

The



Bulletin

CLA Website: 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	News and Announcements	121
	Coming Events	
	Ethics Column	
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	Editorial Department	125
	Current Issues in IT and Communications Law in China	127
	By: Matthew A. Murphy Beijing, China	
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	Addressing OSS Issues in Product Development	131
	By: Stephen Mutkoski Redmond, Washington	
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	Data Privacy and Personal Information Protection in Mexico	136
	By: Luis Vera Vallejo Mexico City, Mexico	
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	United States Law Updates	142
	International Law Updates	146
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	Editor's Report	159
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	Websites for Government and Related Reports	

Computer Law Association News & Announcements

Coming Events

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

May 5-6, 2005—CLA World Computer and Internet Law Congress, The Park Hyatt Hotel, Washington DC

Brochures and registration information for all CLA conferences are available in PDF format at WWW.CLA.ORG.

For additional information on the First Asia Conference, see WWW.CLA-INDIA.COM.

Correction and Update

Re “‘Substantially Similar’ Alberta Privacy Law Supersedes PIPEDA,” Vol. 19, No. 2, p.70—The Order was adopted and registered by the Governor in Council on 12 October 2004, not 10 April. Also on 12 October 2004, the Governor in Council adopted and registered a similar Order regarding the British Columbia Personal Information Protection Act, declaring that it too met the “substantially similar” test. Accordingly, henceforth the two provincial acts will apply to intra-provincial private sector data protection matters (unless the matter relates to a federal work, undertaking, or business).

Attention Members

The value of the *CLA Bulletin* depends upon the quality of its content. Before submitting manuscripts elsewhere, consider publishing first in your *Bulletin*. The process is easy. If you wish to publish a feature article, please send the manuscript to me, Esther C. Roditti, for consideration. I always welcome articles on timely topics and issues. The required length is 2,000-4,000 words, with endnotes and standard case citations. My postal and e-mail addresses are on the front cover. Remember, the quality of the *Bulletin* depends on you!

Ethics Column

Technology Lawyers: Saying Too Little, Too Much, or Getting It Just Right

By: Merri A. Baldwin¹

Two recent California Court of Appeal decisions illustrate the increased scrutiny that technology lawyers face in this post-Enron age. The lessons transcend California’s borders. The case of *Vega v. Jones, Day, Reavis & Pogue*,² makes clear that lawyers have to be careful not to say “too little,” even to the other side. The case of *Jasmine Networks, Inc. v. Marvell Semiconductor, Inc.*,³ while involving an unusual fact situation, shows the dangers of saying “too much.” But even more importantly, *Jasmine Networks* reminds us of the important role that technology lawyers can and should play in counseling their clients not to step over lines that should not be crossed. Technology lawyers can learn a number of lessons from these two cases—including guidance about what not to do.

Don’t Say Too Little—In *Vega*, the plaintiff was a shareholder of Monsterbook.com. The law firm of Jones Day had represented Transmedia Pacific in acquiring Monsterbook.com. After the Monsterbook shareholders accepted Transmedia’s merger offer, but before the deal closed, Transmedia secured \$10 million in investment financing from a third party. The financing included “toxic” stock provisions, whereby the third-party investors received convertible stock which “seriously” diluted the stock of the other Transmedia shareholders. After the acquisition, Vega sued Jones Day, alleging that Jones Day fraudulently withheld information concerning the “toxic” terms of that financing. The plaintiff claimed that he had been defrauded into exchanging his valuable stock for toxic stock in the acquiring company, resulting in a substantial loss.

Vega alleged that Jones Day prepared a compre-

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.

hensive disclosure statement concerning the third-party investment, but did not send that statement to Monsterbook or its counsel. Instead, the lawyers allegedly provided a “sanitized” version of the disclosure statement that did not contain information about the toxic terms. Jones Day also allegedly told Monsterbook and its counsel that the financing was “standard” and “nothing unusual.” Jones Day stressed that it had provided each Monsterbook shareholder with a consent form, which said Transmedia would file a “Certificate of Designation” with the Delaware Secretary of State. That certificate, a publicly available document, contained all the terms for the \$10 million financing, including the “toxic” stock provisions.

The trial court sustained Jones Day’s demurrer to the two causes of action (fraud and negligent misrepresentation) and dismissed the complaint, basing its decision on several grounds: (1) the complaint did not allege an actual misstatement by Jones Day; (2) plaintiff could not justifiably have relied on Jones Day’s statements; (3) plaintiff could not state a claim based on omission or nondisclosure, because Jones Day owed no duty to the Monsterbook shareholders; and (4) plaintiff did not allege damages proximately caused by Jones Day.

The court of appeal reversed as to the fraud claim. The court started its analysis with the basic principle that a fraud claim against a lawyer is “no different from a fraud claim against anyone else.” The court first held that calling a transaction “standard” or “not unusual” was not actionable. Those were “casual comments” that no one reasonably could rely on. However, the court concluded that Jones Day’s alleged failure to disclose the terms of the toxic stock provisions constituted “an active concealment or suppression of facts” that was tantamount to a false representation. Jones Day argued that, as counsel for the adverse party in a merger, it had no duty to disclose those terms to Monsterbook. The court disagreed, because “Jones Day specifically undertook to disclose the transaction and, having done so, was not at liberty to conceal a material term.” Quoting *Cicone v. URS Corp.*,⁴ the court noted that

where one does speak he must speak the whole truth to the end that he does not conceal any facts which materially qualify those stated. [Citation.] One who is asked for or volunteers information must be truthful, and the telling of a half-truth calculated to deceive is fraud.

As a general principle of tort law, that conclusion is not too surprising. Somewhat more surprisingly, the court also rejected Jones Day’s argument that the Monsterbook shareholders could not prove justifiable reliance, since the terms of the \$10 million financing, including the toxic stock provisions, were publicly available information, on file with the Delaware Secretary of State. Jones Day argued that, with reasonable diligence, Vega could have discovered the facts he claimed were withheld, especially since Jones Day had notified the shareholders in writing that it would file the certificate that contained the information. The court dismissed that argument with reasoning that is somewhat difficult to understand.

First the court stated that, in a nondisclosure case, the question is whether the defendant is aware of material facts that it knows are “neither known *nor readily accessible*” to the plaintiff. Then, ignoring the fact that the toxic stock provisions were disclosed in a public forum, the court held that Jones Day left itself open to a fraud claim by (1) knowing about the toxic provisions, (2) making disclosures of some financing terms, but (3) not disclosing the toxic provisions. The court said that Jones Day’s reasons for the partial disclosure, and whether the toxic provisions were truly “readily accessible,” were questions of fact that had to be decided on the evidence, not a pleading motion.

Most jurisdictions hold that lawyers can be liable for outright misrepresentation or fraud, even to parties on the other side of a transaction. *Vega* may illustrate that courts are giving increasing scrutiny to law firm conduct. (In fact, prior to the filing of *Vega*, Jones Day had defeated similar fraud claims brought by other Monsterbook shareholders.) *Vega* makes clear that technology lawyers have to be careful not to say “too little.”

If you undertake to make disclosures on behalf of your clients, you must be careful not to withhold any material information from those disclosures, i.e., information that an objective third person would reasonably conclude the other party would want to know. While it should be enough to disclose the existence of other publicly filed documents and leave it up to the other side to investigate, *Vega* makes that practice risky. Thus, if you are going to make reference to other documents containing relevant information, either provide those documents or take the extra step of specifically stating that the other side *should* consult those documents.

Technology lawyers may also want to protect

themselves through a written caveat that they are not representing the non-clients, and an express statement that the non-clients (and their counsel) should (1) independently investigate and verify any facts the lawyers are transmitting and (2) make their own independent risk assessment. If the opposing party is not represented by counsel, you are more at risk, so you might want to add that the other party should not rely on you for factual information or for legal advice, as your sole obligation is to protect your own client's interests.

Don't Say Too Much—The facts in the *Jasmine Networks* case are admittedly (and thankfully) unusual, but the lessons to be learned are nonetheless valuable for technology lawyers as they counsel clients who wish to acquire others' technology. In *Jasmine Networks*, one semiconductor company (Marvell) was in the process of negotiating with another company (Jasmine) for the purchase of a portion of Jasmine's technology and to acquire a group of its engineers. The parties executed a strict non-disclosure agreement.

During the course of negotiations, a group from Marvell placed a call to Jasmine's director of legal and business affairs. When she was not available, they left her a voicemail. After leaving the voicemail, the Marvell group failed to hang up, and they proceeded to have a conversation that they thought was private, but which was actually recorded on the Jasmine employee's voicemail. Based on the recorded message, it appeared that Marvell was intending to take Jasmine's intellectual property "on the pretense of just evaluating it" and put it into their product, with the possibility that at least one of Marvell's officers could go to jail. In the court's words, the message demonstrated Marvell's "theft of Jasmine's trade secret, the potential consequences and the planned cover-up."

After listening to the voicemail message and investigating the facts, Jasmine sued Marvell. Marvell claimed that the conversation was privileged, because the participants in the call included Marvell's general counsel, its in-house patent attorney, and its vice-president of engineering. Based on that argument, Marvell obtained a preliminary injunction prohibiting Jasmine from using or disclosing the transcript of the voicemail message. Jasmine appealed, and the Court of Appeal reversed.

The court first considered that Marvell had waived the privilege because the privilege holder itself (Marvell)—not just its counsel—had made an

uncoerced disclosure, and the relevant statute did not require an intent to disclose. This conclusion was based on two facts: one of the participants was an officer of Marvell, and even the general counsel wore two hats—he was not only general counsel, but also vice-president of business affairs.

The opinion contains a cautionary tale for technology lawyers, because the Court of Appeal also found that the crime-fraud exception to the attorney-client privilege applied. California's crime-fraud exception is typical of other state statutes. It provides that there is no privilege "if the services of the attorney were sought or obtained to aid anyone to commit or plan to commit a fraud." While most attorneys assume they would never be subject to the crime-fraud exception, it often does not take much to invoke the exception. First, the party seeking the communication must provide evidence to support an *inference* of a crime or fraud. Case after case demonstrates that courts often set this threshold very low. Second, that party must then show a "reasonable relationship" between the alleged crime or fraud and the attorney's communication. Again, it does not take much to make that link. Usually, the attorney's "innocence" of the scheme is irrelevant.

In *Jasmine Networks*, the court looked to evidence, obtained from depositions and other discovery, that Marvell had secretly sought and obtained some of the very same information that it was seeking to license. The court also relied on evidence showing that Marvell had obtained that information from a Jasmine employee that Marvell had expressly agreed not to contact. The court found this sufficient to establish a *prima facie* case of a crime or fraud. Since the conversation related to the alleged scheme, the crime-fraud exception applied.

Getting it Just Right—Marvell got "caught" because of the unintended voicemail, but the lesson to be learned from *Jasmine Networks* is much more than "Learn to hang up and start a fresh call after leaving someone a voicemail." Even without the voicemail trail, the conversation between Marvell and its counsel would have been discoverable under most state crime-fraud exceptions to the attorney-client privilege.

A technology lawyer's role—whether as in-house or outside counsel—is not just to do a client's bidding, or to stand by and watch corporate employees breach the corporation's contracts or otherwise violate the law. In this post-Enron age, expect increased scrutiny of a lawyer's role in transactions and of a lawyer's

communications with his or her clients. *Jasmine Networks* makes this point clearly: “In an era where corporate fraud and boardroom misconduct is front-page news, as well as prosecutions of accountants and lawyers in connection with such conduct, our courts are required to ensure that the attorney-client privilege is not used to promote or further any such conduct.” If you perceive fraudulent or criminal activity is being contemplated, or is underway, you should examine your ethical obligations and take appropriate steps to counsel your client on the laws governing, and risks attending, its course of action.

Endnotes

1. Merri A. Baldwin is a shareholder at the San Francisco law firm Rogers Joseph O’Donnell & Phillips, where she is a member of the Professional Liability and Complex Litigation practice groups. She can be reached at MAB@RJOP.COM.
 2. 04 CDOS 7000 (August 2, 2004).
 3. 117 Cal. App. 4th 794 (2004).
 4. 183 Cal. App. 3d 194, 202 (1986).
-

Editorial Department

The Editor

The primary responsibilities of the Editor are many. She coordinates and edits the quarterly reports of recent computer law developments provided by the Regional Editors, selects for publication articles submitted by CLA members and others, and edits the selected manuscripts. She also provides member information regarding significant computer law happenings, updates case citations and reports of selected governmental and related publications, and provides oversight of *Bulletin* production. These tasks are performed with the indispensable and outstanding assistance of **Ruth K. Dargis**, who provides copy editing and production management and coordination with the desktop publishing expert, **Martin Schaefer**. Also of great help is the work of **Lisa Lifshitz**, Chair of the Publications Committee, and of **Barbara Fieser**, our Executive Director, who handles coming events and promotions.

Manuscripts on current computer-related issues are most welcome and will be read by the Editor. In order to conserve CLA resources, authors are asked to, if possible, send manuscripts on diskette or by e-mail in WordPerfect, WP-compatible, or Rich Text Format. Standards for CLA publications are posted on the CLA website, WWW.CLA.ORG.

Esther C. Roditti

Esther C. Roditti has practiced computer law since 1978, focusing on contracts, licensing, and intellectual property law. Her recent books include *Computer Contracts: Negotiating and Drafting Guide* (Lexis Publishing; updated semi-annually 1992 to date), *Glossary of Computer and Internet Terms* (Lexis Publishing, 2000), *Hiring and Firing Knowledge Workers* (Roditti Reports), and *Tax and Business Handbook for Consultants and Clients* (Independent Computer Consultants Association). She is also the former editor and publisher of *Computer Law & Tax Report*. Esther has written hundreds of articles on computer-related issues, and is a conference lecturer both here and abroad. She was the founder of the Computer Law Committees of the Association of the Bar of the City of New York and the American Arbitration Association Advisory Committee for Computer Disputes.

Prior to her computer law practice, Esther was senior program officer of the Ford Foundation, in charge of developing legal programs to achieve gender equality; before that she was assistant director of Columbia Law Legislative Drafting Research Fund, preparing model legislation in the environmental health area. She is a graduate of the University of California at Los Angeles (AB, *magna cum laude*, Phi Beta Kappa) and Harvard Law School, Harvard University (JD).

