for *Internet and Web-Related Forms Collection—2000*

Computer Law Association News & Announcements

Coming Events

April 13-14—The Global Digital Explosion: A Special Millennium World Computer Law Congress and Computer and Telecommunications Law Update, Washington Monarch Hotel, Washington, DC

June 15-16—Computer Law in the Millennium Perspective, CLA/IFCLA Spring Conference, Paris, France

October 12-13—A Balanced Approach to Computer and Internet Legal Issues, Milan, Italy

October 26-27—Representing the Internet Entrepreneur: Practical Approaches for Transforming Ideas into Dollars, Four Seasons, Newport Beach, California

You can register for any and all CLA conferences through our website, HTTP://CLA.ORG.

Inserts for books, promotions, and other items not prepared by the Executive Director must reach her at least two weeks before publication. For Volume 15, No. 2 this is May 3, 2000.

Attention Members

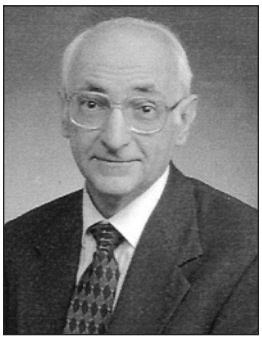
Looking for a publication venue?

The value of the *CLA Bulletin* to members depends upon the quality of its content. Before submitting your manuscripts elsewhere, consider publishing first in your *Bulletin.*

The process is easy. If you wish to publish a feature article, please send the manuscript to me, Esther C. Roditti, for consideration. I am always on the look-out for articles on timely topics and issues. The required length is 2,000-4,000 words, with endnotes and standard case citations. Send a hard and/or electronic copy, but in WordPerfect please. Also, if you have an idea for a timely topic, let me know.

Remember, the quality of the *Bulletin* depends on you!

President's Letter



Our conferences continue to excel. In terms of content and speaker quality, we believe that ours continue to be among the best.

Since I wrote my last *Bulletin* letter, we have sponsored a "Hot Risks, Opportunities, and Strategies for Succeeding in a Digital World" conference in Chicago under the direction of Program Committee Chair Steve Hollman (Co-Chairs, Michele Kane and Hank Jones). We also presented our fourth annual CyberSpaceCamp™ conference in San Jose, California (Chair, Mary Hildebrandt), providing three days of intensive training to newcomers to the area of IT law. Attendance at that program was excellent, confirming our belief that the CyberSpaceCamp continues to be a preferred training vehicle for many corporate law departments and law firms.

With regard to future conferences, Co-Chairs Jay Westermeier and Enrique Batalla have just completed plans for the annual Washington, DC conference, to be held April 13-14. This conference, whose theme is "The Global Digital Explosion," promises to be outstanding. And Co-Chairs Don Martens and Peter Brown are preparing the annual Fall U.S. conference, whose theme is "Representing the Internet Entrepreneur." The Fall conference will be held in Newport Beach, California on October 26-27. Also in October, we will sponsor a conference in Milan, Italy on "A Balanced Approach to Computer and Internet Legal Issues: Customer's Concerns—Supplier's Responses" (Co-Chairs, Enrique Batalla and Steve Davidson). The date is October 12-13.

Our conference co-sponsorships continue. In October 1999, we co-sponsored the annual ABDI

The Computer Law Association Bulletin

(the Brazilian Informatics and Telecommunications Law Association) conference in Sao Paulo, Brazil (Chair, Esther Nunes). And on February 4-5, we co-sponsored a program with Computer und Recht in Frankfurt, Germany, the theme of which was "Cyberlaw: One Business, One Law? EU and USA: Different Concepts for a Single Electronic World" (Co-Chairs, Thomas Heymann and Ray Nimmer). On June 15-16 we shall co-sponsor, with the IFCLA (International Federation of Computer Law Associations), a "Computer Law in the Millennium Perspective" conference in Paris (Chair, Yves Bismuth).

The Publications Committee, under the leadership of Diana McKenzie, has just received copies of the second edition of our popular *Internet and Web-Related Forms Collection.* Editor Paul Hoffman has both updated the forms in the first edition, and added other forms to the collection. Moreover the work will now be sold as a hard copy/CD-ROM unit. And, as readers of the *Bulletin* know well, our periodical continues to publish articles on the leading edge of IT law practice.

One of the major goals I set when taking office was to increase CLA's non-U.S. presence. Under the direction of International Chair Hilary Pearson, CLA has expanded its schedule of international conferences (as described above). Ours is the most ambitious international conference schedule ever initiated by CLA, and we believe it will succeed. In this era of an ever-shrinking world, with transactions increasingly crossing borders, we continue to believe that the interests of CLA members, whether U.S. or not, will best be served by expanding CLA's network of members and conferences. We are in preliminary discussions regarding a number of additional programs in Europe and in nearby regions. We have also invited all attendees of the June 1999 Madrid conference and the October 1999 Sao Paulo conference to join CLA. Barbara Fieser has already sent out membership packets. Because of these many initiatives, the International Committee is seeking to expand its membership. Any member interested in assisting the Committee is encouraged to communicate with Hilary.

Under the aegis of Chair John Carson, the Membership Committee has established a law student writing competition, an event conceived by Marc Friedman and Jennifer Davis. To announce this competition, John has sent letters to numerous law schools, in the United States and other nations, that have IT law programs. Prizes will be awarded separately for U.S. and non-U.S. entries. In each category first prize will be $750, and second prize will be $500. The Membership Committee has also revised the website membership application and developed a new set of pages for the student portion of the website. Fenwick & West has commenced sponsorship of student memberships at Yale and Harvard law schools. Members from any firms interested in sponsoring student memberships at other schools are encouraged to communicate this to John. John has also instituted initiatives designed to increase membership in California, where our membership has not been following the pattern of moderate growth evident in most other areas. Because of the extensive activities of the Membership Committee, John is actively seeking a Co-Chair. Any member interested should communicate with him.

I also encourage members with suggestions regarding any facet of CLA to forward them to me at DBENDER@WHITECASE.COM or at 212-819-8649.

David Bender

President

The Computer Law Association Bulletin

Volume 15, No. 1, 2000 / 4

Russian Legislative Framework for IT and E-Commerce

By: Oxana Iatsyk, Toronto, Canada*

While the Internet growth rate in the Russian Federation reportedly exceeds that in the United States, legislative developments lag behind. Getting a grip on what Russian laws protect is time-consuming, yet the task must be undertaken if one wants to function in that market. It is imperative to understand how different concepts are interpreted in Russian legislative instruments, and how these interpretations differ from the ones we are accustomed to in the West, especially if we are dealing with laws governing information technology and the Internet, and their associated intellectual property rights.

Issues of information protection in Russia arise when Western transactions involve the use of electronic communications; proposed inventions are developed in Russia at, or with the assistance of, a state-run research institute or laboratory; or the subject matter of an invention is of some value to the Russian Federation.

The information subject to protection under the Civil Code of the Russian Federation includes: personal, state, commercial, bank and insurance secrets, advertising, and a person's name and image, honor, dignity, or business reputation. While recent reports indicate that Russian legislation on information protection currently includes up to 500 legislative instruments, defining the scope of information protection still represents a daunting task. In Russia, major legislative acts in this area started to appear at the end of 1991, and as of now include about a dozen major laws:

—*Law on Participation in the International Information Exchange* (July 4, 1995);

—*Law on Information, Informatization, and Protection of Information* (Feb. 20, 1995);

—*Law on Communication* (Feb. 16, 1995);

—*Law on Compulsory Document Sample*s (Dec. 29, 1994);

—*Law on State Secrets* (July 21, 1993);

—*Law on Authors' Rights and Neighboring Rights* (July 9, 1993);

—*Fundamentals on the Archival Fund of the Russian Federation* (July 7, 1993);

—*Patent Law* (Sep. 23, 1992);

—*Law on the Legal Protection of Integral Circuit Topologies* (Sep. 23, 1992);

—*Law on the Legal Protection of Software and Databases* (Sep. 23, 1992);

—*Law on Mass Media* (Dec. 27, 1991).

Russian laws on the protection of patents, trademarks, copyrights, topologies, and computer programs have been reviewed in other publications.[1] This article sets out to review the laws not yet well recognized in the West for their importance in transactions involving Russian intellectual property and information technology.

Law on Participation in the International Information Exchange (No. 85-F3, July 4, 1995) (Information Exchange Law)

The Information Exchange Law governs transactions in which information available in print form is transmitted over the border of the Russian Federation.[2] The information includes that available through mass media, audio and visual communication channels, and in information libraries, systems, archives, funds, databases, and other types of information systems.

Limited access to information applies to: state secrets, confidential information, national treasures of the Russian Federation, information preserved in archival funds, as well as that subject to limited access under other laws of the Russian Federation.[3]

Because access by users located outside of the Russian Federation to such information stored on information systems and networks that are located within the Federation is also limited, it is possible to assume that provisions of this law apply not only to the import/export of information in the form of hard copy documents, but also to accessing such documents through computer networks and information providers. At the same time, although the Information Exchange Law addresses the issue of "information services," it interprets the term so narrowly that electronic money, advertising, investment, and other forms of e-services are not covered.

The Computer Law Association Bulletin

While property rights to information products and the means of international information exchange are subject to the Civil Code of the Russian Federation,[4] individual dealings between information owners/holders or service providers and users are subject to agreement between the parties.[5] International information exchange deals that are paid for by the federal budget or budgets of the subjects of the Russian Federation are subject to special licenses if, as a result of such information exchanges, state information resources are exported out of the Federation or information is brought into the Federation to supplement state information resources, unless such provision is contrary to some international agreement of the Russian Federation or Russian legislation at large.[6]

Law on Information, Informatization, and Protection of Information (Law No. 24-F3, February 20, 1995) (Law on Information)

The Law on Information is considered "the basic law" on information protection. The law protects any information fixed on a material carrier that can be identified by its requisites.[7]

Information governed by the Law on Information is a rather broad category that includes "data about persons, objects, facts, events, phenomena, and processes regardless of the form of its presentation,"[8] owned by physical or legal persons that finance the creation of such information or acquire it on other lawful grounds.[9] Since this covers much, if not all, of what can be called "inventions" and "trade secrets," regardless of their coverage in other legislation, the Law on Information should always be considered when dealing with any kind of Russian intellectual property.

Information in the Russian Federation is subdivided into two classes—information freely available, and information with limited access. The Law on Information further divides documented information with limited access, affixed to a material carrier, into state secrets and confidential information.[10] While the Law on State Secrets governs state secrets, confidential documents and personal information are protected under the Law on Information.[11]

The Law on Information distinguishes between the "owner of information resources" and the "holder of information resources," and provides that ownership title to information resources or systems shall belong to physical or legal persons that have financed the creation of such information systems and the means of their use, or acquired them on other lawful grounds. Holders of information systems are responsible for providing resources to users within the framework set by the owner of these information resources and by Russian legislation.[12]

The Law on Information further outlines provisions in relation to personal information and its treatment[13] and ways to access and use various categories of information,[14] defines obligations and responsibilities imposed on owners of information resources,[15]outlines development, ownership, and authors' rights to information systems, their technologies, and service systems.[16] In addition, the Law on Information permits claiming and trading in property rights concerning information resources.[17]

The Law on Information does not specifically refer to foreign persons; however, general rules under the Civil Code infer that foreigners enjoy the same treatment as Russian residents with respect to ownership rights, except where laws indicate otherwise.[18] Furthermore, the Information Exchange Law, enforced after the Law on Information, indicates that foreigners are able to participate in international information exchange.[19]

Law on Communication (Law No. 15-F3, February 16, 1995)

The Law on Communication regulates relations arising among state authorities, communication providers, officials, and users at the time of providing services and fulfilling communications projects.[20] Article 2 of the Law on Communication includes within the meaning of the term "electrical communication" information exchange between computers, as well as tele-, audio-, and other types of wire communication. The law applies to both communications within the Russian Federation and those originating outside of the country, but only in the area of regulating the provision of communication services within the Russian Federation.

The Law on Communication further defines the rights of users and providers of postal and electrical means of communication,[21] addresses the issue of secrecy of communication,[22] and liability for infringement.[23] Therefore, providers of communication services directed at the Russian Federation should carefully review the Law on Communication.

Law on Compulsory Document Samples (Law No. 77-F3, December 29, 1994)

Article 1 of the Law on Compulsory Document Samples defines "document" as a material object

with information affixed to it in the form of text, sound, or image subject to transmission in space and time for the purpose of preservation and public benefit. At the same time Article 5, in the list of documents subject to compulsory free-of-charge sampling and compulsory paid samples to be supplied to the national library and information fund of the Russian Federation, includes "electronic publications that are or contain computer programs and databases," as well as unpublished documents resulting from scientific research (dissertations, reports, algorithms, and programs).

The Law on Compulsory Document Samples outlines the procedure for submitting compulsory free-of-charge samples of e-publications and computer programs,[24] defines the rights held by document producers,[25] and the obligations of those receiving the samples.[26] The Law on Compulsory Document Samples causes much confusion among legal advisers because "electronic publication," as defined in the law, is so broad that it includes within its scope documents originally from almost any kind of automated information system. As such, it contradicts definitions of the term "publication" in the Law on Mass Media and the Copyright Law. So far, analysis of the above-mentioned laws leads to the conclusion that "electronic publication" should not refer to computer programs.

Law on State Secrets[27] (Law No. 5485-I, July 21, 1993)

The Law on State Secrets defines secret information,[28] provides for the classification of certain categories of information on the basis of its importance to the national security, and covers various kinds of information, including research and development data and technologies designed for, or capable of being used in, weapons and military equipment, or otherwise important to the national security, as well as state secrets saved in computer memory.[29] For the first time in Russian legislation, Article 10 of the Law on State Secrets defined the term "owner of the information" as any corporation, institution, organization, or physical person in possession of secret information, yet the term is not reflected elsewhere in the text of the law.

The Law on State Secrets provides for the issuance by a special government commission of a list of data and agencies responsible for its classification and control. Agencies charged with implementing the regime include the Interdepartmental Commission for the Protection of State Secrets, the Ministry of Security, the Ministry of Defense, the External Intelligence Service, etc.

