

The



Bulletin

CLA Website: [WWW.CLA.ORG](http://www.cla.org)

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

U.S. Developments Editor
Robert M. Weiss
Gordon & Glickson LLC
444 North Michigan Avenue, Suite 3600
Chicago IL 60611 USA
Tel: 312-321-7699; Fax -9324
rmweiss@ggtech.com

International Editors
Ashley Winton
Pillsbury Winthrop LLP
54 Lombard Street
London, England EC3V 9DH
Tel: 44 (0)20 7648 9212; Fax 7067 9048
awinton@pillsburywinthrop.com

Donald S. Hicks
Gowling Lafleur Henderson LLP
40 King Street West, Suite 5800
Toronto, Ontario, Canada M5H 3Z7
Tel: 416-369-4657; Fax -7250
donald.hicks@gowlings.com

Fabrice Perbost
Kahn & Associés
51, rue Dumont d'Urville
75116 Paris, France
Tel: 33 1 45 01 45 01; Fax -45 00
fperbost@kahnlaw.com

Chair, Publications Committee
Lisa R. Lifshitz
Gowling Lafleur Henderson LLP
40 King Street West, Suite 5800
Toronto, Ontario, Canada M5H 3Z7
Tel: 416-369-4632; Fax -7250
lisa.lifshitz@gowlings.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
cla@cla.org

News and Announcements 41
Coming Events
In Memoriam

**No More Junk! An Update on Spam—
Part Two** 42
By: Stephen J. Davidson and David D. Axtell
Minneapolis, Minnesota

**A Legitimate Concern of Outsourcing
to India: Attrition** 50
By: Rajiv Talwar
New Dehli, India

**Risks Associated with Open-Source
Licensing and Usage** 53
By: Chris Nadan
Santa Clara, California

United States Law Updates 60

International Law Updates 68

Editor's Report 80
Websites for Government and Related Reports

Computer Law Association News & Announcements

Coming Events

July 8–9—2004 International Federation of Computer Law Associations' Conference, Keble College, Oxford, England

November 18–19—2004 Annual European Conference, Hilton Hotel, Amsterdam, The Netherlands

November 18–19—2004 European CyberSpace-Camp, Hilton Hotel, Amsterdam, The Netherlands

February 1–2, 2005—CLA First Asia Conference on IT and Telecommunications Law, Hotel Leela, Bangalore, India

In Memoriam

Lee Loevinger

Lawyer, prophetic writer, and public servant, Lee Loevinger was born in St. Paul, Minnesota on April 24, 1913 and died in Washington, DC on April 26, 2004 at the age of 91. In 1933 Lee graduated from the University of Minnesota, *summa cum laude* and a member of Phi Beta Kappa, continuing his education at its law school, where he earned his J.D. in 1936. He worked with the New York office of the National Labor Relations Board from 1937 to 1941 and the Antitrust Division of the Department of Justice from 1941 to 1946. In 1946 Lee became a member of Larson, Loevinger, Lindquist and Fraser in Minneapolis, then becoming an Associate Justice of the Minnesota Supreme Court in 1960.

President John F. Kennedy appointed Lee as Assistant Attorney General and head of the Antitrust Division. In 1963 the President appointed Lee to the Federal Communications Commission, where

he served until 1968. One of Lee's accomplishments with the FCC was development of the national emergency number, 911. Leaving government in 1968, he practiced law as a partner of the Washington law firm of Hogan & Hartson until 1986, when he became of counsel, a position he held for the rest of his life.

Lee always thought—and often wrote—ahead of the rest of the profession. While practicing in Minneapolis, he wrote “Jurimetrics: The Next Step Forward,” 33 *Minn. L. Rev.* 455 (April 1949). It is the seminal article on information processing and its potential impact on the law and the practice of law. His interest in this area continued through the rest of his life. He was responsible for one of the first books on computer law, *Computers and the Law—An Introductory Handbook*, published by the American Bar Association's Special Committee on Electronic Data Retrieval with the Commerce Clearing House. That Special Committee became the Standing Committee on Law and Technology, publishing a second edition of *Computers and the Law* in 1969. In 1981 a third edition was published by the Section of Science and Technology. For the second and third editions Lee wrote the portions on federal regulation. He then chaired the Section of Science and Technology from 1982-1983.

One of the best examples of Lee's intelligent approach to law, his self-effacing attitude, and his sense of humor, is his entry in *Who's Who in America* in the late 1980s:

With age I come increasingly to believe that life is, and should be, a learning experience. This involves a peculiar paradox: Ignorance increases faster than knowledge, as each new fact or principle opens new frontiers for intellectual exploration. Thus, with greater learning comes intellectual humility and skepticism. So, after reaching 75 I am less certain of anything than at 25 I was of everything.

Robert P. Bigelow

Copyright 2004 by the Computer Law Association, Inc. and the authors of each item; all rights reserved. Cover design by Marie-Carmelle Scorsone, Fasken Campbell Godfrey. COMPUTER LAW ASSOCIATION, COMPUTER LAW ASSOCIATION BULLETIN, WORLD COMPUTER LAW CONGRESS, CYBERSPACECAMP, and the CLA logos are trademarks of the Computer Law Association, Inc.

No More Junk! An Update on Spam—Part Two

By: Stephen J. Davidson and David D. Axtell, Minneapolis, Minnesota¹

Part One of this article, which appeared in Volume 19, No. 1 of the Bulletin, discussed the CAN-SPAM Act² and its meaning. This installment reviews case law in relation to the Act, including its likely constitutionality, analyzes case law relevant to various issues related to spam, describes enforcement efforts against spammers, and offers advice relating to the avoidance and control of spam.

Recent Case Law

The Preemption Clause—To date, cases considering the CAN-SPAM Act have focused on the preemption clause. In *Gillman v. Sprint Communications Co.*,³ an appellate court stated as a side note that Utah's anti-spam law was likely preempted. In *White Buffalo Ventures, LLC v. The University of Texas*,⁴ the spammer took the unique approach of filing a suit against the University for blocking its spam. The spammer claimed, in part, that CAN-SPAM's preemption clause preempted the University from enforcing an anti-solicitation policy through filtering software. The court disagreed, stating that: (1) the University's anti-solicitation policy was not specific to e-mail and the Act's preemption clause does not preempt laws not specific to e-mail; (2) the University's policy was not clearly a state statute, regulation, or rule and therefore was not clearly preempted by the Act; and (3) the University is an IT provider; therefore, the Act expressly authorized it to implement policies declining to transmit, route, relay, handle, or store spam.⁵

Constitutionality—In *Nixon v. American Blast Fax, Inc.*,⁶ the Eighth Circuit Court of Appeals upheld the constitutionality of the Telephone Consumer Protection Act's banning of unsolicited advertising via facsimile machines. The TCPA is an opt-in based statute, requiring "prior express invitation or permission" before unsolicited advertisements may be sent to a telephone fax machine.⁷ The defendants argued that the statute violated the First Amendment guarantee of freedom of speech. The district court agreed, questioning whether the government had shown that there was a significant governmental interest in restricting unsolicited fax advertising. Given the increased number of complaints despite the legislation, and the availability of less restrictive options, such as the national no-fax database, the court concluded the government failed to show that the opt-in restriction would materially alleviate the asserted harm or that it was sufficiently narrow.

The appeals court reversed and upheld the constitutionality of the TCPA.⁸ The parties had agreed the fax ads were commercial speech not accused of being misleading or engaged in unlawful activity. Therefore, the relevant test for constitutionality was: (1) whether the asserted governmental interest is substantial; (2) whether the regulation directly advances the governmental interest asserted; and (3) whether it is no more extensive than is necessary to serve that interest.⁹

The court stated that governmental interest may be shown by "anecdotes, history, consensus, and simple common sense."¹⁰ Consequently, the court rejected the argument that the government must prove the significance of the harm through empirical studies. The government had met its burden by showing that junk faxes shift costs to the recipient, tie-up the fax machine and telephone line of the recipient, and interfere with company switchboard operations and computer networks.¹¹ Further, the court held that the ban on only unsolicited commercial faxes directly advanced the government's interest in curtailing unwanted faxes. Congress had noted that non-commercial calls were less intrusive, as they are more expected. Therefore, Congress could choose to regulate commercial faxes as they present a different problem from non-commercial faxes.¹²

Gaps in the statute, including live telemarketing calls, some types of unsolicited faxes, and unsolicited non-commercial faxes did not render the statute ineffective. "Congress is not required to make progress on every front before it can make progress on any front."¹³ The legislation was likely to advance the goal of Congress to protect members of the public from bearing the costs of unwanted advertisements. In short, the court found that "By placing restrictions on those responsible for a large portion of the problem, TCPA directly and materially advances the congressional goal of limiting the harm arising from unsolicited fax advertisements."¹⁴

Finally, the court held the TCPA was not more extensive than necessary to serve the interests it supports. The court emphasized that the “least restrictive means” test is not appropriate for commercial speech cases; rather, there must be a reasonable fit between the legislature’s ends and the means, where the means are narrowly tailored to obtain the objective.¹⁵ Here the legislation was concerned not with the content of the message, but with the method of delivery of the message. Furthermore, the TCPA neither eliminated advertisement of the same products and goods through other media nor banned advertisement by fax as long as it complied with the law. Consequently, “It was not unreasonable for Congress to choose a system that protects those who would otherwise be forced to bear unwanted burdens over those who wish to send and receive unsolicited advertising.”¹⁶

In *Mainstream Marketing Services, Inc. v. Federal Trade Commission*,¹⁷ the Tenth Circuit Court of Appeals upheld the constitutionality of the Do-Not-Call Registry. Its analysis generally mimicked the Eighth Circuit’s analysis of the TCPA. The Registry’s restriction on telemarketing was found content restrictive; therefore, constitutionality was analyzed under the *Central Hudson*¹⁸ three-part test. The court found (1) that the government had a substantial interest in protecting both privacy of individuals in their homes and in preventing abuse and coercive sales practices,¹⁹ (2) the Registry was a reasonable fit as it blocks a significant number of the calls that cause the problems the government sought to redress,²⁰ and (3) the Registry did indeed reduce intrusions into personal privacy and reduced fraud and abuse.²¹ Consequently, the court found the Registry constitutional.

The analysis of the constitutionality of the TCPA and the Do-Not-Call Registry provides preliminary insight into whether the CAN-SPAM Act will be found to violate the First Amendment. Similar to the TCPA, the goal of the CAN-SPAM Act is freeing the e-mail recipient from unwanted e-mails.²² As with unsolicited commercial faxes, spam is properly targeted as it is the main cause of costly, annoying, unwanted, and often fraudulent e-mail.

Because the CAN-SPAM Act does not regulate non-commercial e-mail and creates a sender-by-sender opt-out program, defendants may claim that the Act is even less effective at relieving recipients of unwanted communications than the TCPA or Do-Not-Call Registry. Furthermore, the Act creates different standards for e-mail containing sexual material

and for those with false or misleading information. However, Congress has not been irrational overall.²³ Each of the prohibited categories poses its own relative harm to the government’s interests. For example, it is not inconsistent to create stricter standards for e-mails with sexual content where that type of e-mail is especially prolific and unwanted.

CAN-SPAM also is unlikely to be viewed as over-broad. While some portions concern sending even one e-mail versus the bulk e-mailing that is a main cause of overburdened inboxes, those sanctions are narrowly directed toward highly undesirable activity. Similarly, guidelines for sexually oriented e-mail are specifically tailored to a persistent problem of unwanted pornographic and obscene images popping up in front users. Perhaps most importantly, large marketing groups supported passage of the CAN-SPAM Act and are not likely to challenge its constitutionality. Consequently, based upon the Eighth Circuit’s decision regarding the TCPA and the Tenth Circuit’s decision regarding the Do-Not-Call Registry, it seems likely most, if not all, of the provisions of the CAN-SPAM Act will be upheld in the face of a First Amendment attack.

No TCPA Private Right of Action—At least one plaintiff’s attempt to sue a spammer under the TCPA has failed. The issue was whether the definition of a “telephone facsimile machine” could include a computer. The TCPA defines “telephone facsimile machine” as “equipment which has the capacity... to transcribe text or images (or both) from an electronic signal received over a regular telephone line onto paper.” In *Aronson v. Bright-Teeth Now, LLC*,²⁴ the plaintiff argued this definition was broad enough to cover a computer attached to a printer and that the defendant was liable under the Act for sending spam e-mail to such a computer. The court rejected such a broad definition, stating that: (1) the TCPA used “fax machine” and “computer” in the alternative in other portions of the Act; (2) the common usage of the terms “facsimile machine” and “computer” gives them different meanings; and (3) a computer standing alone does not have the capacity to print.²⁵ Consequently, according to one court, the TCPA and its opt-in provision regarding commercial faxes does not create a private right of action against spammers.

Individuals May Sue Spammers for Trespass Under California Law—In *Intel Corp. v. Hamidi*,²⁶ the Supreme Court of California struck a blow against anyone seeking to sue spammers under a theory of

trespass to chattels. Such causes of action still remain viable, as CAN-SPAM does not preempt their prosecution.²⁷ While the case did not deal with unsolicited commercial e-mail, its pronouncement as to the tort doctrine appears applicable to all California e-mail cases. Hamidi was a former Intel employee who, without breaching any computer security, sent e-mails criticizing the company's employment practices to Intel's employees. Hamidi offered to, and did, remove recipients from his e-mail list when they requested not to receive further e-mails. While his e-mail did precipitate discussion among Intel employees and managers, it did not cause physical damage or functional disruption to Intel's computers. Intel claimed it suffered consequential damages due to lost productivity and efforts to block the messages; however, the court noted that none of these damages caused direct injury to Intel's computers.²⁸

In a tort action for trespass to chattels, California law requires evidence of "injury to the plaintiff's personal property or legal interest therein."²⁹ Based on case precedent from multiple jurisdictions, the court held that an action based on trespass to chattels requires either threatened or actual damage to the recipient's computer system or impairment of the system's functioning.³⁰ It further held that Hamidi's temporary use of Intel's computers' processors or storage was insufficient unless Intel could show some demonstrable loss from the use.³¹ Consequently, the lower court's finding of liability against him was reversed.³²

The ramifications of *Hamidi* are limited. Aside from the case's limitation to California law, the *Hamidi* facts are not likely to be similar to lawsuits involving spam. Also, the California Supreme Court specifically distinguished cases involving spammers because the liability was based on the "vast quantities" of spam e-mail that overburdened computer systems.³³ There are similarities to spam cases in that Intel felt its employees' time was wasted, as were its resources in attempting to block Hamidi's e-mail, but it was the content of his messages that Intel feared, not the quantity.³⁴ However, in spamming cases where the computer system was either damaged or impaired by the volume of spam e-mail, California will recognize the tort as a trespass to chattels.

Moreover, the California court recognized that activities by spammers, such as taxing a computer system's resources by harvesting e-mail addresses, has been found sufficient for a claim based in trespass to chattels. In such cases, while the activities of one

individual might not overly burden the resources of a computer system, the threat of others joining in the activity to cause real damage can suffice to warrant at least an injunction.³⁵ This line of reasoning is especially important in situations where the plaintiff can show that its computer system was slowed down by a sea of spam but cannot prove that any one individual alone was sending enough spam to independently cause any real harm. This reasoning also is helpful where the computer system is not yet impaired, but the actions of a spammer in conjunction with other spammers threaten the future operation of the system.

The court further declined to extend California's tort law so as to treat a trespass to a computer system more as a trespass to land than to chattel. The court refused to create a fiction of the company's servers as a homestead and e-mail messages as tiny electrical intruders. Understandably, the court was unwilling to create a new body of law giving parties the right to sue for electronic trespass of a computer system. In theory, everyone would need advance permission to send another person an e-mail, and visitors to any given website might be liable for trespass, depending on the views of the owner of that website.³⁶

No Compensation for Locating CFAA Violators—In *Tyco International (US) Inc. v. John Does*,³⁷ the district court held a plaintiff cannot recover the expense of locating a violator of the Computer Fraud and Abuse Act.³⁸ Here, the defendant tried to overload the Tyco e-mail server with a "denial of service" or "spamming attack." The attack was unsuccessful and did not cause any service outage. Nevertheless, Tyco hired an investigative firm to locate the hacker. Ultimately Tyco was granted a default judgment as the defendant failed to respond to Tyco's complaints, and Tyco sought to recover the investigator's fees. Tyco claimed these fees were a "natural and foreseeable result" that it was entitled to recover under the CFAA.