The Regional Editors

Reports of regional computer law developments are sent to Regional Editors, who collect and edit the material and then forward manuscripts to the Editor for final editing and publishing in the upcoming *CLA Bulletin*. The Regional Editor for the United States is Robert M. Weiss; he supervises, coordinates, selects, and edits reports of state and federal case updates from CLA member reporters in each of the Federal Circuits. Outside the United States, the Regional Editors are Donald Hicks—the rest of North and South America, and Australia, Ashley Winton—Western Europe and the European Union, and Fabrice Perbost—the rest of the world. Reporters' bylines appear with their published reports.

Donald S. Hicks

Donald S. Hicks is a partner in the Toronto office of Gowing Lafleur Henderson LLP. He has broad corporate and commercial experience both as outside and inside counsel, and focuses primarily on the law related to information technology and related business transactions, particularly outsourcing.

Donald received his law degree from Osgoode Hall Law School of York University, and his BA (Hons.) and MBA from Queen's University at Kingston. He is a frequent speaker, and has published a number of articles relating to outsourcing and the governance of joint ventures and strategic alliances.



Fabrice Perbost

Fabrice Perbost is a partner at Kahn & Associés law firm in Paris, France. He heads the firm's information technology/intellectual property group. Fabrice gives advice and assistance in various areas such as intellectual property, media, and telecom, as well as hardware, software, and services.

He also assists clients across a wide range of contract-drafting and negotiations, and provides intellectual property and regulatory advice in the fields of media, telecommunications, and biotech. Fabrice has also published numerous articles in these fields and regularly speaks on IT issues. He is a lecturer at Paris II Panthéon-Assas University as well as at Paris X-Nanterre University.

**Robert M. Weiss**

Robert M. Weiss is a partner at the Chicago-based law firm of Gordon & Glickson LLC, which provides strategic legal advice to the information technology and e-commerce marketplace. Robert's practice focuses on software development, licensing, systems integration, IT outsourcing, ERP, and telecommunications. He is Chairman of the Computer Law Committee of the Chicago Bar Association. Robert received his JD from Stanford University and his BA from Dartmouth College. He is a frequent lecturer and has written several published articles relating to dynamic pricing on the Internet. Robert was recently named as one of the "40 Under Forty" leading Illinois attorneys by the Law Bulletin Publishing Company.

**Ashley Winton**

Ashley Winton is a partner in the London office of Pillsbury Winthrop LLP. Ashley specializes in European regulatory issues, including technology transfer, trade, data protection, and privacy. He advises on intellectual property, domain name, and confidentiality issues, as well as licensing matters, particularly those with

an antitrust component. Ashley is a graduate of the College of Law, Guildford; he received his Master of Engineering and Bachelor of Science degrees from the University of Manchester Institute of Science and Technology. He is recognized in the Legal 500, Global Counsel, and the Chambers legal directories as an expert in IT and e-commerce. Prior to his legal career, Ashley was a computer programmer and electronic engineer for a large systems house. He regularly speaks on IT issues and has for over nine years been an International Editor for the *Bulletin*.



Current Issues in IT and Communications Law in China

By: Matthew A. Murphy, Beijing, China¹

Unless you have been on another planet for the last few years, you will have heard about and possibly directly experienced China's hunger for technology. China's appetite for the latest software, e-commerce applications, and telecommunications devices and functions seems insatiable. In addition to the well-known foreign brands in the local Chinese market, a number of local brands are beginning to emerge as leaders in IT and communications. The more important legal issues associated with IT and communications in China are discussed herein. Recent changes to foreign trade regulations, telecommunications services classifications, and the way courts and government agencies view unfair competitive practices signal that the legal framework for IT and communications, and the convergence of these industries, is laying the foundations for a well-regulated market sector.

Regulators and Convergence

As in many countries around the world, the convergence of technologies has forced the convergence of regulations and of the regulators themselves. China has been well aware of this phenomenon; the Ministry of Information Industry (MII) was formed in 1998 by the merging of the Ministry of Post and Telecommunications, the Ministry of Electronics Industry, and part of the Ministry of Radio, Film, and Television. The MII now regulates the IT, the Internet, and telecommunications industries, albeit by separate departments.

The State Administration of Radio, Film, and Television (SARFT) continues to retain control over the general media; however, given the rapid convergence of industries, it is likely that it will need to work much more closely with the MII over the next few years. The State Administration of Industry and Commerce (SAIC) continues to exercise jurisdiction over some aspects of e-commerce (e.g., business and website registration in Beijing), and is expected to continue to do so in relation to non-technical issues, given that China and the rest of the world have tended to prefer to put the "bricks" back into "clicks and mortar," rather than establish and maintain two

separate administrative regimes. Similarly, the Ministry of Commerce (MOFCOM) will remain in charge of regulating foreign investment in the IT and communications sectors, as it does in other sectors of the economy.

E-Commerce

China was one of the first countries able to claim that it had legislated in the area of e-commerce. The 1996 *Guangdong Province E-Commerce Regulations* were revolutionary in showing a legislature that had the courage to legislate in an area that suffered from a lack of country-specific legislative precedents. One of the main achievements of these regulations was to make it clear that e-contracts involving a foreign element would be upheld as valid.

In 1999, the long-awaited *PRC Contract Law* was unveiled, bringing together the contract law regimes for domestic and foreign-related transactions. The law stated that contracts could be in written form, with Article 11 confirming that "written form" refers to a "written contractual agreement, letter, e-data text (including a telegram, telex, fax, e-data exchange, and e-mail) that can tangibly express the contents contained therein." Article 16 basically produced a postal acceptance rule for e-mail-concluded contracts.

Then, in 2000, the Beijing AIC issued a regulation requiring any entity in Beijing engaging in various forms of e-commerce and Internet services to register with the AIC and other government agencies. In 2002, it issued a further set of regulations (*Supervision and Administration of Electronic Commerce Tentative Procedures*), which reaffirmed its 2000 licensing and registration regime and also set out various helpful consumer protection provisions, such as mandating a cooling-off period.

One issue that has continued to frustrate local and foreign companies wishing to engage in e-commerce in China has been consumer and technical concerns with security issues such as hacking, viruses, and privacy. To the surprise of many foreign companies, China has an intimidating legislative framework relating to computer network security. How often the laws are enforced remains a concern, as is the lack of

deterrence in the penalties imposed when the laws are enforced.

As early as 1994, the *Regulations Regarding the Security of Computer Information Systems* was enacted, Article 6(1) of which prohibits the intrusion into or use of a computer information network without authorization. Article 285 of the *PRC Criminal Law* imposes criminal liability for the unauthorized entry into computer systems in limited circumstances. It provides that whoever, in violation of state regulations, enters without authorization computer information systems in the fields of state affairs, national defense construction, or sophisticated science and technology shall be sentenced to a prison term of no more than three years or to criminal detention.

As far as viruses are concerned, the *PRC Criminal Law*, the *1994 Regulations*, the *Administrative Measures for the Prevention and Control of Computer Viruses*, and various other regulations clearly make writing and spreading a virus a risky proposition in China. For example, Article 23 of the *Regulations for the Security Protection of Computer Information Systems* provides that whoever intentionally inputs computer viruses or other harmful data to endanger the safety of computer information systems shall be given a warning or fined by the public security authorities.

There also appears to be potential for privacy and personal data to be protected under various laws in China. The *PRC Constitution* refers to a right of “personal dignity.” The *PRC Civil Law* refers to this right, as well as a right to “reputation.” Given the Supreme Court 2001 Interpretations regarding a person’s right to claim loss for mental anguish, the concerns regarding the need to prove damage in a “personal dignity” or “reputation” privacy invasion case have lessened. Further, the *PRC Criminal Law* prohibits the unauthorized opening of correspondence, and it is thought that a court would have little trouble in concluding that this includes e-correspondence, given that 100 million people in China use e-mail as their preferred method of correspondence. Finally, Article 12 of the *Internet Messaging Services Provisions 2000* requires that ICPs

shall keep users’ personal information confidential and shall not disclose such personal information to any third party without the consent of the users, *unless the law otherwise requires such disclosure.*

It is the last part of this sentence that continues to cause concern, since China’s law enforcers have extremely wide search powers.

The 2004 amendments to the *PRC Foreign Trade Law* and the issuing of the *Foreign Investment in the Commercial Sector Procedures* have the potential to see far more effective e-commerce in China. Individuals will now be able to engage in import and export, thus largely removing concerns by e-commerce operators that contracts formed on-line with a PRC citizen may not be enforceable due to lack of capacity. Foreign entities also will be able to engage in domestic wholesale and retail services (a major breakthrough for “bricks and mortar” as well), without having to form a costly joint venture or engage in a fiction of adding value to their imported goods before selling them into the China market.

The US Digital Millennium Copyright Act (DMCA) has been seen as a vital tool in ensuring the confidence of businesses to engage in online services. It makes ISPs liable in certain circumstances and sets up a regime for efficient dispute resolution regarding copyright material that is placed on an ISP’s website without the copyright owner’s consent. China’s Supreme People’s Court’s *Several Issues Concerning the Laws Applicable to the Trial of Copyright Disputes Involving Computer Networks Interpretation* (ISP Interpretation) was first issued in December 2000, and was amended in January 2004. An article was added to the 2004 revision of the Interpretation prohibiting an ISP from uploading, broadcasting, or providing methods or equipment that it knows are used to avoid the technical protection measures used to safeguard another’s copyright works. Article 5 sets up a “take-down” notice procedure similar to that in the DMCA. Article 6 requires an ISP/ICP to provide the copyright owner with information regarding the person that has carried out the online copyright infringement.

Software

The *PRC Contract Law* sets out a number of provisions affecting technology contracts. Most of these are not controversial and are addressed in any standard software licensing or outsourcing contract. The *PRC Technology Import and Export Regulations 2002* (Technology Import Regulations), do however contain some provisions that have caught many foreign software sellers off-guard.

Article 2 of the Technology Import Regulations states that

technology import and export as referred to in these Regulations means acts of transferring technology from outside the territory of the People's Republic of China into the territory of the People's Republic of China or vice versa by way of trade, investment, or economic and technical cooperation. The acts mentioned . . . include assignment of the patent right, assignment of the patent application right, licensing for patent exploitation, assignment of technical secrets, technical services, and transfer of technology by other means.

Upon a literal reading, it would appear that the regulations cover software licensing and outsourcing arrangements. Article 17 requires that the relevant technology agreement be registered with the local department of MOFCOM. It is understood that many software sellers have been able to obtain exemptions from MOFCOM because some of its officials take the view that software licenses should be registered with the MII under other regulations (discussed below) and therefore do not need to be registered under the Technology Import Regulations. Given that the Regulations contain a number of clauses that concern technology owners, such as prohibitions on certain restrictive covenants and mandatory improvement-ownership provisions, sellers prefer to avoid this regime. Failure to comply could cause problems when it comes to enforcing the provisions of an agreement (a defendant could claim some type of equity-related claim, such as that regarding "clean hands," thus persuading a court to require registration prior to proceeding to deal with a dispute) or attempting to convert RMB into foreign currency for royalty remittance.

The *Computer Software Regulations* issued in 2002 allow for the optional registration of software and licenses with the Computer Software Protection Centre. There is no doubt that registering software with this body will allow for easier enforcement in copyright infringement actions, since a plaintiff will not have to prove that it owns the copyright in order to be able to take advantage of interlocutory injunctions and to proceed with a successful infringement action. Further, given that software enterprises are able to obtain favorable tax treatment in China, registration under these regulations may be required by the

software enterprise approval authority as a condition of being offered the preferential treatment. The MII also requires registration—in 2000, it issued the *Administration of Software Products Procedures*, which state that only those products that are registered with the MII can be sold in China.

There is much discussion about the long-awaited general competition law that will be unveiled in the near future. Many are concerned that this law will be aimed at large foreign multinationals that have been able to corner more than 90 percent of the market in some sectors. No doubt freeing up the commercial sectors of wholesale and retail to small foreign companies will in itself have an impact on competition in many of these sectors. Some reports have stated that the government intends to issue a special software procurement law to force government departments and possibly state-owned entities to use no more than 30 percent of foreign software. Given the size of the government in China, this could cause significant concerns for foreign software suppliers. Such a step would also be a concern for China's move toward improving efficiency in government.

Another interesting development is the increased willingness of the courts to apply the *PRC Anti-Unfair Competition Law* to technology-related cases. For example, a software developer was found liable for unfair competition when it set up some software that, when downloaded, stopped a competitor's software from functioning adequately. If the courts continue to move in this direction, local and foreign IT companies will have increased confidence that the judiciary will continue to address anti-competitive conduct.

As far as foreign investment in software enterprises and R&D centers in China is concerned, the incentives still seem to favor software enterprises. The *Encouraging the Development of the Software and Integrated Circuit Industries Several Policies* and the *Questions Relating to Foreign Investors Investing in and Establishing Research and Development Centres Circular* were issued in 2000. While the minimum investment required to establish an R&D center has remained at US\$2 million, most of the tax incentives (two years tax free, and then three years of 50 percent income tax) seem to favor software enterprises. One difficulty in obtaining these very favorable incentives is the need to be registered as a software enterprise, allowing subjectivity to enter the equation.

Conclusion

There is great potential for China to become a leader in the IT and communications markets, given new technologies, the passion and dedication of people in the industry, and foreign cooperation in relation to new technologies. It is hoped that China will also continue to ensure that its laws keep pace with the technological and industrial developments, so as to continue to encourage investment in these very important areas of the economy.

Endnote

1. Matthew A. Murphy is Managing Director of the MMLC Group in Beijing. He may be reached at MMURPHY@MMLCGROUP.COM. An oral version of this article was presented at the Society for Computers and Law “Global IT Law Conference” at Keble College, Oxford University, in July 2004.

Addressing OSS Issues in Product Development

By: Stephen Mutkoski, Redmond, Washington¹

Whether you are in-house counsel for a software company or a lawyer representing clients who develop software, it is imperative that you understand the risks that can arise when software developers download and incorporate open source software (OSS) into company products. This article provides a broad overview of some of the steps that legal counsel can take to address these risks, including making sure that the client company has a coherent policy that addresses these risks, that your company staff understands the company policy, and that the company has effective procedures or mechanisms in place to address OS issues as they arise.²

Create an OS Policy

Most important is thinking through carefully some of the common OSS issues or scenarios that are likely to arise and determine in advance—in a well-reasoned fashion—how a company should address or respond to these common issues or scenarios. For example, if a developer requests permission to download and incorporate source code governed by the GPL into company products, how would you respond? How would your response differ if the code were governed by the BSD license? What if the request was for permission merely to download and install OS applications for use within the company? It is important to understand that there is no single “one-size-fits-all” OS policy; each company will have somewhat different answers for these common OS questions. Each company’s distinct business plan and licensing model (and level of aversion to uncertainty and risks) will dictate the appropriate response for that company to each of these common OS issues.