Presidential Decree No. 1203 of November 30, 1995 enacted a List of Classifiable Data that includes "data revealing the substance of the newest achievements in the area of science and technology which can be used in the development of substantively new products, technological processes in various areas of economy, as well as determining qualitatively new levels in the development of weapons and military equipment, enhancement of their battle effectiveness, whose disclosure may be detrimental to national interests." In addition, the document designates 15 more agencies responsible for the classification of such data, including the Ministry of Defense and the State Committee for the Defense Industry.

Possession of classifiable data must be reported to the appropriate agency. When privately owned information is of the classifiable nature, the owner is entitled to compensation (to be agreed upon between the owner and the classifying agency). Failure to agree on compensation does not relieve the owner of such data from duties imposed by the Law on State Secrets, most importantly the duty not to divulge such information without proper authorization.

The Law on State Secrets defines procedures for classifying information as secret,[30] declassifying information,[31] and for transferring state secret information to other legal entities or foreign governments when fulfilling state orders and other joint projects.[32] Note that this law does not apply to data and information owned by foreign investors. The law provides that ownership rights of foreign organizations and citizens to information shall not be restricted, if its acquisition (development) did not violate Russian legislation.[33] This provision appears to mean that information owned by foreign entities or individuals cannot be classified and that foreign owners retain all rights to use and dispose of such information in any lawful way. At the same time, since application of this provision is conditioned on lawful acquisition of the owner's rights to the data, its value is rather low due to the limited number of ways a foreigner in Russia can lawfully acquire classified or classifiable data.

However, the Law on State Secrets is designed to exclude, or at least to significantly restrict access of, foreign entities or individuals to data and information governed by the law. For example, the Law on State Secrets considers an applicant's residence outside of

The Computer Law Association Bulletin

Russia to be a disqualifying criterion for accessing classified information.[34] Moreover, under the Law on State Secrets the process of obtaining a license required for dealing with classified information is so designed as to virtually exclude the possibility of issuing such license to a foreign person. Yet, the Law on State Secrets does not directly exclude the possibility that foreign entities or individuals lawfully may acquire ownership of classified or classifiable data.

Fundamentals on the Archival Fund of the Russian Federation and Archives (No. 5341-I, July 7, 1993) (Archive Law)

The Archive Law defines the terms "archive," "secret archive," "archival document," and "archival fund,"[35] and establishes a procedure and scope for compiling archives,[36] transferring archival documents,[37] releasing state archival documents into circulation,[38] temporary and permanent safekeeping of archival documents,[39] and protecting one's rights to them.[40] The term "archival document" is defined as "any document that is protected or subject to protection because of its value to the society or its owner." An archive represents either a collection of such archival documents or an institution in charge of collecting and safekeeping such documents.

The Archive Law covers a collection of documents that reflect the material and spiritual life of the Russian peoples, have historical, scholarly, social, economic, political, or cultural value, and are inseparable from the historical and cultural heritage of the peoples of the Russian Federation.[41] The Archive Law distinguishes between state, federal, and non-state archival documents.

Archival documents from the state part of the Archival Fund of the Russian Federation, and especially valuable documents from the non-state part of the Archival Fund, cannot be removed from the country, except when the State Archival Service permits temporary removal of such documents from the Russian Federation on the basis of legislation dealing with cultural valuables.[42]

Copies of archival documents and excerpts from them (including those received as a result of purchase and sale agreements with their owners, gifts, or other types of lawful transactions) can be exported without limitation, unless such copies or excerpts are made from secret archival documents.[43] Provisions in this law are subject to international agreements on archives to which the Russian Federation is a signatory.

Law on Mass Media (Law No. 2124-I, December 27, 1991)

In Russia, mass media include both traditional methods of information dissemination and those created by the new information technologies. The Law on Mass Media regulates traditional periodical publications; text transmissions of a thousand or more issues, prepared on or stored in computers and/or databases; and other mass media sources, whose products are distributed in the form of publications, texts, or images.[44]

Currently, the Law on Mass Media forbids censorship of mass communications or the creation of institutions that may censor contents of periodical publications.[45] The only type of communication explicitly prohibited by this law is that encouraging criminal offenses, disseminating state secrets, or promoting political uprisings, and nationalistic, religious, or social intolerance.[46]

Unless additional legislative acts are introduced to regulate information dissemination by means of the new technologies, Internet publications and other forms of telecommunications are subject to the Law on Mass Media,[47] as long as they publish at least one issue per year.[48] Persons involved in information dissemination must keep in mind that the Law on Mass Media governs both periodicals issued in the Russian Federation, and those transmitted into the Federation.[49]

E-Commerce

Although there is no specific legal basis for e-commerce in Russia, the necessary framework is in the making. Articles 428, 434, 437, and 438 of the Civil Code are relevant. According to these articles, contracts between two parties can be made in any form if no particular form is mentioned in the governing law. A written contract evidencing a transaction can be exchanged both by standard methods of communication and electronically. Furthermore, according to the Law on Information, documents stored and transmitted via automated systems that are authenticated by "an electronic digital signature" are enforceable. Although the law does not define "electronic digital signature," it gives legal force to automated information systems that can verify the signature in the regime established by its user. E-commerce is strengthened by the fact that, in the case of a dispute, Russian courts accept e-generated documents and e-signatures as evidence.

Currently, obstacles to the development of e-commerce in Russia include logistical problems with

the transportation of goods, vague banking procedures, and low numbers of credit card holders. Yet, whatever the problems are for an e-commerce boom in Russia, it is not a lack of digital know-how, government enthusiasm, or international support. In November 1998 the Russian Association for Electronic Commerce was created, following the EU announcement of EU-Russian cooperation on the development of e-commerce in Russia. Furthermore, the Russian Federation Chamber of Commerce and Industry and the American Chamber of Commerce in Russia designed an initiative to establish a US-Russian Institute for the Development of E-Commerce. These and other initiatives will strengthen and forward the development of e-commerce in Russia and promise to provide unlimited opportunities for businesses interested in the region.

Conclusion

Transactions of any kind in the Russian market are not easy. Complications arise in deals involving intellectual property rights because various information technology laws must be taken into consideration and dealt with to ensure the legality and validity of the transaction under Russian legislation that includes the term "information." A single approach to information technology issues has not yet developed and, therefore, issues involved in information technology transactions have to be considered from the point of view of any legislative instrument that may directly or indirectly affect their treatment.

Endnotes

* Oxana Iatsyk has been specializing in the Russian IP matters for the past three years, and is currently fulfilling her articling requirements at the Toronto office of Gowling, Strathy & Henderson.

1. E.g., O. Iatsyk, "Russian Intellectual Property Law Provisions and Their Implications for Western Parties," *Computers & Law* (Dec. 1997) at 24; O. Iatsyk and E.V. Kapoustina, "Intricacies of Dealing with Intellectual Property in Russia," *Intellectual Property Journal* (June 1998) at 145.
2. Art. 1(1)-2, Information Exchange Law.
3. *Id*., Art. 8(1).
4. *Id*., Art. 6(1).
5. *Id*., Art. 6(2).
6. *Id*., Art. 18.
7. Art. 21(1), Law on Information.
8. *Id*., Art. 2.
9. *Id*., Art. 6(2).
10. *Id*., Art. 10.
11. *Id*., Art. 21.
12. *Id*., Art. 15(1).
13. *Id*., Art. 11: collection, storage, use and dissemination of information about one's personal life, and any information that is subject to personal secrets, family secrets, confidential correspondence, telephone conversations, mail, facsimile, or other types of correspondence transmission without the author's permission is forbidden unless specifically allowed by a court decision.
14. *Id*., Art. 12: access to information does not have to be justified before the owner or holder of such information, unless information is of limited access; the information owner or its holder defines terms of access to information.
15. *Id*., Art. 15.
16. *Id*., Arts. 16-19.
17. *Id*., Art. 6(5)-(6).
18. Art. 2(1), Civil Code of the Russian Federation.
19. Art. 3(2), Information Exchange Law.
20. Art. 3, Law on Communication.
21. *Id*., Art. 27.
22. *Id*., Art. 32.
23. *Id*., Arts. 37-39.
24. Art. 13, Law on Compulsory Document Samples.
25. *Id*., Art. 16.
26. *Id*., Arts. 17-18.
27. The concept of "state secrets" is also dealt with in the Russian Federation laws On the Fundamentals of State Service of the Russian Federation, On Federal Bodies of State Communication and Information, On Participation in the International Information Exchange, On the Archival Fund of the Russian Federation and Archives, and others.
28. Art. 5, Law on State Secrets.
29. *Id*., Art. 2.
30. *Id*., Arts. 9 and 11.
31. *Id*., Arts. 13-15.
32. *Id*., Arts. 16-19.
33. *Id*., Art.10.
34. *Id*., Art. 22.
35. Art. 1, Law on Archives.
36. *Id*., Arts. 7 and 18.
37. *Id*., Art. 8.

The Computer Law Association Bulletin

38. *Id*., Art. 20.
39. *Id*., Art. 17.
40. *Id*., Arts. 9 and 21.
41. Art. 1, Law on Mass Media.
42. *Id*., Art. 23.
43. *Id*., Art. 24.
44. *Id*.
45. *Id*., Art. 3.
46. *Id*., Art. 4.
47. *Id*., Art. 24.
48. *Id*., Art. 2.
49. *Id*., Art. 6.

Congress Aims Its Cannons at Domain Name Pirates

By: Joel Voelzke, Los Angeles, California*

President Clinton signed the Anticybersquatting Consumer Protection Act on November 29, 1999. The Act articulates a strong federal policy against registering or keeping domain names for the main purpose of profiting by selling those domain names to trademark owners or to people whose personal names are similar to the domain name. Under the new law, it will be much easier for a plaintiff to take action against the owner of a domain name that corresponds to his or her trademark or personal name, and to obtain an order canceling or transferring the domain name.

The new law also gives a trademark owner the option to proceed *in rem* against the domain name itself, remedying the previous difficulties raised by unlocatable registrants. Additionally, domain name registrars will enjoy immunity from suit with respect to the "reasonable" registering, suspending, canceling, or transferring of domain names. International implications of the new law, and steps to take to strengthen cybersquatting challenges, are also discussed.

Liability Standard

In General: "Bad Faith" Is the Key—The Act protects owners of both registered and unregistered trademarks against use of their marks within domain names, and also protects living persons against use of their personal names within domain names, under certain circumstances. Under §43(d) of the Lanham Act as added by the Act, a domain name holder becomes liable if he or she:

- "has a bad faith intent to profit from" a mark or personal name protected by §43 (see below), and
- registers, traffics in, or uses a domain name that is:

  —identical or confusingly similar to a distinctive mark;

  —identical, confusingly similar, or dilutive of a mark that is famous at the time of registration; or

  —protected under 18 USC 706 (Red Cross) or 36 USC 220506 (Olympics and related marks).

The "confusingly similar" standard is to be applied without regard to the parties' respective goods and services. This is an important change. Previously, a trademark owner had two primary avenues for pursuing a cybersquatter. First, the owner could try to prove that the cybersquatter was diluting the trademark. This required a showing that the trademark was "famous." In at least one case, the owner of two well known marks lost its case against an accused cybersquatter when the court ruled that the marks were not famous. In the case of a non-famous mark, the second possibility was to charge the cybersquatter with infringement. However, traditional trademark infringement analysis requires a likelihood of consumer confusion *after* taking into account how closely related are the goods and services of the parties. Since most cybersquatters do not actually sell any goods or services, there was some question as to whether trademark owners could prove infringement where the domain name was not actually ever used to sell goods or services. Under the new law it suffices if the domain name is confusingly similar to the mark, without reference to the parties' goods or services.

Multi-Factored "Bad Faith" Test—At a loss as to exactly how to define "cybersquatting," Congress eschewed any bright lines for judging when the use of a domain name was wrongful. Instead, the Act directs courts to apply a multi-factored "bad faith" test. The bad faith factors include:

- whether the domain name holder has any legitimate trademark or other intellectual property rights in the domain name, or whether the domain name is the holder's own name;
- any prior use of the domain name by the holder in the bona fide offering of goods/services;
- the holder's intent to divert consumers from the mark owner's own site, either for commercial gain or to tarnish or disparage the mark;
- the holder's attempts to sell the domain name without a prior bona fide offering of or intent to offer goods/services, or the holder's past pattern of doing so;
- whether the holder supplied false or misleading contact information when applying to register the domain name, or other domain names;
- whether the holder has acquired other domain names that are the same or similar to other trademarks; and
- how distinctive or famous the mark is.

Although the domain name holder's legitimate rights to use the disputed domain name within his or her own field is listed as only one factor for the court to consider, the Act goes on to specifically exclude a finding of bad faith in those cases in which the domain name holder reasonably believed that the use of the domain was a fair use or "otherwise lawful." This somewhat circular definition would seem to follow the recent holding in *Hasbro Inc. v. Clue Computing Inc.*,[1] the CLUE.COM case. The *Clue* court held that a smaller company that uses a domain name that incorporates a mark being used in a field that does not infringe on the larger company's mark, and which registered the disputed domain name first, has every right to use the domain name as long as it uses the domain name for legitimate commerce and does not try to sell the domain name to the other trademark owner.

The bad faith factors are not exclusive, nor is it even necessary that the domain name holder intends to sell the name in order to be guilty of the requisite "bad faith intent to profit from [the] mark."[2] In *Sporty's Farm L.L.C. v. Sportsman's Market, Inc.*,[3] the first appellate court ruling to interpret the Act, the original domain name registrant, Omega, had registered the domain SPORTYS.COM, which it knew to be identical to Sportsman's famous and registered mark Sporty's. Omega intended at the time to set up a competing business. Omega later sold the mark to Sporty's Farm, a subsidiary that sells Christmas trees. The Second Circuit noted that Omega had registered SPORTYS.COM for the primary purpose of keeping Sportsman's from using that domain name, and that, even though "the unique circumstances of [the case] did not fit neatly into the specific factors enumerated by Congress," there was nevertheless "ample and overwhelming evidence" that, as a matter of law, Sporty's Farm had acted with a "bad faith intent to profit" from the disputed domain name.[4] Accordingly, the court affirmed on both trademark dilution and cybersquatting grounds the district court's order[5] that Sporty's Farm transfer the disputed domain name to Sportsman's.