The court held that recoverable damages beyond physical damage to property were generally limited to those costs necessary to assess the damage or to re-secure the system after an attack. "Tyco's investigative costs would be compensable only if the instigation was necessary in order to reveal the actionable activity—i.e., the spamming attack."³⁹ Given the likelihood that violators of the CFAA will hide from their victims, many parties inevitably have to expend time and/or money to locate the offending party. The court's decision to render such costs unavailable for recompense may put a damper on a party's interest in pursuing violators.

Enforcement Actions Against Spammers

The FTC—In 1998, the FTC began a spam-collecting project by asking people to forward spam they had received to UCE@FTC.GOV.⁴⁰ The FTC now has the most complete spam database in the world, holding over 20 million messages. Called “The Refrigerator” by FTC employees, the database is sorted into libraries viewable by date received and subject matter. Due to privacy concerns, private organizations are not permitted to view the database. While no one reads all the spam messages, some are selected and reviewed for FTC investigations. Before CAN-SPAM, the FTC was limited to prosecuting cases where spam involved scams or fraudulent business activities. Using the database, the FTC has increased enforcement over the past year. In the words of one FTC staff attorney, “[S]topping fraudulent spam has become a major priority here.”⁴¹

The FTC has formed a “NetForce” posse in conjunction with the Securities and Exchange Commission, the United States Postal Service, United States Attorneys, state attorneys general, and state regulatory agencies.⁴² The FTC is also working with 21 other U.S. agencies and with agencies in 59 other countries to close open relays that allow spammers to avoid detection.⁴³ These actions represent a wide array of suits, a few of which are described below.

FTC Settlements—The FTC has charged GM Funding et al. with using deceptive spam, including the logos of well-known financial institutions. The defendants used forged e-mail headers and claimed recipients could opt-out of further offers. Recipients were induced to provide financial information—including income, mortgage balances, and home values—while the spammers offered competitive financing. The defendants were charged with unfair and deceptive practices under the FTC Act and for “pretexting” (posing as an entity it was not) in order to gain sensitive financial information, which is a violation of the Gramm-Leach-Bliley Act. Defendants GM Funding, Inc., Global Mortgage Funding Inc., and two individuals settled the case by agreeing to a permanent ban from sending spam and disgorgement of \$60,500 in illegal gains. Defendants Universal IT Solutions, Inc. and Anthony Tamras settled by agreeing to a bar against making misrepresentations, or assisting others in making misrepresentations, and a suspended \$60,500 judgment.⁴⁴

The FTC has charged five individuals with promoting a fraudulent, work-at-home envelope-stuffing

scheme. Spam and websites claimed that for a \$50 fee, consumers would receive envelopes and pamphlets and be paid \$500 to \$1500 per week for stuffing the envelopes. Instead, consumers received a booklet of instructions on how to market the defendants’ deceptive credit repair manual. Settlements barred various defendants from sending spam, making deceptive representations, and from providing others with the means to commit deception. The sum of \$7,000 was provided for consumer redress and, if the financial representations are found to be inaccurate, a total of \$536,412 in ill-gotten gains will be due.⁴⁵

The “Instant Internet Empires” company spam advertised five pre-packaged Internet businesses promising that buyers could make up to \$115,000 a year with the product. For a \$47.77 fee, consumers received the right to reproduce the defendants’ website and the right to resell its contents. In other words, the consumer bought the right to market the scam to other consumers. To achieve the \$115,000 in earnings, a consumer would have to sell 2,400 units to additional consumers. To continue making that level of earnings, by the third generation of the scam the entire group of participants would have to generate 13,829,760,000 in unit sales, essentially selling an average of two units to every person on earth. The defendants were barred from making false or misleading income claims, from participating in chain marketing schemes, and from providing the means for others to violate the law. In addition, \$247,000 was provided for consumer redress and, should the financial representations be found to be inaccurate, the entire \$634,222 in ill-gotten gains will become due.⁴⁶

To support its efforts, in 2003 the FTC requested a budget of \$191.1 million to, in part, battle spam, educate consumers, and conduct research. For example, in the past the FTC initiated a “Spam Harvest” study to test which actions taken by consumers put them at the greatest risk of receiving spam.⁴⁷ The FTC brought its first lawsuits under the CAN-SPAM Act in April 2004.⁴⁸ The suits charged Detroit-based Phoenix Avatar and Australian Global Web Promotions Pty Ltd. with civil and criminal violations of the Act. In both cases, the spammers allegedly sent false and misleading advertising for diet patches. Moreover, they forged headers to make the e-mails appear to have come from other senders. As a result of the suits, a U.S. district judge has frozen the defendants’ assets and barred further spamming.

The FTC testified before Congress in May 2004 that it was targeting 50 of the worst spammers for

prosecution this year. It appears the spammers will be charged with both criminal and civil actions under CAN-SPAM or related laws. Unfortunately, despite CAN-SPAM or its enforcement, spam has risen to become between 64 and 83 percent of all e-mail traffic on the Internet. Hopefully, as investigations proceed and enforcement widens, spam levels will decrease.⁴⁹

States—December 2003 was a busy month for states seeking to enforce their own anti-spam laws. Virginia prosecutors led the battle by arresting one of the nation's most prolific spammers, Jeremy Jaynes (a.k.a. "Gaven Stubberfield"). Jaynes was charged with four felony counts under Virginia's anti-spam statute, the first defendant in the nation to be charged with a felony for spamming. He and his co-conspirator allegedly sent thousands of spam per day through America Online and UUNet. The messages included solicitations to purchase penny stocks, mortgage schemes, and advertisements for software that erases traces of where a computer user has surfed the web. Under the Virginia statute, spammers are guilty of a felony if they send more than 10,000 messages in 24 hours or 100,000 e-mails over a 30-day period. Conviction carries up to five years in jail and fines.⁵⁰ Note that Virginia's law, to the extent it prohibits more than fraudulent or misleading e-mails, was preempted by the CAN-SPAM Act on January 1, 2004.

New York Attorney General Eliot Spitzer has filed civil lawsuits against three marketing companies. The State of New York is reportedly seeking tens of millions of dollars in the lawsuit, claiming that the proceeds were ill-gotten gains because the e-mails' subject lines and other information were forged. New York claims that one defendant, Delta Seven, broke into computers owned by others to relay the messages.⁵¹ Specifically targeted was Scott Richter, the president of OptInRealBig, which Spitzer stated was the third-most-prolific sender of spam. In contrast to the reported millions Richter brings in each month in his marketing business, the other two defendants appear to have no real financial assets. The key issue appears to be whether the state can tie all three companies together for purposes of liability.

Companies—Several ISPs are suing spammers who use their networks to send unsolicited commercial e-mail. A visit to America Online's legal webpage shows it has filed over 20 lawsuits for what it deems "junk e-mail."⁵² EarthLink has sued over 100 spammers and last year won a verdict for \$24 million against Kahn Smith, a.k.a. the "Genghis Spammer."⁵³ United Parcel

Service of America is currently conducting discovery regarding several individuals who allegedly used the company's e-mail system to send sexually explicit spam to UPS's customers.⁵⁴ Microsoft has announced it also will file an \$18.8 million lawsuit against the trio of companies recently sued by New York, claiming that the spammers targeted Microsoft's Hotmail service.⁵⁵ Microsoft similarly filed 15 other suits in the United States and the United Kingdom against spammers it claims flooded its MSN Internet service with over 2 billion unsolicited messages.⁵⁶ These lawsuits are in addition to those filed by various ISPs against spammers under CAN-SPAM (see Part One of this article).

Individuals—In two separate cases, individuals who have recently sued for relief against spammers have not had success. In Maine, the court ruled that Louis Philippe would have to go to Virginia to sue AOL for the \$1,680 he claims the company owes him in time spent dealing with spam the company sent or allowed to get through.⁵⁷ The judge upheld the choice of venue in AOL's terms-of-service contract, which requires that all suits against the company be brought in Virginia. Philippe said he would file a new lawsuit under Maine's anti-spam law, which took effect on September 13, 2003.

In Utah, a court dismissed Terry Gillman's case against Sprint for violating Utah's anti-spam law.⁵⁸ Gillman had given permission to receive promotions when he signed onto the Audio Galaxy website. Audio Galaxy sold Gillman's address to Traffix, Inc., which contracts with businesses to send promotional e-mail. Traffix, through its subsidiary GroupLotto, initiated a campaign to promote Sprint's services. Gillman requested that his address be removed from GroupLotto's e-mail distribution lists, but previously queued e-mail to Gillman was sent to his address. Gillman sued under Utah's anti-spam law, which provides that a person may opt-out of future commercial e-mail if he is the recipient of "unsolicited commercial e-mail."⁵⁹ The court held that the term "unsolicited" meant that because of Gillman's initial approval to receive commercial e-mail, all future e-mail was no longer unsolicited. Consequently, Gillman lost his right under the Utah law to opt-out of future e-mails.⁶⁰

Even Spammers—In a move to protect the "legitimate" spamming industry, the Direct Marketing Association formed "Operation Slam Spam" to pursue major spammers and turn them over to state and federal prosecutors.⁶¹ DMA's motive was to stop those

that violate the law by fraud and misrepresentation. According to the DMA [fraudulent] spam comes from 200-300 offenders globally. Consequently, the DMA hopes that the industry, in cooperation with the FBI, will be able to provide technical expertise to aid in the prosecution of such spammers.⁶²

Prevention and Technology May Provide the Answer

Considering the nature of the spam-harvesting beast, experts recommend that all e-mail users take the following precautions:

- Do not display your e-mail address in public, including webpages, chat rooms, newsgroups, message boards, or any other generally accessible e-web source. If an e-mail address must be displayed on a website, consider “masking” or “munging” it. Munging is the attempt to alter an address so that humans can figure out the recipient’s true address but an automated bot cannot. For example, one simple method of munging is altering the familiar @ sign to read “at.” Munging is a double-edged sword. The more simple the mung, the easier it is for bot programmers to alter their program to harvest your munged address. The more complicated the mung, the less likely your real address can be decoded.⁶³
- Review a website’s policy before submitting your e-mail address, and be sure to properly select your preference as to receiving future e-mail from that site. Some sites default the selection to “yes,” and others default to “no.”
- Set your web browser’s security settings at least to the “default” setting, since some websites you visit may contain malicious programs whose purpose is to secretly harvest your e-mail address from your computer.⁶⁴
- Never respond to spam unless you are certain it comes from a business you have dealt with in the past and consider legitimate. Similarly, avoid unfamiliar e-mail removal services. They could be doing nothing more than harvesting your address.
- Consider using an alternative e-mail address for any commercial purpose. Whether you keep a consistent alternative address or use the disposable e-mail accounts offered by many websites, be sure to give your primary e-mail address only to those you trust. Disposable addresses, such as those offered at WWW.BUMPYMAIL.COM,⁶⁵ allow us-

ers to create e-mail addresses with limited lives. E-mail sent to these addresses is then forwarded to your primary address. Once the temporary e-mail address expires, so does the forwarded spam.

- Use a firewall, and run an anti-virus program to avoid spam viruses. Some virus programs can actually turn your computer into a spam-sending machine.

When avoidance fails, users must turn to technology to block spam. There are numerous anti-spam products from several different companies. Microsoft, for example, is creating new anti-spam products, such as “SmartScreen,” and is due to roll out its Intelligent Message Filter this year. Some groups are working on an entire change to the current e-mail system in the hope of stopping spam. Such programs strive to create a method for authenticating e-mail senders. One group of researchers is a commercial alliance between Microsoft, Yahoo, America Online, and Earthlink. Others include the Anti-Spam Research Group, which is affiliated with the Internet’s main standards-setting body, the Internet Engineering Task Force, and ICS, a small vendor of proprietary sender-authentication services.

When all else fails, some prefer to toy with the spammers. Cookies placed on individual’s computers by SNARK.com will cause any spammer whose bot picks up on the cookie’s bait to receive a bill for \$500 and insulting text.⁶⁶ Still others target those sending out the popular “Nigerian” e-mail scam. Often called a 419 fraud (after the violated section of the Nigerian penal code), the scam asks people to give the spammer personal bank account information in order to process large payments in return for help in clearing up a personal legal matter. Those that run the website WWW419EATER.COM reverse the scam by luring the spammers into thinking that individuals are willing to go along and give the spammer money. Once the spammer is baited, the resourceful spam recipients reverse the con and waste the spammer’s time, energy, and money.⁶⁷

Unfortunately, spammers themselves are fighting back against anti-spam activist groups. For example, the Mimail-L virus attacked anti-spam websites by sending e-mail to infected users claiming their credit cards had been charged to pay for a CD of child pornography. The e-mail address given to complain about the charge was that of an anti-spam group, the Spamhaus Project.⁶⁸

Conclusion

Spam, which is arguably the greatest global nuisance today, has no complete solution. Appealing to the decency of spammers has been fruitless when countered by the raw power of profit. Similarly, educating consumers to exercise enough common sense to not throw money toward unsolicited commercial e-mail has been an uphill battle. As long as there is money to be made, spam will clog the arteries of the Internet.

The CAN-SPAM Act and state statutes take steps toward stemming the spam tide, but are plagued with loopholes and generally impotent enforcement. Even if CAN-SPAM were to be successful against spammers in the United States, foreign spammers still have the legal and technological ability to continue “waging war” against our inboxes. Technology provides partial relief, but the battle between anti-spam software developers and spammers seems at this time to be endless. Currently, the e-mail user’s best hope is that the combination of personal common sense, legal enforcement, and technological means will reduce spam to a manageable level. Perhaps through these efforts, spam will become a mild, chronic inbox illness instead of an Internet epidemic.

Endnotes

1. Stephen Davidson is Chairman of the Intellectual Property and Information Technology Law Department at the Minneapolis, Minnesota-based law firm of Leonard, Street and Deinard. A former president of the Computer Law Association, he may be reached at STEVED@LEONARD.COM. David Axtell is an associate in the Law Department at Leonard, Street and Deinard. He may be reached at DAVID.AXTELL@LEONARD.COM.
2. The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 15 USC §7701.
3. 2004 WL 964083 at *3, n. 3 (Utah App. 2004).
4. No. A-03-CA-296-SS, (W.D. Tex. March 22, 2004).
5. *Id.* slip op. at 7, citing 15 USC 7707(b)(1), (b)(2) and (c).
6. 323 F.3d 649, 652-53 (8th Cir. 2003).
7. 47 USC §227(b)(1)(C) (2000).
8. *Nixon*, 323 F.3d 649 at 660.
9. *Id.* at 653, citing *Central Hudson Gas & Electric Corp. v. Public Service Commission*, 447 U.S. 557, 566 (1980).
10. *Nixon* at 654 (citations omitted).
11. *Id.*
12. *Id.* at 655-58 (distinguishing *City of Cincinnati v. Discovery Network, Inc.*, 507 U.S. 410 (1993), where the only difference between regulating commercial and non-commercial speech was the low value of commercial speech, not because the distinction itself was relevant to the asserted government interest).
13. *Nixon* at 658 (citation omitted).
14. *Id.*
15. *Id.* at 659, citing *Florida Bar v. Went For It, Inc.*, 515 U.S. 618, 632 (1995).
16. *Nixon* at 659-60.
17. 358 F.3d 1228 (10th Cir. 2004).
18. *Central Hudson Gas & Electric Corp. v. Publ. Serv. Comm’n of N.Y.*, 447 U.S. 557, 566 (1980).
19. *Mainstream Marketing Services*, 358 F.3d at 1238.
20. *Id.*
21. *Id.* at 1240 (noting that 50 million people had signed up for the list, reducing telemarketing calls by an estimated 6.85 billion calls per year).
22. As noted in Part One, spam costs individuals money, time, and frustration.
23. *Cf. Rubin v. Coors Brewing Co.*, 514 U.S. 476 (1995) (finding an “overall irrationality” in a statute whose purpose was to stop competition for customers based upon the alcohol content of beverages where the statute only banned the display of alcohol content on labels and not in advertisements generally).
24. 824 A.2d 320, 321 (Pa. Super. 2003).
25. *Id.* at 321-22. Here the court’s point seems more centered on the fact that, in contrast to a fax machine, a computer does not automatically print an incoming fax at the expense of resources of the recipient. Given today’s integration of various technologies, it is extraordinarily difficult to define just what a computer is. For example, there is no reason why a desktop or laptop “computer” today could not have a built-in printer. Moreover, many fax machines today might qualify to many as meeting yesteryear’s common definition of a “computer.” Therefore, courts should use an abundance of caution when drawing distinctions that, in a technologically evolving world, are or may soon be without a difference.
26. 1 Cal. Rptr.3d 32 (Cal. 2003).
27. CAN-SPAM Act of 2003, 15 USC §7707.
28. *Intel Corp.*, 1 Cal. Rptr.3d at 36.
29. *Id.* at 37.
30. *Id.* at 36.
31. *Id.* at 44.
32. *Id.* at 51.