Why Every Company Needs an OS Policy—There are two primary risks relating to OS software. First, and most obvious, are the outbound licensing conditions or requirements that come into play when one incorporates GPL or other similar “copyleft”³ code into a company product. By incorporating GPL code into a product, your company would likely be required to release source code and grant broad IP licenses to the larger work it creates. The GPL does, after all, condition its license grants on the licensee making the same grants with respect to the larger work it creates. These “reciprocal” grants (and access to the product’s

source code) could be inconsistent with your company’s existing or planned outbound licensing regime.

The second—less appreciated—risk relates to concerns about source code “pedigree.” Code of unknown or dubious pedigree can transmit with it risks of third party intellectual property claims. Some, perhaps much, OS code is written by a loosely knit group of developers, often with little or no legal supervision to make sure that infringing code or concepts are not being added by the contributors. Many contributors to OS projects have day jobs at companies where they work on related technologies. The employment agreements that are common in the technology industry might well dictate that the “contributions” being made to the OS project are actually owned by the employer. Because IP claims are not dependent on intent or knowledge, your company would be an infringer if unauthorized third party intellectual property were transmitted in the OS code.

Factors to Consider—The range of responses that various companies might have to these risks results from the fact that the IP issues presented can look surprisingly different when viewed through the lenses of each individual company’s business plan and licensing model. In other words, while one company might be very concerned that incorporation of GPL code into one of its products would require it to make the source code to the entire product available (and to grant broad IP licenses to that entire product), another company might be willing to live with the conditions imposed by the GPL. Such differences depend primarily on the extent to which the company derives revenue from licensing its products for a fee to users, because although the GPL does not rule out the collection of a fee in connection with the distribution of a work, it does rule out charging a license fee. Moreover, the broad IP license grants in the GPL (as well as the requirement of providing source code) effectively destroy the ability of a company to prevent others from obtaining, reproducing, and redistributing the GPL work without paying the licensing fee (in fact the GPL is intended to encourage such redistribution). Even within a company there may be varied approaches, depending on the circumstances and the particular product. A company might have one set of rules for incorporation of OS code into “core” soft-

ware assets (where IP licenses generate significant revenues), but different rules for non-core software assets (where the company might not extract much in the way of licensing revenues).

As a preliminary step to formulating an OSS policy, you should first consider the company business model, specifically the outbound licensing plans for software products. Consider (1) which products the company licenses for a fee to end users, (2) how significantly those license fees contribute to the company's bottom line, and (3) whether reducing those licensing revenues (a likely result of releasing products under GPL terms) will significantly impact the company business plan. If the company generates revenue primarily through consulting and other services, or the sale of hardware, and there are no future plans to generate revenues from licensing software, then you might not be averse to including GPL code in company products (and thus broadly licensing your IP on a royalty free basis), because a reduction in revenues might not be foreseeable. In fact, there may be situations where giving away software and associated IP in source code form might drive services revenues or sales of collateral company hardware or software products, resulting in an overall increase in revenues. On the other hand, if the company's revenues are generated by both services/consulting work and software licensing fees, the potential implications on licensing revenues of particular products should be considered, particularly those core products that account for high percentages of software licensing revenues. If company revenues are generated primarily by software license fees, you should carefully scrutinize each proposed instance of OS use to make sure that the significant revenues from licensing fees are not jeopardized.

Some Specific Scenarios—In drafting a company's OS policy, consider the range of potential scenarios that developers may bring to you. Obviously one of the most important scenarios is the one in which the developers ask to include OS code in a company product. But you will also want to consider whether or when (1) code should be released under an OS license, (2) staff should be allowed to participate in external "community" projects, and (3) the company will set up external community projects for its products, including taking back in community contributions.

Depending on business plans and licensing models, a company might decide to allow developers to include OS code into a particular company product. But, given the fact-specific nature of each inquiry, the

complexity of OS licenses, and the unsettled questions concerning what product architectures might require compliance with certain OS license provisions, a company should have a policy that requires [written] approval of each specific instance where OS code is incorporated in a company product. For example, depending on the terms of the OS license, it might make a difference if the employee (1) cuts and pastes the code into company product, (2) statically links to the code, or (3) dynamically links to the code. And remember that the developers might interpret an OS license quite differently from legal counsel. Overall then, it makes sense to have a policy that requires approval prior to any incorporation of OS code into a company product, with each specific request being reviewed by an appropriate legal or business decision maker (namely, one who has a solid understanding of the company's IP policy and its licensing plans).

The person(s) responsible for reviewing requests to incorporate OS code into a company product should be guided by a detailed policy document that (1) reflects the company's business plan and (2) spells out acceptable and unacceptable requests. For instance, a company might decide that its reliance on end user licensing mitigates against using any copyleft code, but that with appropriate review it may be comfortable with "pedigree" risks from non-copyleft code. Another company, while generally restricting incorporation of GPL licensed code, might allow incorporation of code licensed under the Common Public License (CPL) or Mozilla Public License (MPL) if certain product architecture requirements are met (e.g., files are segregated). In the end, a detailed policy document should reflect what each OS license means (when it comes into play, what it requires you to do, etc.), what products your company needs to continue licensing for a fee, as well as company policy with regard to potential pedigree issues that accompany OS code.

In addition to addressing OS code incorporation into company products, company policy should consider the internal use of OS products. There are a number of useful development tools released under OS licenses that company developers may want or need to use for developing company products. The vast majority of these tools are used only in the development process and are not incorporated into the shipping product.⁴ Company policy can either explain that tools may be used without limitation, provided they are not in whole or in part incorporated into a company product, or set out an approved list of tools that the

company has confirmed as not causing incorporation of code into the product under development.

The policy also should address whether and when staff may release company code under an OS license. Many developers may not understand the implications of releasing company code under an OS license. If the code includes valuable company IP, the company may lose a competitive advantage in the marketplace, since release under most OS licenses would result in the grant of broad licenses to use the IP. Again, the specific instances where a company might want to prohibit or allow the release of certain source code under an OS license will vary from company to company, but each instance should be reviewed by an appropriate legal or business decision maker.

Whether the company knows it or not, its developers are likely involved in “community” projects and activities. Community is a broad term used to refer to newsgroups, Sourceforge-like sites, and other areas where developers gather and collectively work on building code or solving more general problems. You should consider whether these activities expose the company to risks. For instance, the company should restrict developers who work on end user licensed products from involvement in community projects that relate to the same or similar functionality. Without such restrictions, a developer might end up contributing valuable trade secrets, copyrights, and/or patents to the community project, including the know-how and other IP that make the company’s product superior to similar OS products. Developers also might bring something back from the community and incorporate it into a company product. The OS policy should explain the risks of participating in community projects, whether or not on company time, and at a minimum require pre-approval for work on projects involving functionality similar to what the staff develops at the company.

A final area to consider in addressing OS concerns is whether or when the company will set up or sponsor community projects and what the company will do with the fruits of such projects. While a community project might seem like an obvious choice for one or more company products (to harness free developer resources), there are a number of risks and administrative burdens that should be considered. For instance, just as there are potential pedigree concerns with code downloaded from the Internet, there are similar concerns with code added in a community process. A company would want to know who its

contributors are, confirm that they have IP rights in the contribution sufficient to allow incorporation into the company product (the Free Software Foundation in fact does just this), and possibly have them assign in writing their rights in such contributions to ease future administrative burdens.

Education—and More Education

Once the company’s OS policy is formulated, it is essential to educate company staff on the issues or concerns that OS software can raise. You should consider tailoring this training to specific groups within the company. Developers, architects, managers, executives, and legal personnel all have different technical and legal backgrounds and would benefit from tailored training. Legal personnel might need education regarding technical concepts such as dynamic and static linking, or even the distinction between source and object code.

The tone of the training should be oriented so as to encourage a partnership between legal counsel and the developers, who might be inclined to resist what they see as legal meddling into the product development process. Explaining the conflict with the company’s licensing plan that might be created by incorporating OS code into company products is one important way to relay to developers the need to be alert to OS issues.

Finally, OS training is usually best done in person, with a format and time allotment that permits real-time Q&A. The Q&A helps ensure that the audience understands the message. It can also help the trainer in future training sessions. The materials may need to be revised or expanded to cover certain FAQs or intricate concepts.

Create a Mechanism for Developer Requests

OS policy likely will include areas where developers are required to seek pre-approval to incorporate OS code into a company product, to contribute to a community project, to release company code under an OS license, and/or to set up a community project. A mechanism should be created to ensure that these requests are resolved early in the development process. If OS code is introduced into the company code base without approval and not located until just prior to release, it could delay product shipment. It is easier to review and resolve these issues early in the product development cycle, well before shipment deadlines.

The request mechanism should route requests to the appropriate decision maker. Initially, consider centralizing the task of reviewing and responding to requests. Many companies find that during the initial period after implementing an OS policy, it may be advisable to consolidate authority for reviewing OS requests in a centralized group or committee, which can draw upon each successive determination and ensure that the requests are resolved in a manner consistent with the company's long-term goals.

Carefully Document OS Use

If a request to incorporate OS code into company products is approved, that use should be carefully documented. At a minimum, the developers must preserve copyright notices in the code and archive an e-copy of the OS license attached to the code. It is also helpful to have a system that connects all of this information together, including precisely tracking what code is subject to which OS license. Such a system will enable compliance with OS license terms, and if the product is part of an M&A transaction, the company will need to quickly inform the potential licensee or buyer about the product's OS dependencies. Also consider how to flag and comply with any obligations imposed by the OS license—for instance, the obligation to carry forward attribution or to provide source code.

Find the Experts

Although the majority of OS requests may be addressed by legal counsel, there will be questions that require outside legal and technical expertise. Frequently these complex questions relate to how alternative product architectures might bring certain license provisions into play. Given the high stakes of these decisions, technical and legal experts who routinely analyze these problems and can draw upon a wealth of past experiences should be consulted.

Tune-Up M&A Diligence

If there is any concern about what OS code the developers might put into a company product, the company should be equally concerned about OS code present in third party code that the company acquires or licenses. How can OS code be identified in a potential M&A target? Unfortunately, there is no magic tool. OS code is freely and widely available for download and there is nothing inherently distinct or different about the way OS code is written. Other than the copyright notices and references to license terms that

the original authors may have included in comments to program files (e.g., references to the GPL, MPL, or other copyleft licenses), there is no practical way to identify OS code incorporated into a larger work. Even the presence of copyright notices does not guarantee the presence or absence of OS code. The code's authors may not include copyright or license references in their source code files (after all, this is a convention and not a requirement of copyright law). Also, subsequent users of these files may have removed notices that the original authors included.

Consequently, the principal (and sometimes only) tool at your disposal is the due diligence process—in other words, the statements, representations, and warranties that a potential target will make to you about the presence or absence of OS code in its products. To make the most of due diligence, ask very specific questions. Make sure that the potential target has verified its responses with its code writing developers, rather than relying on generalized statements made by managers. The following questions provide a starting point:

Question #1: Do any of the potential target's products include code, modules, utilities, or libraries that are covered in whole or in part by a copyleft license (i.e., a license that requires, as a condition of use, modification, and/or distribution of such software and/or other software combined and/or distributed with such software that it be (1) disclosed or distributed in source code form, (2) licensed for the purpose of making derivative works, or (3) redistributable at no charge)? What specific code, modules, utilities, or libraries?

Question #2: If yes, does the potential target ship this product or does it run internally on the target's servers? Since what date has the target shipped this product? Has the potential target granted rights to (1) disclose or distribute this product in source code form, (2) make derivative works of the product, or (3) redistribute the product at no charge?

Question #3: Do any of the potential target's products include code, modules, utilities, or libraries that are covered in whole or in part by any non-copyleft license?

Question #4: Does the potential target have in place policies to ensure (1) that OS code is not incorporated into its products without management approval, and (2) that such incorporation is carefully documented? What are these policies? How does the target track

OS license obligations and ensure compliance with these obligations?

Audit before Release

As the company nears completion and release of its products, consider performing an OS audit to confirm the documented instances of OS use and gain some assurances that developers did not incorporate additional OS code without obtaining an approval. If good records have been kept of the instances where OS incorporation was approved, then the first part of the audit will be straightforward. Also reconfirm that there is a plan in place to comply with OS license obligations, such as attribution or source code distribution requirements.

Finally, additional steps should be taken to ensure that the company's records reflect all instances of OS incorporation into the product. This typically involves meeting with the development team to confirm that each member of the team followed the company OS policy. Additionally, although there is currently no technology that can find all instances of OS code in a code base, basic scans can be performed on file head-

ers and comments and searches made for copyright strings to catch the most obvious errors.

Endnotes

1. Stephen Mutkoski, Intellectual Property and Licensing Group, Microsoft Corporation in Redmond, Washington, may be reached at STEPHEM@MICROSOFT.COM. This article is copyrighted by Microsoft.
2. General familiarity with OS licensing issues and the common OS licenses such as the GNU General Public License (GPL), Lesser General Public License (LGPL), Mozilla Public License (MPL) and the Berkeley Software Distribution License (BSD) is assumed.
3. "Copyleft says that anyone who redistributes the software, with or without changes, must pass along the freedom to further copy and change it... [A Copyleft license] gives everyone the rights to use, modify, and redistribute the program's code or any program derived from it but only if the distribution terms are unchanged.... Copyleft is a general concept; there are many ways to fill in the details." See WWW.GNU.ORG/LICENSES/LICENSES.HTML#WHATISCOPYLEFT.
4. A tool called Bison is one exception. See WWW.GNU.ORG/LICENSES/GPL-FAQ.HTML.

Data Privacy and Personal Information Protection in Mexico

By: Luis Vera Vallejo, Mexico City, Mexico¹

Since the enactment of the Federal Constitution in 1917, post-revolution administrations have shown no particular interest in implementing either formal or comprehensive legislation and policies regarding the protection of personal privacy. This situation has partially changed with the advent of the administration of President Fox. Bills governing the access and protection of personal data in credit bureaus and public government files were introduced and passed by the Federal Congress.

This article describes the current legal framework of the data privacy provisions that have been enacted in an array of federal legislation. As will be noted, the principal federal legislation, which is embodied in recent amendments to the Federal Consumer Protection Act, focuses on consumer protection, both online and off-line. Our conclusion is that, in the globalized world, companies in Mexico, and in particular U.S. subsidiaries, should implement corporate data privacy policies and procedures in order to comply with U.S., foreign, and local laws and regulations.