Names of Living Individuals—The substantive standard for determining when the name of a person is being cyber pirated is different from the standard that applies to a trademark used as a domain name. Specifically, the Act prohibits registering a domain name that is identical or confusingly similar to the name of a living person "with the specific intent to profit from such name by selling the domain name." There is an exception for copyright owners and licensees that register a domain name in connection with a "work of authorship," where the copyright owner/licensee intends to sell the domain name "in conjunction with the lawful exploitation of the work."

Because the liability standard turns on the registrant's subjective intent, even someone coincidentally named Vanna White would run afoul of the law if she registers her own name as a domain name with the intent to sell it, either to the famous Ms. White or to a third party. Note that the Act makes no distinction between whether the person whose name is similar to the domain name is famous or not. Even ordinary people are protected against having their names cyberpirated by companies or individuals scooping up large numbers of domain names in the hopes of ransoming them back to the people who happen to have those names.

The Computer Law Association Bulletin

Additionally, the Act directs the Secretary of Commerce to conduct further studies and make recommendations for additional rules to prevent "abusive" registration of domain names that consist in whole or in part of personal names, including the names of government officials and candidates for public office.

Remedies and Effective Dates

Two different remedies apply, depending on whether the right violated is a trademark or a right in a personal name already protected under §43 of the Lanham Act, or merely a person's unregistrable name.

Violations Under §43—*Monetary Remedies.* For wrongful registration, trafficking, or use of a domain name that occurs after the enactment of the Act, plaintiffs are eligible for the same monetary remedies and injunctions as currently apply to other Lanham Act violations, i.e., (1) defendant's profits, (2) up to three times damages, (3) costs, and (4) in exceptional cases, attorney fees. Additionally, the Act gives plaintiffs the option of statutory damages.

Cancellation or Transfer Order. An important feature of the Act is that it specifically provides for injunctions ordering cancellation or transfer of domain names that were registered before, on, or after the Act's enactment. Thus, even though the defendant's original bad faith registration may have occurred years ago and the defendant is now using the domain name in a more or less legitimate business, an aggrieved trademark owner can still obtain a transfer order.[6]

Violations of a Person's Name—With respect to a domain name that violates a person's name under the Act, but that does not rise to the level of an independent §43 violation, and was registered on or after the date of enactment, a court may award the aggrieved individual an injunction ordering cancellation or transfer of the domain name, as well as costs and attorney fees.

In Rem Proceedings

One of the most important changes is that a trademark owner can now bring an *in rem* action against the domain name itself. This overturns the holding in *Porsche Cars North America Inc. v. Porsch.Com*,[7] in which the court held that the Lanham Act did not authorize *in rem* actions. Under the new law, if the trademark owner cannot obtain personal jurisdiction, or if it sends notice to the holder at both the postal address and the e-mail address listed in the registration and the registrant does not answer, the trademark owner can then proceed *in rem* against the mark itself. Sending the notice constitutes service of process.

An *in rem* suit can be brought in the judicial district where the registrar is located, or where "documents sufficient to establish control and authority regarding the disposition of the registration and use of the domain are deposited with the court." It would appear therefore that a trademark owner can bring an *in rem* action in any judicial district, as long as the registrar, i.e., the company which registered the domain name, agrees either before or after the suit has been filed to deposit the necessary documents with the court. (For brevity, depositing the required documents with the court will be referred to as depositing the domain name with the court.)

One obvious advantage to proceeding *in rem* is that a domain name holder can no longer hide from the trademark owner, and the notice and service procedures are extremely simple to fulfill. An additional and important advantage is that as soon as the plaintiff gives to the registrar a file stamped copy of the complaint, the registrar must freeze the domain name, i.e., the registrar must not transfer or cancel the registration except as ordered by the court. The registrar must also deposit the domain name with the court.

The disadvantage to proceeding *in rem* is that the court can grant only injunctive relief in the form of a forfeiture, cancellation, or transfer order. Damages and attorney fees cannot be awarded. However, the *in rem* procedure is not exclusive; a trademark owner can still bring a regular civil action for damages against the domain name holder in addition to the *in rem* action against the domain name itself.

If you are trademark owner, it appears that, subject to the advice of your counsel, the quickest and most efficient method of proceeding against a cybersquatter who cannot be readily identified and/or located, would be to:

1. Contact the registrar of the disputed domain name, and ask whether the registrar would be willing to deposit the domain name in the court of your choosing. Most registrars will probably be willing to do so. If the registrar agrees, you can file the action in the venue of your choice. If the registrar does not agree, you will have to

file the action in the judicial district that is the situs of the domain name, which is defined by the Act to be the district where the registrar, registry, or other authority that registered or assigned the domain name is located.

2. Send notice via mail and e-mail to the domain name holder that you intend to file an *in rem* action against the domain name.

3. File both an *in personam* action naming the putative domain name holder and Does as defendants, and an *in rem* action against the domain name.

4. Immediately deliver a file stamped copy of the complaint to the registrar. This will force the registrar to freeze the domain name, thus preventing the domain name from being sold or transferred.

Current Domain Name Holder Protection

What if a company accuses someone of cybersquatting, and the registrar suspends or cancels the disputed domain name as a result? Does the former domain name holder have a procedure for recovering the domain name? The answer is, "Yes." If a registrar suspends or transfers a domain name, the original domain name holder can then bring a civil suit presumably against the registrar, with notice to the trademark owner, seeking a judicial declaration that use of the domain name was in fact lawful. If the original holder is successful, the court can issue an order that the domain name be reactivated or transferred back to the original holder.

What if a domain name was canceled in response to a cybersquatting accusation that was based on a misrepresentation by the accuser? In that case, the domain name holder has an additional remedy. Anyone who makes a knowing and false representation that a domain name is identical, confusingly similar to, or dilutive of a mark, thereby inducing the registrar to take action against the disputed domain name, is liable for both the domain name holder's actual damages as well as a non-discretionary award of costs and attorney fees.

Provisions Affecting Registrars

Domain name registrars such as Network Solutions, Inc. will not be monetarily liable for registering domain names unless they act with a "bad faith intent to profit" from the registrations, or act in "bad faith or reckless disregard."

Domain name registrars receive an additional safe harbor to encourage them to develop and implement their own policies for policing domain names. If the registrar adopts and follows a "reasonable policy" of refusing to register, removing from registration, transferring, or temporarily or permanently canceling a domain name registration, then the registrar will not be liable for damages caused by action that it takes under that policy.

As noted, a registrar that receives a file stamped copy of an *in rem* complaint must freeze the domain name and deposit the domain name with the court.

International Implications

***In Rem* Actions**—Under traditional U.S. law regarding *in rem* actions, property is subject to jurisdiction where the property is located. Since the Act declares that the "property" of a domain name is located in the judicial district where the registrar is located or where control documents have been deposited with the court, a U.S. plaintiff will be able to institute an *in rem* action within the United States for control of any domain name that has been registered with a U.S. registrar by a foreign person.

ICANN Arbitration—If the domain name in dispute was not registered with a U.S. registrar but nevertheless includes a top level domain of .com, .net, or .org, the complaining party can bring an arbitration proceeding under the domain name dispute policy of ICANN,[8] the non-profit organization responsible for overseeing registration of those TLDs.

Civil Actions Against a Domain Name Holder—What about domain names that are not .com, .net, or .org, and that are not registered with a U.S. registrar? Suppose for example, someone has registered MICROSOFT.BF in Burkina Faso. How can the trademark owner proceed?

First, many countries offer trademark protection to holders of famous domain names. The trademark owner should therefore first look to the law of the country of registration to see whether it can obtain effective relief under the local law. If the national laws in that country do not help, or if the trademark owner wishes to proceed in a U.S. court regardless of whether it can proceed in a foreign court, can it? According to well established law, a U.S. court has personal jurisdiction over a defendant that is not physically present in the forum if the test for either general or special jurisdiction is satisfied. General jurisdiction is satisfied if the defendant has "substantial" or

The Computer Law Association Bulletin

"continuous and systematic" contacts with the forum. Special jurisdiction may be present when the claim arises directly from the contacts with the forum.

Personal jurisdiction may or may not be satisfied by the registering of a domain name and the operation of a website, depending on the specific facts of the case. If the defendant maintains an active website from which it sells products or enters into contracts with individuals who reside within the forum, the defendant is subject to jurisdiction. On the other hand, operating a "passive" site that merely provides information about products and services is not sufficient for jurisdiction.

The purpose of the website and domain name registration must also be considered. Jurisdiction exists when a defendant registers a domain name for the purpose of selling it to the trademark holder, because this creates a sufficient harm to the trademark owner in the trademark owner's own state of residence. This is different from a case in which a defendant registers the domain name for the purpose of operating a legitimate business at the site rather than selling the domain name to the plaintiff; in such a case, registering the domain name and operating the website are not, by themselves, sufficient for jurisdiction. Thus, according to the Ninth Circuit at least,[9] whether a court has jurisdiction over a domain name registrant will depend in large part on whether the registration was done with the intent to sell the domain name for profit, which is essentially the same "bad faith" test embodied in the Act's substantive provisions. Whether foreign registrars will respect judgments of U.S. courts with respect to disputed domain names remains to be seen.

Conclusions

By consulting with their counsel to take the following steps now, companies will help to strengthen their cybersquatting challenges to domain names held by others, and will help to protect their own domain names from cybersquatting challenges brought by others.

- If possible, register, or apply to register, your domain name as a trademark with the U.S. Patent and Trademark Office.
- Document your bona fide selling of goods and services or bona fide intention to sell goods and services using your domain name. This will help to fend off, if necessary, a challenge by another to your company's right to use that domain name or to warehouse the domain name for future use.
- Immediately identify all domain names that are owned by others but that are similar to your trademarks. Visit those sites. Print out the pages that show whether or not the domain name is being used in the bona fide offering of goods and services. Some cybersquatters freely admit (or even brag) on their pages that they are cybersquatters, and that they intend to sell to the highest bidder. Obtaining printouts of such pages now—before the cybersquatter can change them—will be extremely helpful in making your cybersquatting case later.
- Collect and document any explicit or implicit offers that you have received from cybersquatters to sell their domain names.
- Study the domain name dispute policy, if any, of the registrars that registered the domain names that you would like to obtain. Determine with your counsel whether you would prefer to proceed under the dispute policy, including arbitration if provided for, or via court action. Ask the registrar whether it is willing to deposit the domain name in the court that you prefer to hear the dispute.
- If applicable, have your counsel send notices via U.S. mail and e-mail to those persons who are cybersquatting in violation of your rights, asking them to identify themselves and informing them that you intend to file an *in rem* action against the disputed domain name under the Anticybersquatting Consumer Protection Act,[10] if they do not identify themselves by a specific deadline. Once you file your *in rem* complaint, immediately deliver a file stamped copy of the complaint to the registrar, thereby forcing it to freeze the domain name and deposit the domain name with the court.

Endnotes

* Joel Voelzke, with Oppenheimer Wolff & Donnelly LLP in Los Angeles, California, may be reached at 310-788-5021 or JVOELZKE@OWDLAW.COM.

1. 66 F.Supp.2d 117 (D MA 1999).
2. 15 USC §1125(d)(1)(A)(i), (B)(i).
3. Nos. 98-7452, 98-7538 (2d Cir. Feb. 2, 2000). The case is available at WWW.TOUROLAW.EDU/2NDCIRCUIT/FEBRUARY00/98-7452.
4. *Id.*
5. The district court's decision and order had origi-

nally been based only on dilution grounds, because the Act was not enacted until after it had issued its decision.

6. See note 3.

7. 51 F.Supp.2d 707 (ED VA 1999).

8. The ICANN dispute resolution policy can be found at WWW.ICANN.ORG/UDRP/UDRP.HTM.

9. E.g., *Panavision v. Toeppen*, 141 F.3d 1316 (9th Cir. 1998).

10. 15 USC §1125(d)(2).

Insurance for Internet and E-Commerce Liabilities

By: David B. Goodwin and Rene L. Siemens, San Francisco, California*

With the growth of the Internet there has been a corresponding increase in Internet-related business risks. Potential sources of loss or liability for Internet businesses include cyber attacks,[1] defects that may cause a network "crash," and software glitches that result in data loss. Such losses may result in high stakes litigation.

Traditional insurance policies cover some of the new risks, but all too often carriers view traditional policies as giving the policyholder standing to sue, rather than as comprehensive protection against losses and litigation. Moreover, technologies risks may fall outside the scope of traditional insurance policies. The insurance industry is starting to respond with special policies; however, some of these new policies ignore the real risks created by the Internet and e-commerce, and therefore may not be worth the cost.

This article addresses the issues that arise in making Internet or e-commerce claims under three traditional insurance policies: commercial general liability (CGL), directors' and officers' (D&O) and errors and omissions (E&O) liability policies, as well as special Internet policies. For each type of policy we briefly describe the potential claims covered, and then analyze the basic insurance issues of which companies and their risk managers should be aware.

CGL Policies

Comprehensive General Liability policies pay to (1) defend the insured against suits seeking damages that the policies potentially cover,[2] and (2) indemnify the insured against any judgments or settlements that the policy actually covers. The standard CGL policy covers claims for damages that involve "bodily injury," "property damage," "personal injury" (typically, specified torts not involving bodily injury), and "advertising injury" (typically, specified offenses committed in the course of advertising). Each affords some protection for businesses using the Internet or engaging in e-commerce. However, the standard CGL policy language was drafted long before and therefore does not really provide the promised "comprehensive" liability coverage needed in the new economy.

Property Damage Liability Coverage

Standard CGL policies cover not only damage to "tangible property," but also "loss of use of tangible property that is not physically injured." Thus, for example, if a consultant writes a defective program that causes an electronic retailer to lose access to essential data and shut down temporarily, the CGL policy may cover a subsequent lawsuit against the consultant even though physical damage to tangible property did not occur.

However, the requirement of "tangible property" raises the issue as to whether electronically stored data are tangible property. *Black's Law Dictionary* defines tangible property as that which may be felt or touched, and is necessarily corporeal, whereas intangible property is defined as property that has no intrinsic and marketable value, but merely represents value. Electronically stored data rarely fall into either of these categories. Unless printed, they cannot be touched; however, they often have a great deal of intrinsic value. To date, most courts that have approached the issue of tangibility have not done so in connection with insurance claims. While court holdings have varied, most have held that data stored on a disk are not tangible property.[3]

The Computer Law Association Bulletin

Insurance coverage cases in which courts have found data loss to constitute damage to tangible property have tended to involve physical damage to the computer hardware or disk on which the data were stored.[4] However, other courts have suggested that even where data loss is caused by damage to the storage medium, there would be no CGL coverage for the value of the lost data.[5] To date, courts have been reluctant to decide whether pure data loss, unaccompanied by damage to a disk or a hardware component, constitutes "tangible property damage."[6] With the proliferation of e-commerce and Internet communications, and the attendant increase in risk of valuable data loss, courts will be forced to resolve this question. The outcome will have major insurance ramifications.