33. *Id.* at 37, 44.
34. *Id.* at 37.
35. *Id.* at 42-44, citing *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F.Supp.2d 1058, 1061, 1063, 1065-66 (N.D. Cal. 2000).
36. *Intel* at 45-50.
37. 2003 WL 21638205 at *1 (S.D.N.Y. 2003).
38. 18 USC §1030.
39. *Tyco* at *1.
40. During its first year, the project only collected about 100 e-mails. The next year it collected 4,000 forwarded spams daily. That number grew to 40,000 pieces a day in 2001 and 70,000 a day in 2002.
41. Michelle Delio, FTC: "Where Spam Goes to Die," *Wired News*, www.wired.com/news/politics/0,1283,55972,00.html (Nov. 5, 2002). In May 2003, the FTC announced that it, along with other federal and state agencies, had filed 45 criminal and civil law enforcement actions targeting Internet scams and deceptive spam. On November 20, 2003, the FTC announced that it, in conjunction with several other agencies, had filed more than 285 such actions. *Federal, State, and Local Law Enforcers Target Internet Scams and Deceptive Spam* (hereinafter, *Federal, State, and Local*), FTC at www.ftc.gov/opa/2003/11/DOJSWEEP.HTM (Nov. 20, 2003).
42. Robert Longley, *Federal Posse Busts Spammers and Scammers*, About, at [USGOVINFO.ABOUT.COM/CS/CONSUMER/A/SPAMPOSSE_P.HTM](http://usgovinfo.about.com/cs/consumer/a/spamposse_p.htm) (Dec. 9, 2003).
43. *Law Enforcement Posse Tackles Internet Scammers, Deceptive Spammers*, FTC, at www.ftc.gov/opa/2003/11/DOJSWEEP.HTM (Dec. 9, 2003).
44. *Federal, State, and Local*, *supra*.
45. *Id.*
46. *Id.*
47. Roy Mark, *FTC Pledges to Continue Spam War*, *Internetnews.com*, www.internetnews.com/bus-news/print.php/2183991 (April 10, 2003).
48. *FTC Announces First Can-Spam Act Cases*, FTC, www.ftc.gov/opa/200404/040429CANSPPAM.HTM (April 10, 2003).
49. Declan McCullagh, "FBI Plans Spammer Smack-down," *CNETNews.com*, news.com.com/2100-1028_3-5217299.html (May 20, 2004).
50. Jonathan Krim, "Virginia Indicts Two Men on Spam Charges," *Washingtonpost.com*, www.washingtonpost.com/ac2/wp-dyn?pagename=ARTICLE&NODE=&CONTENTID=A56209-2003DEC11&NOTFOUND=TRUE (Dec. 11, 2003).
51. *Id.* (e.g., the e-mails were reportedly sent through "a grade school in Korea, an Internet provider in Slovenia and the ministry of finance in Kuwait").
52. *AOL Junk E-Mail Archive*, America Online Legal Department, LEGAL.WEB.AOL.COM/DECISIONS/DLJUNK/AOLARCHIVE.HTML (Dec. 9, 2003).
53. Justin Rubner, "Anti-Spam Bill: Public Policy or Public Relations?" *Atlanta Business Chronicle*, ATLANTA.BIZJOURNALS.COM/ATLANTA/STORIES/2003/12/01/STORY7.HTML (Dec. 1, 2003).
54. *Id.*
55. Hansell, *supra*.
56. Reardon, *supra*.
57. "Portland Man Sues AOL Over E-Mail Spam," *USA Today*, www.usatoday.com/tech/news/techpolicy/2003-11-14-spam-suit-site_x.htm (Nov. 14, 2003) ("I think most people who sign these agreements have no idea what they are getting into," [Judge] Powers said, "It's not good public policy. And it may not be helpful to you. But they don't want to be sued in 50 places").
58. *Gillman v. Sprint Communications Co. LP*, No. 020406640, slip.op. at 2 (Dist. Ct. Utah Feb. 28, 2003), *aff'd* 2004 WL 964083 (Utah App. 2004).
59. *Id.* at 5.
60. *Id.* at 5-6.
61. "DMA Launches 'Operation Slam Spam'" *Email Universe.com*, EMAILUNIVERSE.COM/LIST-NEWS/2003/08/22.HTML (Aug. 22, 2003).
62. "DMA Statement Re: Operation Slam Spam," DMA, [HTTP://WWW.THE-DMA.ORG/CGI/DISPPRESSRELEASE?ARTICLE=484](http://www.the-dma.org/cgi/disppressrelease?article=484) (Aug. 22, 2003).
63. "Address Munging FAQ: Spam-Blocking Your Email Address," *Members.AOL.com/EmailFAQ/MUNGFAQ.HTML* (Dec. 9, 2003).
64. Spam Software: Email Harvesting, *supra*.
65. [WWW.BUMPYMAIL.COM/ABOUT.HTML](http://www.bumpymail.com/about.html) (Dec. 9, 2003).
66. Spam Software: Email Harvesting, *supra*.
67. Tony Thompson, "Nigerian Email Conmen Fall Into Their Targets' Net," *Guardian Unlimited*, MONEY.GUARDIAN.CO.UK/SCAMSANDFRAUD/STORY/0,13802,1086308,00.html (Nov. 16, 2003).
68. "Porn Virus Targets Spam Stoppers," *BBC News*, NEWS.BBC.CO.UK/GO/PR/FR/-/2/hi/technology/3287965.stm (Dec. 3, 2003).

A Legitimate Concern of Outsourcing to India: Attrition

By: Rajiv Talwar, New Delhi, India¹

The growth in the last year of the Indian IT-enabled services (ITES) and business process outsourcing (BPO) industries has been phenomenal. As to be expected, such spectacular growth has been accompanied by a number of deterrents. One such problem is attrition, a legitimate concern of many companies. This article briefly addresses this concern in the framework of Indian laws—the Indian Contract Act, Specific Relief Act, and Code of Civil Procedure—and the precedents set by the Supreme Court of India.

In the ITES and BPO sectors, entry level attrition rates have been found to be as high as 30 to 40 percent.² A significant number of managerial staff also engage in job hopping. The problem is such that the entire staff of a company has been known to change in a year. Be that as it may, why an employee cannot be forced to work, and the lawful remedies available to an employer in India, are discussed below.

No-One Can Be Compelled to Work

Employer (Company) absorbs an employee on the terms that he shall work for Company for an uninterrupted period of three years and agree to a non-compete clause. Employee defaults, abandons the job. All attempts of Employer to reach him fail. Employer sues employee for relief:

- to specifically perform obligations under the Employment Contract and work for Company;
- for an injunction not to work for Competitor; or, alternatively,
- for damages.

Company, as a result of the brilliance of its lawyer, wins and gets the relief sought. The employee is directed by a Decree of Specific Performance to work for Company for a three-year period. Employee is also directed not to work for others during those three years. Employee is unmoved, rigid, and turns a blind eye to the Decree. Employer is advised to move for penal action for willful disobedience. Employee is found guilty and spends a fortnight in civil prison. Employee rejoins the Competitor in utter disregard of court orders.

Employer finds itself in a strange position: the court Decree of Specific Performance is literally in-

capable of being enforced and employee cannot be compelled to work for Company under the terms of the Employment Contract. The penalty has also failed to compel employee to perform his contractual obligations. Yet another penal action may also fail.

How can a court decree prove so ineffective? The law is clear, and courts would not pass any order that is incapable of being enforced. In other words, since the court order of performance remains unenforceable, such an order would not have been passed in the first place. A contract, which depends on the personal qualification or volition of the parties, is not specifically enforceable.³ An Order and Decree of Specific Performance of an Employment Contract is incapable of being enforced.⁴ (The exception is when it involves a public servant or an industrial worker.)⁵

Employer's lawyer recommends that Company accept such a legal anomaly. Company is relentless and determined, sacks the lawyer, and seeks the view of another brilliant lawyer. The new lawyer argues that Company's interests are not served by penalizing the employee, but by seeking compliance with the Court Decree, which, having been passed, must be enforced and given meaning. Under such advice, Company moves for execution/enforcement of the Decree of Specific Performance.⁶ The court acts. Consequently, warrants in terms of the Decree of Specific Performance of the Employment Contract are issued against employee. Employee remains unyielding. Employer is in an aggressive mood too, and gets the assistance of the police. Employee is picked up physically and is brought to the Company office. The cops are happy; they did what was nearly impossible. Employer is happy like the cat that swallowed the canary. Employee, however, continues to be the same, uncompromising and stern. Although physically in the office, employee does not work. The only other way to execute the Decree of Specific Performance would be to attach his property or to appoint some other person to perform the act.⁷ However, neither act would serve the purpose.

Employer fails in its requests, pleadings, and force: everything fails. Employer is back in court, lawyer two fails in his legalistic enforcement of the court order yet again. Company realizes precious time and money have been lost without any result.

This illustrates that a court decree directing an employee to perform its obligations under an employment contract, and to actually physically force him to work for the company, is incapable of being performed. And courts do not pass orders that are incapable of being performed. The courts also do not enforce a contract, which requires day-to-day monitoring.⁸ The law does not permit the enforcement of a contract of a personal nature by a decree for specific performance.⁹ Consequently, there is no way that an employee can ever be forced to work for a company if he does not want to do so. The grant of specific performance is also purely discretionary and is ordinarily refused. Such relief can be granted only on sound legal principles. In the absence of any statutory requirement, courts do not ordinarily force an employer to recruit or retain in service an employee not required by the employer or force an employee to work for an employer for whom the employee does not wish to work. Thus, the conclusion that nobody can be compelled to work against his will.

Injunction to Perform Negative Agreement

That being so, is the employer remediless? Not at all, as every right has a remedy. Contractual rights are protected. The employee cannot act to the prejudice of the employer and violate his non-compete clause. Where an employment contract contains terms providing that the employee shall work for a specified period and not do certain acts, like joining a competitor company, then the circumstances that the specific performance of such a contract in the affirmative is incapable of performance shall not preclude the employer from seeking an injunction to perform the negative agreement.¹⁰ If a contract provides that the employee shall not join or become employed with any competitor in the same business, such a right is protected and an injunction will be granted against the employee.

An employee can be directed not to engage in or carry on the same/similar activities for others in the terms of an employment contract. It is accepted that such a restraint can be safely enforced through the contractual term of employment. A covenant to restrict employment for two years after leaving the employment was held to be a clause amounting to restraint on trade and profession by the Supreme Court. In a nutshell, an employee cannot damage the rights of the employer by accepting a job with a competitor company or by opening up his own shop during the subsistence of the employment contract. The employee can be restrained and such an injunction is ca-

pable of being enforced and executed. The injunction however has to be restricted to the time and the nature of employment.¹¹ A negative covenant restricting an employee during his tenure of employment would not amount to a restraint of free trade and vocation, guaranteed under §27 of the Contract Act. Section 27 of the Contract Act governs the restraint on profession. Every agreement that restrains anyone from exercising a lawful profession, trade, or business of any kind is, to that extent, regarded as void under §27. However, the Law Commission of India in its Thirteenth Report has recommended that the provision should be suitably amended to allow such restrictions and all contracts in restraint of trade, general or partial, as are reasonable, in the interest of the parties as well as of the public. Parliament has yet to act on the Commission's recommendation;¹² thus reliance continues to be on judicial precedents.

In this view of the legal position, the drafting of a negative covenant in an employment contract is often a matter of great difficulty. The issue is the validity of the covenant operating after the end of the period of service. Restrictions on competition during the employment period are normally valid, as noted, and indeed may be implied by law by virtue of the employee's duty of fidelity. In such cases the restriction is generally accepted as reasonable, having regard to the interest of the employer. But if the covenant is to continue after the termination of services, or is too broadly worded, a court may refuse to enforce it. The courts view with disfavor a restrictive covenant against an employee to not become engaged in a vocation or business similar to or competitive with that of the employer after the termination of the employment contract. In a commercial dispute between cola giants Pepsi and Coca Cola, the Supreme Court, while enforcing a negative covenant, clearly held that such a restriction is not a restraint on trade as envisaged under §27 of the Contract Act. An injunction to give effect to the negative covenant was maintained.¹³

Compensation

Although the restraints on an employee for becoming employed elsewhere may have a deterrent effect, the employer is at a loss for having failed to obtain work from the employee. After all, the employee committed a default/breach of the employment contract. The employer has to be compensated and placed in the same position he would have been in before such breach. That is the general law of breach of contract.¹⁴ As shown, an employment contract ordinarily

cannot be specifically enforced by or against an employer. The remedy therefore is to sue for damages.¹⁵ The claim for damages would lie only if the breach is proved to be wrongful.¹⁶ An agreement to train an employee and to seek his service for a reasonable period is a lawful right of an employer. Upon training at his employer's expense, an employee is liable to place his services at the disposal of the employer and, upon failure to do so, is liable to pay compensation to the employer.¹⁷ The clause for liquidated damages, if it is not by way of penalty and is a genuine pre-estimate envisaged under contract, is enforceable. The liquidated damages would also be adjustable against any outstanding dues of the employee (except statutory dues like gratuities), if the contract so provides. The onus to prove that no liquidated damages are owed because no loss was suffered by the employer would be on the employee.¹⁸

From this legal perspective, it is clear that the control over attrition under a contract document would be best achieved by adhering to the above-stated legal norms.

Endnotes

1. Rajiv Talwar is an Advocate of the Supreme Court of India. He has been a member of Supreme Court Bar since 1986 and is a managing partner of Focus on Documents, a legal firm. He may be contacted at RAJIV@FOCUSDOCUMENTS.COM.

2. *Economic Times*, April 14, 2004.
3. S.R. Act 1963, §14.
4. *Bank of Baroda v. Jeewan Lal Mehrotra* (1970) 3 Supreme Court Cases 77.
5. *Executive Committee UPSWCL v. C.K. Tyagi* (1969) 2 Supreme Court Cases 838.
6. Code of Civil Procedures (1908), Order 21, Rule 32.
7. *Id.*, Order 21, Rule 32(5).
8. S.R. Act, §4(1)(d).
9. *Nandganj Sihori Sugar v. Badri Nath* (1991) 3 Supreme Court Cases 54.
10. S.R. Act, §42.
11. *Niranjan Shankar v. Century Spinning* (1967) 2 Supreme Court Reports 378.
12. *Superintendence Co. of India v. Krishan Murgai* (1981) 2 Supreme Court Cases 246.
13. *Gujarat Bottling Co. v. Coca Cola Co.* (1995) 5 Supreme Court Cases 545.
14. Contract Act, §§73 and 74.
15. *Nandganj Sihori Sugar v. Badri Nath* (1991) 3 Supreme Court Cases 54.
16. *S.S. Shety v. Bharat Nidhi Ltd.* (1958), Supreme Court Reports 442, and *Vidya Ram v. Managing Committee* (1972) 1 Supreme Court Cases 623.
17. *M Sham Singh v. State of Mysore* (1973), 2 Supreme Court Cases 303.
18. *ONGC v. Saw Pipes* (2003) 5 Supreme Court Cases 705.

Risks Associated with Open-Source Licensing and Usage

By: Chris Nadan, Santa Clara, California (*This is an edited transcript of a speech to the Computer Law Association.*)¹

Hypothetical Problem

Imagine that you are the general counsel of a large software company, a world-renowned market leader famous for a word-processing software product. The bulk of your company's revenues are derived from sales of this product. Your company is about to come out with the next release, which has many new features and innovations. Assume that the word-processing portion is finished—all that remains to be completed is a little piece of the spell-checker feature.

One of your company's engineers is working diligently on that last little piece of the spell checker. Looking for inspiration, he decides to surf the Web. He goes on the Internet and looks up various technology sites, and comes across a little piece of code, just a couple of lines, that would fit nicely into the little piece of the spell checker.

He notices that this code is offered under something called the GPL (GNU General Public License), and he knows enough about software to know that this is a very common open-source license; indeed, it is the open-source license that is used for Linux, perhaps the most common of all open-source products. So he downloads this code. He puts it into the little piece of the spell checker, finishes the spell checker, and adds that spell checker functionality to the already-completed word-processing portion. The release is packaged, put on CDs, and shipped out the door. At that very moment, your company's proprietary word-processing product has just become an open-source product, thanks to the GPL. The GPL provides that if a product is contaminated in any way by GPL code, you have to open-source the entire product—even though the word-processing portion was independently completed before the engineer ever downloaded the GPL code. Licensees all over the world can now request and obtain your source code, and they can do almost whatever they want with it. In fact, somebody could go into business with your source code and sell copies of your word-processing program in competition with you. Your office will be the CEO's first stop when he discovers what just happened.

