WorldTrade Executive, Inc.

Global eCommerce
law and business report

The International Business Information Source™

May 2003
Volume 5,
Number 5

New Survey Reveals Moving Data Across Borders Poses Legal Challenges for Multinationals

BY ROBERT L. RASKOPF (WHITE & CASE LLP)

Multinational businesses are finding it harder and harder to cope with the worldwide spread of laws that restrict their ability to move data across borders. The problem is not merely one of how many countries are adopting these data-transfer laws, but also that so many of these laws are not harmonized with each other.

For example, if you needed to move data between Spain and Australia to protect a data subject's vital economic interests, you could send it from Australia, but not Spain. If you needed to transfer the same data due to a legal claim, you could send it from Spain, but not Australia. Thus, compliance gets very tricky for any company doing business with multinational operations or markets.

To help firms better understand the various laws and rules governing cross border transfers, global law firm White & Case LLP surveyed cross-border data transfer laws in 22 major jurisdictions. The survey found that divergent legal restrictions present a growing obstacle to multinational companies that must move information between countries.

The survey takes an in-depth look at laws governing the transfer of personal data across borders that are enacted or proposed in 22 commercially prominent jurisdictions in North America, Europe and the Asia-Pa-

continued on page 12

Japan Implements New Basic Law on Intellectual Property

BY KYM BAVCEVICH (COUDERT BROTHERS), SHINTARO KURODA AND NORIMASA TOGASHI (YODOYABASHI & YAMAGAMI L.P.C.)

In his General Policy Speech to the 156th session of the Japanese Diet in January 2003, Prime Minister Junichiro Koizumi declared that Japan would aim to be a nation "built on the platform of intellectual property." This remark echoed earlier statements by the Prime Minister, advocating a national strategy to be pursued in furtherance of the goals of encouraging creation and developing the protection and exploitation of intellectual property. Recognition of the pivotal role which intellectual property is to play in Japan's future economic development if the objective of revitalization of the Japanese economy is to be achieved also manifested itself in the convocation in 2002 of the Strategic Council on Intellectual Property (the "Council"), which was charged with the responsibility of establishing and advancing a national strategy for intellectual property.

continued on page 2

in this issue

Japan from page 1

The Council, which consisted of Ministers from various Ministries, business leaders and experts from the scientific and legal disciplines, issued the Intellectual Property Policy Outline on July 3, 2002, which incorporated a proposal for the establishment of the Basic Law on Intellectual Property (Law No. 122 of 2002) (the "Basic Law"), under which the Intellectual Property Policy Headquarters was established in March 2003.

The Basic Law requires the Intellectual Property Policy Headquarters to develop a Promotion Program which must set forth basic policy and measures for the creation, protection and exploitation of intellectual property.

The Basic Law, which was enacted on November 27, 2002 came into effect on March 1, 2003, and its objective is to establish parameters in accordance with which the Japanese government (led by the Intellectual Property Policy Headquarters) will attempt to fulfill the objective of "making Japan a nation that is built on intellectual property." This article will set forth the objectives and mechanisms of the Basic Law and the historical circumstances which necessitated its development.

Background

The phenomenal growth enjoyed by the Japanese economy in the years following World War II is often credited to the Japanese utilization of an economic model which focused on the introduction and adaptation of pre-existing foreign technology, applied by an industriousness, obedient and teamwork orientated workforce. This confluence of factors contributed to Japan becoming highly competitive in manufacturing and assembly. However, the emphasis on introduction and adaptation, rather than innovation, and teamwork and obedience, rather than individual creativity, is now recognized as hampering the capacity of the Japanese economy to move forward in the era of information technology, with its premium on high value-added intangible products. This realization prompted the release of the Intellectual Property Policy Outline and the Basic Law.

continued on page 7

GLOBAL eCOMMERCE LAW AND BUSINESS REPORT

Published by WorldTrade Executive, Inc.

EDITORIAL STAFF
WorldTrade Executive, Inc. staff involved with ***Global eCommerce Law and Business Report*** includes:
PUBLISHER: Gary A. Brown, Esq.; CONTRIBUTING EDITORS: Alex McCallum, Scott P. Studebaker, Esq.
ASSISTANT EDITOR: Dana Pierce; BUSINESS MANAGER: Ken Parker

Global eCommerce Law and Business Report is published 12 times per year by WorldTrade Executive, Inc., P.O. Box 761, Concord, MA 01742 USA. Tel: (978) 287-0301; Fax: (978) 287-0302. Electronic Mail: [info@wtexec.com].
Home page: http://www.wtexec.com. Subscriptions: $641 per year; $691 non-U.S. addresses.

Effect of European Union Enlargement on Community Trademark Law

BY LISA M. TITTEMORE (BROMBERG & SUNSTEIN LLP)

Ten new countries will join the European Union on May 1, 2004 ("date of accession").[1] Rights arising under a Community Trademark ("CTM") application filed prior to the date of accession will automatically be extended to the new countries joining the European Union (this is also true for CTM applications filed after the date of accession that claim priority prior to the date of accession).

Enlargement of the European Union will also result in possible obstacles to registration for CTM applications, including new issues relating to descriptiveness, non-distinctiveness, and genericness, and a larger pool of potential opposers claiming prior use. It is also likely that official filing fees will increase, perhaps as much as US$1,000-2,000 with the addition of new countries.

For example, a CTM application filed after the date of accession may be refused registration as being descriptive, non-distinctive or generic in one of the new member countries, but if it had been filed prior to the date of accession, would be automatically extended to provide the owner with rights in the new member countries without being subject to refusals because of problems in the new countries. In other words, after the date of accession, the trademark RYBA for fish would be refused registration as being generic (ryba is the Polish word for fish), but if the application had been filed prior to the date of accession, this issue would not have precluded the owner from obtaining a CTM registration (although third parties in Poland would still be able to make fair use of the term RYBA under CTM rules).[2]

Thus, there are a number of advantages to getting a CTM application on file prior to May 1, 2004.

There is further additional benefit to filing new CTM applications before November 1, 2003, as owners of prior national trademark rights in a new member country will be able to file oppositions based on those national rights against new trademark applications filed after the date of accession and against CTM applications filed up to 6 months before the accession of the new member country, namely, applications filed after November 1, 2003.[3] Accordingly, "filing often and early" has special meaning for trademark owners in light of the upcoming European Union enlargement. ❑

Enlargement of the European Union will also result in additional possible obstacles to registration for CTM applications, including new issues relating to descriptiveness, non-distinctiveness, and genericness, and a larger pool of potential opposers claiming prior use.

[1] See note below on EU enlargement, p.3.

[2] If the trademark is considered to be against public policy or accepted principals of morality in the new member country, then use may be prohibited in that country even if the application was filed prior to the date of accession.