Most CGL policies contain an exclusion for certain liabilities resulting from "your product" or "your work," as well as for product recall costs. Therefore, coverage could depend on whether software is characterized as a product or a service. To date, this issue is also unresolved. Under the UCC, software is a product when mass designed and distributed; a service when custom designed and installed for a unique use.[7] Courts may use this distinction in resolving insurance coverage.

Bodily Injury Liability Coverage

The most common injuries resulting from computer products are repetitive stress injuries; however, the range of possible claims is astounding. For example, a bystander wounded during an armed robbery in the District of Columbia sued the District and its IT vendor for negligence,[8] claiming that her injury was caused by the vendor's failure properly to maintain a computer system on which an arraignment judge, who had recently released the robber, relied for obtaining arrestees' criminal records. Companies may also face bodily injury claims resulting from publishing incorrect information online. For example, a website that publishes incomplete or incorrect medical information could be sued by an injured recipient of the information.[9] In the few cases involving published information, courts have been hesitant to find liability for publishing incorrect information.[10]

Advertising Injury and Personal Injury Coverage

The "advertising injury" clause may afford coverage for a broad range of other claims because Internet activity that promotes a company's name, goods, or services for commercial purposes arguably constitutes "advertising." In addition, the "personal injury" clause may cover many Internet breach of privacy claims.

CGL policies use a number of advertising injury clauses. The original version, issued in 1973, covers injuries "aris[ing] out of libel, slander, defamation, violation of right of privacy, piracy, unfair competition or infringement of copyright, title or slogan." The 1973 clauses excluded coverage for "injury arising out of…infringement of trademark, service mark or trade name, other than titles or slogans." In 1986, the standard policy language was modified to cover injuries "arising out of…publication of material that slanders or libels a person or organization or disparages a person's or organization's goods, products or services, [or] that violates a person's right of privacy; misappropriation of advertising ideas or style of doing business; and infringement of copyright, title or slogan." Some recent policies include different lists of covered offenses, e.g., the 1998 standard CGL policy omits "misappropriation of style of doing business."[11]

Copyright Infringement—There is great risk of copyright infringement on the Internet. While ISPs are largely shielded,[12] users and website operators may be liable if copyrighted material is uploaded or downloaded without the copyright owner's permission, a web page contains a border or "frame" of text or graphics pulled from another site, or a site enables users to link to another site that contains protected material.[13] Copyright infringement is a covered offense under the standard advertising injury clause. Therefore, the primary coverage issue will be whether the requisite connection exists between the injury and the policyholder's advertising activities. This connection has been much easier to prove in copyright than in other intellectual property cases.[14]

Trademark Infringement—Infringement can occur when material containing a company's trademark is downloaded or uploaded without authorization, website pages and other online publications make unauthorized use of a company's trademark or style of doing business, a cybersquatter's use of a domain name violates an existing mark, one company uses a metatag containing the trademark or trade name of a competitor, or a search engine sells advertisers "keys" consisting of other companies' trademarks or trade names.

Whether trademark infringement is a CGL-enumerated offense is complicated by changes in policy language. Under the 1973 standard policy, trademark infringement was an expressly enumerated covered offense. However, a 1981 version excluded advertising injury arising out of "[i]nfringement of trademark, service mark or trade name, other than titles or slogans, by use thereof on or in connection with goods, products or services sold, offered for sale or advertised." This exclusion for trademark infringement was deleted from the 1986 CGL form, which added the enumerated offense of "misappropriation of advertising ideas or style of doing business." The 1986 language has given rise to a split among the courts as to whether trademark infringement is covered.[15]

Patent Infringement—Courts have been reluctant to find advertising injury coverage for patent infringement unless the insured has a specialized intellectual property policy. The vast majority have held that patent infringement is not a covered offense under an advertising injury clause.[16] However, a few courts have concluded that patent infringement claims fall within the "piracy" offense in the 1973 advertising injury clause or other provisions.[17]

Even if patent infringement is covered, courts typically fail to find a causal connection between the injury and the policyholder's advertising activities, concluding that since a patent cannot be infringed by advertising a causal connection cannot exist between advertising and patent infringement.[18] When policyholders attempt to establish the requisite connection through a claim involving inducement to infringe a patent, the courts have ruled (almost certainly incorrectly) that an inducement claim necessarily requires "willful" conduct,[19] which cannot be covered as a matter of public policy in most states and by statute in California.[20]

Effective in 1996, Congress expanded the definition of "patent infringement" to include "offers to sell" a patented invention.[21] While this expansion causes exposure to much greater liability, it also increases the chances of obtaining insurance coverage. Advertising patented items would constitute an offer to sell. Also, the very act of advertising the item would lead to the injury, thus creating a causal connection between the advertising and the injury. A few cases have addressed the scope of coverage for patent infringement under the new law.[22]

Defamation and Invasion of Privacy—The number of defamation and invasion of privacy claims against Internet users and providers is likely to increase. The advertising injury clause in a standard CGL policy insures liability arising out of "[o]ral or written publication of material that slanders or libels a person or organization or disparages a person's or organization's goods, products, or services." This coverage extends to defamation and invasion of privacy on the Internet.

Liability for defamation depends on the defendant's knowledge of and control over the content of the material containing the defamatory statement. The author or speaker of the defamatory comment is the least likely source for substantial damages and, therefore, not the primary target of most defamation actions. Publishers, including broadcasters, newspapers, and magazines, are also liable for defamatory statements that they disseminate because they exercise editorial control over their publications or broadcasts. In contrast, common carriers, such as telephone companies, are not liable because they exercise no editorial control over online messages. Secondary publishers, such as bookstores and newsstands, are also generally not liable except when they have knowledge of the defamatory nature of the materials distributed.

These principles carry over into cyberspace. Accordingly, writers, website creators, and other originating sources face liability for defamation claims. Congress has limited the liability of online service providers, depending on the degree of editorial control exercised over the content of transmitted statements. The ISPs may be liable as publishers if they exercise substantial editorial discretion; if they exercise little or no editorial discretion, they will be considered secondary publishers.[23]

The standard CGL personal injury clause covers defamation as well as "publication of material that violates a person's right to privacy." However, there is an exclusion from personal injury coverage for "advertising, publishing, broadcasting, or telecasting done by [your company]." This exclusion is designed to limit advertising claims to the advertising injury clause, but the advertising injury clause itself contains an exclusion for "an offense committed by an insured whose business is advertising, broadcasting, publishing, or telecasting." Therefore, whether websites constitute "advertising" or "publishing," as well as whether site designers and managers are in

The Computer Law Association Bulletin

the business of "advertising" or "publishing," could have important ramifications on the availability of insurance coverage for defamation claims under either the personal injury or advertising injury clauses. Courts have yet to address these issues. Risk adverse businesses may do well to purchase media or Internet liability policies to avoid this exclusion.

D&O and E&O Policies

D&O insurance covers losses due to the wrongful acts of a company's directors and/or officers. E&O policies cover errors on the part of the company and its employees. In the standard D&O or E&O policy, a "wrongful act" is defined as "any active or alleged error, installment, misleading statement, act or omission or negligent breach of duty." "Loss" is defined as "damages, settlements, judgments, and defense costs."

D&O and E&O policies typically exclude coverage for property damage and bodily injury, but afford broad coverage for purely economic damages. As with CGL policies, the Internet raises new questions. Applying traditional contract law to this new medium raises concerns regarding the authenticity and integrity of e-documents, the difficulty of differentiating the original document from a copy or a draft, and the opportunities to alter or falsify documents without being detected. In addition, electronic transactions challenge common law elements concerning the formation of a contract: What constitutes an offer in cyberspace? When was the offer received? When was it accepted? How does the statute of frauds apply electronically? Which party bears the risk of loss in the event of a botched electronic communication?

Issues of security and confidentiality are also heightened when transacting business over the Internet because e-documents are far more susceptible to security breaches than tangible documents. Internet commerce substantially increases the risk of both employee and third party theft or misappropriation. Last, there is the issue of who should bear the risk of loss in the event of a transmission malfunction. If there is no provision in the contract that places this risk on one of the parties, then the parties may seek to hold the ISP liable.[24]

The Internet has also provided a global, convenient, and quick medium to trade securities. Since 1995, the Securities and Exchange Commission has treated electronic information as the substantial equivalent of printed information if certain steps are taken to ensure proper delivery.[25] However, e-transmissions are not identical to printed transmissions. First, insurance issues arise from the potential for misrepresentations and fraud in e-trading. Second, there is a potential for unreliable transmission of an e-trade. Third, the use of hypertext links creates potential liability because any text linked to a prospectus may be considered part of the prospectus and, thus, subject to the securities laws. Fourth, an e-securities solicitation may be subject to securities regulations in each of the 50 states, and even the laws of other countries. Finally, ISPs used in e-securities trading must be careful to charge a flat fee for their services rather than a fee related to the value of the transaction, or they could be characterized as brokers or dealers and subjected to SEC broker-dealer registration requirements.

Anyone who engages in a commercial or securities transaction over the Internet is a potential defendant in these types of claims. However, Internet retailers, bankers, securities dealers, and other financial service providers, product manufacturers and distributors, ISPs, and securities issuers and their underwriters should be most aware of the potential liabilities inherent in electronic transactions.

Where a third party claims that it has suffered economic losses as a result of an e-transaction gone wrong, the company's D&O policy may provide coverage to the extent that its directors and officers are held directly liable for the loss or to the extent the company is permitted or required to indemnify them. Unlike CGL insurance, however, D&O policies cover the liabilities of corporate directors and officers, but typically not those of the company itself. Therefore, given that CGL policies' coverage for bodily injury and property damage excludes liabilities based on contract and does not extend to purely economic loss, the company may need to look to other types of insurance—E&O policies or special media and Internet liability policies—for coverage of its own e-commerce related liabilities, at least to the degree they fall outside the categories included in advertising coverage.

Special Internet Insurance Policies

In recent years, insurance companies have developed policies targeted toward Internet and e-commerce liabilities, which are designed to fill the gaps left by traditional CGL and D&O policies. Some of the new policies cover liabilities for economic losses and damage to intangible property (e.g., e-data), as

well as contractual liabilities and liabilities arising from professional web publishing. In addition, coverage for the insured's own losses due to hacking and virus attacks is afforded by special anti-hacker policies. Although the new policies may be useful, there are still no standard form Internet insurance policies. Consequently, read the policy first, or risk paying for insurance that is either duplicative of existing policies or so limited that it is a waste of money.

Internet Liability Policies

Internet liability policies issued by several insurers (e.g., AIG, CNA, Admiral Reliance) cover acts or omissions by the insured that result in economic damage. Most complement CGL insurance by excluding coverage for bodily injury or property damage, and by expressly covering personal injury and advertising injury torts arising out of the insured's web publishing and webcasting activities. Some policies also complement existing CGL insurance by promising to cover claims that many courts have held not to be covered under standard CGL policy forms, such as patent infringement.

Insureds should note that Internet liability policies often contain restrictions that severely limit the value of the coverage. Although most cover losses due to security breaches and virus attacks, others expressly exclude them by, for example, broadly excluding claims arising out of "transmission of a computer virus; unauthorized access; unauthorized use; or loss of service." Given that such losses are what many Internet businesses are chiefly interested in insuring against, such an exclusion substantially eliminates the value of an Internet liability policy. Similarly, policies that exclude coverage for claims or investigations by state or federal agencies may be of limited value, because breaches of security and users' privacy rights are increasingly the focus of governmental—as opposed to private—scrutiny.

First-Party Anti-Hacker Insurance

The insurance policies discussed only cover the insured's liabilities to third parties, not losses to the insured itself, in the form of valuable data lost because of a security breach, business interruption and lost revenues caused by downtime, or the cost of remediating or fixing a security or other software problem. Losses to the insured directly are covered instead by first-party insurance. The most common first-party insurance is the "all risk" or "named perils" property insurance that protects business premises and inventories, and that may also cover business interruption resulting from damage to property. The main problem with traditional property insurance when applied to the Internet is that—like CGL coverage for bodily injury and property damage—policies require damage to "tangible property,"[26] and many cyberspace losses do not neatly fit into this category.

For first-party losses, companies should consider the Internet first-party policies issued by several insurers, including Lloyd's, ACE, CNA, and Reliance National, sometimes called anti-hacker insurance because they cover losses to the insured as a result of hacking and virus attacks, including business interruption losses due to a covered cause. Some of these policies also include coverage for costs of preventing security breaches and virus attacks that have not yet occurred but have been threatened, such as by hackers who extort by demanding a ransom for not attacking the company's network.

Endnotes

* David B. Goodwin and Rene Siemens are with Heller Ehrman White & McAuliffe LLP in San Francisco. They may be reached at 415-772-6000; their respective e-mail addresses are DGOODWIN@HEWM.COM and RSIEMENS@HEWM.COM.

1. "Locking Out the Hackers," *Businessweek*, Feb. 28, 2000, at 32-33.

2. *Montrose Chem. Corp. v. Superior Court*, 6 Cal.4th 287, 24 Cal.Rptr.2d 467 (1993); *George Muhlstock & Co. v. American Home Assur. Co.*, 502 N.Y.S.2d 174, 178 (App. Div. 1986).

3. See *Retail Systems Inc. v. CNA Ins. Co.*, 469 N.W.2d 735, 738 (Minn. App. 1991) (summarizing the tax rulings but refusing to apply them to insurance).

4. See *id.; Centennial Ins. Co. v. Applied Health Care Systems*, 710 F.2d 1288 (7th Cir. 1993).

5. See *Lucker Mfg. v. Home Ins. Co.*, 23 F.3d 808, 818-21 (3d Cir. 1994); *St. Paul Fire and Marine Ins. Co. v. National Computer Systems, Inc.*, 490 N.W.2d 626 (Minn. Ct. App. 1992) (information stored in a binder is not tangible property).