Topics

The above story illustrates how imperative it is to

understand open-source licensing before using open-source code. To that end, I will cover five topic areas: (1) What is open-source licensing, as compared with some other forms of source code licensing? (2) What is the benefit of the open-source process? (3) How do the open-source licenses work? (4) What issues do you need to consider in order to make a decision to open-source some of your code, deciding to distribute one of your products under an open-source license? and (5) What considerations do you need to think through in deciding whether to take someone else's open-source code and use it in your product or in your IT environment?

Open-Source Licensing Defined

What is open-source licensing? The key element is providing source code under a license with broad rights to modify and redistribute. Open-source is not about simply giving the code away. The license agreement gives you control over what people do with the code; you rely on intellectual property rights to enforce the license. However, by making the source code publicly available it is no longer confidential. So, although you are relying on intellectual property rights, you are giving up trade-secret protection.

Some of the elements typically found in an open-source license, or in open-source code, include the following:

(1) You may be required to post or disclose your "diffs," the changes that you made to the open-source code. Some licenses require that you identify, post, or disclose what you changed from the original program. Thus, if I download your version, I would know what was different and what changes you made.

(2) The license may contain restrictions on your ability to charge for distribution either in binary and/or source code form. The GPL, for example, has severe restrictions on your ability to charge for the code.

(3) Open-source licenses usually include limitation of liability provisions, disclaimers of warranties (and, potentially, attribution or flow-through requirements), protecting you and all the upstream contributors to that code.

What Open-Source Licensing Is Not

Binary-Code Product—If you purchase an off-the-shelf software program, it is extremely likely that it will be a proprietary product in binary-code form.² The code is a series of ones and zeroes. You look at the code and you cannot learn anything. Trade-secret protection is retained for the source code because you cannot see it. This proprietary, closed-source approach is the classic model. Pick any product you are used to using, whether Adobe Photoshop, TurboTax, or Microsoft Office—they are all proprietary products.

Public Domain—There are some source-code distribution models that are not open-source. One of them is public domain. If you post your source code on the Internet with no restrictions and no license agreement, that is a dedication to the public domain. Public domain is not open-source, where you have some control over what people do with the source code and you can protect yourself with a disclaimer of warranties and a limitation of liability provision.

If somebody downloads your public domain code, uses it, suffers a catastrophic loss, and sues you, you are not going to have the benefit of a limitation of liability provision. Donating to the public domain is actually more risky than open-source.

Public Source—Some licenses make source-code publicly available, but with a restriction. For example, Sun Microsystems has a technology called Java. The real advantage to Java is that it allows one to write an application in the Java programming language, and that application will run on any operating system that has a Java runtime environment. All the major operating systems today have Java runtime environments in them. That means that you can write your application once and it will work on all the different operating systems.

However, this only works if the Java runtime environments have essentially identical interfaces, so that your application can work on all of them seamlessly. In other words, it only works if everybody has compatible interfaces. The classic open-source license, which permits free, unrestricted modification, does not work in this scenario. If people could modify these Java runtime environment interfaces, it is possible they could improve them, but the effect would be that Java applications would not work on that platform. Sun makes Java source code openly available, freely downloadable, so it is public source. But Sun does not permit unlimited modification. If you ship

a Java runtime environment, it needs to be compatible, because otherwise you break the whole premise of Java.

Another example of public source, on the other end of the spectrum, is the Microsoft shared-source license. That license generally allows one to do whatever one wants with the shared source code—with one important caveat: it has to remain noncommercial. The source code is publicly available; anyone can download the source code and do with it what he wants—even make modifications. It just cannot be commercialized.

Importance of Open-Source Software

What is the value and what are the advantages of the open-source process? Why is open-source important in the “e-commerce world”?

One of the dynamics of open-source code is best illustrated by comparison with the proprietary licensing model. Consider the TurboTax program from Intuit. That program is only as good as the number of engineers at Intuit who work on it. If there is a bug in the program, or you want some additional or changed feature, you must wait until Intuit decides to fix that bug or add that feature. Or, Intuit may not be willing to make that fix for you, or it might charge you whatever it feels like. That is the downside of the proprietary model.

Compare this with open-source. With open-source technology, a world of engineers is working on the program for you. It is not only as good as the sum total of the engineers in the manufacturer’s company, it is as good as every engineer in the world who works on the product. If enough developers work on it, the user gets all that talent applied to this product. Instead of a hundred people poking and prodding and seeing if the program is robust and works, there are thousands of people from all over the world, with different perspectives, from different backgrounds, working on the program. That diversity can make an open-source product better than a proprietary, closed-source product.

Then, consider the bug-fixing issue. If there is a problem with the way the program works, there are hundreds of engineers who might fix it, perhaps free of charge. And if not, or if the price suggested is unacceptable, the user can fix it himself, because the source code is available. One is not locked into a particular company and its particular schedule of bug fixes, modifications, and alterations. That is a real advantage of the open-source process.

Open-source also encourages interoperability. For example, with a closed-source word-processing program the spell checker is only as good as the engineers in that company make it. But if that word-processing program remained proprietary, and the spell-checking module open-sourced, developers outside the company might enhance the spell checker. For example, a grammar checker feature might be added. If the spell checker is better, people will like the word-processing program that much more. In this way open-source code can actually enhance the value of proprietary software. That is a major benefit of the open-source process.

Licenses³

The vehicle for delivering and distributing open-source code is the open-source license. Some of the common licenses are:

BSD (Berkeley Software Distribution) License—This is a very short, one-page agreement, which says little more than if you redistribute this product, you've got to include in your redistribution a notice that you can't rely on the licensor's name to sell this product, with a disclaimer of warranties and limitation of liabilities. You can do almost anything you want with the code. It is an open, relaxed, user-friendly license.

However, under the BSD license one can appropriate the open-source code. For example, assume Linux was offered under a BSD license. One could take the Linux code, modify it, compile it into binary code form, and make it a proprietary product and sell it at a high price. It might be even better than the open-source version, so people would actually pay for it. One would have usurped the donated efforts of all those engineers who toiled over this product. A BSD license permits such appropriation, allowing the licensee to take the open-source code and make it proprietary.

GPL (GNU General Public License)—On the other end of the spectrum is the GNU General Public License. The GNU General Public License has a feature to counteract the ability to make the code proprietary, which is called "copyleft." The basic idea is that if one creates a derivative of GPL code, any distribution of that derivative must be under the same GPL terms. So as that code passes from person to person, even if it changes, it remains GPL code. Thus, the source code cannot be appropriated for proprietary use.

GPL is a "copyleft" license because, instead of donating the program to the public domain or using the BSD license, the GPL uses copyright law not to take away people's freedoms but to guarantee that

the code cannot be made proprietary. That is why the name was reversed from "copyright" to "copyleft."

The problem is that it does not stop there. GPL also has a component that is called the "viral nature" of GPL (or, as the open-source folks like to call it, "the concept of inheritance"). The GPL states that software that "contains . . . any part" of the GPL program must be licensed under the GPL. Recall the word-processing program example. You have this enormous, incredibly valuable, proprietary word-processing program. You then have a separate spell-checker program. Both of these were completed except for one little piece. Somebody then added two or three lines of GPL code, and it was all combined into a single product. That little piece of GPL code in the spell checker has infected the entire product, making it all GPL, according to the GPL license. That finished word-processing suite is software that "contains [a] part" of the GPL program—so it must be licensed under the GPL. That is why it is so critical to understand open-source licensing. Not all open-source licenses are viral, of course, but it is an issue that you must address before deciding to use open-source code.

Urban Legends

Copyright License Only—Open-source licenses like BSD and GPL are often not written by lawyers. The provisions are ambiguous, and replete with conflicting language. As a result, people fashion rules of thumb on which to rely. Some of these "urban legends" seemingly are grounded in the language of GPL; others are just completely wrong.

For example, the BSD license is a copyright license. That is all it purports to be. If I download some BSD code from you and use it in my product, you have not actually given me a patent license. I could argue that there is an implied license to use your code (since you gave it to me), but if I redistribute it, or if I change it at all, you might then sue me for patent infringement. Even if I had the right to use it under an implied license, does my customer? One of the urban legends around BSD is that it covers all the rights you need.

Copying Binary Code—Another urban legend is that one cannot copy others' binaries that are offered under GPL. This is not true. I can buy a copy of Red Hat binary software at my local store, start making thousands of copies of the Red Hat CD, and sell them to the public in competition with Red Hat. I have never seen the source, I have never added an ounce of value, and yet GPL permits me to do that.

Although Red Hat and other companies have developed strategies to make such competition less effective (relying on their trademark rights to distinguish their distribution, making updates and bug fixes available to their customers), they cannot escape the underlying fact—the legend is false.

Releasing Source Code—Another urban legend is that if something is open-sourced under GPL, you have to publish the source code. That is not quite accurate. You do not have to post it on the Internet; you simply have to agree to provide source code to anyone to whom you provide the binary. That is, if I have an open-source product, and I license it to three people, I have to give those three people the source code. But I do not have to put it on my website for the public to download.

Dynamic Linking—The most pernicious urban legend is that dynamic linking is not viral under GPL. The GPL is rather ambiguous about whether proprietary code dynamically linked to GPL code becomes contaminated (dynamic linking is where the interaction between GPL code and non-GPL code occurs only at runtime).

Returning to our earlier example, assume that the few lines of GPL code were never incorporated in the spell checker; the integrated word-processing program had no GPL code in it at all. Rather, a separate GPL application provided that additional functionality. Even then there may be a problem, if the spell checker product, when running, relies upon a shared library in that GPL application. Such dynamic linking could contaminate the entire word-processing product. Indeed, the so-called “Lesser GPL” (LGPL) says explicitly that it applies to code that is statically linked (in other words, compiled as a single product, as in the opening example), or that links to an LGPL library at runtime. So, if the limited, lesser license would contaminate that code, surely GPL, the most contaminating license of all, would apply to that code.

There is hearty debate in the open-source community about the contaminating effect of dynamic linking. The open-source community typically claims that such linking does not contaminate. The question I would pose to you, as a legal advisor, is: Maybe they’re right, maybe they’re not. But can your client afford to be the test case?

Open-Source Goals

There are a number of reasons that even commercial enterprises use open-source licenses for their products. For example:

Creating a Standard—A goal of open-source licensing is to create an industry standard. If open-source code is successful or innovative, people are attracted to it because it is free and easily distributed. A standard may be created almost overnight. It is a good option, particularly for a small company that has neither market share nor a dominant product into which to bundle the proposed standard. The Apache web server is a good example. It is open-source code and it is one of the Internet standards.

Selling Services—A second goal of open-source licensing is to sell services in connection with the open-source code. You give away the code, and then sell services to help people use the code. Red Hat software and a lot of open-source Linux companies are based on this strategy.

Supporting Other Products—A third goal is to help a complementary product work better. For example, you sell hardware and people buy your hardware because it has desirable applications. If there are no attractive applications associated with your hardware, people may not be as interested in it. Why not start an open-source community to develop great open-source applications that work on your hardware? You do not need to make money from the applications, because their popularity will drive hardware sales. The open-source process can thus increase hardware sales and provide real revenue benefit.

Attracting Developers—Another goal is to capture developer mind-share. The idea is to get people interested in your products and get your name known, particularly with students. That is the dynamic you want to create. You can also gain goodwill from donating code to the open-source community.

Attracting Assistance—And the fifth reason? You can get free help. Get your code out there and you might entice talented developers to work on it. They do not charge for that service; it is free.

To prove the point that open-source indeed works in a commercial setting: Sun Microsystems uses LGPL for its OPENOFFICE.ORG project, the Sun Public License, a variation of the Mozilla Public License (an open-source license), for its NetBeans tool suite, and the BSD license for Sun’s Project JXTA (a peer-to-peer networking software project donated to the open-source community). Sun, a for-profit enterprise, engages in these and several other open-source products and projects.

Considerations for Posting

What are the basics to be considered before participating in the open-source world and launching a product under an open-source license? First, carefully review the code for quality. If it is garbage code, no one will be interested; you will be wasting your time. Then carefully read the source code for inappropriate comments before it becomes public, because you do not want embarrassing surprises. Also review it for third-party code. Most licenses do not permit re-licensing of source code under an open-source license, so you will have to excise any third-party code portions that cannot be open-sourced.

Finally, carefully consider which license to use. Are you concerned about others taking your valuable code private? In that case, do not use the BSD license; consider using the GPL. On the other hand, if you want people to take up your product, if you want it to become widely used and easy to get, you might want to use BSD. Many other open-source licenses are available, each offering different features and effects.

Managing Contributions—The person running an open-source project must manage the contributions for the community. For example, the BSD license does not include a patent license. So if you are managing an open-source code project, you should require that all contributors give you a patent license along with their BSD copyright licenses. That way, you can safely put those contributions into your code base, and re-license the code base under whatever license you want—including BSD—with the confidence that your community will not be sued by those contributors for patent infringement, because everybody whose contributions are included has granted a patent license.

The GPL does not mix well with other licenses. If someone provides his contributions under GPL, also secure a copyright assignment from him. Then, as the copyright owner, you can decide under what license you want to distribute the code. You could distribute it as proprietary, under BSD or GPL. But if people are contributing only under GPL, as a licensee you must re-license those contributions (and any of your code they touch) under GPL. This limits your options, as the entity managing the open-source project, as to how you license the code base.

Trademark—If the product is not commercial, as is typical for open-source, it is very expensive and probably cost-prohibitive to gain worldwide trademark protection (particularly because, outside the United

States, you generally have no protection unless you register your mark). Also, with a trademark, you need to be worried about licensees using your name when they change your code. They might turn your good code into bad code, or they might introduce a virus or disabling code. You do not want them to dilute or tarnish your trademark.

On the other hand, a trademark can be a valuable tool in trying to achieve a level of compatibility. Linux is a good example. There are many flavors of Linux, and they do not all work the same. That is, an application written for Red Hat Linux might not work on some other form of Linux. So trademark is a way for Red Hat to convince software developers to write to Red Hat Linux, because they have a broad market share and developers know lots of people will be able to use their applications written to run on Red Hat Linux. If someone distributes a version of Linux that is not Red Hat, application developers might not write to that platform. Thus, Red Hat uses trademark to force application developers to comply with the Red Hat standard, if they want to sell applications to the large Red Hat community.

Enforceability—The final consideration is whether the open-source license is in fact enforceable. Typically, open-source licenses require only that you provide a notice in or with the code saying that it is covered by a license and provide a copy of that license. However, if someone obtains your code without being made aware of the license, she is not bound by it.⁴ So if you merely place the notice or license in the code, and the downloader does not become aware of it, the downloader is not bound by your open-source license.

So if you are relying on GPL to keep others from taking your product and making it proprietary, this strategy might not work if they are not, in fact, bound by a GPL license. Even if a notice in the code were sufficient in the United States, it might not be sufficient elsewhere. And if the code is on the Internet, it is accessible everywhere. In many countries, even shrink-wrap licenses that are noticed are not enforceable. So even if an argument could be made that a (possibly unseen) GPL license is enforceable in the United States, its enforceability is uncertain elsewhere. This is another point to consider when deciding whether to launch an open-source project.

Downloading Open-Source

What are the basics to consider before deciding to take open-source code from a third party or an open-

source community, and deploying it in your products or IT environment?

Warranties and Support—Open-source code almost never comes with a warranty or any support. If you decide to use open-source code and it breaks, you may be on your own. You may be unable to find anyone to help you. If you are a bank, for example, and not in the business of software development, open-source might not be for you. At the least, warranties and support offered deserve careful consideration.

Indemnity and Pedigree—Open-source code virtually never comes with an indemnity or a warranty of non-infringement. You do not know where this open-source code came from; even if you trust the party from whom you obtain the code, it may contain contributions from thousands of other, unidentified contributors. You do not know these people, or where they got their code. They could have stolen it.

To reiterate: When you use open-source code you do not necessarily know the pedigree of the code, which presents some risk. This has become a famous issue, thanks to the lawsuit between SCO and IBM. SCO (Santa Cruz Operation) has sued IBM, claiming that IBM took some of SCO's UNIX code—code that IBM was permitted to use only in its version of UNIX—and contributed that code to the open-source Linux community. The code allegedly made its way into Linux, and, years later, SCO said, "That's my code in Linux," so anyone using Linux is infringing SCO's rights.