Current Privacy Legislation

1. **Constitutional Provisions**—The bill of rights guarantees the privacy of private communications, including PTT (post, telegraph, and telephone) communications. Likewise, the Constitution also mandates due process of law regarding search and seizure procedures.

2. **PTT's Confidentiality-Related Provisions**—The Federal Communications Act establishes in Articles 383, 576, 577, and 578 that government and private officers must keep in strict confidentiality the content of any messages, except by order of competent court. Severe fines and imprisonment can be imposed on infractors. Article 49 of the Federal Telecommunications Act establishes that any information transmitted through telecommunication networks shall be confidential, except for information in the public domain or as ordered by competent authorities.

3. **Statistical/Census Information**—Under Article 5 of the law governing Geographical and Statistical Information (the Census Act), all statistical information

collected, as well as the informants' data, must be kept in strict confidentiality.

4. **Federal Tax Records**—Per Article 69 of the Federal Tax Code, all employees and officers of the Mexican IRS (SAT) must keep in strict confidence all data concerning tax returns, tax payments, tax audits, etc. Violators may be fined from US\$4,500 to US\$6,000 per violation.

5. **Federal Government Procedures Act**—Under Article 33, petitioners or any interested party in any governmental matter shall have the right to be informed about the content of related and pertinent files, which otherwise must be kept confidential. However, any information regarding national defense and security, or protected by industrial or trade secret or by any other law, also must be kept confidential.

6. **Banking Secrecy**—The Credit Institutions Act, Article 117, establishes "Bank Secrecy," under which financial institutions cannot disclose any information related to the deposits or other banking activities of their customers to any person, except to the tax authorities or by judicial resolution issued by competent court. Violators shall be punished by imprisonment from 3 to 9 years, per the provision of Article 112 Bis of the Act.

7. **Insurance and Medical Records**—Per Articles 136, 137, and 138 of the General Health Act, all medical information and clinical records must be kept in strict confidentiality and must not be disclosed without the patient's authorization, except in cases when doctors and hospitals have an obligation to report to the Health Authorities. (The same obligation is established in Article 36 of the law governing Professional Practice.)

8. **Foreign Investment Law and its Regulations**—All information that must be disclosed by foreign investors to the government must be kept confidential. The authorities shall not allow any third-party access to the files and records in the Foreign Investment Office or in the Registry of Foreign Investment.

9. **Copyright Law**—The confidentiality of software

products and databases is protected. Copyright Office files regarding software products must be kept confidential and access to such files is not permitted, except by the copyright holder. Severe fines may be imposed by the Institute of Industrial Property.

10. **Industrial Property Law**—Under this law, disclosure of trade secrets or unlawful access to such information by third parties is a crime sanctioned with imprisonment for up to 10 years.

11. **Moral Damage: Civil Remedies**—When collecting, disclosing, transferring, marketing, publishing, disseminating, or using personal data, and in particular “Sensitive Data,” one person may suffer or be affected in his feelings, affections, beliefs, honor, reputation, private life, etc. Such damages are protected by Article 1916 of the Federal Civil Code, which grants a civil action allowing the affected party to claim payment of damages, whether contractual or in tort. The amount of the damages shall be determined by the judiciary, depending upon the injury caused, the degree of the liability, or other related circumstances.

12. **Federal Criminal Code**

Post and Communications

- Anyone who deciphers or decodes telecommunications signals, or is engaged in the marketing or use of apparatuses, devices, or instruments permitting such activities, shall be punished by imprisonment up to 2 years (Article 168-Bis of the Code).
- Anyone who opens or intercepts any written communication without a reason sanctioned by law shall be punished with up to 380 days of community service.
- Anyone who trespasses or obtains undue access to private communications without proper judicial authorization shall be punished with up to 12 years of imprisonment.

Child Pornography

- Child pornography, including transmission by e-means such as the Internet, is punishable with up to 16 years of imprisonment.

Trade Secret Disclosure; Unlawful Access

- Disclosure of confidential information learned as a consequence of an employment or labor relationship shall be punished with up to 200 days of community service.

- In the event of disclosure by a person rendering professional or technical services, or in the event that the nature of the information disclosed is a confidential trade secret, the punishment will be imprisonment of up to 5 years.
- Access to, or disclosure or use of, information or images obtained from a private communication shall be punished with imprisonment up to 12 years.
- Anyone who accesses or copies information contained in data processing equipment or systems shall be imprisoned for up to 1 year.

13. **Workplace Environment**—The Federal Labor Law was enacted in 1931. Since enactment, labor courts have resolved claims in a manner most favorable to employees. Legislation provides that an employer must respect the dignity of its employees’ workplace labor conditions (Articles 3 and 56). This principle cannot be waived by the employees; any pact to the contrary shall be considered null and void. Under Article 133–VII, employers are forbidden to perform any act that restrains the labor rights of the employees.

These Labor Law provisions must be considered when implementing any employment data privacy or surveillance procedures at the workplace, including accessing and searching electronic and computer technology to collect, analyze, reproduce, and disseminate information about employees. Likewise, it is important to note that any such workplace practices—including monitoring e-mails or intranets—should be clearly specified in both the employment agreement and the interior working regulations. A written employee consent to any company policy must be obtained.

The Personal Data Protection Bill

The Bill was initiated on 31 January 2001 at the Senate House and sponsored by Senator Antonio Garcia Torres. It was inspired by and adapted from the European Union Directive on Data Privacy, and more particularly on the Spanish law derived from the EU Directive. The Bill’s aim is the protection of personal data collected, gathered, or stored in databases, whether owned, managed, or controlled by individuals and/or corporations.

Sensitive Data—In the event of “Sensitive Data,” prior written permission from the interested party

must be obtained. No one is obligated to disclose “Sensitive Personal Data” unless the interested party has granted his or her prior written consent. The creation of files, registries, or databases that might reveal Sensitive Data is forbidden.

Personal Data—The collection and electronic data processing of personal data also requires the prior written consent of the interested party (opt-in). However, prior consent does not apply to personal data derived from a commercial, labor, or contractual relationship.

Databases—Those who service or have databases must ensure that they have implemented the technology required to assure the integrity and security of the information contained therein. The information can only be assigned or transferred to a third party with a legitimate interest, and only with the prior authorization of the affected party, which at the same time must be informed about the identity of the entity to which the information will be transferred, as well as the purpose for such transfer.

As in the EU Directive, the Bill prohibits the data flow transfer of personal data from Mexico to foreign countries or international organizations that do not grant the same level of security and protection as granted by the Mexican government. The Bill contains an exception concerning the transfer of data as agreed in any international treaty in effect to which Mexico is a signatory. It is uncertain if this exception applies to the NAFTA treaty. However, there are no specific provisions in NAFTA regarding the transfer of personal data; NAFTA only requires freedom of telecommunications between the three countries (Mexico, Canada, and the United States). Therefore, one may conclude that if the Bill is passed Mexican organizations may be forbidden to transfer data to the United States. The Bill thus would adversely affect Mexican-based subsidiaries of U.S. companies, which would be forbidden to transmit personal data concerning their employees and commercial interests to their U.S. parent companies.

Habeas Data Rights—The Bill grants several habeas data rights: (1) to access, (2) to be informed, (3) to oppose data collection, (4) to oppose the disclosure, transfer, or dissemination of personal information, and (5) to correct and update.

Individuals or corporations that have or maintain databases must be registered with a new government agency, the Federal Institute for the Protection of Per-

sonal Data. The Institute is empowered to perform all legal actions to ensure compliance to provisions of the Bill. The opt-in concept is emphasized in several provisions of the Bill. Sanctions may include fines and the faculty to shut down archives, records, files, or data banks. Individuals or any interested party may institute several actions before district courts in order to obtain enforcement or redress.

In summary, if the Bill is passed, it undoubtedly will adversely affect the business operations of Mexican companies and in particular Mexican subsidiaries of U.S. companies, because its proposed provisions include:

- The obligation to report and register with the government the existence of any database or data bank under which the company collects, gathers, or stores personal data of any kind.
- The opt-in concept.
- Prohibition of data flow transfer from Mexico to the USA.
- Prohibition on collection of Sensitive Data, with certain exceptions, but in every case with the prior written consent of the individual.
- The risk of sanctions by the Institute, including shutting down data banks.
- Exposure to legal liabilities in the event federal civil actions are claimed by any affected party.

Despite a strong lobbying campaign by the Mexican Alliance for the Defense of Privacy and Information Freedom, the Bill was stopped at the House of Representatives and is now dormant. If this Bill passes, it may produce an adverse impact on the businesses and operations of all companies collecting and marketing personal data, and will restrain the trans-border data flow of information from Mexico to the USA.

New Data Privacy Legislation

As noted, only recently has specific data privacy legislation been proposed by the Executive Branch and/or sponsored by Congress. Congress has approved the (1) Credit Bureaus Act, (2) Federal Law for the Access to the Governmental Public Records and Information, and (3) Federal Consumer Protection Act. The first two acts were approved in 2002; the third in 2004.

The Credit Bureaus Act—This law permits consumers or users of the banking system and credit applicants to obtain access to their own credit records, and also to request and/or to claim corrections and information updates, including the elimination of personal data from credit bureau databases when applicable, as provided by the Act.

Access to Governmental Public Records and Information—This law, published on 11 June 2002, was widely advertised by the Presidency as an outstanding achievement of the promised new democracy. Under this law, citizens are entitled to, and government officers are obligated to permit, access to federal government agencies' records and files. Citizens are also entitled to access other data, such as government services. This information may be accessed by e-means, such as the Internet. However, information that is considered reserved, classified, or that affects the national security or the national defense shall remain confidential (Article 13).

Government officers are obligated to keep confidential citizens' personal data contained in public records. Citizens are entitled to access their own information and to request correction, modification, and updating of their personal data. Government officers are forbidden to disclose, distribute, disseminate, or market a citizen's personal data, either online or off-line, without the citizen's express written consent, with certain exceptions, including when such disclosure is decreed by resolution of competent courts.

A new governmental body, the Federal Institute for Access to Public Information, was created to handle and ensure the proper compliance with the provisions of this law and to grant remedies and impose sanctions in the event of violation of its provisions.

Federal Consumer Protection Act—The Act, as amended on 4 February 2004, includes consumer protections in online transactions, which were introduced into this law in 2000.

The 2000 Online Protections

- The vendor is obligated to keep confidential the information provided by the consumer, and such information cannot be disclosed, transferred, or disseminated to other vendors, unless previous authorization was granted by the consumer.
 - The vendor must inform the consumer of the technology used to ensure the safety and confidentiality of the information provided by the consumer.
 - Before any transaction is concluded, the vendor must inform the consumer of its physical domicile, telephone numbers, its warranty policies, and how to seek warranty protection.
 - Vendor shall avoid deceptive marketing and advertising practices.
 - Whenever products or services are addressed to the elderly, children, or the ill, disclosure requirements are more onerous.
- The 2004 Amendment*—The law now emphasizes consumer protections in both online and off-line transactions.
- The concept of "consumer" is modified to include corporations, as well as individuals, wherever a transaction does not exceed US\$30,000. Accordingly, corporations that execute vendor transactions not exceeding US\$30,000 are entitled to file complaints before the Federal Consumers Protection Agency (FCPA).
 - The FCPA is also entitled to monitor websites in order to verify proper fulfillment of the provisions of this law.
 - Vendors and companies that collect, gather, and use consumer information are obligated to report to any person what information they keep and to provide a report on such information, including whether it has been shared with any third party and, if so, identifying the third party. Consumers have the right to request corrections if appropriate, and vendors or the third party must comply with such petition within 30 days.
 - All advertising sent to consumers, whether online or off-line, must indicate the name, address, telephone number, and e-mail of the vendor. Consumers are entitled to request to not be sent, whether in their domiciles or workplaces, e-mails with advertising (spam).
 - Consumers may request that vendors and advertising companies not transfer or assign their information to any third party.
 - The FCPA shall keep a public registry listing the names of the consumers who have elected not to receive information or advertising materials, both

off-line and online. Prior to sending any marketing or advertising messages, vendors must consult the list of consumers who have requested not to receive spam.

- Any contract shall be considered as concluded five days after delivery of the merchandise or the execution of the agreement, whichever is later. During this five-day period, the consumer is entitled to revoke its consent without any liability.
- Vendors engaged in repair or maintenance must use “new spare parts” unless prior written authorization of the consumer has been given.
- To be valid, standard agreements (adhesion contracts), whether online or off-line, must be written in the Spanish language, in a clear and conspicuous manner.
- The FCPA is entitled to declare which standard agreements must be registered and approved by it. Article 90 establishes that certain contractual provisions cannot be included, such as jurisdictional submission to foreign courts. The forbidden clauses shall be null and void.

Remedies—Consumers have the right, at their choice, to replacement of merchandise or refund of the price paid, if the goods or services do not meet with the quantity or quality requested, the trademark, or any other specifications of the products, or, in the case of services, if the equipment is not properly repaired. In such cases, consumers also are entitled to compensation in an amount not less than the equivalent of 20 percent of the price paid, regardless of the following additional statutory damages: if the consumer has paid the price in full, he is entitled to collect 30 percent of the price; if he has paid more than 50 percent, he may collect 25 percent of the price; and payment of up to 50 percent of the price entitles the consumer to compensation equivalent to 20 percent of the contractual obligation. In any other case, compensation will be no less than 20 percent of the total amount established in the contract. In addition, and depending upon the violation, the FCPA will impose very steep fines on the vendor. The fines have been increased to an average ranging from US\$50,000 to \$500,000. The FCPA is also empowered to shut down the vendor’s premises.

Corporate Data Privacy Practices

Although the Department of Commerce is trying to encourage industry chambers and trade associations to formalize ethics codes and to promote self-regulations, such codes and regulations have not been successfully implemented. Accordingly, very few industry organizations have ethics codes. This may be because there is no formal law governing data privacy in the private sector.²

Due to the global nature of Internet, several multinational U.S. subsidiaries based in Mexico have implemented their own ethics codes and data privacy procedures, in order to comply with parent global policies. At this time, it is difficult to ascertain whether or not the Personal Data Protection Bill will be revived; nonetheless, industry needs to be prepared to comply with data privacy policies and procedures. In any case, since the impact of privacy is now a part of the corporate culture, particularly in U.S. multinational companies, local subsidiaries need to know how to avoid privacy risks and legal exposures. It is highly recommended that procedures be adopted to address:³

- website privacy policies (and the extensive internal due diligence and procedures necessary to implement them);
- online information collection, use, and dissemination practices;
- cookies and other tracking technologies;
- online profiling;
- third-party databases and publicly available personal information;
- privacy issues associated with digital signatures, smart cards, and other key technologies;
- crossing virtual borders in transmitting data;
- collecting and using certain types of sensitive information (e.g., financial, medical, from children);
- privacy and data protection issues in the e-workplace; and
- new laws and pending legislation on privacy at both the federal and state level.