6. See *Magnetic Data, Inc. v. St. Paul Fire and Marine Ins. Co.*, 442 N.W.2d 153, 156 (Minn. 1989) (finding it unnecessary to decide whether data loss was damage to tangible property because it was accompanied by damage to drives on which the data was stored).

7. See *RRX Industries, Inc. v. Lab-Con Inc.*, 772 F.2d 543 (9th Cir. 1985); *Advent Systems Ltd. v. Unisys Corp.*, 925 F.2d 670 (3d Cir. 1991).

8. *Akin v. District of Columbia*, 526 A.2d 933 (D.C. App. 1987).

9. See N.P. Terry, "Cyber-Malpractice: Legal Exposure for Cybermedicine," 25 *Am.J.L. & Med.* 327 (1999).

10. See, e.g., *Winter v. G.P. Putnam's Sons*, 938 F.2d 1033 (9th Cir. 1991) (holding that the publisher of *The Encyclopedia of Mushrooms* was not liable to plaintiffs who became sick from eating mushrooms in reliance on information in the *Encyclopedia*).

11. The scope of the advertising injury offenses has been a source of substantial litigation in recent years. Some courts hold that CGL policies only cover claims actually bearing the names of the advertising offenses. See, e.g., *Advance Watch Co. v. Kemper Nat'l Ins. Co.*, 99 F.3d 795 (6th Cir. 1996). Other courts conclude the covered offenses are general terms that encompass a variety of claims, e.g., *Lebas Fashions, Inc. v. ITT Hartford Ins. Co.*, 50 Cal.App.4th 548, 559, 59 Cal.Rptr.2d 36 (1996).

12. See 17 USC §512(c).

13. E.g., *Intellectual Reserve Inc. v. Utah Lighthouse Ministry, Inc.*, 75 F.Supp.2d 1290 (D. Utah 1999); *Sega Enterprises, Ltd. v. MAPHIA*, 857 F.Supp. 679, 686-87 (N.D. Cal. 1994); *Playboy Enterprises v. Frena*, 839 F.Supp. 1552, 1556 (M.D. Fla. 1993).

14. See, e.g., *Federal Ins. Co. v. Microsoft Corp.*, 1993 U.S. Dist. LEXIS 5468 (W.D. Wash. 1993).

15. Compare *Advance Watch*, n. 11 *supra* (rejecting coverage for trademark infringement) with *Lebas*, n. 11 *supra*.

16. See *Simply Fresh Fruit v. Continental Ins. Co.*, 84 F.3d 1105 (9th Cir. 1996); *Intex Plastic Sales v. United National Ins. Co.*, 23 F.3d 254 (9th Cir. 1994); *Heil Co. v. Hartford Acc. and Indem. Co.*, 937 F.Supp. 1355, 1365 (E.D. Wis. 1996); *Owens-Brockway Glass Container, Inc. v. Int. Ins. Co.*, 884 F.Supp. 363 (E.D. Cal. 1995); *Atlantic Mut. Ins. Co. v. Brotech Corp.*, 857 F.Supp. 423 (E.D. Pa. 1994), *aff'd*, 60 F.3d 813 (3d Cir. 1995); *St. Paul Fire & Marine Ins. Co. v. Advanced Interventional Systems, Inc.*, 824 F.Supp. 583 (E.D. Va. 1993), *aff'd*, 21 F.3d 424 (4th Cir. 1994).

17. See *U.S. Fidelity & Guar. v. Star Technologies*, 935 F.Supp. 1110 (D. Or. 1996); *New Hampshire Ins. Co. v. R.L. Chaides Constr. Co.*, 847 F.Supp. 1452, 1456 (N.D. Cal. 1994); *National Union Fire Ins. Co. v. Siliconix, Inc.*, 729 F.Supp. 77 (N.D. Cal. 1989); *Union Ins. Co. v. Land and Sky, Inc.*, 529 N.W.2d 773 (Neb. 1995).

18. See, e.g., *Aetna Cas. & Sur. Co. v. Superior Court*, 19 Cal.App.4th 320, 23 Cal.Rptr.2d 442 (1993); *National Union Fire Ins. Co. v. Siliconix, Inc.*, 729 F.Supp. 77 (N.D. Cal. 1989); but see *Union Ins. Co. v. Land and Sky, Inc.*, 529 N.W.2d 773 (Neb. 1995) (find a duty to defend); *Elan Pharmaceutical Research Corp. v. Employers Ins. of Wausau*, 144 F.3d 1372 (11th Cir. 1998) (CGL insurer owed a duty to defend against a patent infringement claim where patent infringement was one of the policy's enumerated advertising injury offenses).

19. *Aetna, id.*

20. For example, California Insurance Code §533 excludes insurance coverage for willful acts.

21. 35 USC 271(a) ("Except as otherwise provided in this title, whoever without authority makes, uses, offers to sell or sells any patented invention, within the United States or imports into the United States any patented invention during the term of the patent therefor, infringes the patent").

22. E.g., *Maxconn Inc. v. Truck Insurance Exchange*, 74 Cal.App. 4th 1267, 88 Cal Rptr.2d 750 (1999), considered whether patent infringement is covered under a CGL policy defining advertising injury as "infringement of copyright, title or slogan." The court noted that because of the amendment, defendants could no longer argue "that patent infringement could not arise out of the insured's advertising activities as a matter of law." Nevertheless, it found the infringement not covered.

23. See Communications Decency Act of 1996, 47 USC §230. The Act also offers some protection to ISPs against "Good Samaritan" blocking and screening of offensive material.

24. The National Conference of Commissioners on Uniform State Laws has proposed adding a new article to the UCC, addressing some of the above issues. See UCC Article 2B-103 (proposed 2/96). California has enacted these proposals.

25. See SEC Release No. 33-7233, Oct. 6, 1995.

26. See *Home Indem. Co. v. Hyplains Beef, L.C.*, 893 F.Supp. 987, 990 (D. Kan. 1995), *aff'd* 89 F.3d 850 (10th Cir. 1996) (no coverage under a first-party property policy for reduced meat production due to a computer malfunction resulting from a loss of electronic data, because the data were not tangible property).

United States Law Developments

SECOND CIRCUIT REGION

By: Aram Sarafian and John Flock,
Kenyon & Kenyon, New York, New York

NSI ENTITLED TO ANTITRUST IMMUNITY

Name.Space Inc. v. Network Solutions, Inc., 2000 U.S. App. LEXIS 770 (2d Cir. January 21, 2000)

The Second Circuit has affirmed the district court's dismissal of Name.Space's complaint that Network Solutions violated the Sherman Act by refusing to register additional generic top level domains (TLDs) in the master root zone file. In so affirming, the Second Circuit held that NSI does not have status-based antitrust immunity under the federal instrumentality doctrine.

The federal instrumentality doctrine arose in *Sea-Land Service, Inc. v. Alaska Railroad*, 659 F.2d 243 (DC Cir. 1981), where the court held that, based on their status as federal instrumentalities, any such agencies and officials remain outside the reach of the Sherman Act. The Second Circuit determined that applying this status-based doctrine to a private entity such as NSI "might improperly insulate NSI and other private entities that are or will be involved in administering the DNS from liability for future anticompetitive conduct." The Second Circuit therefore rejected status-based immunity but found implied conduct-based immunity for NSI because its actions were compelled by a Cooperative Agreement between NSI and the National Science Foundation.

The Second Circuit found that the Cooperative Agreement, which allows NSI to administer the master root zone file, removed any NSI discretion over registering TLDs. For this reason, NSI has implied conduct-based immunity under the federal instrumentality doctrine for registering TLDs. The Second Circuit clearly limited NSI's implied immunity to the registration of TLDs, a process over which all control was maintained by the federal government through the Internet Assigned Numbers Authority and NSF.

This case arose in March 1997 when Name.Space requested that NSI record 530 new gTLDs in the root zone file. NSI consulted with IANA, which disclaimed any supervision authority over NSI. NSI also consulted with NSF, which rejected Name.Space's proposal to add the new gTLDs. Furthermore, NSF stipulated in its response that NSI must obtain written approval before "making or rejecting any modifications, additions, or deletions to the root zone file." As a result, the case commenced with motions filed for preliminary injunction and summary judgment.

The Computer Law Association Bulletin

By: Richard J. Caira, Jr., Womble Carlyle Sandridge & Rice, PLLC, Raleigh, North Carolina

FOURTH CIRCUIT REGION

DOMAIN NAME REGISTRATION NOT SUBJECT TO LIEN

Dorer v. Arel, 60 F.Supp.2d 558, 1999 U.S. Dist. LEXIS 13558 (E.D. Va. September 3, 1999)

Dorer prevailed, via default judgment, on a trademark infringement action in which Arel was using Dorer's trademark as a domain name. The relief granted included money damages of $5,000 and an injunction against Arel, ordering it to cease use of the domain name, but did not address disposition of the domain name.

Dorer then moved for a writ of *fieri facias* against the domain name, a method by which judgment may be satisfied by levying a lien on the debtor's personal property. The court addressed the issue, one of first impression, of whether a domain name registration is "personal property" and can be subject to a judgment lien. Noting that under trademark law the words that comprise a trademark are not property that can be owned, a trademark owner only can enjoin others from using such words in commerce if the use would cause confusion as to source or dilute the value of the mark. Furthermore, trademarks cannot be transferred as property without the accompanying goodwill of the business to which they are attached.

After analyzing whether domain names are personal property, the court concluded that it did not need to resolve the issue. Domain names are subject to contract rights as between the domain name owner and the register of the domain name (in this case, NSI). NSI has in place two resolution policies regarding disposition of domain names that are the subject of a dispute, either one of which reasonably could have been invoked by Dorer. The court held that Dorer should exhaust its reasonable self-help remedies (such as the NSI dispute resolution procedures) before compelling the court to transfer a domain name.

By: Paul C. Van Slyke and Hieu Dang, Locke Liddell & Sapp LLP, Houston, Texas

FIFTH CIRCUIT REGION

E-MAILS HELD SUFFICIENT FOR PERSONAL JURISDICTION

Bellino v. Simon, 1999 WL 1059753, 1999 U.S. Dist. LEXIS 18081 (E.D. La. November 22, 1999)

The court held that allegedly defamatory e-mails sent from New York to Louisiana constituted sufficient minimum contacts to establish personal jurisdiction by a Louisiana court over the sender of the e-mails.

Christopher Aubert, a resident of Louisiana, purchased two baseballs autographed by Babe Ruth and Lou Gehrig from Forensic Document Services. Aubert then visited a website run by Richard Simon Sports, Inc., a New York corporation that buys, sells, and authenticates sports memorabilia and autographs. Richard Simon is president of Richard Simon Sports. Aubert e-mailed Simon via the website and the two exchanged multiple e-mails concerning the authenticity of the autographed baseballs Aubert had purchased from FDS. In an e-mail and a telephone conversation initiated by Aubert, Simon stated that the autographs were forgeries. Upon Simon's recommendation, Aubert also contacted James Spence, Jr., the Managing Member of James Spence III Vintage Autographs, LLC, formed in Pennsylvania. In a telephone conversation and a written report sent to

Aubert, Spence indicated he also could not authenticate the autographed baseballs. Based on the foregoing, FDS and its president, Bellino, sued Simon and Spence, alleging, among other claims, that they had made defamatory statements regarding Bellino.

Spence and Simon responded by moving to dismiss on the grounds that the court lacked personal jurisdiction over them. As to Spence, the court found that the one unsolicited telephone call from the forum state Louisiana to Spence, a resident of Pennsylvania, was not sufficient to establish specific personal jurisdiction. The court also rejected Bellino's arguments that general personal jurisdiction was supported by the Spence Vintage Autographs website, because the site was maintained by Spence Vintage Autographs, not by Spence individually.

However, the court found that Simon had made enough contacts with Louisiana to support specific personal jurisdiction. Even if the telephone conversations between him and Aubert, who was in Louisiana, were not sufficient to establish minimum contacts, the allegedly defamatory e-mails sent to Louisiana constituted sufficient minimum contacts. That the contacts occurred over the Internet did not affect the court's jurisdictional analysis.

EIGHTH CIRCUIT REGION

By: Scott J. Bergs, Leonard, Street and Deinard P.A., Minneapolis, Minnesota

INTERCONNECT FEES ORDERED BY STATE PSC

Southwestern Bell Telephone Co. v. Connect Communications Corp., 1999 WL 996994 (E.D. Ark. September 22, 1999)

Southwestern Bell Telephone filed suit against Connect Communications, asking the court to declare an order issued by the Arkansas Public Service Commission unlawful. The APSC order required SBT to pay interconnect fees to CCC for calls from SBT's customers to CCC's ISP customers ("Internet connections") based on CCC's argument that Internet connections "terminate" at the ISP as defined by the interconnect agreement and therefore constitute "local calls" subject to an interconnect charge. SBT denied that Internet connections are local calls, arguing that the calls do not terminate at the ISP but rather pass through to the Internet, which extends worldwide.

In addition, SBT argued that the determination of whether Internet connections are local calls is a federal question determined under the Telecommunications Act of 1996 (47 USC §251 et seq.). CCC argued that the determination is merely a question of state contract law and, therefore, SBT's claims must be dismissed for lack of subject matter jurisdiction. The court agreed.

The court reasoned that (1) the Telecommunications Act of 1996 provides that companies may independently negotiate and establish interconnect agreements subject only to approval by a state commission, and (2) no federal court or FCC decision has determined that Internet calls are local calls for purposes of interconnect agreements. Having dismissed the case, the court did not address the merits of whether Internet calls constitute local calls.

The Computer Law Association Bulletin

IN-HOUSE CONSULTANT OWNS PROGRAM COPYRIGHT

Kirk v. Harter, 188 F.3d 1005 (8th Cir. 1999), *rehearing denied* (8th Cir. October 13, 1999)

Kirk, the owner and operator of Iowa Pedigree, filed suit against Harter, an in-house consultant and the developer of a software program, when Harter began providing maintenance services to Kirk's customers.