One of the ways to address this issue is to ask how long the code has been out there, and what is the reputation of the code contributor. If the open-source project is new, the risk is obviously higher than if the code has been available for years without any claim. But the fallacy of this assumption is illustrated by the SCO suit. Linux was available for many years, and the contribution came from IBM, an established and reliable company. And yet IBM allegedly introduced infringing code into Linux. The fact that code has been available for a long time, or that the contributions come from established parties, is no guarantee.

Other Issues—The target product is an important consideration. If the open-source code is put into your key cash-cow product, be more careful. If it is incorporated into an ancillary product that is given away for free, the risks are much lower. Also, how are you incorporating the open-source code? Remind the engineering department that permission to use open-

source code is contingent on including it in a specific place. Keep it in its own module, so, if there's a problem later, you can remove it. You should not let the open-source code migrate throughout the entire product, because then, if it must be pulled out, it is impossible. By then, the entire code is infected.

Also consider the intended use of the open-source code. If used internally only (for example, to run your internal systems), you do not actually have to disclose anything; the GPL viralness becomes irrelevant. Further, is the open-source project manager using contributor agreements? It can make a code base much safer if agreements are obtained from contributors, assigning the rights needed to exploit the products completely. And, finally, look through the code for attribution requirements. The last thing you want is for your open-source code to include a little piece of code from your arch-competitor, which has a requirement that you must give them credit.

These are the issues you need to consider before deciding to download open-source code to use in your product or IT environment.

Conclusion

First, whether licensing out or bringing open-source code in-house, choose or review the license extremely carefully.

Second, free is not free. As some people put it, a lot of open-source—Linux, particularly—is "puppy free." Like a puppy, it may cost nothing to obtain, but it is expensive to maintain. It is even expensive to give away. The project has to be managed. The code has to be tracked. There must be a website or e-mail service to answer questions. The code that comes back has to be reviewed to ensure it is worthy of being accepted in the official code base.

Third, weigh the liabilities. There are a lot of risks to balance. If you need some code that is under GPL, that is how it must be licensed. So decide how the code is going to be used, how it will be incorporated, how your product will be engineered to minimize the risk of contamination.

Fourth, tracking the code and managing your license obligations are also important, because a problem can surface down the line. It would be prudent to know where that open-source code went, so you can remove it.

In sum, these considerations are not meant to deter, but to caution. Open-source code is a very valuable and efficient tool to use in business, but it can also have devastating consequences. If you know what you are doing, open-source can be used safely and effectively. There is an important place for open-source software in the commercial world.

Endnotes

1. Chris Nadan is an Associate General Counsel for Sun Microsystems, Inc. in Santa Clara, California, where he heads the legal group responsible for supporting worldwide software licensing and OEM sales. This article repre-

sents the views and analysis of the author alone, and not of Sun Microsystems, Inc. Mr. Nadan, who is also an Adjunct Professor at the University of California Boalt Hall School of Law, may be reached at CHRIS.NADAN@SUN.COM.

2. Source code is the alpha-numeric human-readable language used to write programs. Binary code or object code is the machine-readable language the program is compiled into, which humans typically cannot read.

3. A very helpful list of all the approved open-source licenses may be found at WWW.OPENSOURCE.ORG.

4. See, e.g., *Specht v. Netscape Comm. Corp.*, 306 F.3d 17 (2d Cir. 2002); *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393 (2d Cir. 2004).

United States Law Updates

FIRST

By: Scott Russell,
Ropes & Gray, Boston, Massachusetts

CIRCUIT

REGION

ADMISSIBILITY OF INTERNET EVIDENCE

John Doe, ppa Jane Doe v. Antonio Lasaga, 2004 WL 503699, 2004 Conn.Super. LEXIS 444 (Conn. Feb. 25, 2004)

►Evidence

While participating in a mentoring program run by defendant New Haven Board of Education, plaintiff, a minor, was sexually assaulted by Lasaga, a mentor in the program. Plaintiff alleged that NHBE was negligent in failing to investigate Lasaga's background. Specifically, plaintiff alleged that NHBE should have discovered Lasaga's past incidents of sexual assaults from information that was available. Because of NHBE's failure to adequately investigate, plaintiff claimed that NHBE was liable for Lasaga's sexual assault.

In anticipation of plaintiff introducing material obtained from the Internet to demonstrate that NHBE could have found information regarding Lasaga's past incidents of sexual assaults, and that NHBE's failure to find such information amounted to a breach of the applicable standard of care, NHBE filed a motion *in limine* to preclude any such testimony regarding information available on the Internet. NHBE argued that plaintiff was required to present expert witness testimony regarding what information, if any, regarding Lasaga was available on the Internet when he was accepted as a mentor by NHBE. NHBE contended that "this is not information that is within the common and ordinary knowledge of an average person, and as the plaintiff, to date, has not disclosed such an expert, plaintiff should be precluded from presenting this testimony."

In determining whether expert testimony was required, the court recognized that

[e]xpert testimony should be admitted when:
(1) the witness has a special skill or knowledge directly applicable to a matter in issue,

(2) that skill or knowledge is not common to the average person, and (3) the testimony would be helpful to the court or jury in considering the issues.

While it is within the common knowledge of the average trier of fact that in the year 2004, law enforcement and governmental agencies, as well as private industry, utilize the Internet to conduct security checks, the question was whether this was the standard of care prior to 1998 for the reasonably prudent employer seeking to recruit school mentors. Resolution of this question was "manifestly beyond the ken of the average trier of fact" and, therefore, expert testimony was required to establish the applicable standard of care and whether defendant breached that standard.

The court recognized that in medical and legal malpractice cases, the general rule requires expert testimony to establish standard of care unless plaintiff's claim is such that it amounts to gross negligence. After discussing negligence, gross negligence, and recklessness, the court held that any alleged failure by NHBE to search the Internet for information regarding Lasaga prior to his arrest in 1998 did not rise to the level of gross negligence. Accordingly, the court held that plaintiff must establish, by expert testimony, the standard of care and any deviation from this standard by NHBE, before plaintiff can address causation and proximate cause. Because the plaintiff had not filed any disclosure of expert witnesses relating to the subject matter of Internet material available to NHBE or the appropriate standard of care, the court granted NHBE's motion *in limine* precluding such expert testimony.

By: Steve Englund,
Arnold & Porter LLP, McLean, Virginia

FOURTH

CIRCUIT

REGION

BANKRUPTCY CODE PREVENTS ASSUMPTION OF EXECUTORY LICENSE

In Re: Sunterra Corporation, 361 F.3d 257 (4th Cir. 2004)

► *Bankruptcy*

RCI Technology Corp. developed and distributed software for the resort industry. In 1997, Sunterra, a resort management company, acquired a license to RCI's software for use in managing a timeshare trading program. In 2000, Sunterra filed a bankruptcy petition in the District of Maryland. Sunterra's plan of reorganization assumed that it would continue to use the licensed software. Prior to confirmation of the reorganization plan, RCI moved to have the bankruptcy court deem the software license rejected on the ground that Sunterra, as debtor in possession, was precluded by 11 USC §365(c) from assuming the license without RCI's consent. In 2002, the bankruptcy court denied the motion and confirmed the plan of reorganization. The district court affirmed. RCI appealed to the Fourth Circuit.

Section 365(c) of the Bankruptcy Code provides that

[t]he trustee may not *assume or assign* any executory contract ... of the debtor ... if ... (A) applicable law excuses a party, other than the debtor, to such contract ... from accepting performance from or rendering performance to an entity other than the debtor or the debtor in possession ...; and (B) such party does not consent to such assumption or assignment....

The court found that the software license was an executory contract because, at a minimum, each party

had ongoing confidentiality obligations. There does not appear to have been any dispute that copyright law would excuse RCI from accepting performance by a party other than Sunterra.

The court described a split in the circuits concerning the construction of the phrase "assume or assign" in §365(c), with some courts following its literal language and applying 365(c) to require consent to mere assumption, and other courts applying 365(c) only where both assignment and assumption are contemplated. While noting arguable conflict with general principles of bankruptcy law, the court ultimately concluded it was constrained by the plain meaning of the statutory language to permit assumption of the license only with RCI's consent. The court held that the provisions of a license agreement may be relevant in determining if a party has consented for purposes of §365(c). Here, however, while the license agreement permitted assignment in certain circumstances, it was (as is usually the case) silent as to assumption. Accordingly, the court found that Sunterra was precluded from assuming the agreement without RCI's consent.

This decision may be of considerable consequence for bankrupt companies and their software licensors, at least in the Fourth Circuit. Most bankrupt companies probably have software licenses that could be considered executory. Under this decision, bankrupt companies typically may be precluded from retaining those licenses. In acquiring software, licensees might seek to avoid this result by explicitly obtaining consent to assumption in their license agreements.

SIXTH

By: David R. Syrowik,
Brooks & Kushman P.C., Southfield, Michigan

CIRCUIT**REGION****COMPLAINT WEBSITE DOES NOT VIOLATE ACPA**

Lucas Nursery and Landscaping v. Grosse, 359 F.3d 806 (6th Cir. 2004)

►Trademark/Cybersquatting

The U.S. Court of Appeals for the Sixth Circuit held that Grosse did not act in “bad faith” under the Anti-cybersquatting Consumer Protection Act by registering a domain name and creating a website utilizing Lucas Nursery’s mark on which Grosse detailed her complaints against Lucas for its alleged bad service in landscaping her front yard. Therefore, Grosse was not liable under the ACPA. The web page was titled, “My Lucas Landscaping Experience.” The court noted that to find liability under the ACPA, a court must consider

a defendant’s “bad faith intent to profit” from the use of a mark held by another party. Analyzing the case on the basis of the nine factors listed in the ACPA for determining such intent, the court found that there was no such “bad faith.” The website had been established by Grosse for informing fellow consumers about the practices of the landscaping company, which she believed had performed inferior work on her yard, and not for trading on the goodwill of Lucas Nursery’s mark.

FORMULA IN SOFTWARE NOT PROTECTED BY STATE FOIA

City of Warren v. City of Detroit, 261 Mich.App. 165, 680 N.W.2d 57 (Mich. App. 2004)

►Freedom of Information Act

In a case of first impression within Michigan, the Michigan Court of Appeals held that a formula contained in a software program used to generate water and sewer fees was not “software” as defined in Michigan’s Freedom of Information Act and, therefore, was disclosable under the state’s FOIA. The case arose when the City of Warren, through the Michigan FOIA, sought to obtain the formula that the City of Detroit, a municipality, used to calculate water and sewer fees. Michigan’s FOIA requires public bodies to release certain information at a citizen’s request. The FOIA provides a disclosure exemption for “software,” which, under MCL 15.232(f), is defined as:

[a] set of statements or instructions that when incorporated in a machine usable medium is capable of causing a machine or device having information processing capabilities to indicate, perform, or achieve a particular

function, task, or result. Software does not include computer-stored information or data, or a field name if disclosure of that field name does not violate a software license.

The court rejected Detroit’s argument that because the formula was contained only in a software program and nowhere else, it was inextricable and thus exempt from FOIA disclosure. The court agreed with the trial court that the formula was not software, but rather was “computer-stored information and data” under the statute. The court distinguished the formula from the “set of statements or instructions” that the software developers presumably created for the purpose of using the formula to generate results. The court also found that the formula, together with software, was contained on a computer disk and that portion of the disk containing the formula was a “public record” under MCL 15.232(e) and therefore subject to disclosure.

By: Matthew T. Furton,
Gordon & Glickson LLC, Chicago, Illinois

SEVENTH

CIRCUIT

REGION

MAGNUSON-MOSS NO BAR TO CONSUMER CONTRACT ARBITRATION REQUIREMENT

Borowiec v. Gateway 2000, Inc., 808 N.E.2d 957 (Ill. 2004)

► *Contracts*

The Illinois Supreme Court joined several federal appellate courts in holding that the Magnuson-Moss Warranty—Federal Trade Commission Improvement Act does not bar arbitration of a consumer’s claims under the Act.

Dissatisfied consumers of personal computers manufactured by Gateway 2000 filed several lawsuits that were consolidated by the Illinois courts. The consumers sought damages for breach of express and implied warranties under the Magnuson-Moss Warranty—Federal Trade Commission Improvement Act, 15 USC§2301 *et seq.*, and violations of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 *et seq.* The Magnuson-Moss Act is a consumer protection statute that establishes standards for consumer product warranties and service contracts. The unhappy consumers alleged, *inter alia*, that the personal computers they purchased from Gateway had numerous defects and nonconformities and that Gateway refused to perform on-site repair as specified in its “Labor Services Service Contract” and the “Limited Warranty Agreement” that related to the parties’ transactions.

Gateway moved to dismiss the consumers’ complaints and moved to compel arbitration based on dispute resolution provisions in the Labor Services Service Contract and the Limited Warranty Agreement. The trial court and appellate court held that the Magnuson-Moss Act precluded binding arbitration of consumer disputes and thus held that the binding arbitration provisions of the consumer agreements were unenforceable. The appellate court relied upon the fact that the Federal Trade Commission had interpreted the Act to prohibit enforcement of binding

arbitration provisions in consumer contracts. Indeed, the FTC ruled that a

warrantor shall not indicate in any written warranty or service contract either directly or indirectly that the decision of the warrantor, service contractor, or any designated third party is final or binding in any dispute concerning the warranty or service contract.

The Illinois Supreme Court reversed, holding that the Magnuson-Moss Act does not prohibit consumer agreements requiring binding arbitration. The court noted that the Federal Arbitration Act, 9 USC §1 *et seq.*, reflects a “liberal federal policy favoring arbitration provisions.” The court also concluded, based upon a detailed examination of the text and legislative history of the Act, that Congress did not intend to bar arbitration of warranty claims. Finally, the court ruled that the FTC’s interpretation of the Act was incorrect. In essence, the court stated that the FTC confused “informal dispute resolution procedures” with binding arbitration. Although warrantors are encouraged to adopt “informal dispute resolution procedures” under the Magnuson-Moss Act, warrantors are not permitted to make those mechanisms binding. This prohibition did not extend, however, to binding arbitration because binding arbitration is not an “informal dispute resolution procedure.” Rather, binding arbitration is an alternative to a civil action, and it may be used in addition to a nonbinding informal dispute resolution process.

This case is important to practitioners in the field of computer law because it confirms that arbitration clauses in consumer agreements may be held to be enforceable despite FTC statements to the contrary.

NINTH

CIRCUIT

REGION

By: Scott G. Warner and Theresa A. Simpson,
Garvey, Schubert & Barer, Seattle, Washington

U.S. COURT REFUSES TO ENJOIN FOREIGN TRADEMARK RULINGS

Microsoft Corporation v. Lindows.com, 2004 U.S. Dist. LEXIS 5584, 69 U.S.P.Q.2d (BNA) 1863 (W.D. Wash. Feb. 10, 2004); 2004 WL 1202309, 2004 U.S. Dist. LEXIS 6552 (W.D. Wash. April 2, 2004)

►Trademarks/International Comity

The District Court for the Western District of Washington has issued two decisions of note so far this year in the ongoing trademark dispute between Microsoft Corporation and Lindows.com over Lindows.com's use of the "LINDOWS" mark for its Linux-based operating system and other computer products and services. First, some history. In March 2002 the district court denied Microsoft's request for a preliminary injunction prohibiting use of LINDOWS, finding that Lindows.com had presented sufficient evidence rebutting the presumption of validity for Microsoft's WINDOWS mark, based on evidence that WINDOWS was a generic mark, and thus not eligible for protection.

In the first of the two decisions this year, on February 10, 2004, the district court addressed the issue of how to determine whether a given term, such as "windows," is generic, because a generic term cannot be the subject of trademark protection. The court certified for appeal as a controlling question of law its determination that the relevant and proper time with respect to whether or not WINDOWS is generic is the period before Microsoft's Windows 1.0 entered the marketplace in November 1985. The court also stated that it would not instruct the jury that even if WINDOWS had been generic prior to November 1985, it would nevertheless be eligible for protection currently if its primary significance today is not generic.