Conclusions and Recommendations

Mexico has enacted and put in force a variety of federal data privacy statutes. The most important ones for the private sector are those related to data privacy policies and procedures in the workplace environment and the newly enacted Federal Consumer Protection Act. Other statutes might also apply, in particular provisions regarding access to telecommunications facilities, labor, and criminal legislation. When implementing international corporate policies, the local subsidiary should take care as to how to implement such policies in order to adapt them to the Mexican environment and current legislation.

Endnotes

1. Luis Vera Vallejo is with Vera Abogados S.C. in Mexico City. He may be reached by telephone at 52 5 5271-6731, or at LVERA@VERAABOGADOS.COM.MX.
2. As discussed, Senator Garcia Torres' Personal Data Protection Bill is still dormant at the House of Representatives in the Congress.
3. See Ruth Hill Bro, *E-Privacy Law Committee Targets the E-Commerce Legal Issues Facing Every Client*, ABA E-Privacy Law Committee.

United States Law Updates

SIXTH

CIRCUIT

REGION

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

COPYRIGHT OWNER HOLDS EXCLUSIVE DIGITAL SAMPLING RIGHT

Bridgeport Music, Inc. v. Dimension Films, 383 F.3d 390 (6th Cir. 2004)

► Copyright

Without authorization, Dimension Films digitally “sampled” a song (over which Bridgeport Music held copyrights) in another song that Dimension Films included in a soundtrack to one of its films. Confronted with these facts, the Sixth Circuit held that those who own copyrights in sound recordings hold the exclusive right to “sample” the recordings under §114(b) of the Copyright Act. The court’s conclusion was based on its reading of 17 USC §114(b), which, with added emphasis, states:

[T]he exclusive right of the owner of copyright in a sound recording [to prepare derivative works based upon the copyrighted work]

is limited to the right to prepare a derivative work in which the actual sounds fixed in the sound recording are rearranged, remixed, or otherwise altered in sequence or quality....

Under this provision, the owner of a copyright in a sound recording “has the exclusive right to ‘sample’ his own recording.” There is no need for the copyright owner to establish substantial similarity and there is no *de minimis* copying defense with respect to sound recordings. The court concluded that anyone wanting to use a sample should obtain a license thereto. This decision appears to conflict with the Ninth Circuit’s ruling in *Newton d/b/a Janew Music v. Diamond*, 349 F.3d 59, 68 USPQ2d 1740 (9th Cir. 2003).

TWO-PART “SUBSTANTIAL SIMILARITY” TEST DETERMINES COPYRIGHT CASE

Stromback v. New Line Cinema, 384 F.3d 283 (6th Cir. 2004)

► Copyright

Stromback alleged that New Line Cinema’s *Little Nicky* motion picture infringed his original screenplay. In analyzing the case, the Sixth Circuit noted that a plaintiff may establish an infringement by showing (1) access to the plaintiff’s work, and (2) a substantial similarity between the two works at issue. In considering the “substantial similarity” factor, the district court had applied an “ordinary observer” test—that is, a test whereby the trier-of-fact may “gauge his ‘net impression’ of the two works by conducting a side-by-side

comparison without the benefit of expert testimony.” However, the Sixth Circuit rejected this approach in favor of the two-part test it adopted in *Kohus v. Mario*, 328 F.3d 848 (6th Cir. 2003). The first part requires identifying which elements of a creator’s work are protectible by copyright; the second part requires determining whether the allegedly infringing work is “substantially similar” to protectible parts of the creator’s work. Applying the test, the court of appeals affirmed the lower court’s summary judgment of non-infringement in favor of the producers of *Little Nicky*.

By: George Spatz,
Gordon & Glickson, Chicago, Illinois

SEVENTH

CIRCUIT

REGION

DILUTION EVIDENCE SUFFICIENT IN TRADEMARK DILUTION CLAIM

Nike, Inc. v. Circle Group Internet, Inc., 318 F.Supp.2d 688 (N.D. Ill. 2004)

► Trademark Dilution

In *Moseley v. V Secret Catalogue, Inc.*, 537 U.S. 418 (2003), the Supreme Court held that to establish trademark dilution under the Lanham Act proof of “actual dilution” is necessary. However, the Court noted that “direct evidence of dilution such as consumer surveys will not be necessary if actual dilution can reliably be proved through circumstantial evidence—the obvious case is one where the junior and senior marks are identical.” Since the Supreme Court’s proclamation, lower courts have split on whether, under *Moseley*, an identity between competing marks is sufficient circumstantial evidence to establish dilution or whether proof of actual dilution by other circumstantial evidence is required to establish dilution where the competing marks are identical.

In *Nike*, Circle Group Internet moved for summary judgment on Nike’s dilution claim, arguing that its

registration and use of the domain name JUSTDOIT.NET did not dilute Nike’s admittedly famous Just Do It trademark. The District Court for the Northern District of Illinois, denying CGI’s motion, declined to resolve whether, under *Moseley*, an identity between competing marks is sufficient to establish dilution. According to the court, there was no need to resolve such question because there was sufficient other circumstantial evidence of dilution to support a denial of summary judgment. Thus, the court found that in addition to an identity of the marks, CGI’s concession that the JUSTDOIT.NET domain name had “become recognized as having some relation to CGI by its employees and customers,” and the testimony of CGI’s CEO that “I have got to believe that at some point somebody said . . . ‘Oh, like Nike,’” was sufficient circumstantial evidence of dilution to create an issue of fact.

By: Matthew T. Furton,
Lord Bissell & Brook LLP, Chicago, Illinois

SEVENTH

CIRCUIT

REGION

OSS IN COMMERCIAL SOFTWARE NO IMPAIRMENT TO IP RIGHTS

Computer Associates International v. Quest Software, Inc., 333 F. Supp.2d 688 (N.D. Ill. 2004)

► Copyright

Computer Associates sued several of its former employees and their new employer, claiming the former employees developed software for their new employer that violated CA’s intellectual property rights. The case is one of very few decisions from U.S. courts evaluating the consequence of using open source software (OSS) in the development of a proprietary commercial software product.

In 1996, CA’s predecessor released database administration software called Enterprise Database Administrator (EDBA). Three years later, CA’s pre-

decessor was in the process of developing a version of EDBA for use with IBM’s DB2 database when several programmers and programming management personnel left and accepted jobs with Quest Software. Quest assigned these former CA employees to work on a project to develop database administration software for use with DB2. In 2000, Quest released Quest Central for DB2 (QCDB2), which became one of four major competitive products in the market for DB2 administration software. In 2002, CA received an unsigned letter detailing specific uses of CA-developed source code by Quest and various computer pro-

grammers working for Quest on the development of QCDB2. CA sued Quest and the former CA employees that were then working at Quest, alleging copyright infringement and trade secret misappropriation.

CA sought to enjoin the distribution of QCDB2 after forensic discovery revealed that Quest programming personnel repeatedly accessed the EDDBA source code during the development of QCDB2 and that a large number of lines in the QCDB2 source code were identical to the EDDBA source code. Quest defended its conduct, in part on the fact that EDDBA contained hundreds or thousands of lines of publicly available source code. EDDBA contained code created from Bison, a program distributed by the Free Software Foundation under the GNU General Public License. Quest argued that CA was violating the GPL by attempting to claim a copy-

right in a program that contained Bison source code.

The court rejected Quest's argument because the particular version of the GPL included a provision specifically permitting the use of a Bison output file without any of the restrictions of the GPL. Therefore, the fact that 4 to 4.5 percent of the EDDBA source code was third-party material that could not be copyrighted did not impair the ability of CA to enforce its copyright in the work as a whole.

This case reveals the growing importance of open source licensing terms for commercially developed software. In this particular instance, the inclusion of open source material in an otherwise proprietary software product did not prevent a software company from enforcing its intellectual property rights in the product.

TENTH
CIRCUIT
REGION

By: Robert D. Traver,
Sheridan Ross, P.C., Denver, Colorado

“GRAY MARKET” WEB SALE VIOLATED LANHAM ACT

Bayer HealthCare, L.L.C. v. Nagrom, Inc., 2004 WL 2216491, 2004 U.S. Dist LEXIS 19454 (D. Kan. 2004)

► Trademarks

A U.S. subsidiary of Bayer brought a trademark infringement and unfair competition suit against Nagrom to enjoin the sale by Nagrom in the United States of Bayer's foreign manufactured Advantage flea control preparations. Nagrom marketed and sold in the United States Bayer's animal flea control preparations that were packaged exclusively for sale and use in the U.K. and Ireland. (Bayer tailors the manufacture of its products to suit the requirements and laws of specific countries.) The U.K. products sold by Nagrom in the United States were not properly labeled for U.S. sale and had not been properly registered with the Environmental Protection Agency or under the Kansas Agricultural Chemical Act. Before intervention by the federal or state governments based on the sale of unregistered and misbranded pesticides, Bayer sued Nagrom under the Lanham Act and the laws of Kansas, alleging trademark infringement and consumer confusion as to the source, nature, or approval of the Advantage products.

Nagrom used three websites to advertise and sell the U.K. Advantage product in the United States, used Advantage in the titles of the websites, depicted the packaging of the Bayer products on the websites, used the Advantage mark in metatags for the three sites, and paid at least one Internet search engine to secure highly prominent placement for one of Nagrom's websites following Internet searches for Advantage products.

The court noted that Bayer's incontestable federal trademark registration for the Advantage mark in the United States conclusively established the validity and ownership of the mark. The court also pointed out that the sale of gray market products in the United States is likely to result in consumer confusion if the gray market products differ materially from authorized products. The court found relevant differences between Bayer's authorized U.S. products and the U.K. products marketed and sold by Nagrom, including the lack of federal and state registrations for the U.K. products, and the fact that Nagrom's

products were distributed through a website as opposed to Bayer's authorized U.S. products, which are sold through, and supervised by, veterinarians in the States. Additionally, the court found Nagrom's use of Bayer's mark in website metatags likely to create initial interest confusion. Based on these findings, the court held that Nagrom's unauthorized use of Bayer's Advantage mark constituted trademark infringement

and unfair competition, and issued a permanent injunction against Nagrom from using the mark or selling Advantage products in the United States.

This case demonstrates the successful use of federal and state trademark and unfair competition laws to stop the unauthorized sale over the Internet of "gray market" goods.

International Law Updates

CANADA

By: Charles Morgan, McCarthy Tétrault LLP,
Montréal, Québec

RADIO STATION'S LICENSE NOT RENEWED: FREEDOM OF EXPRESSION IMPLICATIONS

The Canadian Radio-Television and Telecommunications Commission (CRTC) rendered Broadcasting Decision CRTC 2004-271 (13 July 2004) to not renew the broadcasting license held by Genex Communications Inc. for the French-language commercial radio station CHOI-FM Québec. The CRTC decision followed Genex's application for renewal of the broadcasting license, which was set to expire on 31 August 2004. In Canada, broadcasting licenses are typically granted for seven-year terms. Where licensees fail to meet the terms and conditions of their licenses, the CRTC might accord only a short-term, two-year "administrative" renewal by way of sanction. The CRTC's decision not to renew the license, due to violations of content-related licensing conditions, is a first in Canada.

CHOI-FM has had a long history of controversial radio programming; various hosted talk-shows are deliberately polemic and, in some cases, offensive, following the "shock jock" model. Following a public hearing in 2002, the CRTC had issued a short-term license renewal for CHOI-FM (Broadcasting Decision CRTC 2002-189 (16 July 2002)). CHOI-FM's license was renewed for only two years, due to its repeated failure to comply with broadcasting regulations regarding, among other things, abusive comments, the submission of logger tapes, the broadcast of French-language vocal music, and the condition of its license related to sex-role portrayal. The CRTC also noted the licensee's failure to meet the objective that programming be of high standard, as set out in §3 of the Broadcasting Act.

These findings were based, notably, on the CRTC's analysis of 47 complaints it had received since Genex acquired CHOI-FM in February 1997. These complaints concerned the broadcast of abusive comments, offensive on-air contests, personal attacks, and harassment on a daily program aired during peak morning hours. The decision noted that CRTC had given Genex numerous warnings of the possible consequences of its actions (including the administrative

renewal and numerous explicit warnings to the effect that continued breach of the station's licensing conditions might result in non-renewal). Nevertheless, the station continued to air programming that violated both industry and CRTC-imposed norms of acceptable content.

Ultimately, in view of the licensee's perceived inflexible behavior, its lack of acceptance of its responsibilities, and the lack of any demonstrated commitment to rectify the situation, the CRTC concluded that Genex would not comply with the Broadcasting Act, the Regulations, and its Code of Ethics if its license were renewed. The CRTC also concluded that the measures available to it, such as another short-term renewal, the issuance of a mandatory order, or license suspension, would not be effective in overcoming the problems. Consequently, the CRTC denied the application for renewal of the license and ordered CHOI-FM Québec to cease broadcasting by 31 August 2004.

The decision raises important issues related to the limits of freedom of expression. The CRTC found that the freedom of expression of broadcasters is counterbalanced by the right of listeners to programming that complies with the Broadcasting Act and associated regulatory requirements. In the CRTC's view, remarks that are abusive and that risk exposing an individual or a group to contempt or hatred contravene the objectives of the broadcasting policy for Canada set out in §3(1) of the Broadcasting Act. Those objectives are reinforced by §§15 and 27 of the Canadian Charter of Rights and Freedoms. According to the CRTC:

The regulation prohibiting abusive comment that tends or is likely to expose a person or a group to hatred or contempt is necessary not only to avoid harm to the persons targeted, but also to ensure that Canadian values are respected for all Canadians. The broadcast of remarks that could expose individuals or

groups to hatred or contempt can attract individuals to its cause and in the process create serious discord between various groups in Canadian society to the detriment of all of Canadian society. This harm undermines the cultural, political and social fabric of Canada which the Canadian broadcasting system is expressly meant to safeguard, enrich and strengthen. It also undermines the multicultural and multiracial nature of Canadian society, which the programming of the Canadian broadcasting system should reflect. Protection from the harms of abusive comment is for the benefit of all Canadians.