Iowa Pedigree assisted dog breeders and brokers in complying with AKC and USDA licensing and registration requirements. Kirk hired Harter to develop a computer program for use by Kirk's customers. For six years Harter developed such programs exclusively for Kirk. In 1996, however, several of Kirk's customers terminated their relationships with Kirk and began purchasing programs and services directly from Harter. Kirk filed suit for copyright infringement and various other claims, asserting that by selling updated versions of the software developed for Kirk, Harter infringed its copyrights. Harter argued that no infringement had occurred. Because he was an independent contractor, the copyright in the program was his; the program was not a "work made for hire" under the Copyright Act (17 USC §101).

The court held that Harter was an independent contractor, recognizing that Harter worked primarily on-site at Kirk's facility and utilized Kirk's equipment to create the programs. However, Kirk failed to treat Harter as an employee for tax purposes, did not provide employee benefits, and made payments to Harter on an irregular schedule. Harter had also undertaken projects for other customers, in one instance hiring a subcontractor. On balance, the facts weighed in favor of finding that Harter was an independent contractor and, therefore, the copyright to the program belonged to him.

MISSOURI "HOT NEWS" MISAPPROPRIATION CLAIMS NOT PRE-EMPTED

Fred Wehrenberg Circuit of Theatres, Inc. v. Moviefone, Inc., 73 F.Supp.2d 1044, 1999 WL 1000469, 1999 U.S. Dist. LEXIS 17574 (E.D. Mo. November 1, 1999)

Wehrenberg, a movie theater company, publishes movie playtimes for its own theaters and those of a few others on an Internet website (CINE-TEX). Moviefone provides movie playtime information over the telephone and on an Internet website (MOVIEFONE) for several markets across the United States, including St. Louis, the market in which Wehrenberg operates. Wehrenberg sued Moviefone for unfair competition under Missouri law, on the grounds of misappropriation of movie theater playtime information. Specifically, Moviefone took information from CINE-TEX and posted it on MOVIEFONE, constituting commercial "free-riding" on the costly efforts made by Wehrenberg to gather and display its information.

Wehrenberg's claim was based on the "hot news" doctrine established in *International News Service v. Associated Press*, 248 U.S. 215 (1918) ("hot news" is given a quasi-property value due to its time sensitivity, commercial value, and the time, skill, effort, and money required to gather it). Moviefone claimed that the Copyright Act, enacted after the holding in *International News*, preempts Wehrenberg's state law claim.

The court found that hot news claims are not preempted by the Copyright Act. Relying on the legislative history of the preemption section of the Copyright Act (17 USC 301), the court found that Congress specifically intended to provide an exception to the preemption rule for hot news claims. The court recognized that the Second Circuit and the Northern District of Illinois have both issued decisions agreeing with this holding.

Despite this ruling, the court ruled for Moviefone on the ground that one of the hot news requirements—that the free-riding activities so reduce the incentive to produce the product or service that its existence or quality would be substantially threatened—was missing. The court concluded that, despite Moviefone's actions, Wehrenberg could still generate movie schedules and publicize them through a variety of media.

HOME-MARKET.COM NOT LIKELY TO BE CONFUSED WITH HOME-MARKET.NET

Shade's Landing, Inc. v. Williams, 76 F.Supp.2d 983, 1999 U.S. Dist. LEXIS 19782 (D. Minn. December 22, 1999)

Shade, owner of the Internet domain name HOME-MARKET.COM, sued Williams, owner of the Internet domain name HOME-MARKET.NET, alleging trademark infringement and deceptive trade practices. Shade sought an order enjoining Williams from further use of its domain name during the course of the litigation. Shade's website targeted home owners and referred them to home-related services such as real estate agents, mortgage services, and landscapers. Shade also developed websites for real estate agents and brokers. Williams' site offered website development services for real estate agents and brokers, and provided advertising space for businesses in the real estate industry. Neither party had a federally registered trademark.

In the context of Shade's motion for a preliminary injunction, the court first sought to determine the validity of its mark by classifying it. Was it generic? descriptive? suggestive? or was it arbitrary and fanciful? Applying the "imagination" test, the court held that the mark HOME-MARKET.COM was descriptive of Shade's services and, therefore, not entitled to trademark protection absent a showing of secondary meaning. The court reasoned that the term "home" described services related to homes, "market" described services available to consumers, and ".com" described services available over the Internet.

In addition to finding that Shade's mark was descriptive, the court also concluded that there was little likelihood of confusion between the two marks, ultimately denying Shade's motion for a preliminary injunction. After recognizing that the domain names were virtually identical and that both companies offered web-based advertising and site development services to real estate agents, the court held that no likelihood of confusion had been proven. It stated that the mark was weak, that Williams was not alleged to have intentionally passed off its services as Shade's, and that very little evidence of actual confusion had been presented. Therefore, while a possibility of consumer confusion existed, that "possibility is not so strong that it constitutes a 'substantial likelihood' of confusion."

TENTH CIRCUIT REGION

By: Barry Weiss, Cooley Godward LLP, Denver, Colorado

FEDERAL JURISDICTION OF INTRASTATE E-MAIL ROUTED OUT OF STATE

United States v. Kammersell, 196 F.3d 1137 (10th Cir. 1999)

Federal jurisdiction was found in a criminal case involving a bomb threat transmitted via AOL's instant message service, even though the sender and the recipient were physically located in the same state. Kammersell, then 19 years old, sent a bomb threat to his girlfriend's computer terminal at work, hoping that the threat would enable her to leave work early so they could go on a date. Kammersell sent the threat from his home computer in Riverdale, Utah. His girlfriend received the threat at her worksite in Ogden, Utah. Every message sent via AOL is automatically routed through interstate telephone lines to AOL's main server in Virginia, where it is rerouted to its final destination. Kammersell was charged with transmitting a threatening communication in interstate commerce, in violation of 18 USC §875(c). That statute was enacted in 1934, and its last significant amendment was in 1939.

Today, many intrastate telephone calls and locally-sent Internet messages are routed out of state. Under the court's ruling, federal jurisdiction would exist to cover a large number of communications that otherwise appear to be intrastate in nature. The court agreed that in light of the current state of telecommunications, Congress may want to re-examine the statute.

The Computer Law Association Bulletin

By: John Carson and Eric M. Nelson,
Knobbe, Martens, Olson & Bear, LLP, San Diego, California

FEDERAL CIRCUIT REGION

PATENT UPHELD

Atmel Corp. v. Information Storage Devices, Inc., 198 F.3d 1374 (Fed. Cir. December 28, 1999)

Atmel, having developed and patented an improved charge pump circuit to boost voltage in computer memory, sued Information Storage Devices for patent infringement.

In a summary judgment motion, ISD argued that Atmel's patent was invalid because the claims failed to sufficiently define the invention under 35 USC §112, ¶2. Section 112 states that "[t]he specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention." Claim 1 recited the limitation of "high voltage generating means disposed on [a] semiconductor circuit for generating a high voltage from a lower voltage from a lower voltage power supply." The district court granted the motion based on the "technical form" of the specification, not including any structure corresponding to the disputed high voltage means. The court refused to consider whether the claim was indefinite based on the way the disclosure would be understood by one skilled in the art.

On appeal, the Federal Circuit determined that the district court erred in its analysis. Where a claim is written in means-plus-function language, 35 USC §112, ¶6 states that "[a]n element in a claim for a combination may be expressed as a means or step for performing a specified function with the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts *described in the specification* and equivalents thereof." Thus, ¶6 sets forth a simple requirement that a structure corresponding to a means-plus-function element must be included in the specification, and cannot be included by reference to an article. However, under ¶2, the district court erred in not determining whether sufficient structure was disclosed in the specification based on the understanding of a skilled technologist.

The court noted that although no specific structure was recited in the patent application, the specification did state that "[k]nown circuit techniques are used to implement high-voltage circuit 34. See On-Chip High Voltage Generation in NMOS Integrated Circuits Using an Improved Voltage Multiplier Technique, IEEE Journal of Solid State Circuits." Atmel's expert testified that the title alone was sufficient to indicate to one skilled in the art the precise structure of the means recited in the specification. The court held that, since such testimony was unrebutted, the summary judgment of invalidity was improperly granted and reversed the lower court ruling.

Practice Tip: In preparing a patent application for filing in the United States, confirm that each means-plus-function limitation of the claim has corresponding structure recited in the specification. Mere mention of a "black box," and a statement that the function is "well known," could prove to be a fatal defect to the patent's validity. Also, this case reinforces the need for patent practitioners to be wary of sole reliance on means-plus-function claim language.

International Law Updates

BELGIUM

By: Els Kindt, De Bandt, van Hecke, Lagae & Loesch - Linklaters & Alliance, Brussels

HYPERLINKS TO MP3 SITES HELD ILLEGAL

In two recent decisions, IFPI Belgium ASBL, an association that defends the rights and interests of the producers and distributors of phonograms, obtained favorable judgments imposing the removal of hyperlinks to illegal MP3 sites.

In the first case, IFPI sought injunctive relief against Belgacom Skynet S.A., a Belgian ISP and affiliate of the telephone operator Belgacom. Skynet was hosting Internet sites hyperlinked to other sites containing MP3 files with unauthorized digital copies of songs of famous pop groups.

IFPI argued that Skynet acted contrary to the Fair Trade Practices Act by not removing the hyperlinks to the MP3 sites while knowing that they enabled illegal copying (Article 93 WHPC). Skynet had been notified at least twice by IFPI about the illegal nature of the sites and was requested to remove the hyperlinks or the websites containing the links. IFPI also stated that Skynet had MP3 file scanners that enabled it to identify the MP3 sites and links.

Skynet argued that an ISP is not under an obligation to review the content of the homepages hosted on its server and is therefore not responsible for the content. The president of the Commercial Court refused to accept this defense, particularly because Skynet had been notified of the links to the illegal sites.

Accepting these arguments, the court granted an injunction in favor of IFPI, with a penalty of 500,000 BEF per day, and ordered Skynet to publish a summary of the judgment (President of the Commercial Court of Brussels, 2 November 1999). This decision is in line with a recent decision of the court of s'Gravenhage in the Netherlands (Arrondissementsrechtbank s'Gravenhage, 9 June 1999).

A few weeks later, IFPI obtained a second injunction against a student who had a website on which 25,000 links to MP3 sites were cited (President of the Court of First Instance of Antwerp, in summary proceedings, 21 December 1999). Previously, IFPI had notified the student of his illegal activities and had asked the ISP to close the site. The student, however, set up new websites with other ISPs.

In summary proceedings, the court rejected the argument that the student was not involved with the two new websites and prohibited him from publishing hyperlinks to unauthorized MP3 files on any website, under penalty of 50,000 BEF per day. The court also rejected a limitation of free speech defense, stating that publishing such links does not fall under the doctrine of free speech. The student was not a merchant and therefore the injunctive relief was not based on the Fair Trade Practices Act, but rather on the general rules of tort (Article 1382 of the Civil Code). The student has also been summoned in a procedure on the merits, in which IFPI claims damages for an amount of 15,000,000 BEF.

It is not known whether an appeal has been launched against either of the above decisions.

The Computer Law Association Bulletin

BRAZIL

By: Georges Charles Fischer, Fischer & Forster, São Paulo

E-COMMERCE LAW IN BRAZIL

There are no laws in Brazil dealing specifically with e-commerce. E-contracts generally are governed by the principles inscribed in the 1916 Civil Code (CC), the 1850 Commercial Code, and the 1990 Consumer Code.

Civil Code—As a general rule, the validity of a contract is contingent upon the following legal requisites: (1) legal capacity of the parties, (2) legality of the object of the contract, and (3) the form required or not prohibited by law (CC, Art. 82). Only a limited number of contracts, such as those involving real estate (CC, Art. 134, II) are subject to specific legal formalities. Under Brazilian law, contracts need not be written or, when written, formally signed in order to be valid and enforceable (CC, Art. 129). In fact, acceptance of a contract can be inferred from the acts or conduct of the parties. In principle, mail contracts or even verbal contracts—provided the latter are duly witnessed—are fully enforceable, to the extent relevant legal requirements and formalities, if any, are complied with (CC, Art. 1079 and 1086).

Thus, the general rule under Brazilian law is freedom of contract form. The essential element of a contract is the parties' agreement, which is often expressed by the acceptance of an offer. As a result, the mere fact that a contract has been formed by electronic means should not impair its validity or enforceability.

As a general rule, the offeror is bound by the offer, unless the offer itself states the contrary or the very nature of the business or the circumstances surrounding the transaction warrant a different conclusion (CC, Art. 1080). Thus, when a prospective customer accesses an electronic page and places an order, a binding contract between offeror and customer is created.

Offeror and customer become bound to the contract at the very moment the customer mails its acceptance, except if: (1) customer reneges before its acceptance reaches offeror, (2) customer undertook to await offeror's acceptance, or (3) acceptance is not received by offeror by the close of the term of validity of the offer (CC, Art. 1086).

In our view, real-time transactions would in all likelihood be deemed contracts between "present" parties (as opposed to "absent" parties), despite the fact that they are distance transactions. As a result, failure by offeree to immediately accept an offer that does not contain a fixed term of validity releases offeror from the obligation to honor the offer (CC, Art. 1081, I). E-mail contracts, in which transactions are not concluded on the spot, would probably be deemed contracts between absent parties, similar to those that take place by mail (CC, Art. 1086).

Consumer Code—Under the Consumer Code, consumers may renege (within seven days from execution of the contract or delivery of goods) on contracts entered into outside the offeror's premises. The Consumer Code accords protection to both individuals and legal entities that acquire goods as end users.

Adhesion contracts commonly are used for commercialization of goods on the Internet. Although Brazilian law made no specific reference to adhesion contracts before the Consumer Code was enacted, such contracts long were recognized as generally valid and enforceable, subject to special rules. An adhesion contract may be defined as a standardized contract that the seller of a good or service offers to a customer on an essentially "take it or leave it" basis; that is, the adhering party is not afforded an opportunity to bargain. Although many adhesion contracts are signed by the adhering parties, signatures are not prerequisite for validity and enforceability under Brazilian law. Acceptance of an adhesion contract can very well be inferred from the adhering party's acts or conduct.

Because an adhesion contract relegates to the subscribing party only the opportunity to adhere or reject, it does not satisfy the freedom of bargaining principle, so dear to Brazilian civil law. Legal scholars, the courts, and, more recently, positive law have established a number of rules to protect the party in the weaker bargaining position.