The district court's second decision, on April 2, 2004, involves Microsoft's efforts to protect WINDOWS in foreign jurisdictions. At some point between 2002 and 2003, Lindows.com began to appoint local distributors for its products in countries outside the United States. Microsoft filed suits against Lindows.com in Finland, France, Sweden, the Netherlands, Canada, Mexico, Spain, and the European Community, based on its trademark registrations in

those jurisdictions. Finland and Sweden granted Microsoft's requests for preliminary injunctions, and the Netherlands took things a step further, granting a preliminary injunction prohibiting sale and distribution of Lindows.com's products in the Benelux countries and ordering Lindows.com to make its websites, including the site located at WWW.LINDOWS.COM, inaccessible to visitors from that jurisdiction.

Lindows.com thereafter asked the U.S. District Court for an injunction prohibiting Microsoft from pursuing its foreign litigation, and for a declaration of non-enforceability of the Dutch court's preliminary injunction. The court declined both requests, finding no precedent to support an order enjoining foreign trademark litigation, especially in light of issues of international comity. In seeking a declaration of non-enforceability, Lindows.com argued that in order to comply with the Dutch order it would be required to shut down its website entirely, which would violate its First Amendment rights since the website contained both expressive and informative speech and some protected commercial speech. Microsoft countered that it did not intend to shut down Lindows.com entirely, and that if it appeared impossible to render Lindows.com 100 percent inaccessible to Benelux visitors, Microsoft would not require Lindows.com to do so, but would be satisfied with use of existing commercial software limiting access to the site. In refusing to make a declaration of non-enforceability of the Dutch order, the court noted that, in the absence of a clear constitutional violation, it would not impose its own interpretation of the law on the Dutch court's decision.

On April 14, 2004 Lindows.com announced that it had changed the name of its Linux operating system from LindowsOS to LINSPIRE, hoping to end Microsoft's international litigation pending a decision in the United States as to the genericness of the WINDOWS mark.

James E.B. Sanders,
Morris, Manning & Martin, LLP, Atlanta, Georgia

ELEVENTH

CIRCUIT

REGION

REGISTRY DOMAIN NAME BLOCKING NOT REVERSE HIJACKING

Davies v. Afilias Limited, 293 F.Supp.2d 1265 (M.D. Fla. 2003)

► *Trademark, Cybersquatting*

Davies, a registrant of certain domain names, alleged that Afilias, an operator of a domain name registry, violated the Anticybersquatting Consumer Protection Act by preventing him from using a domain name that Afilias had previously transferred to him.

Afilias implemented a multi-step registration process for all .INFO domain names. The process consisted of a Sunrise Period and a Land Rush Period. During the Sunrise Period owners of any current trademark were eligible to register a domain name associated with the trademark. (The Land Rush Period commenced after the Sunrise Period, and did not impose any restrictions on who could register a domain name.) During the Sunrise Period, any person—even one who did not own any trademarks—could challenge a domain name that allegedly had been registered improperly (that is, by a party who did not own the qualifying trademark). At that point, a successful challenger could request transfer of the domain name, and would be issued an authorization code with which to register the domain name. The registry did not verify that the challenger owned the necessary trademark.

Davies, an individual, challenged the domain HOTEL.INFO and others during the Sunrise Period, based on the claim that the names had been improperly registered by persons who did not own the corresponding trademarks. The World Intellectual Property Organization (to whom Afilias subcontracted administration of the registration process) issued an order that the domain had been improperly registered and ordered the transfer of the domain to Davies, even though he admitted he was not the owner of the mark; WIPO also sent him the corresponding codes to register the domain at a registrar of his choice. Sometime thereafter, Afilias determined that Davies did not own the mark in the domain name, and therefore locked

the domain name to prevent its use by Davies.

Davies sued Afilias for violation of the reverse domain name hijacking provision of the ACPA, which provides that a domain name registrant whose name is disabled due to a registry's policy may file a civil action to establish the lawful registration. Afilias counterclaimed for violation of the Computer Fraud and Abuse Act, which provides that a person cannot knowingly and with intent to defraud access a protected computer without authorization (unless the damages caused are less than \$5,000 in any one year period).

The Florida district court first noted that the issue of whether a claim under the reverse domain name hijacking provision of the ACPA could be brought against a registry rather than a trademark holder had not been previously considered by the courts. The court confirmed that the ACPA only contemplated claims against an overreaching trademark holder because the actual text of ACPA only mentions the trademark holder as the person to whom notice must be given before filing suit. The court therefore dismissed Davies' claim.

Afilias' CFAA counterclaim was based on an allegation that Davies had improperly used the authorization codes to register domain names he did not have the right to use, and therefore caused Afilias to lock those domain names, which prevented it from commercializing them. The court gave little consideration to this claim, however, and dismissed the claim because the codes were freely given to Davies and there was no evidence he actually accessed Afilias' computer system to register the domain names. While the court's decision on both the claims is not surprising, the case provides further clarification as to the scope of the ACPA and CFAA in settling domain name disputes.

FEDERAL

TRADE

COMMISSION

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

FTC ABUSE ALLEGATIONS DISMISSED AS TO STANDARDS SETTING ORGANIZATION MEMBER

In re Rambus Inc., Docket No. 9302, 2003 WL 1866415 (Mar. 17, 2003) (FTC Feb. 24, 2004)

► *FTC Act/Unfair Competition*

The Federal Trade Commission alleged that Rambus Inc. violated §5 of the FTC Act (15 USC §45), a federal unfair competition law that forbids antitrust activities that would also violate the Sherman Antitrust Act. The FTC charged Rambus with three violations: (1) Rambus illegally monopolized the synchronous DRAM (a popular type of personal computer memory) technology market; (2) Rambus illegally attempted to monopolize those markets (i.e., Rambus had the specific intent to monopolize plus a dangerous probability of success); and (3) Rambus unreasonably restrained trade in the synchronous DRAM market with practices that constitute unfair competition. Rambus had participated in an industry standard-setting organization known as JEDEC. Although it was a regular participant, Rambus did not inform JEDEC or its members that Rambus sought to obtain patents on technologies adopted in some JEDEC standards.

Rambus' alleged scheme entailed obtaining patent rights over these technologies, and then, once the standards had become widely adopted within the DRAM industry, enforcing those patents worldwide against companies manufacturing DRAM complying with JEDEC standards. The FTC further alleged that Rambus' conduct caused anticompetitive effects, including increased royalties, increases in the price of synchronous DRAM products, decreased incentives to produce memory using synchronous DRAM technology, and harms to standard-setting organizations and activities.

FTC Chief Administrative Law Judge Stephen J. McGuire ruled that the FTC failed to sustain its burden of proof with respect to all three violations alleged. Specifically, the ALJ ruled that: (1) the JEDEC patent policy encouraged the early, voluntary disclosure of essential patents, and Rambus did not violate this policy; (2) the case law upon which the FTC relied to impose antitrust liability was distinguishable on the facts of this case; (3) Rambus' conduct did not amount to deception and did not violate any

"extrinsic duties," such as a duty of good faith to disclose relevant patent information; (4) during the time that it was a JEDEC member Rambus did not have any undisclosed patents or patent applications that it was obligated to disclose; (5) amendments to broaden Rambus' patent applications while a member of JEDEC were not improper, either as a matter of law or fact; (6) by having legitimate business justification for its actions, Rambus did not engage in exclusionary conduct; (7) Rambus did not intentionally mislead JEDEC by violating a JEDEC disclosure rule; (8) there is no causal link between JEDEC standardization and Rambus' acquisition of monopoly power; (9) members of JEDEC did not rely on any alleged omission or misrepresentation by Rambus and, if they had, such reliance would not have been reasonable; (10) the challenged conduct did not result in anticompetitive effects, as the FTC did not demonstrate that there were viable alternatives to Rambus' superior technologies; (11) the challenged conduct did not result in anticompetitive effects, as the conduct did not result in higher prices to consumers; and (12) JEDEC is not locked in to using Rambus' technologies in its current standardization efforts. For these reasons, the complaint was dismissed.

This was reportedly the longest administrative trial in FTC history. In this case, as in last year's Rambus case before the U.S. Federal Circuit (*Rambus Inc. v. Infineon Techs. A.G.*, 318 F.3d 1081 (Fed. Cir. 2003)), in which Infineon accused Rambus of fraud in connection with the same underlying JEDEC activities, Rambus escaped liability, in part because of JEDEC's lack of mandatory patent disclosure rules. The FTC has filed a notice to appeal the ALJ's decision to the full Commission. Even if the ruling is not upheld, this and other *Rambus* decisions underscore the need for standard-setting organizations to set explicit and comprehensive patent disclosure policies.

A standard-setting body should seek to avoid having a member "hide" pending or issued patent claims that (1) cover technologies that may be adopt-



ed as a standard, and (2) may later be asserted against other members of the standard-setting body. Policies should have a well-defined requirement that members disclose all relevant patent claims, and specifications that could be used for future claiming, that are either issued or pending at any time during membership in the standard-setting body. In the absence of clear-cut

and inclusive policies, a member may be permitted to ambush other members for infringing undisclosed patents whose claims cover a standard developed by the standard-setting body. Ultimately, this type of anticompetitive behavior is encouraged where the duty of disclosure in standards bodies is not broadly and well defined.

International Law Updates

AUSTRIA

By: Markus Andréewitch,
Andréewitch & Simon, Vienna

E-GOVERNMENT ACT

The E-Government Act went into effect in Austria on 1 April 2004. The Act makes it possible to carry out official communications, from the e-filing of a submission to the e-service of the authority's disposition of the matter. The "Citizen Card," the centerpiece of this Act, is a virtual concept allowing for proof of the unique identity of an applicant, as well as of the authenticity of any submission made. The unique identity is created by a source identification number (sourcePIN) allocated to an individual's Citizen Card. Allocations are overseen by the Data Protection Commission, which functions as the sourcePIN Register Authority. The sourcePIN for natural persons is derived from the registration numbers in the Central Register of Residents, which is secured by strong cryptography. If a natural person is not entered into the Central Register, his data is entered into a Supplementary Register and the sourcePIN is derived from the entry number in that register. With respect to legal persons, the sourcePIN is the entry number in the Company Register, the Central Register of Associations, or the registration number allocated in the Supplementary Register.

The authenticity of an e-submission is proven by the e-signature contained on the Citizen Card. Since it is a virtual concept, the Citizen Card is not limited to a certain medium (such as a chip card), but can be used in connection with all media that are suitable for a secure e-signature—e.g., cellular telephones.

For data protection reasons, authorities are not permitted—in instances of identification with a Citizen Card—to store the sourcePIN of a natural person in the course of data processing. It is only permitted to store a sector-specific personal identifier, a derivation of the sourcePIN generated by a calculation, which cannot be reversed; therefore, the personal identifier can be generated from the sourcePIN, but the sourcePIN cannot be calculated from the personal identifier.

Furthermore, no single, encompassing personal identifier exists; rather, a separate personal identifier is generated from the sourcePIN for each sector of government activity. No such protection is necessary for legal entities, which are obliged to use their sourcePIN in any event.

The use of sector-specific personal identifiers also enables use of the Citizen Card in the private sector. From the sourcePINs of both communicating parties, private sector-specific personal identifiers are generated. The generating process for this pin is done in a manner that requires the intentional use of the Citizen Card; therefore, the pin may only be generated with the cooperation of the person involved.

In addition to the possibility of making e-submissions to the authorities, it is also possible to submit any requested documentation (e.g., birth certificate, proof of citizenship) electronically. For this purpose existing registers, such as the Central Register of Residents, are used. The local registration authorities inform the Central Register as to which original documents have been verified and note this in an electronically legible form. An e-registration confirmation is issued, and such legible notification—following e-signature by the Central Register—has the same power of proof as a public document and can be electronically used by the person concerned at any time. Such e-proof will be available as of 1 January 2005.

Simultaneously with passage of the E-Government Act, the Act on Service of Documents was amended and a new section added. In the future, e-service of documents can also be undertaken by every private-sector ISP that has been approved by the Federal Chancellery. In addition, detailed provisions will be issued concerning registration for providing e-service (with and without proof of service), as well as for e-receipt of deposited documents.

Alan James,
Gowling Lafleur Henderson, Toronto

CANADA

FEDERAL PRIVACY ACTS

The Canadian government has long recognized the need to balance the privacy rights of individuals against the need to protect the public from fraud and other crimes. Until recently, many private sector investigative agencies have argued that the pendulum had swung too far in favor of the protection of individual rights. These agencies found themselves in the awkward position of being able to gather an individual's personal information in the course of investigating crimes, but being unable to disclose such information to their clients and other governmental agencies. Recent amendments to certain federal regulations have corrected this imbalance.

In Canada, two pieces of federal legislation protect Canadians' right to privacy: the 1983 Privacy Act and the more recent 2001 Personal Information Protection and Electronic Documents Act (PIPEDA). PIPEDA regulates how private sector organizations collect, use, and disclose personal information, whereas the Privacy Act regulates the federal government itself. PIPEDA may, in some cases, be superseded by provincial laws that are "substantially similar" to PIPEDA.

Under PIPEDA, organizations engaged in a commercial activity must, prior to collecting personal information and subject to certain exceptions, explain and document the purpose for which they are collecting the information and obtain the informed consent of the individual providing the information. An exception to this requirement is set out in ¶7(1)(b) of PIPEDA, which exempts organizations from the consent requirement when they are investigating the breach of an agreement or the contravention of a law.

PIPEDA also requires organizations to obtain the informed consent of individuals before the organization discloses their personal information. An exception to this requirement to obtain prior consent is set out in ¶7(3)(d) and 7(3)(h.2), which exempt dis-

closures to and by "investigative bodies" during the course of investigating the breach of an agreement or the contravention of a law. This disclosure exemption applies only to specified investigative bodies. Hence, while all organizations are legally entitled to collect information in the course of a qualified investigation without the consent of the individual, only "investigative bodies" are permitted to disclose the results of such investigations.

Until recently, only two agencies were recognized as "investigative bodies" under the Regulations Specifying Investigative Bodies (SOR/2001-6): the Insurance Crime Prevention Bureau, a division of the Insurance Council of Canada, and the Bank Crime Prevention and Investigation Office of the Canadian Bankers Association. As a result, although most investigative agencies were entitled to "collect" personal information for investigative purposes without the consent of an individual, they were not legally able to "disclose" the results of their investigations.

As noted in Industry Canada's Regulatory Impact Analysis Statement, a variety of private sector organizations either conduct their own investigations or use the services of independent, non-governmental investigative bodies to conduct investigations (*Canada Gazette*, Vol. 138, No. 8, 21 April 2004). To facilitate investigations by these private sector organizations, with the goal of combatting fraud, Industry Canada has significantly increased the number of specified "investigative bodies" by registering, on 30 March 2004, Regulations Amending the Regulations Specifying Investigative Bodies (SOR/2004-60). The organizations listed in this Regulation are generally of two types: professional regulatory bodies responsible for the conduct of their members, such as provincial law societies, and investigation agencies, such as licensed private investigators and licensed insurance adjusters.

CANADA

By: Charles Morgan,
McCarthy Tétrault LLP, Montreal

“SUBSTANTIALLY SIMILAR” ALBERTA PRIVACY LAW SUPERSEDES PIPEDA

The Governor in Council issued an Order on 10 April 2004, stating that any organization in the province of Alberta, other than a federal work, undertaking, or business, to which the Alberta *Personal Information Protection Act*, S.A. 2003, c. P-6.5, applies is to be exempt from the application of Part I of the federal Personal Information Protection and Electronic Documents Act (PIPEDA) “in respect of the collection, use and disclosure of personal information that occurs within the province of Alberta.”

This action was prompted by the finding that the content of Alberta’s privacy legislation with respect to the “collection, use or disclosure of personal information within the province or territory” was “substantially similar,” in the words of ¶26(2)(b) of PIPEDA, to the content of the federal privacy law. The purpose of such a provision is to encourage “provinces and territories to develop their own privacy laws in a manner that addresses their particular needs and circumstances” while attempting to maintain a certain uniformity throughout the landscape of Canadian privacy legislation and, ultimately, injecting “trust and confidence into the Canadian marketplace.”

The “substantially similar” criterion is composed of several elements set forth by Industry Canada on 3 August 2002—namely, that the provincial or territorial law (1) grants privacy protection that is consistent with that in PIPEDA, (2) incorporates the ten principles in the Canadian Standards Association’s *Model Code for the Protection of Personal Information*, CAN/CSA-Q830-96, found at Schedule I of PIPEDA, (3) provides for an independent and effective oversight and redress mechanism with powers to investigate, and (4) restricts the collection, use, and disclosure of personal information to purposes that are legitimate.