[3] The owner of earlier rights (e.g., rights arising from national applications or registrations, International Registrations under the Madrid Agreement or Protocol, and unregistered trademark rights such as common law rights, acquired prior to the date of accession) in a new member country will have the right to exclude the use of an automatically-extended CTM application in that country unless the earlier rights are invalid or were obtained in bad faith. The owner of earlier rights in a new member country will not be able to use those rights to oppose or revoke an automatically-extended CTM application or registration; it can only prevent use of the trademark in that country.

Lisa M. Tittemore is a Partner at Bromberg & Sunstein LLP in Boston, MA.

European Union Enlargement

Currently, the European Union includes the following countries: Austria, Belgium, Luxembourg, Netherlands, Denmark, France, Finland, Germany, Greece, Ireland, Italy, Portugal, Spain, Sweden, and the United Kingdom. Thirteen additional countries have applied to join the European Union, and ten of these countries, namely, Cyprus, the Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, the Slovak Republic, and Slovenia, known as the "acceding countries," are set to join on May 1, 2004. Bulgaria and Romania are hoping to join in 2007. Turkey, another applicant, is not currently negotiating its membership. Applicants must conform to the Copenhagen criteria, which require that the country meet certain economic and political conditions, including that the country be a stable democracy, have a functioning market economy, and adopt the common rules, standards and policies that make up European Union law.

New European Community Design Law

BY LISA M. TITTEMORE (BROMBERG & SUNSTEIN LLP)

Is your product design an important business asset? Are your products being sold in Europe? Under a new law recently enacted by the European Union, enhanced protection for product designs is now available throughout the entire European Union.[1] The new law provides a European Union-wide mechanism for registration and enforcement of rights in product designs for the first time. Under this new law, protection for unregistered product designs took effect on March 6, 2002, and protection for registered product designs took effect on April 1, 2003. [2]

In general, the new law provides owners of product designs the exclusive right to use the design and to prevent others from using it, although protection for registered designs is broader than for unregistered designs. The new law is broader than many of the national design laws already in force in the European Union. It also covers a greater number of European Union countries than the international system of the Hague Agreement administered by the World Intellectual Property Organization.[3] The new law explicitly exists in tandem with other intellectual property laws.[4] Interestingly, the new law incorporates concepts drawn from patent, copyright and trademark law.

Under a new law recently enacted by the European Union, enhanced protection for product designs is now available throughout the entire European Union.

With respect to registration of product designs, the new law provides a number of additional advantages, including a single application, a single language of filing, a single administrative center, the possibility of filing a single application for multiple designs, and payment of fees to one entity rather than 15 separate countries. The new law also includes a provision that allows applicants to keep the design undisclosed for up to 30 months.

Covered Product Designs

Under the new law, the definitions of the terms "design" and "product" are quite broad. The term design generally refers to the outward appearance of a product.[5] The term product generally refers to industrial or handicraft items, and is defined to include graphic symbols and typographic typefaces.[6] Indeed, it appears that trademarks may be protected as Community designs. Thus, for example, it is possible for a trademark that is not inherently distinctive, which would not be protected under trademark law without proof that it had acquired distinctiveness through use ("secondary meaning"), could be protected under the Community design law until it acquires secondary meaning, and thereafter under the Community Trademark Act or national trademark law.

In order to be protected under the new law, the product design must be new and have individual character.[7] Product designs which meet the requirements of the new law are deemed "Community designs." Features or appearance of a product that are dictated solely by its technical function are not protected as Community designs.[8] There is no requirement that the design have an aesthetic quality (e.g., that it be "pleasing to the eye"), however. A design that is contrary to public policy or "accepted principals of morality" will also not be protected as a Community design.[9]

Registered Versus Unregistered Community Designs

Registration of product designs under the new law is worth careful consideration, as the new law provides for different levels of protection for unregistered and registered Community designs. Registered Community designs are protected from the date of filing of the application for an initial period of five years, which may be extended in five year increments up to 25 years.[10] A registered Community design gives its owner the exclusive right to make, offer, put on the market, import, export, stock, or use a product in which the design is incorporated or to which it is applied, and to prevent any third party not having the owner's consent from doing so ("Infringing Acts").[11] Not included in Infringing Acts are acts done privately and for non-commercial purposes; acts done for experimental purposes; and, acts of reproduction for citation or teaching, subject to certain limitations.[12]

Unregistered Community designs are protected for a period of three years from the date on which the design was first made available to the public within the European Union.[13] The unregistered Community design gives the owner the right to prevent Infringing Acts, but only if the Infringing Acts result from copying the protected de-

sign. Thus, independent design will not be a defense in the case of registered Community designs, but, in light of this copying requirement, would be a defense in the case of unregistered Community designs.[14]

Another important defense against a claim with respect to infringement of a registered Community design is the "right of prior use." This right entitles third parties to exploit a design for purposes for which it had been used or for which serious and effective preparations had been made to use it before the priority date of the registered Community design. The right of prior use cannot be licensed and cannot be transferred apart from a transfer of the relevant part of the business, however.[15]

The Application Process

Applications for registration of Community designs may be filed with the Office of Harmonization in the Internal Market ("OHIM"), the same agency that handles registration of trademarks under the Community Trademark Act, or at the central industrial property office of a participating country.[16] A registration fee of 230 Euro per design must be made at the time of filing the application, along with a publication fee of 120 Euro per design if publication is not deferred or 40 Euro if deferment of publication is requested (with an additional 120 Euro fee at the time publication is requested). Applications may be filed for multiple designs, and additional fees per design are charged on a reduced basis, depending on the number of additional designs.[17]

A 12 month "grace period" is provided for registered Community designs. This means that a disclosure of the design made by the designer or successor in title made during the 12 months prior to the date of filing, or if priority is claimed, prior to the date of priority, will not be considered to affect the new and/or individual character of the design.[18] In other words, registration may still be sought even if the design has already been disclosed, provided that the disclosure falls within this 12 month period. Thus, a Community design may be protected as an unregistered design for the first 12 months after it has been disclosed and thereafter may be protected as a registered design as long as timely application is made. This provision was provided in order to allow owners of product designs time to "test the products embodying the design in the market place before deciding whether the protection resulting from a registered Community design is desirable."[19]

OHIM review of the Community design applications is limited to determining whether the application meets the formal requirements and whether requirements relating to priority claims are satisfied. OHIM will also refuse registration if the design does not conform to the statutory definition or is contrary to public policy.[20] OHIM will not examine whether the design conflicts with prior designs. There is no opposition period provided prior to registration.

Publication may be deferred for a period of 30 months from the date of filing, or if priority is claimed, from the date of priority. Upon registration, the design will be published in the Community Design Bulletin, unless the applicant requests deferment of publication.[21] OHIM is required to maintain a register of Community designs, which is open for public inspection (except that, in the case of a request for deferred publication, only limited information will be provided during the deferment period).[22]

The new law provides owners of product designs the exclusive right to use the design and to prevent others from using it, although protection for registered designs is broader than for unregistered designs.