Thus, obscure or ambiguous language in an adhesion contract is generally interpreted against the offeror. This is because the offeror drafted and im-

posed the language and, in all likelihood, had more time to examine it than the adhering party. Moreover, courts have repeatedly declared null and void provisions deemed to be abusive or that contain terms and conditions that are flagrantly disadvantageous to the adhering party. The abusive or disadvantageous nature of a contractual provision is determined on a case by case basis.

The Consumer Code also provides that consumer contracts may be invalidated if the buyer is denied the opportunity to review the contract before acceptance, or if the contractual terms are difficult to understand (Art. 46). The risks of entering into agreements with individuals that do not have legal capacity (e.g., minors) or employees without legal authority should be attenuated by the resort to codes, encryption keys, digital signatures, and certifying authorities. If the person accepting an e-contract does not have the proper capacity or authority, the transaction would be either void or voidable. The transaction should be canceled, goods returned to supplier, and monies refunded to payor. If goods are not returned and the supplier has not been paid, supplier would be entitled to claim indemnity (CC, Art. 158).

In our view, the most sensitive issue that a plaintiff would face if it had to dispute an e-contract in a Brazilian court is not so much demonstrating that this form of contracting is valid and enforceable, but rather convincing the court that the media and the form of acceptance of the contract are sufficiently reliable to constitute legal evidence. To that end, the court is likely to rely on the opinion of technical experts.

Digital Signatures—Brazil does not have a digital signature law. The São Paulo Chapter of the Brazilian Bar Association has produced a draft bill regulating e-documents and digital signatures. Moreover, at least one private entity (Certisign Certificação Digital Ltda.) issues digital certificates, which are stored on a browser or server to identify the communicating parties.

In addition, several bills that aim to render e-commerce safer are pending before Congress (e.g., No. 1713 of 1996, dealing with computer crimes; No. 2644 of 1996, regulating the preparation, storage, and use of e-documents; No. 3173 of 1997, on the legal validity of digitalized documents; No. 84 of 1999, also dealing with computer crimes). Under Brazilian law, a bill that is not enacted in the congressional session in which it was introduced is automatically transferred to the ensuing session.

CHILE

By: Jose Luis Donoso, Kelley, Drye & Warren LLP, Washington DC

IT DEVELOPMENTS

Internet—At the end of 1999, the Network Information Center Chile announced changes to Internet regulation in Chile. A new regulation adopted ICANN's criteria that revoke domain names when the registrations are found to be illegal or made with abusive intent. This change will protect companies from cybersquatters. The other major change is the introduction of a "previous mediation phase" in every conflict between a registered domain name and a new application, or between two simultaneous applications. This process will be free, and formal arbitration will proceed only if agreement is not reached in the previous mediation.

E-Commerce—As a way to strengthen Internet use and reduce customers' fears about the safety of e-commerce, several commercial banks are introducing new credit cards specially created for online transactions. These cards contain different security mechanisms, special data encryption, and purchase limits to ensure safe use. The new system has been a success, particularly with consumers who are just beginning to use e-commerce.

Digital Signatures—In 1999 the government passed the first Chilean Digital Signature Law, based on a private/public key encryption system. The new regulation defines terms like digital signature, private key, public key, and digital certificate. Although currently applicable only to governmental documents and administrative procedures, it is the first step toward future commercial regulation.

The Computer Law Association Bulletin

By: Richard Fawcett, Bird & Bird, Hong Kong — CHINA

NEW ENCRYPTION REGULATIONS

New regulations in China require foreign organizations or individuals using encryption products or equipment containing encryption technology in China to have applied for permission by 31 January 2000 (State Council Order Number 273). Foreign companies will be required to submit the following information to the authorities:

—name and version of all encryption software in use;

—country of origin of the software;

—where the software was purchased;

—location of all computers using the software;

—name, telephone number, and e-mail address of each employee using the software.

These disclosures make it easier for the Chinese government to monitor personal and commercial use of the Internet. The new regulations also prohibit Chinese companies from buying products containing foreign encryption software and provide that "no organization or individual can sell foreign commercial encryption products."

These new regulations have aroused a great deal of debate in Hong Kong and the United States because they could affect China's entry to the World Trade Organization. The new rules also may slow down Internet growth by driving away foreign companies and investors that do not want their transmissions monitored. It remains to be seen to what extent they will be enforced.

NEW REGULATIONS TO PROTECT "STATE SECRETS" OVER THE INTERNET

The State Secrecy Bureau has issued new rules prohibiting individuals and institutions from disseminating over the Internet any information that falls within the category of "state secrets." There is no formal definition of state secrets and consequently the prohibition could cover a very wide range of information, including economic information.

Internet users are prohibited from discussing, publishing, or spreading state secrets using e-mail, bulletin board systems, or chat rooms. Individuals leaking state secrets may be imprisoned. The regulations are effective from 1 January 2000.

Before releasing state secret information websites must undergo security checks and obtain state approval; however, there is serious concern about the practicality of obtaining such approval. Although the regulations do not specifically encompass Hong Kong, Macau SARs, and Taiwan, they state that "the secrets management on computer information systems should be carried [out] by using this regulation as reference."

By: Hilary E. Pearson, Bird & Bird, London — EUROPEAN UNION

DIGITAL SIGNATURE DIRECTIVE ADOPTED

As reported in the *Bulletin* (Vol. 14, No. 1 (1999)), progress on the Digital Signatures Directive was stalled by differences between Member States in the Council of Ministers. On 22 April 1999 the Council announced that it had reached political agreement on a Common Position, which did not generally require that specific technology be used for an e-signature to be recognized, but which provided for an advanced form of certified e-signature. The formal Common Position was issued on 28 June. It defines an "advanced electronic signature" as one that is:

—uniquely linked to the signatory;

—capable of identifying the signatory;

—created using means that the signatory can maintain under his sole control; and

—linked to the data which it relates in such a manner that any subsequent change of the data is detectable.

Advanced e-signatures, which must comply with the regulations in the three Annexes, are given the same legal status as handwritten signatures on paper documents. Other forms of e-signatures are merely subject to the principle of non-discrimination, i.e., Member States' national laws cannot automatically deny legal effectiveness or admissibility for such signatures.

Following approval by the European Parliament on 27 October, the final directive was adopted by the Council of Telecommunications Ministers on 30 November 1999 (final version available at WWW.EUROPA.EU.INT/COMM/DG15/EN/MEDIA/SIGN/DIR99-93-EC%20EN.PDF).

DRAFT EUROPEAN E-COMMERCE DIRECTIVE

As reported in the *Bulletin* (Vol. 14, No. 1 (1999)), in November 1998 the Commission proposed a directive "on certain legal aspects of electronic commerce in the internal market." The proposal was submitted to the European Parliament on 23 December 1998, and the Parliament responded promptly with its Report, including proposed amendments, on 23 April 1999. Substantive amendments were put forward to improve consumer protection and to provide for protection of minors. Express anti-spam provisions were added. Additional amendments made changes to gain consistency with existing legislation, and to provide individual nations more scope to regulate in the public interest.

The Commission responded with an amended proposal, adopting many of the Parliament amendments in whole or in part. On 7 December 1999 it was announced that the Council of Ministers had agreed on a Common Position on this amended proposal (the definitive text was not available at this writing). This Common Position will have its second reading by Parliament early in 2000, so there should be a final directive fairly soon.

Perhaps the most controversial issue that has arisen in connection with the e-commerce directive is the question of which law governs consumer e-contracts. Within the EU, the governing law of contracts is generally dealt with by the 1980 Rome Convention, which permits the parties to select the governing law, except that in consumer contracts the choice of law may not deprive the consumer of the protection of certain "mandatory rules" of the law of the state of the customer's residence. These are rules that by that state's laws cannot be derogated from by contract, and typically include provisions about unfair terms in standard form contracts, obligations of the supplier to provide certain information, and cooling-off periods for certain types of transactions. Similar provisions are found in the Distance Selling Directive and the proposed Distance Financial Services Directive. The result of these rules is that those dealing with consumers cannot effectively choose which law is to govern their contracts. When the Commission announced that, under the E-Commerce Directive, the governing principle would be that the law of the country of origin of the supplier would govern, there was an outcry from consumer interest groups. Those involved in e-commerce argued that exposing online merchants to the consumer protection laws of all 15 Member States would chill e-commerce development. The text of the proposal makes it clear that the existing provisions relating to the law of consumer contracts would not be changed.

The Computer Law Association Bulletin

By: Dr. Jochen Dieselhorst, Bruckhaus Westrick Heller Lober, Frankfurt GERMANY

TWO RECENT DOMAIN NAME DECISIONS

Company domain names given priority rights over trademarks (Decision of Court of Appeal of Munich of July 29, 1999 (29 U 5973/98))—In an important decision concerning domain names, the Court of Appeal of Munich decided that the use of domain names could give priority rights over subsequent trademark registrations.

The plaintiff, a German telecommunications provider, registered two trademarks, Tnet and T-net, in July 1995 for the provision of its services. The defendant Munich-based ISP, Touchnet GmbH, registered the domain name TNET.DE in August 1993. The plaintiff sought to prohibit Touchnet from using its domain name, on the ground that it had registered trademarks. The Local Court of Munich found for Touchnet, and refused to grant an injunction. The Court of Appeal confirmed.

The appellate court found that TNET.DE enjoyed protection as a company name under §5(2) of the German Trademark Act and could, therefore, not be prohibited on the grounds that trademarks were subsequently registered by the plaintiff. Although not all domain names enjoy protection under §5(2), protection is given if the name constitutes a recognized abbreviated form of the domain name owner's company name. "Tnet" is an abbreviation for "Touchnet"; therefore, TNET.DE enjoyed priority rights over the plaintiff's trademarks and its use could not be prohibited.

This is the first decision of an appellate German court to grant protection to domain names as company names under the Trademark Act. Although the decision makes it clear that domain name owners may resist infringement claims brought by subsequent trademark owners, the question as to whether a domain name owner could also prohibit subsequent trademarks on the basis of its pre-existing domain name remains open. Plaintiff has appealed to the Federal Court of Justice.

Prohibition of descriptive domain names (Decision of Court of Appeal of Hamburg of July 13, 1999 (3 U 58/98))—The Court of Appeal of Hamburg held that the use of descriptive domain names could constitute unfair competition under the German Unfair Competition Act because of its monopolizing effect. The parties to the proceedings were two competing associations of *Mitwohnzentralen. Mitwohnzentrale* is a descriptive term used to describe agencies for short-term apartment rentals for a particular city. Both associations used *Mitwohnzentrale* in their names.

Defendant used the domain name MITWOHNZENTRALE.DE for its homepage, where it listed association members and provided links to their services. Plaintiff claimed that the use of the descriptive term *Mitwohnzentrale* as part of the domain name constituted unfair competition, and applied for an injunction. In the first instance, an injunction was granted by the Local Court of Hamburg (January 21, 1998 (315 O 531/97)); this decision was confirmed by the Court of Appeal.

The appellate court based its decision on §1 of the German Unfair Competition Act, which prohibits acts that are contrary to "good commercial manners." The court found that in using MITWOHNZENTRALE.DE defendant essentially monopolized the descriptive domain *Mitwohnzentrale*, thereby excluding plaintiff from potential Internet traffic. Internet users who typed in MITWOHNZENTRALE.DE would be directed only to offers from defendant's member organizations and would not receive any information about competing offers from plaintiff's members. Therefore use of MITWOHNZENTRALE.DE constituted an unfair drawing-away of plaintiff's potential customers, which is not permitted by §1 of the German Unfair Competition Act. The court rejected defendant's argument that Internet users normally use search engines, which would also lead them to defendant's site. Agreeing that users could find offers made by defendant by using search engines, the court noted that many users would first type in the descriptive MITWOHNZENTRALE.DE to look for corresponding offers. Their numbers were considerable enough for the court to prohibit defendant's monopolization of the domain name.

This is the first decision in Germany in which a descriptive domain name was prohibited on the basis of unfair competition law. The defendant has appealed to the Federal Court of Justice. If confirmed, the decision will have far-reaching consequences on the use of Internet domain names in Germany.

HONG KONG

By: Richard Fawcett, Bird & Bird, Hong Kong

ENCRYPTION REGULATION IN HONG KONG

In October 1999 the Import/Export (Strategic Commodities) Regulations were amended to restrict the use of any encryption software employing a key length in excess of 56 bits in Hong Kong. Application to import the restricted software may be made to the Trade Department, and so Hong Kong companies with the necessary permits may still benefit from the relaxation of the U.S. regulations.

As yet Hong Kong companies will only be directly affected by the increased restrictions if they have a presence there and either employ or market encryption software in China. However if the Chinese government continues to impose restraints upon e-commerce, there is a growing anxiety that this will undermine the prevailing confidence in the wealth of opportunities available in China and frighten away foreign investors. The Hong Kong economy also may be affected if foreign trade restraints harm China's bid to gain WTO entry.

ELECTRONIC TRANSACTION BILL COMES INTO FORCE

The Electronic Transactions Ordinance was enacted by the Legislative Council on 5 January 2000. The ETO provides a legal framework for facilitating e-transactions, conferring legal status on digital signatures and e-records, and establishing a voluntary system of registration for certification authorities.

The following provisions of the ETO came into effect on 7 January 2000:

—Part I, definitions and interpretations;

—Sections 4 and 9, the legal effect of the ETO on the government and the admissibility of computer records in legal proceedings;

—Part V, the formation and validity of e-contracts;

—Sections 31 and 33, obligations of the Director of Information Technology Services to maintain certain information and issue a Code of Practice for recognized certification authorities;

—Part IX, the PostMaster General as the first recognized certification authority;

—Part X, general provisions as to recognized certification authorities maintaining a trustworthy system (such as publication of certificates);

—Part XI, secrecy, disclosure, and offenses;

—Part XII, the power of the Secretary for Information Technology and Broadcasting to amend schedules and subsidiary legislation.

Other ETO provisions relating to the power of the Director to grant recognized status to certification authorities, the procedures and criteria for becoming a recognized certification authority, and the Director's powers of revocation and suspension, became effective on 18 February 2000. The ETO does not impose a mandatory system of registration for certification authorities; certification authorities may choose whether or not to apply for recognition with the Director.