The effect of the Order is that all complaints and investigations about the privacy-related practices of organizations in Alberta will be dealt with exclusively by the Information and Privacy Commissioner of Alberta. Complaints and investigations involving federal works, businesses, undertakings, or cross-border transactions will continue to constitute the jurisdiction of the Privacy Commissioner of Canada. The Canada Privacy Commission statement is at [HTTP://CANADAGAZETTE.GC.CA/PARTI/2004/20040410/HTML/REGLE3-E.HTML](http://CANADAGAZETTE.GC.CA/PARTI/2004/20040410/HTML/REGLE3-E.HTML).

CRTC TO DECIDE STATUS OF VOICE-OVER INTERNET PROTOCOL

The recent proliferation of voice communications using Internet Protocol (IP), by which subscribers to a service provider can make voice calls, has triggered an initial reaction from the Canadian Radio-Television and Telecommunications Commission (CRTC) to define the regulatory status of this service. The voice calls use a broadband connection to a conventional phone set attached to an adaptor or IP telephone.

Telecom Public Notice CRTC 2004-2 (at WWW.CRTC.GC.CA/ARCHIVE/ENG/NOTICES/2004/PT2004-2.HTM) sets forth the Commission’s preliminary view that the adherence of VoIP to the North American Numbering Plan (NANP), as well as its provision of universal access both to and from the Public Switched Telephone Network (PSTN), renders it “functionally the same” service as circuit-switched voice telecommunications (traditional telephone) service and, therefore, subject to the same regulatory scheme. This accords with the CRTC’s practice to remain neutral with respect to the technology, while focusing exclusively on the service being provided. It is noteworthy that this finding contrasts with that of

the CRTC’s equivalent in the United States, the Federal Communications Commission (FCC).

The consequence of this finding is that VoIP providers will have to register with the CRTC, given the specified class within which they operate. Moreover, they would be responsible for the tariffs applicable to their class, for a contribution for the subsidization of high-cost residential local services in rural and remote areas, and, possibly, for adherence to rules of 911 emergency access, wherever the technology permits. Ultimately, to the extent that VoIP services provide access to the PSTN, they are considered local exchange services, subject to the regulatory framework for local competition set forth in *Local Competition*, Telecom Decision CRTC 97-8, 1 May 1997.

The preliminary views of the CRTC will be the subject of a public dialogue to be held on 21 and 22 September 2004 before the Commission makes its final decision, most likely by Spring 2005. Additionally, initial comments on the views outlined by the CRTC in its public notice were due 18 June.

ISPs NEED NOT DISCLOSE IDENTITIES OF MUSIC DOWNLOADERS

Justice von Finckenstein of the Federal Court of Canada rendered decision in *BMG Canada Inc. et al. v. John Doe et al.*, 2004 FC 488 (31 March 2004), refusing the motion of the plaintiffs (members of Canada's recording industry) to force the defendants (five Canadian ISPs) to disclose the identities of certain customers who have allegedly infringed copyright laws by illegally trading in music downloaded from the Internet (see DECISIONS.FCT-CF.GC.CA/FCT/2004/2004FC488.SHTML). The motion was brought following an investigation commissioned by the plaintiffs, which found that individuals operating under certain pseudonyms for the purposes of downloading music with software such as KaZaA or iMesh were using Internet Protocol (IP) addresses registered with the ISPs.

Both parties submitted, as common ground, that the individual ISP account holders were entitled to confidentiality of their identities by virtue of their contracts with the ISPs, as well as §§3 and 5 of the Personal Information Protection and Electronic Documents Act (PIPEDA), Canada's federal privacy legislation, yet they all acknowledged that §7(3)(c) of PIPEDA could also be availed in this case to force an ISP, by means of a court order, to disclose a customer's personal information without that person's consent.

With respect to the test that should govern the granting of such a motion for an "equitable bill of discovery" under Rule 238 of the Federal Court Rules, 1998, SOR/98-106, the court found favor in that outlined in the House of Lords Decision, *Norwich Pharmacal Co. v. Customs and Excise Commissioners*, [1974] A.C. 133, and the Canadian decision which adopted its ratio, *Glaxo Wellcome PLC v. Canada (Minister of National Revenue)* (1998), 81 CPR (3rd) 372. This test is composed of five criteria:

- (1) the applicant must establish a *prima facie* case against the unknown alleged wrongdoer;
- (2) the person from whom discovery is sought must be involved in some way in the matter under dispute—he must be more than an innocent bystander;
- (3) the person from whom discovery is sought must be the only practical source of information available to the applicants;
- (4) the person from whom discovery is sought must be reasonably compensated for his expenses arising out of compliance with the discovery order, in addition to his legal costs;

- (5) the public interests in favor of disclosure must outweigh the legitimate privacy concerns.

With respect to part (1), the Federal Court found that a *prima facie* case against the unknown alleged wrongdoers was not established. First, the affidavits from the organization investigating the anonymous downloaders were comprised of hearsay testimony, which could not be admitted. Second, the court was not convinced that the plaintiffs could decipher the actual identities of Internet users operating under pseudonyms by determining the IP addresses they may have used to effect downloads of music files and by locating the ISPs to which the IP addresses were allegedly allotted. Third, reiterating that downloading a song for personal use is not a copyright infringement by reason of §80(1) of the Copyright Act, the court did not receive any evidence that the "alleged infringers either distributed or authorized the reproduction of sound recordings," which would have constituted the illegal activity. The court also emphasized that placing a copy of a song on a shared directory where it can subsequently be accessed via a peer-to-peer (P2P) service "does not amount to distribution."

With respect to part (2) of the test, the court found that the ISPs were directly involved with the alleged infringers of the plaintiffs' copyrights and were not mere bystanders within the meaning of the motion, yet, in reference to part (3) of the test, the court could not categorically determine that the ISPs were or were not the only practical source of information available to the plaintiffs.

Although it is most likely *obiter dicta*, the court found, regarding part (4) of the test, that isolating the names of the ISP clients who were using the IP addresses found by the plaintiffs to have been downloading music from the Internet was an extremely arduous and costly process, necessitating reimbursement by the plaintiffs to the defendants in the event that the court would have issued an order for the ISPs to furnish the names of the targeted clients. Ultimately, and in a related vein, the court found that "given the age of the data, its unreliability and the serious possibility of an innocent account holder being identified," the privacy concerns of the individuals outweighed the public interest concerns in favor of disclosure. Thus, the plaintiffs also failed to establish part (5) of the test.

In conclusion, the court discussed the ramifications that would have flown from granting the

requested order. First, the order would have to limit the use to which the identities would be used within the proceedings. Second, only the Internet pseudonyms could be substituted as the names of the defendants instead of John and Jane Doe; the actual identities would be relegated to an annex, subject to a

confidentiality order. Finally, on a procedural note, the court suggested that the ISPs did not need to have supplied affidavits in support of their motion; they merely needed to request the disclosure of the defendants' names and last known addresses in order to proceed with their action.

FRANCE

By: Sabine Lipovetsky and Céline Mutz,
Kahn & Associés, Paris

RELAXING OF .FR NAMING POLICY

On 11 May 2004, the new .FR naming policy of the French Association for Internet Naming in Cooperation (AFNIC—*Association Française pour le nommage Internet en Coopération*) came into force, liberalizing the registration of .FR domain names. Indeed, AFNIC suppressed the so-called “right to name” (*droit au nom*), i.e., the rule that only entities having a legal existence or a registered trademark on French territory could register a .FR domain name. Before the new policy came into force, the rules applicable to the assignment of .FR domain names were very restrictive. AFNIC used to apply the right to name, and .FR domain names could only be owned by:

- legal entities having a SIREN/SIRET number. A company had to provide a *K Bis* excerpt, while other organizations had to provide their identifying entry in the INSEE (*Institut National de la Statistique et des Etudes Economiques*) directory;
- entities owning a registered (not only filed) trademark in France, provided that the trademark corresponded to the domain name;
- entities created by law or decree or registered with a professional syndicate, but not registered with the INSEE, if they provided the law, decree, or registration form issued by the competent authority; and
- associations identified in the INSEE directory.

This system ensured a very low rate of disputes resulting from the assignment of domain names. But its strictness prevented entities from filing .FR domain names and their number was therefore fairly low: in April 2004, there were approximately 180,000 .FR names, compared to approximately 6 million .DE names.

Furthermore, in view of the existence of a new Registry (Eurid), which will be entrusted with the organization, administration, and management of the .EU Top Level Domain, AFNIC feared that .FR registrations would decrease even more. AFNIC therefore implemented the project for relaxing the .FR naming policy. The new policy elaborated by AFNIC concerns several issues: (1) conditions of .FR access, (2) control policy, and (3) resolution of disputes.

Conditions of .FR Access—All persons identifiable online in public and national databases (businesses, artisans, associations registered with the INSEE, trademark owners, etc.) may obtain any domain name without such name having to appear on any document. These databases are those of the National Council of Clerk’s Offices (*Conseil National des Greffes*), the National Institute of Industrial Property (*Institut National de la Propriété Industrielle*), and the INSEE. At the beginning of 2005, this will also apply to all natural or legal persons that are not identifiable in public databases (individuals, associations not registered with the INSEE, etc.). However, all entities or individuals will still need to have a legal existence in France.

Finally, the new naming policy provides for the registration of a .FR domain name on the basis of a filed trademark designating France, even if it is not yet registered. Moreover, it is possible to register a domain name by choosing one or several elements of a French trademark, but not necessarily identical to such trademark.

It now seems possible to register almost any domain name, even geographic names or series of numbers. The only exception is the use of syntactic

restrictions and prejudicial or *fundamental words*, i.e., words related to law and order and accepted standards of morals, words related to the functioning of the Internet, and names of the signatories of the Convention of Paris. However, in view of this liberalization of the registration of .FR domain names, a draft law was proposed on 12 May 2004 to protect the names of public authorities.

Control Policy—Until 11 May, AFNIC strictly controlled an applicant's identity before proceeding to the registration of a .FR domain name. According to the new naming policy, such control will still be systematic, but will occur only after registration. Any domain name that does not comply with the applicable rules will then be suspended and removed if the applicant cannot be identified in France.

In addition, AFNIC wishes to implement a system that allows verification of the source of identification of the applicant. In particular, it intends to display on its database WHOIS links allowing visitors to .FR websites to access the information included in the public databases. Thanks to such post-registration control, an automatic registration system of .FR domain names, without any paperwork, would then be implemented.

Dispute Resolution—However, the liberalization of the registration of .FR domain names carries a risk that the number of disputes will increase. In order to resolve disputes, AFNIC will inform the owners of .FR names of the existence of dispute resolution centers, in addition to the traditional recourse to French courts. Two dispute resolution alternatives have been implemented, to ensure a quick procedure (one to two months maximum), and a low cost (less than €1500),

as well as the possibility of bringing a court action.

The two dispute resolution centers are the Paris Center for Mediation and Arbitration (*Centre de Mediation et d'Arbitrage de Paris—CMAP*) and the mediation and arbitration center of the World Intellectual Property Organization. The CMAP offers an online dispute resolution procedure with the intervention of an arbitrator who shall resolve the dispute within 15 days. The WIPO arbitrator offers a technical solution within two months. If a resolution is not challenged within 20 days, AFNIC will apply the solution.

AFNIC does not interfere in dispute resolutions, but stays a neutral entity. Its role is merely to communicate information on the owner of the domain name, freeze operations relating to domain names subject to disputes, and apply the solutions adopted by the arbitrator and accepted by the parties.

Legal Force—The effectiveness of the AFNIC .FR naming policy results from French case law (*Conseil de la Concurrence, 9 June 2000; Tribunal de Grande Instance of Versailles, 3 October 2000; Tribunal de Grande Instance of Nanterre, 18 November 2002*). Moreover, a recent law adopted by Parliament on 13 May 2004 (*Loi pour la confiance dans confiance en l'économie numérique*) provides that the Minister of Telecommunications shall appoint the entities in charge of the allocation and administration of .FR domain names. These entities shall proceed to the allocation of domain names in the general interest, according to non-discriminatory public rules ensuring that the applicant respects intellectual property rights. This law should soon be published. It appears that the .FR extension has become flexible and open, subject only to the territoriality rule.

By: Susan L. Donegan,
Van Doorne N.V., Amsterdam

NETHERLANDS

SPAM REGULATION (FINALLY!)

The Netherlands was one of the EU Member States that failed to meet the 31 October 2003 deadline to transpose EU Directive 2002/58/EC into national law. The Directive on Privacy and Electronic Communications contains the regulatory framework for unsolicited communications (spam). After two warnings, the last in early April, the European Commission took legal action against the non-compliant Member States. The much-anticipated legislation regulating spam was adopted on 22 April 2004 and placed into the Dutch Telecommunications Act (*Telecommunicatiewet*) (*Wet Implementatie Europees regelgevingskader voor de elektronische communicatiesector 2002*, State Gazette 2004, 184). The law entered into force on 19 May 2004 by Royal Decree.

The amendments to the Dutch Telecommunications Act are largely in step with the EU Directive. In both laws, the opt-in (permission granted prior to transmission) regime not only applies to e-mail but also to other means of communication such as fax, telephone, text messaging, and I-mode. However, there are some variations in the Dutch law. In contrast to the Directive, the Dutch legislation concerns unsolicited communications not only for direct marketing purposes, but also those of a non-commercial nature or for charity purposes. And the amended Act explicitly states that the burden of proof is imposed on the marketers. In other words, a marketer should be able to demonstrate that the recipients have given their prior consent.

In both the Directive and the Dutch Act, the opt-out (refuse future transmission) regime for existing customers is allowed if the marketer has obtained the

e-mail address in the context of the sale of its “own similar products or services.” Both also state that the opt-out regime is not applicable to faxes. However, in contrast to the Directive, the Act includes unsolicited communications for non-commercial and charity purposes. In the final version of the amended Telecommunications Act the applicability of the opt-in regime for business (e-mail) addresses was excluded but will be addressed in further legislation.

In terms of remedies for breach of the Telecommunications Act, the Netherlands Post and Telecommunications Authority (OPTA) is charged with enforcement of the new legislation and can impose fines up to €450,000 for violations. If the processing of personal data is tied to spam, some supervisory powers will be exercised by the Dutch Data Protection Authority (*College Bescherming Persoonsgegevens*). The Fiscal Intelligence and Investigation Service (FIOD) and the Economic Investigation Service (ECD) are the government agencies charged with the enforcement of the Economic Offences Act (*Wet op de Economische Delicten*). Under that law, stating a false identity and/or an invalid e-mail address is an offense. A cause of action against a company may also be brought by a person to whom messages were unlawfully sent or by a third party such as the ISP. Other traditional legal actions based in tort, property, privacy, and penal law are still available under the civil and criminal codes.

The Dutch government has indicated that it will tackle the issue of spam in a proactive manner during the second half of 2004 when The Netherlands assumes the position of Chair of the European Union.

By: Sónia Queiróz Vaz,
Barrocas & Alves Pereira, Lisbon

PORTUGAL

CONSTITUTION TRUMPS COPYRIGHT CODE

The Portuguese Constitutional Court recently found the provisions of Article 3, Nos. 1 and 2 of Law 62/98, 1 September, which regulates Article 82 of the Portuguese Copyright Code, were unconstitutional. The basis for the decision was its non-compliance with Art. 103, No. 2 of the Portuguese Republic Constitution, which governs the principle of legality concerning tax issues.

First of all, Art. 82 of the Copyright Code specifically provides that compensation shall be included for the benefit of the authors, artists, editors, publishers, and phonographic and video producers in the sale price of any mechanical, chemical, electric, electronic, or other equipment used to copy or reproduce any works and of any media that enables such copy. Portuguese authors generally accept that the purpose of Art. 82 is to compensate rights owners for the use of recording procedures difficult to control. Article 82, No. 2 specifically establishes that the amount of such compensation shall be determined by a decree-law. Law 62/98 regulates Art. 82 of the Copyright Code and specifically establishes at Art. 3, No.1 that the amount of the compensation due for recording

media or equipment should be determined annually through a joint decree issued by the Finance and Cultural Ministers.

The Constitutional Court considered that this compensation or levy is a unilateral and mandatory revenue included in the price of such equipment and media and, with no compensation in return, it qualified as a tax. That is, the compensation should be legally treated pursuant to Art. 103, No. 2 of the Constitution, which governs the principle of legality concerning tax issues. The amount of compensation due should have been settled by law and not through a joint decree issued by the Finance and Cultural Ministers or through an agreement between the association created pursuant to Art. 6 of Law 62/98 and the public or private entities using the recording equipment. Also important is the fact that Law 62/98 is not applicable to computer programs, electronic databases, and digital equipment and media.