Invalidity and Infringement Proceedings

Challenges to Community designs, including claims of conflict with prior designs are addressed by means of an application for a declaration of invalidity, which is an inter-partes procedure.[23] Applications for invalidity in connection with registered Community designs may be filed with OHIM or one of the Community Design Courts, which are to be identified by each member state pursuant to the new law.[24] In the case of an unregistered mark, the application of invalidity may only be filed in one of the Community Design Courts.

The Community Design Courts also have exclusive jurisdiction over infringement actions, and, if permitted under national law, actions relating to threatened infringement and actions for declaration of non-infringement. Although the Community design law provides significant uniformity, it is worth noting that matters not covered by EC 6/2002 will be subject to the national law of the Community Design Court where the action takes place.[25]

continued on page 6

New Law **from page 5**

Possible sanctions for infringement include European Union-wide injunctive relief, seizure of infringing products, notably, seizure of equipment used to manufacture the infringing goods, "if their owner knew the effect for which such use was intended or if such effect would have been obvious in the circumstances." Other possible sanctions include "sanctions appropriate under the circumstances which are provided by the law of the Member State in which the acts of infringement or threatened infringement are committed, including its private international law."[26] Thus, sanctions could vary depending on where the alleged infringing conduct occurs.

In order to be protected under the new law, the product design must be new and have individual character.

Conclusion

Despite some variation depending on where allegedly infringement conduct occurs and where enforcement actions are initiated, the new Community design law provides significant uniformity and expanded protection for product designs in the European Union. In light of the new law, owners seeking to protect rights in product designs should consider whether to seek registration under the new law. ❑

---

[1] As of May 1, 2004, the European Union will include ten additional countries. See Sidebar, p. 3 of this issue.
[2] The new law is set forth in Council Regulation (EC) No. 6/2002 of 12 December 2001 on Community Designs ("EC 6/2002"). Commission Regulation (EC) No 2245/2002 of 21 October 2002 is the implementing regulation for EC 6/2002. Both are available at http://oami.eu.int/en/design/legalaspects.htm.
[3] The international system of the Hague Agreement is applicable in Germany, Belgium, Spain with limited effect, France, Greece, Italy, Luxembourg, Netherlands, and certain other non-European Union countries.
[4] EC 6/2002 Article 96.
[5] The term "design" is defined as "the appearance of the whole or a part of a product resulting from the features of, in particular, the lines, contours, colours, shape, texture, and/or materials of the product itself or its ornamentation." EC 6/2002 Article 3.
[6] The term "product" is defined as "any industrial or handicraft item, including *inter alia* parts intended to be assembled into a complex product, packaging, get-up, graphic symbols and typographic typefaces, but excluding computer programs." EC 6/2002 Article 3. Computer programs are protected under other intellectual property laws in the European Union, such as copyright law.
[7] A design is considered to be "new" if no identical design has been made available to the public prior to, for unregistered designs, the date on which the design has first been made available to the public, and, for registered designs, the date of filing of the application for registration or, if priority is claimed, the date of the claimed priority. Designs are deemed identical if their features differ only in immaterial respects. EC 6/2002 Article 5. A design is considered to have "individual character" "if the overall commercial impression it produces on the informed user differs from the overall impression produced on such a user by any design which has been made available to the public" prior to, for unregistered designs, the date on which the design has first been made available to the public, and, for registered designs, the date of filing of the application for registration or, if priority is claimed, the date of the claimed priority. EC 6/2002 Article 6.
[8] EC 6/2002 Article 8.
[9] EC 6/2002 Article 9.
[10] EC 6/2002 Article 12.
[11] EC 6/2002 Article 19.
[12] Also not subject to Community design law are equipment on ships and aircraft registered outside of the European Union when they temporarily enter the European Union. EC 6/2002 Article 20.
[13] Under the new law, an unregistered Community design is "deemed to have been made available to the public within the Community" if it has been published, exhibited, used in trade or otherwise disclosed in such a way that, in the normal course of business, these events could reasonably have become known to the circles specialised in the sector concerned, operating within the Community." Proof of this disclosure is required for enforcement of an unregistered Community design. EC 6/2002 Article 11.
[14] EC 6/2002 Article 19.
[15] EC 6/2002 Article 22.
[16] EC 6/2002 Article 35.
[17] EC 6/2002 Article 37.
[18] Priority of six months from the date of filing of the first application may be claimed pursuant to the Paris Convention by a person who has filed an application for a design right or for a utility model, including a design patent, in or for "Any State party to the Paris Convention for the Protection of Industrial Property, or to the Agreement establishing the World Trade Organization, or his successors in title." Priority of six months from the date of exhibition at an officially recognized international exhibition may also be claimed. EC 6/2002 Articles 41 and 44.
[19] EC 6/2002 Introductory ¶ 20.
[20] EC 6/2002 Articles 45-47.
[21] EC 6/2002 Article 50.
[22] EC 6/2002 Article 72.
[23] EC 6/2002 Articles 25, 26 and 52-54.
[24] EC 6/2002 Articles 80 and 81.
[25] EC 6/2002 Article 88.
[26] EC 6/2002 Article 89.

Lisa M. Tittemore is a Partner at Bromberg & Sunstein LLP in Boston, MA.

Japan from page 2

Intellectual Property Policy Outline and the Basic Law

While the Intellectual Property Policy Outline was well received for the number of specific measures it advocated and the setting of concrete timelines to achieve those measures (mainly by fiscal year 2005), the Basic Law does not mandate a specific time-frame for the achievement of its goals.

In fact, the Basic Law goes no further than to state that specific objectives and time limits for achieving those objectives should, *in principle* be set for the achievement of measures in relation to the creation, protection and exploitation of intellectual property.

Objectives of the Basic Law

The objective of the Basic Law is to increase the international competitiveness of Japanese industry through the development of measures for the:

(i) creation,
(ii) protection; and
(iii) exploitation of intellectual property.

The Basic Law does not descend into detail with regards to these measures, however. Instead, the Basic Law imposes sweeping obligations on the State, local government, tertiary education institutions and businesses to advance the aims of the Basic Law through the implementation of basic measures. The obligations are not detailed, and do not have quantifiable objectives. Accordingly, there are no punitive measures for failure to meet obligations.

However, the Basic Law does provide for the establishment of a concrete goal with respect to the establishment of the Intellectual Property Policy Headquarters (which was established in Cabinet this year). The Basic Law requires the Intellectual Property Policy Headquarters to develop a Promotion Program which must set forth basic policy and measures for the creation, protection and exploitation of intellectual property.

Obligations of the State

The Basic Law obliges the state, local government, universities and businesses to assume responsibility for the formulation and implementation of measures for the creation, protection and exploitation of intellectual property. The measures include:

(i) strengthening cooperation between the State, local government, universities and business (Article 9);
(ii) promotion of research and development (Article 12);
(iii) improvement of procedures to enable enterprises to promptly secure rights with respect to intellectual property (Article 14):
(iv) increasing the speed and effectiveness of legal proceedings and alternative dispute resolution systems, etc, in relation to intellectual property (Article 15);

The Basic Law obliges the state, local government, universities and businesses to assume responsibility for the formulation and implementation of measures for the creation, protection and exploitation of intellectual property.