The CRTC concluded that the broadcast of abusive comments that could expose a person, group, or class

of persons to hatred or contempt based on race, religion, color, ethnic origin, sex, mental disability, or other grounds referred to in §3(b) of the Regulations is incompatible with the standards and values of the Canadian broadcasting system and the values in the Charter. The purpose of §3(b) is to prevent the real harms that such remarks can cause, harms that undermine the objectives of the broadcasting policy set out in the Act, and that have been recognized by the courts.

The licensee is widely expected to seek leave to appeal the decision to the Federal Court on the grounds, among other things, that the CRTC's decision erred in law by imposing unacceptable restrictions on the right of freedom of expression. The decision is at www.crtc.gc.ca/ARCHIVE/ENG/DECISIONS/2004/DB2004-271.HTM.

By: Olga Georgiades Van der Pol,
Lellos P. Demetriades Law Office, Nicosia

CYPRUS

RECENT COPYRIGHT DEVELOPMENTS

The Copyright and Neighbouring Rights Law of 1976 to 2004 is the applicable legislation regarding copyright (Law No. 59/1976 as amended by Law No. 18(I)/1993, 54(I)/1999, 12(I)/2001, 128(I)/2002 and 128(I)/2004). The Copyright and Neighbouring Rights (Amending) Law of 2004 (O.J. L 167, 22/06/2001 pp. 10-19), was adopted to harmonize Cypriot legislation with Directive 2001/29/EC of the EP and of the Council on the harmonization of certain aspects of copyright and related rights in the information society.

Software Protection—The 2004 amendment to the Copyright Law provides for the protection of copyrighted works, including software, by “technological measures,” that is, any technology, device, or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works capable of protection, which are not authorized by the rightholder of any copyright or neighboring right. According to the new provisions, a technological measure is deemed to be effective where the use of the software is controlled by the rightholder through the application of an access control or protection process, such as encryption, scrambling, or other transformation of the software or a copy control mechanism that achieves the protection objective.

These provisions apply where the technological measures are used for the effective limitation of acts that are not authorized by the rightholder as an author, without preventing the proper operation of the elec-

tronic equipment and its technological development. These provisions do not, however, prohibit the use of methods or the carrying out of activities that have a commercial purpose or that are used for purposes other than for the circumvention of the technological protection. Encryption research is not prohibited.

New §14B of the Law makes it an offense for a person who knowingly—or has reasonable grounds to know that he is pursuing that objective—and without the authorization of the rightholder, manufactures, imports, distributes, sells, rents, advertises for sale or rental, or possesses for commercial purposes devices, products, or components, or provides services that:

- (1) are the subject matter of promotion, advertisement, or marketing for the purpose of circumvention of technological measures of protection, or
- (2) have only a limited commercially significant purpose or use other than to circumvent the protection, or
- (3) are primarily designed, produced, adapted, or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures.

Such person will, on conviction, be liable to a fine up to £30,000, or to imprisonment for up to 3 years, or both. A second or any subsequent conviction may result in a fine of up to £35,000, or to imprisonment for a term of up to 3 years, or both.

COMPUTER-RELATED CRIME DEVELOPMENTS

Significant progress has been made in the effort to combat computer-related crime and piracy. This was largely due to the government's commitments to harmonize its legislation with the *acquis communautaire* in view of its accession to the EU. One of the most important developments has been the introduction of an amendment to the Copyright and Neighbouring Rights Law (cited above). In an effort to combat copyright infringement, the legal protection afforded in relation to reproductions has expanded and new provisions have been inserted for interactive on-demand broadcasting and rights-management information. There has also been a substantial increase in the fines and imprisonment terms imposed on copyright infringers.

Other important developments included enactment of the Law Ratifying the Cybercrime Convention of 2001 (Law No. 22(III), 30 April 2004), and of the Law Ratifying the Additional Protocol to the Cybercrime Convention concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (Law No. 26(III)/2004).

Cybercrime Convention—The Law of 2004 Ratifying the Cybercrime Convention of 2001 establishes certain criminal offenses in accordance with Chapter II of the Cybercrime Convention (Council of Europe, Budapest, 23.11.2001) in relation to confidentiality, integrity, and availability of computer data and systems. The Convention is applied in combination with other laws of the Republic—in particular, the Law on the International Cooperation in Criminal Matters of 2001 (No. 23(I)/2001) and the Law relating to the Concealment of Investigation and the Confiscation of

the Proceeds from Crime (No. 61(I)/1996, as amended by Law No. 25(I)/1997, 41(I)/1998, 120(I)/1999, 151(I)/2000 and 118(I)/2003). In addition, §15 of the Procedural Law provides that the provisions of Part II of the Criminal Procedure Law (Cap. 155 as amended by Law No. 93/1972, 2/1975, 12/1974, 41/1978, 162/1989, 142/1991, 9/1992, 10I(I)/1996, 89(I)/1997, 54(I)/1998, 96(I)/1998 and 14(I)/2001) also apply by virtue of Chapter II of the Convention.

Section 16 extends the jurisdiction of the courts and provides that, in accordance with the provisions of the Criminal Law, the courts of the Republic shall have jurisdiction over offenses committed in contravention of the provisions of the Convention in any of the cases referred to in Article 22 of the Convention. Accordingly, jurisdiction is granted when the offense is committed within the Republic, on board a ship flying the flag of the Republic, on board an aircraft registered under the laws of Cyprus, or where a Cypriot national commits the offense. In addition, by virtue of §17, the Convention establishes a legal basis for the extradition of fugitives who have committed offenses covered by the Convention where there is no other convention between the Republic and a state requesting extradition.

Additional Protocol—The Law Ratifying the Additional Protocol to the Cybercrime Convention Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems applies in combination with the Law of 2004 Ratifying the Cybercrime Convention of 2001. It establishes certain criminal offenses regarding the dissemination of racist and xenophobic motivated threats and material through computer systems.

By: Milan Chromecek and David Taylor,
Lovells, Paris

CZECHOSLOVAKIA

NEW RULES FOR CYBERSQUATTERS

A new system of alternative dispute resolution was introduced by the Czech NIC as of 1 August 2004. Under the new rules it is possible for a third party to file an action concerning a disputed domain name with the Arbitration Court of the Economic Chamber of the Czech Republic, even if the domain name owner does not agree. Previously, arbitration could be commenced only when there was mutual agreement between both parties (a fairly unlikely scenario where cybersquatters were concerned). Consent to the new rules must

be given by all new registrations, but also before the renewal of existing domain names, meaning that the rules gradually will apply retroactively.

If consent is not provided by the registrant of an existing domain name before its renewal, the registration will be terminated. The new system is expected to provide a far more efficient and effective means of dealing with domain name disputes than any of the options previously available to infringed parties, including the notoriously slow Czech courts.

By: Ole Horsfeldt,
Bech-Bruun Dragsted, Copenhagen

DENMARK

DOMAIN NAME LEGISLATION CONSIDERED

On 6 October 2004 the Department of Science, Technology, and Development appointed a committee to examine the need for introducing legislation regarding domain names in Denmark. There is no legislation concerning this matter. The committee has submitted a report that finds legislation necessary. The intention of the resultant bill is to ensure that the law is administered in a transparent, dynamic, and efficient manner. The major subjects included in the bill are:

- that the administration of domain names be given out for public tender (since 1 July 1999 DK Hostmaster has administrated .DK),
- that, as long as the purpose is legal, anyone can

register a domain name (no change to current practice),

- a general prohibition against domain names registered only for resale or rental purposes (warehousing),
- the idea that good practice will develop over time, and
- that both Danish domain names and other international domain names allocated to Denmark (for example, .DK.EU) are covered by the bill.

The government has decided to table the bill before the end of this year.

EUROPEAN
UNIONBy: David Taylor
Lovells, ParisGENERIC WORDS DIFFICULT
TO DEFEND UNDER UDRP

Companies whose intellectual property rights are based upon, or can be deemed as, broadly generic words and that are seeking to protect themselves on the Internet through use of the Uniform Domain Name Dispute Resolution Policy (UDRP)—which seeks to transfer or deny transfer of domain names to a complainant based upon merit—need to make sure that their cases are extremely strong before proceeding. In the case of *Match.com, LP v. Bill Zag and NWLAWS.ORG* (No. D2004-0230), Match.com's disputed multiple domain names—including FLOWERSMATCH.COM, SCHOLARSMATCH.COM, and SAFEMATCH.COM—were all based upon their registered service mark, MATCH.COM.

However, panelist Scott Donahey ruled against Match.com, saying: “By registering the service mark MATCH.COM, Complainant cannot thereby preclude anyone else from ever registering the common term

‘match’ in combination with other common words in the .COM gTLD. So long as those domain names are used in their generic sense, rather than seeking to profit from the goodwill associated with Respondent's trademark, their registration and use would not violate the Policy.” Donahey added: “The Panel finds that the registrant of a common term or word as a trademark cannot preclude others from using that term in a domain name unless the registrant is attempting to profit from the goodwill associated with that mark.”

Companies considering UDRP action need to carefully consider their timing, arguments, and chances of success before submitting complaints. Although decisions tend to favor the trademark holder, this nevertheless depends upon the trademark holder proving its case and, as evidenced above, the complainant is not always the successful party.

FINLAND

By: Sakari Aalto
Roschier Holmberg Attorneys Ltd., Helsinki

PRIVACY LAW CHANGES

Privacy in Employment—A new Act on the Protection of Privacy in Employment (759/2004) entered into force on 1 October 2004. The Act includes new provisions on the protection of employee e-mail, camera surveillance, and employee drug testing. The Act safeguards the confidentiality of employees' e-mails but also grants, provided certain procedures are followed, the employer the right to access an employee's work-related messages when the employee is unable to do so and the messages are necessary for concluding business negotiations, customer service, or for securing the operations of the employer. On-site camera surveillance is only allowed if it is intended to secure the safety of the employees, to protect property, or to supervise manufacturing processes. Camera surveillance cannot be used for monitoring individual employees, except to prevent an obvious threat of violence or other safety hazard relating to a certain workstation.

An employer may request a drug test certificate from new employees only if the duties presuppose exactness, reliability, independent judgment, or good reaction abilities, and the employee's drug use would endanger lives or cause other major damage. During the employment relationship, an employee may be tested only if there are justified grounds for suspecting drug use, in addition to the aforesaid requirements.

Privacy in E-Communication—The Act on Data Protection in Electronic Communication (516/2004) entered into force on 1 September 2004, implementing EC Directive 2002/25/EC. The Act is aimed at promoting consumers' and users' trust in the information security of e-communication devices, such as e-mail, SMS, and MMS. The Act regulates direct e-marketing to consumers, companies, and public entities, the use of cookies, blocking and filtering of spam, and processing of location data, among other

things. The Act sets forth the principle of opt-in for sending direct e-marketing messages to consumers (opt-out applies to direct marketing messages sent to companies and public entities). As an exception to the opt-in rule, companies may use contact information obtained from a previous relationship to market the same or similar products or services, without the requirement of prior customer consent.

Direct e-marketing messages must clearly and unambiguously be recognizable as such. E-messages

that hide or conceal the identity of the sender and do not include a valid address to which the recipient may send an opt-out request are prohibited and considered to be spam. Operators, corporations, and other entities may, upon the prior request of a user or in certain limited cases on their own initiative, block or filter spam messages directed to the user.

The Data Ombudsman has already received its first case testing interpretation of the Act and its boundaries.

By: Lars Lensdorf,
Willkie Farr & Gallagher, Frankfurt

GERMANY

RECENT DEVELOPMENTS

Decisions—In its judgment of 13 November 2003 (I ZR 40/01), the Federal Supreme Court (BGH) decided whether the advertising and execution of a “reversed auction” on the Internet, where the initial price of a car offered dropped by DM 250 every 20 seconds, violated the provisions of Article 7(1) or Article 1 of the German Act Against Unfair Competition. It concluded that there is no violation if it is obvious that after the end of the auction the “winner” can decide freely, and without suffering any financial prejudice, whether or not he wishes to purchase the “vehicle bought at the auction” at the price obtained.

In a judgment of 16 December 2003 (X ZR 129/01), the BGH decided whether and on what conditions a contractor, who had undertaken to develop a data processing program, was obligated to provide the source code to the customer in the absence of any express agreement to that effect. According to the BGH, the decision depends on the specific circumstances of the particular case, i.e., on the amount of the agreed remuneration and, in particular, on whether the program was developed for distribution by the customer and whether the latter needs to have access to the source code for maintenance and further development purposes.

According to the BGH judgment of 19 February 2004 (I ZR 82/01; *kurt-biedenkopf.de*), the owner of a name, who obtained the cancellation of a domain name by claiming an infringement of his rights, is not entitled to a “permanent injunction” barring any future use of the domain name by third parties. If any other third parties apply for registration of the same

domain name, DENIC, the company responsible for awarding domain names, is under no obligation to check whether the name applied for infringes the rights of the owner of the name.

In its judgment of 11 March 2004 (I ZR 304/01), the BGH determined if and to what extent a service provider, who introduced a web hosting platform where private and commercial suppliers can auction off their products, can be held liable for trademark infringement if a supplier offers counterfeit merchandise (in this case counterfeit Rolex watches) for auction. The BGH decided that the ISP can only be held liable for having participated in the trademark infringement committed by the supplier if the act was committed at least with conditional intent. Any liability as “interferer” (*Störer*) presupposes that the ISP has reasonable control possibilities that enable it to prevent such infringement. It cannot be expected to check each offer that is directly placed online by an automated procedure to determine whether any third party rights have been infringed. However, if an ISP becomes aware of a trademark infringement, it is not only obligated to immediately block the offer, but also to take all reasonable and technically feasible measures to prevent further trademark infringements.

With respect to liability as “joint interferer” (*Mitstörer*), i.e., liability for placing a hyperlink to an illegal Internet offer, the BGH decided in its judgment of 1 April 2004 (I ZR 317/01) that the scope of the duty to check depends on the overall context in which the hyperlink is used. Where hyperlinks only serve

to facilitate access to publicly available sources, the requirements with respect to freedom of opinion and freedom of the press should not be applied too strictly. In particular, it should be taken into account that it would be practically impossible to use the world wide web effectively without using hyperlinks.

The judgment of the Regional Court Munich 1 of 19 May 2004 (21 O 6123/04) is the first by a German court on General Public Licenses (GPL). The court held that a provision of a GPL, which provides for an automatic forfeiture of rights in case of a violation of the code of conduct laid down in other provisions of the contract, does not place the party contracting with the user at an unreasonable disadvantage. However, a provision to that effect does not constitute an admissible restriction of the right of use within the meaning of Article 31, §2, second sentence of the German Copyright Act.