Note that at the date of writing, the following parts of the ETO were not yet in force:

—Part II, §3, matters to which the digital signatures and e-record legal presumptions do not apply;

—Part III (except §9), the legal presumptions that e-records and digital signatures shall be accorded the same legal status as that of their paper-based counterparts;

—Part IV, the limitations of the legal presumptions contained in the ETO;

—Schedules 1 and 2, exempting generic items such as wills, statutory declarations, affidavits, powers of attorney, court orders, warrants, bills of exchange, and court proceedings from the ETO.

A *Bulletin* update will be published when the provisions come into effect. The Director has also published Codes of Practice guidelines for certification authorities (available from the Information Technology and Services Department at WWW.INFO.GOV.ITSD).

The Computer Law Association Bulletin

By: Subramaniam Vutha, Tata Infotech Ltd, Mumbai INDIA

INDIA'S COPYRIGHT ACT AMENDED

By the Copyright (Amendment) Act 1999 India's Copyright Act of 1957 has been amended. Some key amendments are:

—For computer programs, the Act confers upon the copyright owner the exclusive right "to sell or give on commercial rental or offer for sale or for commercial rental any copy of the computer program; provided that such commercial rental does not apply in respect of computer programs where the program itself is not the essential object of the rental."

—Among the acts that will not constitute copyright infringement, the following (pertaining to computer programs) have been added:

(i) the doing of any act necessary to obtain information essential for operating inter-operability of an independently created computer program with other programs by a lawful possessor of a computer program provided that such information is not otherwise readily available;

(ii) the observation, study, or test of functioning of the computer program in order to determine the ideas and principles that underlie any elements of the program while performing such acts necessary for the functions for which the computer program was supplied;

(iii) the making of copies or adaptation of the computer program from a legally obtained copy for non-commercial personal use.

By: Angiolo Luzzati, Zambelli, Luzzati, Meregalli & Associati, Milan ITALY

DISTANCE SELLING CONTRACTS DECREE

Italy recently implemented Directive 97/7/EC, governing consumer protection in distance contracts by way of decree 185/1999. Consumers are given the: (1) right to be informed of certain contract information by the seller, (2) right to withdraw from the contract, and (3) protection of appropriate warranties. If "individual communication" is employed in the distance communication, the information must be in Italian if the consumer so requires.

The information must also be confirmed in writing (or other permanent form) on or before the date that the contract comes into force, together with (1) terms and conditions for the exercise of the right of withdrawal, (2) the supplier's address where claims may be filed, (3) details of assistance services and post-sale warranties, and (4) the conditions for withdrawal in the case of contracts of more than one year's duration or an undetermined term. Also, the consumer's prior consent is required for the supplier's use of certain means of distance communication such as e-mail, automated calling systems, and fax.

The consumer may withdraw from a contract without penalty and without the need to give reasons for withdrawing. However, the consumer must assert the right of withdrawal within 10 working days (the EU Directive states 7 days) from the date of delivery of the goods (for a sale of goods contract) or from the date that the contract comes into force (for a supply of services contract). If the supplier has not provided the information specified above, the consumer is allowed 90 days within which to assert the right of withdrawal. The consumer must communicate his assertion in writing and, if given by fax, it should be confirmed by registered letter with return receipt. The right of withdrawal does not apply to contracts for the supply of audio-visual or information goods in sealed packages if such packages have been opened by the consumer. Like the EU Directive, the decree does not cover contracts relating to financial services.

SINGAPORE | By: Richard Fawcett, Bird & Bird, Hong Kong

COPYRIGHT LAW AMENDED TO COVER INTERNET INFRINGEMENTS

Copyright protection in Singapore has been extended by the Copyright Act Amendment Bill 1999 to make it an infringement for any party to "indiscriminately" copy computer programs, pictures, and articles off the Internet. However, downloading of material for educational and research purposes "within reasonable limits" is permitted. The bill also exempts Internet browsing and copying in a cache system from constituting copyright infringement.

SPAIN | By: Jose Manuel Rey, Batalla, Larrauri & Lopez Ante, Madrid

"ES-NIC" RULES MAY CHANGE

The current ES-NIC rules that govern ".es" domain names are expected to change so as to bring the rules more into line with other Member States. The proposed changes will mean that one company will be able to apply for one or more domain names that do not coincide with the company name.

At present, only organizations legally established in Spain may obtain a second level DNS domain name under ".es". Further, only one second level domain under ".es" may be registered by any one organization. However, once that domain name has been granted, the organization may create the third or lower level hierarchy of sub-domains as it deems appropriate. A corporation may only register as its second level domain name under ".es" its complete name as it appears in the deed of incorporation or an acronym of its complete name that is directly and easily associated with the official name of the organization. Ideally this should be a frequently used acronym, legally registered with the Spanish Patents and Trademarks Registry Office (OEPM). An organization is not entitled to register an acronym that does not correspond reasonably and intuitively to the official name of the organization.

We expect that the changes from the foregoing will dramatically alter the domain name market in Spain.

SPAIN | By: Juan Andres Garcia Alonso, Garrigues Andersen, Madrid

E-COMMERCE DEVELOPMENTS

Government Launches Royal Decree 1906/1999 (17 December 1999)—The Spanish e-commerce regulation follows the basic lines of the draft EU Directive on e-commerce. Its objective is to ensure an open European market for e-commerce. Under the Spanish decree:

—The e-commerce service provider will have to give sufficient identification data to consumers (name, address, e-commerce address, and registration number on the Mercantile Register (or the corresponding professional association), if the activity is levied with the VAT or subject to permission, etc).

—No authorization schemes are foreseen in relation to e-commerce services.

—Commercial communications must be clear and intelligible.

—In certain operations, such as real estate, additional specific formalities may be required.

The Computer Law Association Bulletin

—Network operators will not be liable for any damage caused to the contracting parties, if they merely act as carrier. However, they will be liable if they originated the transmission, chose the addressees, or modified the transmitted data.

—Self-regulation over operators' codes of conduct and arbitration may be carried out, even by automated means.

—The courts will be able to quickly adopt interim relief to end any purported infringement.

—An effective punitive system is provided.

Case Law: OZU Case Decided *(September 1999)*—*Ozu* concerned two companies that initially had been part of the same company. Each wanted to use the OZU domain name in Spain. OZU had been registered as a trademark in Spain by the plaintiff, and OZU.COM had been registered at the InterNIC by the defendants. The Court of First Instance of Bilbao confirmed its previous position, ruling that the OZU trademark owners were the legitimate users of OZU.COM and defendants' use was prohibited. Damages were also awarded.

By: Hilary E. Pearson, Bird & Bird, London

UNITED KINGDOM

THE EFFECT ON IT CONTRACTS OF THE CONTRACTS (RIGHTS OF THIRD PARTIES) ACT 1999

The Contracts (Rights of Third Parties) Act 1999 sweeps away the English doctrine of privity of contract. For all contracts entered into six months after the bill became law in November 1999, a person who is not a party to the contract (a "third party") may enforce any term if either the contract expressly provides that he may, or the term confers a benefit on him and the contract does not show that the parties did not intend him to enforce it directly.

This only applies if the third party is expressly identified in the contract, either by name or by description. A third party seeking enforcement will be bound by all the other relevant contractual terms. It will have the normal remedies for breach of contract and may take advantage of any relevant limitations or exclusions of liability.

Once parties to a contract confer a benefit on a third party, they may not cancel or change that benefit without the third party's consent once the third party has either communicated to the promisor that it assents to the term, or the promisor (the party to the contract who made the promise for the benefit of the third party) is aware or should have been aware that the third party has relied on that term. The contract can exclude this consent requirement.

If the third party sues to enforce the term, the promisor can plead any defense that would be available if the other party had brought the action, as well as any defense specific to the third party. If the other party has already recovered damages for breach of that term, the third party's award will be reduced accordingly.

Contracting in the IT industry involves a number of three-way relationships that may be dealt with more directly under this Act. For example:

Shrink-wrap licenses—In the case of standard software, the contract is between the user and a distributor rather than with the copyright owner. The practice of using shrink-wrap licenses has evolved in order to provide terms of use that the rights owner hopes will be directly enforceable. The validity of such contracts has never been tested in an English court, although a Scottish court has enforced such a license (*Beta v. Adobe* [FSR 367]), under a Scots law doctrine permitting the distributor to contract on behalf of the rights owner as well as itself. Software publishers are advised to review their distribution contracts to require distributors to use contracts with end users that expressly give the publisher direct enforceable rights, rather than relying on the indirect and uncertain shrink-wrap contract.

Group procurement—While there are obvious advantages in centralized IT procurement for a group of companies, up to now it has meant that the subsidiaries were reliant on the contracting parent to enforce the contract. This was not only inconvenient, but losses by a subsidiary often were not recoverable in an action by the parent. Under the new law, the parent will be able to contract for the group while providing that each subsidiary can sue for losses it suffered through breach of the contract.

Outsourcing—A business that thinks it may at some future time outsource its IT functions will be able to ensure when purchasing or licensing software that any future outsourcing contractor will be able to get rights to use the software.

Prime contractor and subcontractor—It often happens in large system contracts that specialized items of software have to be obtained from small software houses. In general, the prime contractor has had to take responsibility for performance by this subcontractor, which is generally not good for damages if the software is defective. Prime contractors will in future seek to provide a pass through of contractual promises by subcontractors to the client. While this gives the client more direct access to enforcing contractual obligations by the subcontractor, it will not be to the client's advantage if it results in the main contractor avoiding any obligation itself for a failure by the subcontractor.

Collective enforcement agencies—Agencies such as FAST and the BSA have been successful in taking action against businesses that have unlicensed copies of software and are therefore infringing copyrights. Under the new law, such agencies could also be given rights to enforce software licenses, thus providing a further cause of action by the agencies.

The Computer Law Association Bulletin

Websites for Government and Related Reports

E-Commerce

Australian Electronic Transactions Act of 1999, Parliament of Australia, WWW.APH.GOV.AU/PARLINFO/BILLSNET/BILLS.

California Tax Policy and the Internet, Legislative Analyst's Office, WWW.LAO.CA.GOV.

Guidelines for Consumer Protection in the Context of Electronic Commerce, OECD, WWW.OECD.ORG/DAF/CLP.

EU Directive 1999 on a Community Framework for Electronic Signatures, European Community, WWW.EUROPA.EU.INT/COMM/DG15/EN/MEDIA/SIGN/99-915.

Export Controls on Computers—Fact Sheet, Bureau of Export Administration, WWW.BXA.DOC.GOV/HPCS/WHITEHOUSEFACTSHEETONHPCS.HTML.

Five Years: Protecting Consumers Online, Federal Trade Commission, WWW.FTC.GOV.

Issues in Accounting for Internet Activities, Securities and Exchange Commission, WWW.SEC.GOV/OFFICES/ACCOUNT/CALT1018.HTM.

Online Brokerage: Keeping Apace of Cyberspace, Securities and Exchange Commission, WWW.SEC.GOV/NEWS/STUDIES/CYBEXSUM.HTM.

Sentencing Guidelines for U.S. Courts (Proposed), U.S. Sentencing Commission, WWW.USSC.GOV.

VAT Collection and Control Procedures—Fourth Report, No. 1553-89, European Commission, EUROPA.EU.INT/EN/COMM/DG21/COMREP/EN/EN28.PDF.

Privacy

Encryption Export Regulations—Draft II, Department of Commerce, available at Center for Democracy & Technology, WWW.CDT.ORG.

Encryption Items, Revisions to: Interim Final Rule, Department of Commerce, Bureau of Export Administration, WWW.ACCESS.GPO.GOV/SU_DOCS/ACES.

Privacy of Consumer Financial Information (draft), Board of Governors of the Federal Reserve System, WWW.BOG.FRB.FED.US.

Security

ID Theft: When Bad Things Happen to Your Good Name, Federal Trade Commission, WWW.FTC.GOV/BCP/CONLINE/PUBS/CREDIT/IDTHEFT.HTM.

Internet Security: Distributed Denial of Services, OCC Alert 20000-1, Office of the Comptroller of the Currency, WWW.OCC.TREAS.GOV/FTP/ALERT/2000-1.TXT.

National Infrastructure Protection Center Information System Alert (Denial of Service), Federal Bureau of Investigation, WWW.FBI.GOV.NIPC/DDOS.HTM.

Software (Free, Downloadable) to Protect Against Denial of Service Tools, Federal Bureau of Investigation, WWW.FBI.GOV/NIPC/TRINOO.HTM.

Y2K

Y2K Aftermath—Crisis Averted (Final Report), U.S. Senate Special Committee on the Year 2000 Technology Problem, WWW.SENATE.GOV/~Y2K/DOCUMENTS/FINAL.PDF.

This page intentionally left blank

The Computer Law Association Bulletin

This page intentionally left blank

3028 JAVIER ROAD • SUITE 402 • FAIRFAX, VIRGINIA 22031
TELEPHONE: (703) 560-7747 • FAX (703) 207-7028
E-MAIL: CLANET@AOL.COM

PLEASE SUBMIT MATERIALS FOR THE *BULLETIN* AS FOLLOWS:

• Feature Articles:
Esther C. Roditti

• U.S. Federal & State Case Summaries:
Randall M. Whitmeyer

• European Case & Legislative Summaries:
Ashley Winton

• EU Directives and Other Developments; Non-European, Non-U.S. Case & Legislative Summaries:
Hilary Pearson

Addresses, telephone and fax numbers for the above editors are on the front cover.

CONTRIBUTORS IN THIS ISSUE:

Juan Andres Garcia Alonso
Madrid, Spain

Scott J. Bergs
Minneapolis MN

Richard J. Caira, Jr.
Raleigh NC

John Carson
San Diego CA

Hieu Dang
Houston TX

Jochen Dieselhorst
Frankfurt, Germany

Jose Luis Donoso
Washington DC

Richard Fawcett
Hong Kong

George Charles Fischer
São Paulo, Brazil

John Flock
New York NY

David B. Goodwin
San Francisco CA

Oxana Iatsyk
Toronto, Canada

Els Kindt
Brussels, Belgium

Angiolo Luzzati
Milan, Italy

Eric M. Nelson
San Diego CA

Hilary E. Pearson
London, England

Jose Manuel Rey
Madrid, Spain

Aram Sarafian
New York NY

Rene L. Siemens
San Francisco CA

Paul C. Van Slyke
Houston TX

Joel Voelzke
Los Angeles CA

Subramaniam Vutha
Mumbai, India

Barry Weiss
Denver CO