(v) measures against infringement in the Japanese domestic market (Article 16);
(vi) measures for the protection of intellectual property owned by Japanese nationals or juridical entities overseas and the promotion of systems which will achieve that objective (Articles 16 and 17);
(vii) conducting research on intellectual property and providing the results of such research to enterprise (Article 20);
(viii) promotion of education of the public about intellectual property (Article 21); and
(ix) securing and developing human resources with technical knowledge on intellectual property.

While the Basic Law has and will make further progress in the area of intellectual property, considering the non-specific nature of the objectives, and the lack of time frames for the achievement of objectives, the implications of the Basic Law for enterprise in Japan and the efficacy of the Basic Law in promoting the creation, protection and exploitation of intellectual property in Japan will not be able to be determined at any time in the near future. ❑

Kym Bavcevich (bavcevichk@coudert.com) is an Associate with Coudert Brothers LLP in Tokyo. Shintaro Kuroda (kuroda@yglo.gr.jp) and Norimasa Togashi (togashi@yglo.gr.jp) are Associates with Yodoyabashi Godo L.P.C. in Tokyo.

¡Viva La Revolución! Mobile Data Technology in Latin America

BY PATRICK J. O'CONNOR (GRAY, CARY, WARE & FREIDENRICH)

[Editor's Note: This article examines the role new mobile data technologies will play in the evolving Latin American telecommunications and e-commerce market.]

Introduction

The market for mobile communications services in Latin America demonstrates several unique characteristics when compared to other markets around the world. Differences both result from and emphasize the nature of the demand for wireless services in the region, the socio-economic characteristics of the bulk of Latin American subscribers, and their unique cultural and demographic characteristics. First and second generation wireless communications technologies and services, with an emphasis on voice and limited data applications, have evolved to take advantage of these characteristics and have thereby surpassed wireline telephony as the primary means of communicating in Latin America today. Wireless data technologies have lagged behind in part because practical and affordable data solutions have not yet been developed.

In order for mobile data to be successful in Latin America, device manufacturers, service and content providers must come together to answer pressing questions about billing and revenue sharing.

As this article presents in more detail, a profitable mass of Latin American data consumers is not a reality, but an eventuality that depends on the development of solutions targeted at the unique characteristics of the Latin American market.[1] Manufacturers and service providers that recognize these unique characteristics and develop accordingly will share in wireless data revenues of an estimated $17 billion by 2006.[2]

Lessons from the Wireless Experience

Two major differences between wireless communications solutions in Latin America and those in North America are readily apparent. First, in the late-1990s Latin America adopted a European-style Calling Party Pays (CPP) system in which the initiator of a telephone call pays a premium for contacting the mobile subscriber, while the terminating mobile subscriber pays nothing. In contrast, the premium associated with mobile service in North America is assessed on the wireless subscriber, and the call initiator is charged a non-premium rate that is the same whether the outgoing call is to a landline or wireless telephone. Second, some 80 percent of wireless communications revenues are based on pre-paid services in Latin America.[3] In the pre-paid system, subscribers purchase a specified usage amount, usually in the form of a pre-paid calling card, and draw from the usage amount as calls are placed. In contrast, the market for wireless services in the United States is 80 percent post-paid, in which subscribers are billed for monthly charges after service has been rendered.[4] Together, these differences have created ownership and wireless service usage incentives for Latin American consumers, resulting in tremendous revenue-generation.

The combination of the CPP system with pre-paid service promotes ownership of wireless devices. Pre-paid services normally require that the subscriber periodically "recharge" his account in order to keep the service active. Because the call originator pays all termination costs, this minimal service maintenance charge is quite likely the only cost assessed on the pre-paid wireless subscriber. As a result, wireless service in Latin America is infinitely more affordable to businesses and individuals of limited means.

By recognizing that the mobile party pays and post-paid mobile service solutions employed by the rest of the world were inappropriate for Latin America, mobile service providers were able to creatively address the unique socio-economic and cultural characteristics of their region. The implementation of CPP encouraged potential users to obtain and maintain mobile accounts, if only to be able to receive calls. The addition of pre-paid solutions further encouraged wireless adoption by minimizing the service maintenance charge associated with mobile service. Wireless service providers thereby

capitalized on the network effects inherent in communications technologies: the more subscribers that participate, the more valuable the service becomes to each individual subscriber because he is able to reach more people. In this instance, device manufacturers, service providers and, indeed, the economy as a whole benefited from the creative development and implementation of culturally-appropriate solutions.

Seeking a Latin America Data Solution

Applying the lessons of wireless telephony to the development of data solutions for Latin America, it seems apparent that the systems implemented in North America, Europe and Asia may not be a perfect fit. Indeed, there are several characteristics of the Latin American data market that make it as, if not more, unique than the market for mobile voice services.

First, wireless technologies are much more widely adopted in Latin America than wireline technologies.

Second, Latin America does not have the installed base of desktop computer users that exists in, for example, North America. In this sense, Latin America is much more like Asia in that consumers are not prejudiced against small screen mobile solutions.

Third, the bulk of Latin American consumers come from a different socio-economic class than wireless subscribers in the North America, Europe and Asia. For this reason, the cost of the end product must be foremost in the mind of anyone developing a data solution for Latin America.

Finally, the embedded characteristics of the wireless market in Latin America, including CPP and pre-paid subscribers, raise a host of billing and revenue-sharing problems that must be answered prior to the introduction of data solutions.

Currently, there are 15 percent more mobile lines in Latin America than traditional landlines.[5] In the decade of the 1990s, wireless adoption in Latin America grew an astonishing 39,000 percent, from 100,000 in 1990 to 39 million in 1999.[6] Moreover, for reasons of both cost and efficiency, the rate of adoption of wireless technologies in Latin America far outpaces the rate of landline adoption. In short, wireless is the communications technology of both the present and the future in Latin America. No other medium can presently rival wireless' ability to get new services to the bulk of the population. As a result, any data solution that is to reach the mass of Latin American businesses and consumers, and provide the revenue to survive, must be based on the evolving wireless platform.

A wireless data solution makes more sense in Latin America than it does in, for example, the United States. Simply stated, many Americans have grown accustomed to the large screen data solutions that they use at home and at the office. Up to this point in the evolution of the Internet, the vast majority of the content has been designed to serve this audience with media-rich information and applications. As a result, there is an inherent bias against a streamlined, information-focused small screen data services. Americans find tiny screens and tiny keyboards unfulfilling and, as a result, the United States has largely failed to adopt the 2.5 and 3G wireless data solutions offered by existing carriers.

Despite the hurdles faced by service and content providers, there is good reason to believe that next-generation devices are poised for widespread adoption in Latin America.