In connection with the question on which conditions a computer-controlled procedure is patentable, the BGH decided in a judgment of 24 May 2004 (X

ZB 20/03) that a patent for a procedure that serves to process a business transaction by using a computer is only patentable if the patent claim is not limited to a proposal for using a computer to process the transaction, but contains additional instructions for dealing with a concrete technical problem, so that the level of invention can be checked and it can be determined whether the procedure constitutes a patentable technological improvement.

Legislation—The new Telecommunications Act (TKG), which entered into force on 26 June 2004, contains numerous new provisions on market regulation, telecommunications monitoring, and data protection. In the future, the Regulatory Authority may obligate all providers with significant market power to maintain “standard offers” for all access services for which there is a public demand, which can then be used by competitors. The new Act also provides that all telecommunications providers that allocate numbers are obligated to collect relevant customer data. As a result, even in the prepaid sector, there will no longer be anonymous calling cards for mobile phones.

HONG KONG

By: Gabriela Kennedy and Paloma Wong,
Lovells (TMT GROUP), Hong Kong

PATEK PHILIPPE RECOVERS .CN DOMAIN NAMES

This case concerns a dispute over two .CN domain names, PATEKPHILIPPE.COM.CN and PATEKPHILIPPE.CN. The disputed domain names were registered on 5 June 2001 and 17 March 2003 respectively. The case was brought before the Hong Kong International Arbitration Centre, which was appointed by the China Internet Network Information Center on 30 September 2002 as an authorized domain name dispute resolution provider for .CN domain names. Since its appointment, HKIAC has handled 18 .CN domain name disputes. Complainants have been from the USA, UK, France, Germany, Italy, and Switzerland.

Complainant Patek Philippe S.A. is a world-famous watch manufacturer with its principal place of business in Switzerland; the respondent, Shengyang Zhongxu Economic Trade Limited, is situated in Shengyang, PRC. The complainant adduced evidence that the substance of the disputed domain names, “patekphilippe,” was identical to or confusingly similar to the complainant’s trademarks. Patek

Philippe first registered its trademark in the PRC in 1992, owns numerous Patek Philippe trademark registrations, and in China has extensively used the trademark Patek Philippe. The complainant also adduced evidence that it had registered domain names incorporating its mark, including PATEK-PHILIPPE.BIZ, PATEKPHILIPPE.COM.CN and PATEK-PHILIPPE.CN.

The complainant contended that the respondent had no rights or legitimate interests in the disputed domain names, arguing that the names had never been used by the respondent and did not refer to any operational websites. The complainant argued that respondent did not hold any registered Patek Philippe trademark rights in the PRC. The complainant also argued that the domain names had been registered in bad faith, providing evidence that the names were registered for the purpose of selling or otherwise transferring them to obtain unjustified benefits. E-mail between the parties was produced, in which the transfer or sale of the names for US\$1,000,000 was proposed.

Finally, the complainant argued that the respondent registered the names to prevent the complainant, as rightful owner of the Patek Philippe name and mark, from reflecting its name and mark in corresponding domain names and that the respondent had engaged in a pattern of such conduct in relation to the rightful owners of other brands and names.

The respondent registered PATEKPHILIPPE.COM.CN on 5 June 2001, prior to commencement of the Priority Period for second level .CN domain name registration in 2003, which was only available to existing third level .CN registrants. The complainant argued that the registration of the second level domain name during the Priority Period was made in bad faith so as to deprive the complainant of the opportunity to obtain a .CN domain name containing the words “patekphilippe.” The complainant also produced ample evidence from CNNIC’s WHOIS database that showed that the respondent had registered and held other domain names incorporating famous brands and names, such as VACHERONCONSTANTIN.CO

M.CN, LONGINES.COM.CN, LONGINE.CN, ORIS.COM.CN, and ORIS.CN. Such a pattern of registering domain names to prevent the rightful owners from reflecting their rights in corresponding domain names constituted bad faith. The complainant again argued that the disputed domain names had never been used by the respondent and did not refer to any operational websites.

The respondent did not submit a response. The sole panelist ruled in favor of the complainant and ordered the transfer of the disputed domain names to complainant. The panelist agreed with the complainant’s arguments and noted that all of its Patek Philippe trademarks in the PRC were valid and protected under the PRC Trade Mark Law. The arguments regarding bad faith also were accepted. Of note was the acceptance of the argument that the registration of a second level .CN domain name during the Priority Period could be construed as an intention to prevent others from registering the same, which amounts to bad faith.

By: Milan Chromecek and David Taylor,
Lovells, Paris

ICELAND

GET YOUR SKATES ON—IDNs LAUNCHED

Internationalized Domain Names (IDNs) became available in Iceland on 1 July 2004, at which time the Icelandic NIC (ISNIC) began registering domains containing the letters ð é í ó ú ý þ æ ö to support Icelandic language domains. For the six month period that began 1 July and ended 31 December 2004, a registration application for a domain containing any of these Icelandic letters was granted to registrants holding the corresponding “non-Icelandic” domain (if any), according to the following mapping:

á – a	ð – d
é – e	í – i
ó – o	ú – u
ý – y	þ – th
æ – ae	ö – o

After the sunrise period, applications will be accepted from all members of the public, regardless of previous domain name registrations.

ITALY

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

TELEMATIC APPLICATIONS TO THE PUBLIC ADMINISTRATION

A draft "Code of the Public Digital Administrations" was sent to the Government. The text includes the main rules of the D.P.R. 445/2000, which introduced the computerization of the Public Administration in Italy. However, certain integrations are included in the Code.

The most significant integration concerns the approach to be followed when producing specific applications (applications are the most common means to start administrative proceedings). Such applications, filed at the Public Administration by telematic means, shall be valid if the applicant can be identified

by other means from his digital signature (e.g., login name and password). In practice, it will be possible to hold a telematic dialogue before an e-identity card is activated. For instance, a telematic application to obtain an authorization or a license, addressed to the Public Administration, will have same value and effect as if it had been signed with an actual autographed signature.

According to the new rules, the documents shall be kept in e-format only. However, for document recording, paper format will also be allowed.

JAPAN

By: Shino Uenuma,
Perkins Coie, Seattle, Washington

PERSONAL INFORMATION PROTECTION LAW

The Personal Information Protection Law, intended comprehensively to apply to commercial activity in the private sector, will become effective on 1 April 2005.

Obligations of Information Dealers—"Personal Information" is any information relating to a living individual that enables a specified individual to be identified (including any data easily collated with other data) (Article 2.1). The name, birth date, or certain types of e-mail addresses containing one's name and organization are included within the definition.

The Law imposes legal obligations on "Commercial Personal Information Dealer(s)," defined as any person or entity that utilizes "Personal information Databases" for its business purposes (Article 2.3). "Personal Information Databases" are computer-based, or paper-based ones with an index, that allow for searches that use, or could identify, a specified individual. The Law does not apply to businesses holding small-sized databases (5,000 or fewer individuals). The legal obligations (based on the 8 principles set out in the relevant OECD guidelines) are:

(1) Purpose specification for the use (Article 15).

- (2) Use limitation: Dealers shall not use Personal Information outside the scope of the specified purpose, without the prior consent from such individuals (Article 16). Without prior consent, the dealers shall not provide Personal Data to any third party except in certain conditions (Article 23). The main exceptions are generally where the dealer provides such individuals the opportunity to opt-out for sharing their data, or in case of outsourcing or of merger or transfer of the business.
- (3) Limitation for collection by unfair means (Article 17).
- (4) Data quality (Article 19).
- (5) Security safeguards (Article 20, 21).
- (6/7) Openness and individual participation: Dealers shall disclose to individuals the purpose of the use and what data they have (Article 18, 24) or, upon request, make corrections (Article 26), or cease to use the data (Article 27).
- (8) Accountability (Article 31).

Violations—It is common in Japanese administrative regulations to provide two-tiered regulations that can give rise to two different legal consequences, even though they regulate the same activity. This custom is found in the regulations dealing with violations of these obligations in that the relevant ministries may issue either a recommendation or an order to cure. In the case of a recommendation, compliance is voluntary; compliance is mandatory for an order. A ministry may issue an order if a dealer does not reasonably comply with an earlier recommendation, or in an emergency (Article 34). Violation of an order is subject to the punishment of imprisonment for a period not exceeding 6 months or a fine of not more than JPY

300,000 (Article 56). An employer or a principal is also subject to the fine for breach by its employee or agent (Article 58).

International Applicability—The Law does not specifically apply to foreign businesses. Generally, unless expressly provided otherwise, Japanese laws apply within the territory of Japan. However, the question as to whether the Law will apply to foreign businesses, particularly in connection with transactions involving the Internet, is now being extensively discussed among authorities. It is clear, however, that the Law shall apply to a branch or a representative existing in Japan.

NEW COPYRIGHT LAW AMENDMENTS

New Amendments to Japanese Copyright Law are grouped under 3 categories: (1) prevention of re-import of commercial records, (2) establishment of the copyright owner's exclusive right in renting books or magazines, and (3) increasing penalties. The Amendments become effective 1 January 2005.

Commercial Records Re-Importation—These Amendments seek to promote Japanese musical culture overseas. They provide that (1) knowingly importing a Record for Foreign Distribution (defined below) with the purpose of distribution thereof in Japan, (2) knowingly distributing the same in Japan, or (3) knowingly possessing the same for the purpose of distribution thereof in Japan, shall be regarded as infringement of the exclusive rights of copyright owners or record publishers, who publish or allow publication of commercial records to be distributed in the territory of Japan (the "Record for Domestic Distribution") where they publish or allow publication of, outside Japan, the same record as the Record for Domestic Distribution to be distributed outside of Japan (the "Record for Foreign Distribution"), only when the profit they expect to gain by the publication of the Record for Domestic Distribution will be unfairly decreased by the domestic distribution of the Record for Foreign Distribution (Copyright Law §113.V).

The Amendments also provide exceptions for commercial records that have been published in Japan for the designated period (not exceeding 7 years)

by the enforcement order. The enforcement order, in which the period is designated as 4 years, was enacted after the due date (13 October 2004) for public comments. The Amendments apply to commercial records already published as of 1 January 2006 for the same period thereafter. In short, under the Amendments, copyright owners or record publishers (under Japanese Copyright Law, the record publishers have "neighboring rights," generally similar to copyright) may prohibit re-import of the same commercial records published in Japan from foreign countries.

Book/Magazine Rental Rights—Copyright Law provides that copyright owners have an exclusive right to rent their copyrighted works (§26-3). However, the Law also provides, in its supplementary provision, that §26-3 does not apply to books or magazines for a specified period of time. The Amendments abolish this supplementary provision so that copyright owners can exercise their exclusive rental rights over books and magazines. This rental right cannot be exercised over books or magazines already held by others as of 1 August 2004, for the purpose of renting them to the public.

Increasing Penalties—The Amendments increase the maximum punishment for violation of the Law: (1) from 3 years' imprisonment to 5 years, and (2) from JPY100,000,000 fine (for entities) to JPY150,000,000. Both can be imposed under the Amendments.

PORTUGAL

By: André Lencastre Bernardo and Manuel Lopes Rocha,
Barrocas Sarmento Rocha, Lisboa

IMPLEMENTATION OF DIRECTIVE 2001/29/EC

Directive 2001/29/EC of the EP and of the Council of 22 May 2001, on the harmonization of certain aspects of copyright and related rights in the information society, was implemented in Portugal by Law 50/2004 of 24 August. This was almost two years after the deadline of 22 December 2002, established in Article 13 of the Directive.

The implementation of the Directive's provisions was important, particularly for those issues that are in need of regulation and harmonization, such as digital rights management and technical protection measures. New technologies and new media formats, together with the Internet, bring new challenges to the protection of copyrighted works that use such supports and technologies; Law 50/2004 provides such protection. With the new copy protection measures available, a higher degree of protection can be achieved, but without the legal protection of these technical measures themselves—namely, as regards circumvention—these technologies would prove fruitless, for it would only be necessary for someone to break such measures, or create software programs toward that end, to illicitly reproduce the underlying copyrighted material.

The implementation of the Directive by Law 50/2004 was made through several addenda and amendments to the Portuguese Copyright and Connected Rights Code, approved by Decree-Law 63/85 of 14 March (as successively amended by Laws 45/85 and

114/91, and Decrees-Law 332/97 and 334/97). Those addenda and amendments were made to achieve compliance with the Directive, especially pertaining to an author's rights of reproduction and distribution (adapted to today's challenges), as well as the right of communication of works to the public, whether by wire or wireless means.

In addition, and also pursuant to the Directive, Law 50/2004 establishes exceptions and limitations to the exclusiveness of the reproduction right conferred upon authors, regarding temporary, transient, or incidental acts of reproduction, where these are an integral and essential part of a technological process whose sole purpose is to enable a transmission, by an intermediary, in a network between third parties, or other lawful use foreseen elsewhere in the applicable legislation.

Pursuant to Articles 6 and 8 of the Directive, Articles 218 and 219 of the Copyright and Connected Rights Code (as introduced therein by Law 50/2004) enforce the protection conferred thereto upon technical protection measures, by criminalizing their unauthorized circumvention. Pursuant to Article 218, whoever breaks an effective technical protection measure on a given copyrighted work shall be subject to a maximum of one year imprisonment; pursuant to Article 219, whoever develops, markets, or otherwise distributes programs to enable such circumvention shall be subject to a maximum imprisonment of six months.

SOUTH AFRICA

By: Mark Hyslop, Edward Nathan & Friedland (Proprietary) Ltd.,
Johannesburg

CRYPTOGRAPHY REGULATIONS

The South African Electronic Communications and Transactions Act, 2002 (No. 25 of 2002) provides for the regulation of cryptography providers. Cryptography providers must be registered in accordance with the Act and pay prescribed administrative fees. Once enacted, draft Cryptography Regulations under the Act will make further and more elaborate provisions regarding the registration of cryptography pro-

viders and the payment of administrative fees.

Under the draft Regulations, a registered cryptography provider must pay an application fee of R100 (± €12.70) and an annual administrative fee of R200 (± €25.40). The annual administrative fee is payable for each and every cryptography product or service. Cryptography providers will also be required to pro-

vide the privacy and security policies that they will follow in the operation of their services and products. Cryptography providers must also provide the names, addresses, and contact details of all customers to whom products were directly delivered, sold, made available, or distributed to, or to whom services were rendered in the preceding six months. These Regulations are likely to create an administrative burden for providers, due to the varying products and services they offer. The increased administrative burden will also increase direct and indirect costs of operation.