The Constitutional Court's decision is at www.TRIBUNALCONSTITUCIONAL.PT/ACORDAOS/ACORDAOS03/601-700/61603.HTM.

SERBIA

By: Jovana Radevic,
SD Petosevic bvba, Overijse, Belgium

TELECOMMUNICATIONS: MONOPOLY PROBLEMS UNTIL 2005?

Precisely a year ago, after two years of negotiation and preparation, the Serbian Telecommunication Law, aiming to be modern, liberal, and fully harmonized with EU law, was adopted and put into force. By this law, the government tried to bring its legislation in line with the real world, and to begin solving long-standing problems. However, after a year, it seems that the main obstacles to liberalization of this market still remain.

The biggest and most disturbing obstacle is the monopoly of the state company Telekom Srbija on fixed-line telephony, provided by its contract with Greek and Italian companies until 2005 and confirmed by the Telecommunication Law. Telekom Srbija was present long before the contracts with its partners was signed in 1997. Although the monopoly of the Serbian Post Company PTT, foreseen by a previous 1991 law, was abolished, Art. 109 of the law confirmed the monopoly of Telekom Srbija agreed in the contracts with the Italian and Greek partners. The government explained that this "contract monopoly" could not be easily abolished, for there was no legal basis for unilateral abolishment and thus abolishment could result in a financial penalty for Serbia. Moreover, the government argued that there have been countries in a similar situation that have had a transition period (e.g., in Greece it was five years) to adapt their markets to liberalization and free competition.

Telekom Srbija often abused its dominant position in the past, especially in relation to Internet providers. The monopolistic behavior of Telekom Srbija caused considerable damage to ISPs, which were accused of violating the contract signed in 1997 by using VoIP and, as a consequence, their use of fixed lines was limited or forbidden. Even though court judgments were brought in favor of the ISPs, Telekom Srbija long refused to comply.

While the government finds these protective measures indispensable, the EU and WTO experts are not satisfied, nor is Serbian public opinion or the professional community. The basis of free competition has not been established, and Serbia risks having difficulties in acceding to both the EU and WTO. Moreover, various problems related to the ownership of Telekom Srbija persist.

In February 2004, structural government reforms were instituted. A new Ministry for Capital Investments was created to replace the Ministry of Telecommunications and Transport. The new Ministry seems determined to solve problems that the Telecommunication Law could not, as well as to achieve goals foreseen by the law but not accomplished to date, such as the creation of an executive body, the Agency for Telecommunications. Will the new government fulfill its promises and liberalize the market that has been monopolized on a legal basis? Or will Serbia be late, once again?

By: Josu Larrauri Elortegi,
Larrauri & López Ante Abogados, Madrid

SPAIN

E-VOTING IN SPAIN

Although Spanish Electoral Law does not permit the use of e-means for voting, both citizens and politicians are anticipating e-voting. Since 1991, Belgium has been conducting pilot experiments on e-voting. Success led the government to reform its Electoral Law in order to establish adequate conditions for e-voting. More recently, the British Government permitted voting by both Internet and mobile phone (SMS) in May 2003.

Spain is also witnessing the modernization of its Electoral System, sometimes through peculiar examples. One of them took place in a little village called Jun (2 kilometers from Granada, in the south of the country). Jun was the first municipality to offer its 2,500 inhabitants the possibility of voting by Internet in the last Andalusian elections. Although current legislation did not permit counting the e-votes, the experiment did serve to prove that the easier the voting system, the higher the level of participation. As self-proclaimed Spanish pioneers in IT, the Mayor of Jun has already announced that it is the desire of the entire village to become the first e-ID cardholders in the country.

Following Jun's example, the Mayor of Madrid, Alberto Ruiz Gallardón, put forward the *Madrid Participa* (Madrid Takes Part) program, which will per-

mit 120,000 city center inhabitants to vote on some municipal initiatives by Internet or SMS on 28, 29, and 30 June 2004. The initiatives cover topics such as urban equipment, activities, and quality of life. Significantly, the Mayor has announced that the e-voting will be binding and that approved measures will be adopted by the Town Council.

Also of note, in February 2003 the University of Leon became headquarters for the Electronic Voting Observatory (OVI). This organization intends to annually gather people from all over the world who are interested in the development of e-voting systems. The program comprises two fields: one technological—Votobit—and the other concerned with social issues—Socialbit. This structure will allow OVI to analyze different aspects of e-voting, not merely technical ones, as it has been proved that similar developments faced serious obstacles because too little attention was paid to social research.

Meanwhile, working groups created in the Senate show that there is an increasing institutional interest in introducing e-voting into the national electoral system. The aim is not only to simplify the recounting of votes, but also to achieve increasing levels of popular participation.

SPAIN

By: Enrique J. Batalla,
Batalla Abogados, Madrid

COPYRIGHTS AND MUSIC DOWNLOADING

In *Arista Records, Inc. et al. v. Sakfield Holding Company, S.L. et al.* (D.C. Cir. July 2003), the plaintiffs, U.S. and foreign record companies, filed a complaint claiming “copyright infringement, violations of the Lanham Act, unfair competition, and tortious interference” against Sakfield. Sakfield is a Spanish company organized under Spanish law and located in Madrid. The plaintiffs alleged that Sakfield owned and controlled a website (WWW.PURETUNES.COM) that allowed the unauthorized downloading of copyrighted musical works owned by plaintiffs. The Puretunes website manager had previously said that the site offered legal services operating under licensing agreements from various Spanish collective management organizations (Sociedad General de Autores (WWW.SGAE.ES) and Sociedad de Artistas Intérpretes y Ejecutantes). Unlike other download services, Puretunes manages a music library and says it will pay royalties to performers.

Sakfield filed two motions to dismiss. In the first, it asserted that it had neither records nor information pointing to any transaction with or music downloaded from PURETUNES.COM by persons or entities in the District of Columbia. Therefore, Sakfield considered the case should be dismissed on the grounds of *forum non conveniens*. Sakfield reiterated this argument in its second motion.

The plaintiffs’ complaint and opposition to this second motion detailed a belief that Sakfield had derived revenue from its DC sales. Thus, jurisdiction was proper under the District’s long arm statute, the assertion of which satisfies the constitutional minimum under the Due Process clause.

The court, in response to Sakfield’s first motion to dismiss, granted a period of jurisdictional discovery to allow plaintiffs an opportunity to discover facts sufficient to support continued jurisdiction, together with an order compelling discovery.

Analysis—According to the available case law, the court assumed that a plaintiff must first establish a factual basis for the court’s exercise of personal jurisdiction over a defendant to withstand a motion to dismiss (*Crane v. NY Zoological Society*), and, second, allege specific facts connecting the defendant with the forum (*Found v. US Conference of Mayors*). The DC Code

provided for specific jurisdiction because plaintiffs’ claim arose from Sakfield’s carrying out of business in the District. The DC Code also provides for general jurisdiction over a defendant even if the claim does not arise from the defendant’s conduct in the District. The test for general jurisdiction is whether the defendant’s contacts with the District were “continuous and systematic” (*Gorman v. Ameritrade Holding Corp.*). The requirements of due process are also satisfied when *in personam* jurisdiction is asserted over a non-resident corporate defendant that has a certain minimum of contacts with the forum. A court will find this fulfilled in any case where the defendant’s conduct is such that he should reasonably anticipate being haled into court in the forum (*World-Wide Volkswagen Corp. v. Woodson*). Moreover, a single act by the defendant in the jurisdiction can be sufficient to constitute “transacting business” (*Mouzavires v. Baxter*), despite this having occurred in cyberspace (*Material Supply Int’l Inc. v. Sunmatch Industrial Co.*).

The plaintiffs alleged, and Sakfield could not deny, that PURETUNES.COM was accessible 24 hours daily to persons in the District, thus constituting “continuous and systematic” contacts with the District. According to the court, Sakfield had therefore purposely targeted its actions at the District and could reasonably be haled into court there. In addition, the free music files received by users of the service after signing up were considered active solicitation.

The order compelling discovery contained two categories: Servers had to be put at the disposal of plaintiffs for their examination, and Sakfield was obliged to disclose credit card transactions with a third party provider, which would provide evidence of DC sales. The result of the first examination showed that important information had been erased from the servers after its ISP informed Sakfield of the plaintiffs’ copyright claims. Sakfield admitted such deletions, which it said it carried out to avoid further transmissions of copyrighted music. The court found this the “most ludicrous” argument it ever encountered, because the website could have been disconnected in any of several ways without destroying any files. Destruction of evidence raised the presumption that disclosure of the materials would be damaging (*Synanon Church v. United States*). Sakfield also failed to

comply with the second order. The court concluded that the credit card records included transactions with District of Columbia residents sufficient to support a finding of “continuous and systematic” contacts.

Conclusion—The court found that the plaintiffs had met both their burden of establishing a factual basis for the assertion of personal jurisdiction and the due process requirements of the Constitution. Therefore, the court denied Sakfield’s motion to dismiss and found itself competent to know of the plaintiffs’ complaint.

By: Astrid Arnold,
Lovells, London

**UNITED
KINGDOM**

CAN METATAGS AND KEY WORD PURCHASES CONSTITUTE TRADEMARK INFRINGEMENT?

Reed Executive plc and another v. Reed Business Information Ltd and others, [2004] All ER (D) 69 (Mar)

In a recent decision involving online recruitment sites, the English Court of Appeal failed to resolve the question of whether the use of trademarks as key word purchases and metatags can constitute trademark infringement under English law. The question arose in a dispute between Reed Elsevier (the publisher) and Reed Employment (the employment agency). Reed Employment owned the registered trademark Reed for employment agency services. Reed Elsevier ran a site advertising jobs under the name TOTALJOBS, a pop-up banner for which was triggered by a search on “Reed” in Yahoo. The TOTALJOBS site also included “Reed Business Information” as a metatag. The judge found that it was unlikely users would be confused into believing there was a trade connection between TOTALJOBS and Reed Employment. In the case of the pop-up, he thought the idea that a search under the name Reed would make anyone think there was a trade connection between a TOTALJOBS banner making no reference to the word “Reed” and Reed Employ-

ment was “fanciful.” In relation to the metatag he said that causing a site to appear in a search result, without more, does not suggest any connection with anyone else.

In the absence of confusion there was no trademark infringement and that meant that the judge did not need to consider the fundamental question of whether such “invisible” use of the trademark Reed could, in principle, constitute “use” at all under trademark law. (Infringement cannot arise without use, even if confusion can be made out.) The judge specifically reserved his view on this point, leaving it to be decided in a future case.

Ultimately it will be for the European Court of Justice to give guidance on this issue as it arises under the European Trademarks Directive (First Council Directive 89/104/EEC to approximate the laws of the Member States relating to trade marks), which harmonized European trademark laws in many respects.

Websites for Government and Related Reports

Intellectual Property

New USPTO Policies Re [] Public Access to Existing Paper Copies of Trademark-Related Documents, Patent and Trademark Office, www.uspto.gov/web/trademarks/notice_paperfiles.htm.

Revision of Patent Term Extension and Patent Term Adjustment Provisions, Patent and Trademark Office, uspto.gov/web/offices/com/aol/notices/69fr21704.pdf.

USPTO Announces New Version of Patent Application Information Retrieval System (PAIR), V. 4.11, Patent and Trademark Office, www.uspto.gov/web/patents/pair411.pdf.

USPTO to Provide E-Access to Cited US Patent References with Office Actions and Cease Supplying Paper Copies, Patent and Trademark Office, www.uspto.gov/web/offices/pac/dapp/opla/preognotice/nocopies.pdf.

Internet

Amendment of Rules Under the Fair and Accurate Credit Transactions Act of 2003 (FACT Act), Federal Trade Commission, www.ftc.gov/os/2004/05/040520factafn.pdf.

Bitstream Access—ERG Common Position, European Union, www.erg.eu.int/doc/whatsnew/erg_0333rev1_bitstream_access_common_position.pdf.

E-Europe 2005: An Information Society for All, European Commission, www.europa.eu.int/information_society/eeurope/2005.

Electronic-Consolidated Targeted Financial Sanctions List (e-CTFSL), European Union, europa.eu.int/comm/external_relations/cfsp/sanctions/index.htm.

ERG Common Position on the Approach to Appropriate Remedies in the New Regulatory Framework, European Union, erg.eu.int/doc/whatsnew/erg_0331rev1_remedies_common_position.pdf.

Formation of the Country-Code Names Supporting Organization (ccNSO), ICANN, ccns0.icann.org/announcements/ccns0-statement-01mar04.pdf.

High Level Group on Digital Rights Management—Highlights of the First Meeting, European Union, www.europa.eu.int/information_society/eeurope/2005.

Label for E-Mail Messages Containing Sexually Oriented Material; Final Rule, Federal Trade Commission, www.ftc.gov/os/2004/04/040413adultmailfinalrule.pdf.

Regulations Amending the Canadian Computer Reservation Systems (CSR) Regulations, Canada Gazette, canadagazette.gc.ca/partii/2004/20040507-x/g2-138x05.pdf.

Privacy

Appointing the Independent Supervisory Body Provided for in Article 286 of the EC Treaty (European Data Protection Supervisor) (2004/55/EC), European Parliament Council, www.europa.eu.int/cgi-bin/eur-lex.

Data Mining: Federal Efforts Cover a Wide Range of Uses, General Accounting Office, www.gao.gov.

Telemarketing Sales Rule—16 CFR Part 310 (FTC File No. R411001), Federal Trade Commission, www.ftc.gov/os/2004/03/trs3/dayfrn.pdf.

Security

Cross-Border Fraud Trends—Jan-Dec 2003, Federal Trade Commission, www.ftc.gov/opa/2004/03/cbcy2003.pdf.

Establishing the European Network and Information Security Agency, EC Directive 460/2004, European Union, www.europa.eu.int/cgi-bin/eur-lex.

How Victims' Information Is Misused, Report-Jan 1-Dec 31, 2003, Federal Trade Commission, www.ftc.gov/os/2004/03/bealsfraudtestappa.pdf.

National and State Trends in Identify Theft—Jan-Dec 2003, Federal Trade Commission, www.consumer.gov/sentinel/pubs/top10fraud2003.pdf.

Secure Hash Standard, FIPS 180-2, National Institute of Standards and Technology, csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf.

Statement Opposing Ratification of the Council of Europe's Convention on Cybercrime, Electronic Privacy Information Center, www.epic.org/privacy/intl/cc.html. (The Council of Europe Convention on Cybercrime, CETS No. 185 (1997), may be read at conventions.coe.int/Treaty/EN/Treaties/HTML/185.htm.)



3028 JAVIER ROAD • SUITE 402 • FAIRFAX, VIRGINIA 22031
TELEPHONE: 703-560-7747 • FAX: 703-207-7028
E-MAIL: CLA@CLA.ORG

**PLEASE SUBMIT MATERIALS FOR
THE BULLETIN AS FOLLOWS:**

- **Feature Articles:**
Esther C. Roditti
 - **U.S. Federal & State Case Updates:**
Robert M. Weiss
 - **European Countries and the EU
Case, Legislative, and Directive Updates:**
Ashley Winton
 - **Non-European, Non-EU Countries
Case and Legislative Updates:**
Donald S. Hicks
Fabrice Perbost
- Addresses and telephone/fax
numbers for the above editors
are on the front cover.

**CONTRIBUTORS
IN THIS ISSUE:**

Markus Andreevitch <i>Vienna, Austria</i>	Steve Englund <i>McLean VA</i>	James E.B. Sanders <i>Atlanta GA</i>
Astrid Arnold <i>London, England</i>	Matthew T. Furton <i>Chicago IL</i>	Theresa A. Simpson <i>Seattle WA</i>
David D. Axtell <i>Minneapolis MN</i>	Alan James <i>Toronto, Ontario, Canada</i>	David R. Syrowik <i>Southfield MI</i>
Enrique J. Batalla <i>Madrid, Spain</i>	Sabine Lipovetsky <i>Paris, France</i>	Rajiv Talwar <i>New Delhi, India</i>
John M. Carson <i>San Diego CA</i>	Charles Morgan <i>Montreal, Quebec, Canada</i>	Sónia Queiróz Vaz <i>Lisbon, Portugal</i>
Stephen J. Davidson <i>Minneapolis MN</i>	Céline Mutz <i>Paris, France</i>	Scott G. Warner <i>Seattle WA</i>
Susan L. Donegan <i>Amsterdam, The Netherlands</i>	Jovana Radevic <i>Overijse, Belgium</i>	
Josu Larrauri Elortegi <i>Madrid, Spain</i>	Scott Russell <i>Boston MA</i>	