The same situation does not exist in Latin America. The predicted number of mobile handset owners dwarfs comparable figures for new personal computers in the region: while the number of homes with traditional personal computers is expected to more than double over the next five years (to 13.5 million),[7] the number of mobile subscribers is expected to triple (to 220 million) over the same period.[8] Latin Americans are far less familiar with the large screen Internet experience and far more comfortable with mobile technologies. The bias, if one may be said to exist, is against large screen solutions and in favor of small screen mobile computing.

Ultimately, however, the rate of adoption will not be based on the size of the screen so much as the cost of the device. The reason that CPP and pre-paid services have been so successful in Latin America is that they make mobile phone use a possibility for all levels of Latin American society. The cost of the device itself is a determining factor in whether the average Latin American consumer can afford

continued on page 10

Latin America **from page 9**

wireless voice service. As previously stated, after the purchase of the device, most service providers require only a minimum service maintenance charge to keep the account active. And under the CPP system, incoming calls are free. Thus, one of the keys to adoption of wireless data solutions in Latin America is the cost of the device itself. One of the several reasons that desktop computing is not popular in Latin America is that the cost of a personal device is prohibitive. With an average income of $3,400 per year,[9] a $1000 computer is out of the question for most Latin Americans. In the same way, the vast bulk of Latin Americans will not be able to afford to pay $500 for a data-capable device. Fortunately, next-generation data-capable devices currently cost approximately 35 percent more than second-generation handsets in Japan, or about $200 to $300.[10] Moreover, data-capable handsets, like their voice-only predecessors, are likely to become more of a commodity than a luxury, and price will continue to decrease significantly. Industry experts agree that Latin Americans will realize, as they did with wireless telephony, that the convenience and usefulness of owning a data-capable handset is worth the minimum investment required.

Major telecommunications companies are confident that "Latin Americans will pay for Internet-ready handsets they can use for chatting, sending short text messages and Web browsing."

In fact, and as evidenced by wireless adoption rates, Latin Americans are notoriously good adopters of new technologies.[11] And the adoption of data-capable devices should be no exception.

Major telecommunications companies are confident that "Latin Americans will pay for Internet-ready handsets they can use for chatting, sending short text messages and Web browsing."[12] The Strategis Group predicts that the number of mobile Web users in the region will grow from 1.4 million today to more than 47 million by 2007, an increase of over 3,300 percent;[13] and the Yankee Group estimates that the Latin American mobile data market will grow to nearly $17 billion by 2006.[14]

However, in order for mobile data to be successful in Latin America, device manufacturers, service and content providers must come together to answer pressing questions about billing and revenue sharing. The average revenue per user in Latin America does not approach that of some other regions of the world. As a result, device manufacturers, service and content providers have a smaller pie to share. Moreover, the predominance of pre-paid subscribers means that revenue is made in advance of use of the service.

Therefore, if available services, including voice, Internet access, e-commerce and other applications, are provided by several different entities, a revenue-sharing scheme must be developed to divide the revenue already paid by the subscriber. In addition, for value-added services, including a variety of e-commerce applications, billing systems must be developed to divert revenue from the subscriber or wireless service provider to the value-added service provider.

All of these issues will take time to solve; nevertheless, it should not be doubted that, where there is money to be made, providers will work together toward a viable solution.

Next-Generation Technologies

Despite the hurdles faced by service and content providers, there is good reason to believe that next-generation devices are poised for widespread adoption in Latin America. First, the Latin American public is already familiar with mobile wireless technology. Second, wireless networks are ubiquitous throughout the region. Finally, the costs of next-generation devices and data transport are rapidly decreasing. The convergence of these factors points to an evolution of the wireless market in Latin America from voice and limited data to voice and robust data. To the extent that this evolution continues to address the needs and socio-economic characteristics of the Latin American populace, it should introduce millions of Latin Americans to the worlds of mobile data and the Internet.

The Latin American public is already familiar with mobile wireless technology. To the extent that moving to data networks can be presented as moving from an inferior handset to a superior handset, much of the fear inherent in being introduced to computing and the Internet should dissipate. This means that Latin Americans will more readily adopt wireless data solutions. Moreover, to the extent that current

mobile subscribers are familiar with service activation and billing systems, that knowledge may be transported into the mobile data context.

Further, wireless networks, in their first and second-generation incarnations, are ubiquitous throughout Latin America today. As a result, many of the siting and network equipment deployment problems have largely been solved. The move to mobile data services requires only a simple (but often expensive) upgrade of the network.

According to industry sources, the first 3G networks in Latin America should be operational by the end of this year. In contrast, the introduction and buildout of new technological solutions often requires that difficult infrastructure deployment questions be answered well before any service is provided.

As data networks are rolled out as a replacement for or on top of existing voice networks, creative infrastructure-sharing arrangements may permit companies to share the costs of network buildout and decrease the cost to the consumer even further.

Finally, the costs of device manufacture are decreasing with each new model release of voice and data capable devices.

Manufacturers are rapidly approaching the price point that will make data solutions affordable for the mass of the Latin American market. Moreover, the costs of data transport in the region and throughout the world are rapidly decreasing.

Overbuilding has led to a glut of fiber optic cable and the transport infrastructure necessary to aggregate and transmit large amounts of data over long distances. That same overbuild has led many companies into bankruptcy. Surviving carriers have become the beneficiaries, as they have been able to pick up transport infrastructure required for advanced services for pennies on the dollar.[15]

Conclusion

A number of unique characteristics define the Latin American wireless market. CPP and pre-paid services are two creative accommodations to these differences that have permitted wireless voice services to reach new subscribers at all socio-economic strata.

Among these characteristics, the familiarity with wireless devices and the low penetration rate of home computers make Latin America a particularly fertile ground for introduction and development of next-generation data solutions. Assuming that providers can address problems of network upgrades, billing and revenue sharing, Latin America is poised to be at the forefront of the evolution of mobile data technologies. ❑

---

[1]"Declaracion de la II Cumbre de presidentes de Alacel," Revista Alacel, Year 1, Number 1 at 14 (March, 2003).

[2]"Los datos salvarán a la industria cellular," Revista Alacel, Year 1, Number 1 at 17 (March, 2003) (citing Yankee Group, January, 2002).

[3]Discussion Panel, "Los desafíos económicos en Latinoamerica," Alacel Annual Latin-American Conference, Wireless 2003 (March 18, 2003).

[4]Id.

[5]"Las ventajas de 'El que llama paga,'" Revista Alacel, Year 1, Number 1 at 6 (March, 2003).

[6]Patrick J. O'Connor, "Growth Ahead for Latin America's Telecom Sector," *Latin American Law and Business Report*, Volume 11, Number 01 at 20 (January 31, 2003) (citing International Telecommunication Union, Americas Telecommunication Indicators 2000, April 2000 at 1 ("Americas Indicators")).