A cryptography service or product is regarded as being provided in South Africa if it is provided from premises within South Africa, or to a person present in South Africa when that person makes use of the service or product, or to a person who uses the service or product for the purpose of a business carried on in South Africa or from premises in South Africa. Cryptography providers who deal with South African persons or businesses or who make or bring products

with encryption capabilities or services into South Africa must therefore be careful to ensure compliance with the registration requirements under the Act and the Regulations. Non-compliance with registration requirements is an offense punishable by a fine or imprisonment of up to two years.

It is felt that the proposed Cryptography Regulations are rather onerous and will lead to an escalation of providers' costs. This is of particular concern to small and medium-sized enterprises that, interestingly, the Act seeks to promote. The increased administrative burden is also contrary to the Act's intended objectives of *inter alia* removing and preventing barriers to e-transactions in South Africa, and promoting the development of e-transaction services that are responsive to the needs of users and consumers. It is surprising that legislation that seeks to facilitate e-communications and transactions should place unnecessary and cumbersome obstacles in their development and operation.

By: Jose M. Rey,

Larrauri & Lopez Ante Abogados, Madrid

SPAIN

PRELIMINARY REJECTION FOR CATALONIAN sgTLD

On 16 March 2004, about 70 associations dedicated to the promotion of the Catalan language and culture presented their application to ICANN for the creation of a new sgTLD (Sponsored Generic Top Level Domain), .CAT. Although to English speaking people (the huge majority on the Web) it may sound like some kind of pet lovers domain, the .CAT TLD stands for "CATalán", the language spoken by Catalanian people.

On 29 October, and despite the fact that the Government had supported the application, ICANN denied approval of .CAT because it does not comply with any of the three requirements: technical competence, financial sufficiency, and that the first level domain belongs to a real sponsored community. This decision is not a definitive denial; the application will now have to pass through a harder approval process, where success is by no means guaranteed. Together with the .CAT domain, nine more applications were sent to ICANN, including .XXX (for the pornographic web user community). Only two of the applications (.TRAVEL and .POST) received ICANN's approval in

this first phase.

Historically, there have been only seven generic TLDs that are valid for everyone (as opposed to a single community). However, since 2000 it has been possible to create a "sponsored TLD." This depends upon whether someone belongs to a 'specific' community and, therefore, whether he can register under the sTLD. For the future .CAT domain, the Associació puntCAT (representative of the Catalan Language and Culture Community) foresees its own dissolution and the creation of the Fundació puntCAT, based in Barcelona, responsible for elaborating and managing the .CAT domain. However, because of ICANN's provisional denial, the creation of such a foundation will have to wait.

The Associació puntCAT clearly states that its application for the .CAT TLD does not imply a renunciation of its main goal: obtaining a specific territorial or country code TLD domain—.CT—for Catalonia. Today it is impossible, given that territorial TLDs are granted by ICANN exclusively to countries recognized as such by the United Nations (the ISO-3166 list).

SWEDEN

By: Lars Perhard,
Advokaterna Wersén & Partners, Stockholm

CONDITIONS FOR SUPPLYING BROADBAND FOUND UNCONSCIONABLE

The Market Court has, through a judgment of 15 September 2004, put an injunction on Telia Internet Services AB, previously one of the leading ISPs in Sweden, concerning one of the stipulations in Telia's general conditions. The prohibition relates to contractual conditions imposed with the supply of broadband access services to private individuals (consumers) with an initial contract period of twelve months.

The legal issue is whether it is unconscionable that the supplier has reserved its right to increase prices or unilaterally change conditions in its favor in other respects. Telia contested a claim raised by the Consumer Ombudsman, arguing that it had been sold to Telia Sonera Sweden AB and was no longer operating the business. The Consumer Ombudsman rebutted, asserting that the condition is common in this type of broadband supply agreement; therefore, it was of interest to have the clause tried.

If an unfair contract term is used by a salesperson in a consumer contract, it may be prohibited. A contract term is typically unfair if it gives the seller an exclusive benefit at the expense of the consumer. The Consumer Ombudsman may apply to the Market Court for the prohibition of an unfair contract term. In 1995 the Act was adapted to conform with EU Directive 93/13/EC on unfair terms in consumer contracts. Hence, it also should be of some interest outside Sweden that the Market Court tried the clause in the light of the Consumer Contract Terms Act (1994: 1512), a result of the implementation of the EU Directive. The Electronic Communications Act (2003: 389), a result of the implementation of EC Directive 2002/58/EC on privacy and e-communications, stipu-

lates at Chapter 5, §16.i.a: "If a party that provides subscribers with electronic communication services wishes to amend the contract, the subscriber shall be notified of the amendment at least one month before it enters into force. A subscriber who does not accept the new conditions may give notice terminating the contract without therefore being adversely affected by any cost, charge or other obligation." Telia referred to this stipulation. The Consumer Ombudsman responded that basically it is applicable to agreements of an undefined period of time.

The Telia agreement stipulated that the customer was bound for an initial period of twelve months. The dispute related to the interpretation of several clauses in Telia's general conditions, all of which are not reported here. In summary, the Market Court concluded that the subscriber or consumer was bound initially for a period of twelve months with no contractual possibility to exit during that period. The court also found that the construction of the agreement implied that Telia unilaterally had reserved a right in its favor to amend the agreement. Furthermore, the court stated that the Electronic Communications Act stipulation only would be interpreted as a minimum level in an agreement between an operator and a subscriber. The Market Court found that no prevailing circumstances gave reason to judge the actual clause as conscionable. On the contrary, it concluded that Telia's unilaterally reserved rights to amend conditions during a period of time when the consumer could not give notice to terminate the agreement disturbed the prerequisites for a reasonable balance between the parties and, hence, must be considered unconscionable. The action of the Consumer Ombudsman was approved.

Websites for Government and Related Reports

Intellectual Property

Copyright Royalty and Distribution Reform Act of 2004 (P.L. 108-419) [BEING UPDATED], Copyright Office, WWW.COPYRIGHT.GOV/TITLE17/INDEX.HTML.

E-Forms Available for Madrid Protocol Filings, USPTO, WWW.USPTO.GOV/TEAS/INDEX.HTML.

New E-Filing Options in Trademark Disputes, USPTO, WWW.USPTO.GOV/WEB/OFFICES/COM/SPEECHES/04-29.HTM.

Risk Management of Free and Open Source Software (Guidance), Federal Financial Institutions Examination Council, WWW.FDIC.GOV/NEWS/NEWS/FINANCIAL/2004/FIL11404A.HTML.

Waiver of Pixel Requirement for Drawings Filed Electronically, USPTO, WWW.USPTO.GOV/WEB/OFFICES/COM/SOL/NOTICES/69FR59809.PDF.

Internet

Agreement Between the Government of the USA and the Government of Canada on the Application of Positive Comity Principles to the Enforcement of Their Competition Laws, Federal Trade Commission, WWW.FTC.GOV/os/2004/10/0410COMITYAGREEENGLISH.PDF.

Analysis of Noncash Payments Trends in the US: 2000-2003, The 2004 Federal Reserve Payment Study, Federal Reserve System, WWW.FRBSERVICES.ORG/RETAIL/PDF/2004PAYMENTRESEARCHREPORT.PDF.

FCC Approves First Software Defined Radio, Federal Communications Commission, [HTTP://HRAUNFOSS.FCC.GOV/EDOCES_PUBLIC/ATTACHMATCH/DOC-254463A1.PDF](http://HRAUNFOSS.FCC.GOV/EDOCES_PUBLIC/ATTACHMATCH/DOC-254463A1.PDF).

Implementation of the Whois Data Reminder Policy, ICANN, WWW.ICANN.ORG/WHOIS/WDRP-IMPLEMENTATION-30NOV04.PDF.

Independent GNSO (Generic Names Supporting Organization) Council Review, ICANN, [HTTP://GNSO.ICANN.ORG/ANNOUNCEMENTS/ANNOUNCEMENT-22DEC04.HTM](http://GNSO.ICANN.ORG/ANNOUNCEMENTS/ANNOUNCEMENT-22DEC04.HTM).

Nation Online: Entering the Broadband Age, National Telecommunications and Information Administration, WWW.NTIA.DOC.GOV/REPORTS/ANOL/NATIONALONLINEBROADBAND04.PDF.

.NET Request for Proposals, ICANN, WWW.ICANN.ORG/TLDS/DOTNET-REASSIGNMENT/NET-RFP-FINAL-10DEC04.PDF.

Ombudsman Framework, ICANN, WWW.ICANN.ORG/OMBUDSMAN/OMBUDSMAN-FRAMEWORK-03DEC04.HTM.

WGIG (Working Group on Internet Governance) Secretariat: ICANN Agrees to Provide Contribution, WWW.ICANN.ORG/ANNOUNCEMENTS/ANNOUNCEMENT-20DEC04.HTM; *see* Special Meeting of the Board—Approved Resolutions, WWW.ICANN.ORG/MINUTES/RESOLUTIONS-20DEC04.HTM.

Privacy

Declaration of the Article 29 Working Party on Enforcement on the Protection of Individuals with Regard to the Processing of Personal Data, Article 29 Working Party, [HTTP://EUROPA.EU.INT/COMM/INTERNAL_MARKET/PRIVACY/DOCS/WPDOCS/2004/WP101_EN.PDF](http://EUROPA.EU.INT/COMM/INTERNAL_MARKET/PRIVACY/DOCS/WPDOCS/2004/WP101_EN.PDF).

Free Credit Report Rollout, Federal Trade Commission, WWW.ANNUALCREDITREPORT.COM.

More Harmonised Information Provisions: Moving Forward on Action 6 of the Work Programme for a Better Implementation of the Data Protection Directive, Data Protection Working Party, [HTTP://EUROPA.EU.INT/COMM/INTERNAL_MARKET/PRIVACY/DOCS/WPDOCS/2004/WP100_EN.PDF](http://EUROPA.EU.INT/COMM/INTERNAL_MARKET/PRIVACY/DOCS/WPDOCS/2004/WP100_EN.PDF).

Proper Disposal of Consumer Information Under the Fair and Accurate Credit Transactions Act of 2003, Department of the Treasury, 69 FR 77610, [HTTP://A257.G.AKAMAITECH.NET/7/257/2422/06JUN20041800/EDOCKET.ACCESS.GPO.GOV/2004/PDF/04-27962.PDF](http://A257.G.AKAMAITECH.NET/7/257/2422/06JUN20041800/EDOCKET.ACCESS.GPO.GOV/2004/PDF/04-27962.PDF).

Q&A re Application of PIPEDA, Alberta and British Columbia's PIPAs, Privacy Commissioner of Canada, WWW.PRIVCOM.GC.CA/LEGISLATION/BC_AB_041105_E.ASP.

Spyware: Consumer Alert, Federal Trade Commission, www.ftc.gov/bcp/conline/pubs/alerts/spywarealrt.htm.

Transferring Personal Information about Canadians Across Borders—Implications of the USA Patriot Act, Privacy Commissioner of Canada, www.privcom.gc.ca/media/nr-c/2004/subusapa_040818_e.asp.

What Canadians Can Do to Protect Their Personal Information Transferred Across Borders, Privacy Commissioner of Canada, www.privcom.gc.ca/fs-fi/02_05_d_23_e.asp.

Security

Action Plan on Spam Enforcement, FTC and International Agencies, www.ftc.gov/opa/2004/10/spamconference.htm.

Anti-Spam Toolkit, Organisation for Economic Cooperation and Development, www.oecd.org/document/50/0,2340,en_2649_201185_33732274_1_1_1_1,00.html.

FACTA (16 CFR 601, 698), Summaries of Rights and Notices of Duties: Publication of Final Guidance of Model Disclosures, Federal Trade Commission, www.ftc.gov/opa/2004/11/0411facta.htm.

London Action Plan On International Spam Enforcement Cooperation, Canadian Commerce Department, www.e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/wwapj/london_action_plan.pdf.

Putting an End to Account-Hijacking Identity Theft, Federal Deposit Insurance Corporation, www.fdic.comsumers/consumer/idtheftstudy/identity_theft.pdf.

Related Identity Theft Definitions, Duration of Active Duty Alerts, and Appropriate Proof of Identity Under the Fair Credit Reporting Act, 16 CFR 603, 613, 614, Federal Trade Commission, www.ftc.gov/os/2004/10/041029idtheftdefsn.pdf.

Revision of the Computer Misuse Act, All Party Parliamentary Group, www.apig.org.uk.

Sarbanes-Oxley Act: Implementation of Information Technology and Security Objectives, Cyber Security Industry Alliance, www.csialliance.org/resources/pdfs/csia_sox_report.pdf.

Task Force on Spam: Recommended Best Practices for Internet Service Providers and Other Network Operators, Canadian Commerce Department, [www.e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/wwapj/bestpractices.pdf/\\$file/bestpractices.pdf](http://www.e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/wwapj/bestpractices.pdf/$file/bestpractices.pdf).



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 Perbot
- Addresses and telephone/fax
 numbers for the above editors
 are on the front cover.

LIST OF
 CONTRIBUTORS

Sakari Aalto <i>Helsinki, Finland</i>	Lars Lensdorf <i>Frankfurt, Germany</i>	David R. Syrowik <i>Southfield MI</i>
Merril A. Baldwin <i>San Francisco CA</i>	Angiolo Luzzati <i>Milan, Italy</i>	David Taylor <i>Paris, France</i>
André Lencastre Bernardo <i>Lisboa, Portugal</i>	Charles Morgan <i>Montréal, Canada</i>	Robert D. Traver <i>Denver CO</i>
Milan Chromceck <i>Paris, France</i>	Matthew A. Murphy <i>Beijing, China</i>	Shino Uenuma <i>Seattle WA</i>
Matthew T. Furton <i>Chicago IL</i>	Stephen Mutkoski <i>Redmond WA</i>	Luis Vera Valledo <i>Mexico City, Mexico</i>
Ole Horsfeldt <i>Copenhagen, Denmark</i>	Lars Perhard <i>Stockholm, Sweden</i>	Olga Georgiades Van der Pol <i>Nicosia, Cyprus</i>
Mark Hyslop <i>Johannesburg, South Africa</i>	Jose M. Rey <i>Madrid, Spain</i>	Paloma Wong <i>Hong Kong</i>
Gabriela Kennedy <i>Hong Kong</i>	Mannuel Lopes Rocha <i>Lisboa, Portugal</i>	
	George Spatz <i>Chicago IL</i>	