[7]Numero de Hogares con PCs en los mayores mercados de Latinoamerica, 2001-2005, Jupiter Research, 2000 (found at <http://www.punto-com/punto/esp/_GRAFICAS/__hogares-pc.htm>).

[8]Deborah Mendez-Wilson, "Latin America's Golden Opportunity," Wireless Week, March 27, 2001 (citing a recent study by StarMedia Network, Inc.).

[9]"Las ventajas de 'El que llama paga,'" Revista Alacel, Year 1, Number 1 at 6 (March, 2003).

[10]Kiyoshi Takenaka, "DoCoMo Unveils New Handsets to Recharge Flagging 3G," ISPWorld, December 10, 2002.

[11]Deborah Mendez-Wilson, "Latin America's Golden Opportunity," Wireless Week (March 27, 2001) (Alfonso Riveroll Pietri, CEO of Miami-based startup Conectium, states, "Latin Americans are kind of gadgety people. We like gadgets.").

[12]Deborah Mendez-Wilson, "Latin America's Golden Opportunity," Wireless Week, March 27, 2001.

[13]Deborah Mendez-Wilson, "Latin America's Golden Opportunity," Wireless Week, March 27, 2001.

[14]"Los datos salvarán a la industria cellular," Revista Alacel, Year 1, Number 1 at 17 (March, 2003) (citing Yankee Group, January, 2002).

[15]Peter J. Howe, "Bargain hunters profit from telecom collapse," *Boston Globe* (March 31, 2003) (available at http://www.boston.com/dailyglobe2/090/business/Bargain_hunters_profit_from_telecom_collapse.html>).

Patrick J. O'Connor is an attorney specializing in antitrust and telecommunications law and policy with Gray, Cary, Ware & Freidenrich in Washington, DC.

Survey **from page 1**

cific region. The complete survey results are published in this and next month's issue of *Global eCommerce Law and Business Report*. (See charts on pages 13-18)

Companies should consider undertaking a privacy audit to determine how their data transfer and other privacy-related policies and practices compare with the laws and rules of the jurisdictions in which they are subject.

The research found that 11 of the surveyed jurisdictions treat cross-border data transfers differently from those moved only within their domestic borders, and five more jurisdictions have laws proposed or pending that would affect cross-border data transfers differently from transfers within their borders.

Moreover, 12 of the jurisdictions impose restrictions of various kinds on moving personal data across borders, and five others would do so under proposed or pending new laws. Of the nations surveyed, only China, Japan and the United States permit such data transfers generally unimpeded.

The survey covers eight jurisdictions in Europe: France, Germany, Hungary, Italy, Poland, Russia, Spain and the United Kingdom; seven in the Asia-Pacific region: Australia, China, Hong Kong, Japan, Malaysia, South Korea and Thailand; and seven in North America: Canada, Mexico and the United States, as well as the Canadian provinces of Ontario and Quebec and U.S. states of California and New York. These four prominent non-sovereign jurisdictions were included because they have been particularly active in the privacy law area.

Most jurisdictions surveyed treat cross-border information flows differently than they do data exchanges within their domestic jurisdiction. The US, including New York and California, Canada (at the federal level), China, and Japan are the key exceptions.

Key findings of the survey include the following:

- Most jurisdictions surveyed treat cross-border information flows differently than they do data exchanges within their domestic jurisdiction. The US, including New York and California, Canada (at the federal level), China, and Japan are the key exceptions. In addition, France, Malaysia, Mexico, Thailand and Ontario are considering proposals that would impose different requirements on cross-border and internal transfers.
- Twelve jurisdictions restrict data flows across borders, and five, Hong Kong, Malaysia, Mexico, Thailand and Ontario, currently are considering proposals to do so. Those without such restrictions are China, Japan, the United States, and the two U.S. states in the survey, California and New York.
- The European Union's Data Protection Directive has become a benchmark by which many jurisdictions measure the adequacy of their data-transfer controls. The Directive permits transfer of data to non-EU jurisdictions where the receiving jurisdictions provide an "adequate level" of privacy protection. Indeed, the Eastern European countries seeking to join the EU are in some cases already bringing their laws into compliance with the Directive.
- Of the 12 jurisdictions that have restrictions on cross-border transfers, and five now considering them, all would permit transfers with the consent of the data subject. Most require "opt in" consent, in which the data subject must affirmatively give consent. Australia, the United Kingdom and Quebec permit "opt out" consent, in which the data subject must affirmatively withdraw consent in order to prevent data from being transferred outside the jurisdiction.

For multinationals that transport data across borders, the survey findings underscore the need to be mindful of some key points. First, multinationals should consult counsel knowledgeable about cross-border transfer laws in the particular jurisdictions where their companies do business to ensure they are in compliance with current laws and to plan accordingly as new laws emerge. Second, companies need to review their current data privacy polices and determine if they are being implemented properly. Third, companies should consider undertaking a privacy audit to determine how their data transfer and other privacy-related policies and practices compare with the laws and rules of the jurisdictions in which they are subject. For example, our firm has developed a privacy audit methodology, a patent for which is pending, that examines a company's data protection policies and practices so as to bring them into conformity with the laws in each jurisdiction where the company collects or processes personally identifiable information.

Though the spreading thicket of privacy laws around the world can be a major challenge for multinationals, foresight and preparation can help keep the headaches of compliance under control. ❑

Robert L. Raskopf chairs White & Case's E-Commerce, Media and Technology Group. He regularly counsels multinational clients concerning compliance with the growing global privacy data requirements. He also litigates cases in which personal and professional privacy, sensitive business information and law enforcement interests are weighed against common law and First Amendment rights to information.

White & Case LLP 2003 Data Protection Survey

For more information about this survey or data privacy issues in general, contact David Bender, Counsel, White & Case LLP, at 212-819-8649, dbender@whitecase.com or visit www.whitecase.com.

Question 1: ***Does your jurisdiction treat cross-border transfer differently than onward transfer within your jurisdiction?***

AUSTRALIA – Yes.	**CANADA – FEDERAL** - No.	**CANADA – ONTARIO DRAFT LEGISLATION** - Yes. Privacy of Personal Information Act ("PPIA") (draft legislation), § 28(1).
CANADA – QUEBEC - Yes. An Act Respecting the Protection of Personal Information in the Private Sector ("APPIPS"), § 17.	**CHINA** - No.	**FRANCE** - Not under current law. However, draft law ("Draft Law No. 1")[1] implementing the EU Data Protection Directive 95/46/EC contains specific provisions regarding cross-border transfers.
GERMANY - Yes.	**HONG KONG** - Yes. Section 33 of the Hong Kong Personal Data (Privacy) Ordinance ("PDPO") (not yet in effect) places restrictions on cross-border transfers.	**HUNGARY** - Yes.[2]
ITALY - Yes.	**JAPAN** - No.[3] There are no specific provisions in the applicable privacy legislation dealing with the transfer of personal data to countries outside Japan.	**MALAYSIA**[4] - Not under existing law. However, the proposed Malaysian Personal Data Protection Bill would treat cross-border transfer differently than onward transfers within Malaysia.
MEXICO – FEDERAL - No, but proposed law would differentiate between cross-border transfers and other transfers.	**POLAND** - Yes.	**RUSSIA** - Yes. Russian law allows processing of personal data only with the consent of a data subject or pursuant to a court decision.[5] This requirement applies to both internal and cross-border transfers. However, cross-border transfers are also subject to additional requirements. In particular, the Federal Law governing international information exchanges requires Government permission for cross-border transfer.[6]
SOUTH KOREA[7] - Yes.	**SPAIN**[8] - Yes.	**THAILAND** - There is currently no specific national legislation on data privacy in Thailand. However, a proposed national Data Protection Act ("Thai Privacy Bill") (not yet promulgated) would treat cross-border transfer differently than onward transfers within Thailand.
UK - Yes. Data Protection Act 1988 ("DPA"), Principle 8.	**UNITED STATES – FEDERAL** - No.	**UNITED STATES – NEW YORK & CALIFORNIA** - No.

[1] Draft Law No. 1 is currently being discussed by the French Parliament. It was adopted with amendments at first reading by the Sénat on April 1, 2003 and now returns to the Assemblée Nationale for second reading.

[2] N.B. The 1992 Hungarian Data Protection Act will be subject to certain revisions shortly to achieve full EU compliance. The Act should then reflect Directive 95/46/EC.

[3] We have not included reference to the new draft privacy legislation which we understand still has to go through the Japanese Diet. We have not seen a copy of the draft privacy legislation.

[4] Information on Malaysia provided by courtesy of Messrs. Shearn Delamore & Co. in Kuala Lumpur. The answers provided are based on the current version of the Malaysian Privacy Bill, which we understand from Malaysian counsel is due to be revised further. We do not have information at this stage as to what the amendments would be, or when the revised Malaysian Privacy Bill will be published.

[5] Federal Law No. 24-FZ "On Information, Informatisation and Information Protection", dated 20 February 1995, Article 11, and the Constitution of the Russian Federation, dated 12 December 1993, Article 24.

[6] Federal Law No. 85-FZ "On Participation in the International Informational Exchange", dated 4 July 1996.

[7] Information on South Korea provided courtesy of Messrs. Kim & Chang in Seoul, Korea.

[8] Prepared by the Mexico City office of White & Case LLP. Responses were prepared by Mexican attorneys not admitted to practice in Spain.

continued on page 14

Question 2: ***Does your jurisdiction place restrictions on cross-border transfer?***

AUSTRALIA – Yes. With regard to cross-border transfer, the National Privacy Principles ("**NPP**"), set out in the Federal **Privacy Act** 1988, provides for specific bases upon which such transfer may be carried out.	**CANADA – FEDERAL** - Yes. Cross-border transfers must comply with rules governing collection, use and disclosure.	**CANADA – ONTARIO DRAFT LEGISLATION** - Yes. Disclosure outside Ontario is not permitted unless the disclosing organization believes on reasonable grounds that the recipient will take appropriate steps to preserve confidentiality. PPIA, § 28(1).
CANADA – QUEBEC - Yes. Disclosure outside Quebec is not permitted unless the disclosing organization takes reasonable steps to ensure that the information will not be used for purposes other than those for which it was collected, or communicated to third persons without the consent of the persons concerned. For transfer of a list of names, addresses or telephone numbers of natural persons ("Nominative List) outside Quebec, the data subjects must be given a valid opportunity to refuse that the information be used for purposes other than commercial or philanthropic prospection. APPIPS, § 17.	**CHINA** - No.	**FRANCE** - Yes. Current law does not place restrictions on cross-border transfer. However, pursuant to Draft Law No. 1, transfer of personal data from France to non-EU countries is permitted to the extent that such countries provide an adequate level of protection for privacy rights and fundamental rights and freedoms of individuals with respect to the processing or intended processing of such personal data. The adequacy of protection will be assessed with respect to current regulations in force, applicable security measures, and specific characteristics of the data processing such as purpose and duration, as well as the nature, origin and destination of the processed data.
GERMANY – Yes.	**HONG KONG** - Yes. Section 33 of the PDPO prohibits the transfer of personal data to third countries save under certain exceptions.	**HUNGARY** - Yes.
ITALY - Yes. Article 28 of the Law of December 31st, 1996 ("Privacy Law"), generally requires the transfer of personal data to foreign countries to be notified in advance to the *Garante* (Data Protection Authority) if the country of destination is not a Member State of the EU or EEA.	**JAPAN** - No.	**MALAYSIA** - No restrictions under existing law. However, the Malaysian Privacy Bill contains provisions that prohibit transfer outside Malaysia save under certain exceptional circumstances, for data collected, held, processed or used in Malaysia, or controlled by a data user whose principal place of business is in Malaysia.
MEXICO – FEDERAL - No. But, pending Federal Personal Data Protection Law ("FPDPL") places restrictions on cross-border transfer.	**POLAND** - Yes.	**RUSSIA** - Yes.
SOUTH KOREA - Yes, in some situations. Restrictions on cross-border transfer are set out in the Real Name Financial Transaction and Guarantee of Secrecy Law ("RNL"), Protection and Use of Credit Information Law ("PUCIL"), and Information and Telecommunications Network Use Promotion and Information Protection Law ("ITL"), with respect to the following organizations: – financial institutions, including post offices (RNL, PUCIL) – small and medium sized enterprises, telecommunications service providers, etc. (PUCIL) – telecommunications and Internet service providers (ITL). RNL and PUCIL do not prohibit the transfer of data overseas as long as prior written consent is obtained from the data subject. This includes cases where the recipient third party is a branch or head office of the same corporation, based overseas. ITL prohibits the overseas transfer of critical information, such as high-technology developed in South Korea, but allows overseas transfer of other data if the data subject's written consent has been obtained.	**SPAIN** - Yes. Article 33 of the Spanish Data Protection Law (*Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal*, the "Data Protection Law") prohibits cross-border transfers except where prior authorization has been obtained from the Spanish Data Protection Agency (*Agencia de Protección de Datos*, the "Agency") or one of the derogations set out in Article 34 applies (see below). The Agency grants authorization in light of (i) the level of protection of the recipient's jurisdiction, (ii) the nature of the data, (iii) the purpose, duration and characteristics of the processing.	**THAILAND** - Yes. The **Thai Privacy Bill** prohibits the transfer of personal data outside Thailand, unless: (1) The recipient country provides protection of personal data at a level "materially equivalent" to the Privacy Bill, and reasonable efforts are made to ensure that the transferred data will be treated in a way so as not to contravene the **Thai Privacy Bill;** (2) The data subject has consented to such transfer; (3) The export of data is in compliance with a contract; or (4) The export of data is undoubtedly for the benefit of the data subject and it is not practicable to obtain consent.
UK - Yes. Transfers to any country or territory outside the European Economic Area ("EEA") are unlawful unless that country ensures an adequate level of protection for the rights and freedoms of data subjects.	**UNITED STATES – FEDERAL** - No.	**UNITED STATES – NEW YORK & CALIFORNIA** - No. Under the Commerce Clause of the US Constitution, the US Congress is vested with authority to regulate commerce among US states, and between the US and foreign nations. Therefore, although we found no existing state or local laws concerning cross-border transfer, any such state or municipal law would likely be unconstitutional, as unduly burdensome on interstate and foreign commerce, and therefore unenforceable.

Question 2(a): ***If so, to what nations?***

AUSTRALIA – No specified nations.	**CANADA – FEDERAL** - Does not restrict transfers to specific nations.	**CANADA – ONTARIO DRAFT LEGISLATION** - Does not restrict transfers to specific nations.
CANADA – QUEBEC - Does not restrict transfers to specific nations.	**CHINA** - N.A.	**FRANCE** - See response to 2 above.
GERMANY - Non-EU/EEA countries. However, even within the EU and the EEA cross-border data transfers are restricted if they are outside the scope of the EU Data Protection Directive (e.g. processing by national security institutions). The following answers assume that the transfer is within the scope of the Directive.	**HONG KONG** - Section 33 of the PDPO empowers the Hong Kong Privacy Commissioner to publish a list of countries to which cross-border transfer of data is permitted, on the basis that the transferee country has in force laws that are substantially similar to, or serves the same purposes as the PDPO. No list has yet been published.	**HUNGARY** - Article 2 of the 1992 Data Protection Act requires consent of the data subject and requires the recipient data processor to ensure adequate safeguards (i.e., protection equivalent to the level of protection in Hungary). This could be achieved, for example, via an agreement between the transferor and recipient obliging the recipient to comply with Hungarian law, as indicated by the data protection Commissioner in informal opinions. However, the law does not provide the Commissioner with the power to approve or prohibit data transfers. EU countries are generally considered to provide equivalent protection. However, a strict interpretation of the Hungarian law indicates that consent is also required.
ITALY - Cross border transfers to non-EU/EEA countries are prohibited where the laws of the country of destination or transit do not ensure adequate protection (Art. 28, paragraph 3). Transfers to Switzerland and Hungary are permitted pursuant to the Garante's general authorization of October 17, 2001 (reflecting Commission Decision 2000/518/EC on Switzerland and Decision 2000/519/EC on Hungary). The Garante has not yet issued such a general authorization in respect of transfers to Canada, despite Commission Decision 2002/2/EC.	**JAPAN** – N. A.	**MALAYSIA** - Under the Malaysian Privacy Bill, the Minister may specify any nation where he has reasonable grounds for believing that there is in force any law which is substantially similar to or serves the same purpose as the Bill or that place ensures an adequate level of protection.
MEXICO – FEDERAL - The proposed FPDPL would prohibit all cross-border transfers to countries and international or supranational organizations with inadequate data protection laws, considering such factors as the nature and purpose of the data processing, as well as the level of protection of the recipient country.	**POLAND** - The transfer of personal data to countries which do not provide a level of protection equivalent to that of Poland is restricted. It is assumed that EU countries which have implemented the 95/46/EC Directive provide equivalent protection.	**RUSSIA** - The same rules apply to all nations.
SOUTH KOREA - So long as a legitimate consent is obtained for the transfer, there is no specific provision listing restricted nations under privacy laws. However, in case of North Korea, depending on the nature of the underlying transaction, compliance with other laws that provide for relationship with North Korea should be examined.	**SPAIN** - Article 34(k) permits transfers to other EU Member States, to EEA countries (as clarified by the Agency's Instruction 1/2000[9]) and to countries which the European Commission considers to provide adequate protection (currently Switzerland, Hungary, Canada, subject to reservations and the US Safe Harbor). When the transfer is to an EEA country or an 'adequate' country, the Agency may nevertheless ask for documentation indicating the country to which the transfer will be made and the grounds under Article 34 for not seeking express authorization from the Agency. Transfers to all other countries ("Non-Recognized Jurisdictions") require prior authorization from the Agency.	**THAILAND** - No specified nations.
UK - Transfer is permitted to any country identified by the European Commission as having an adequate level of protection (currently: Canada (with reservations), Hungary, Switzerland). Transfer to other nations is prohibited unless the data controller believes the country provides adequate levels of protection or a statutory exception applies.	**UNITED STATES – FEDERAL** - N. A.	**UNITED STATES – NEW YORK & CALIFORNIA** - N. A.

[9] Instruction number 1/2000 of December 1, issued by the Data Protection Agency regarding the rules applicable to international data transfers.

continued on page 16

Question 3: ***If so, does your jurisdiction permit cross-border transfer (a) with consent of the data subject? (i) If so, must consent be opt-in?***

AUSTRALIA – (a) Yes. (i) Consent may be express or implied.	**CANADA – FEDERAL** - (a) Yes. (i) Consent must be opt-in if the information is sensitive or the data subject would reasonably expect to be given the opportunity to opt-in. Otherwise, opt-out. Personal Information Protection and Electronic Documents Act ("PIPEDA"), Schedule 1, Clause 4.3.4-4.3.6.	**CANADA – ONTARIO DRAFT LEGISLATION** - (a) Yes. (i) Consent to disclose outside Ontario must be opt-in unless: (1) the purpose of the disclosure is reasonably obvious to individual; (2) it is reasonable to expect that individual would consent; (3) the information is used only for the purpose for which it was collected. Consent to disclose personal health information and genetic information must be opt-in. PPIA, §§ 8(1), (5); 19; 31(2); 33; 38-44.
CANADA – QUEBEC - (a) Yes. (i) Consent must, in general, be "manifest, free and enlightened," and "given for specific purposes." For transfers of Nominative Lists used for commercial or philanthropic prospection, opt-out is sufficient: the data subject must be given "a valid opportunity to refuse that personal information concerning them be used for purposes of commercial or philanthropic prospection." APPIPS, §§ 13, 14, 17, 22.	**CHINA** - N. A.	**FRANCE** - (a) Yes. (i) Consent must be opt-in. Article 69 of Draft Law No. 1.
GERMANY - (a) Yes. (i) Yes.	**HONG KONG** - (a) Yes. (i) Section 33 of the PDPO requires consent to be in writing, but is silent as to whether this must be affirmative, opt-in consent.	**HUNGARY** - (a) Yes, but in addition to consent, the recipient must also ensure an equivalent level of protection to that in Hungary. (i) Yes.
ITALY - (a) Yes. (i) Consent must be given expressly and, if the data transfer concerns sensitive data, in writing (Art. 28, paragraph 4, a).	**JAPAN** - N. A.	**MALAYSIA** - (a) Yes. (i) Yes.
MEXICO – FEDERAL - (a) Yes. (i) Under the proposed FPDPL, free, express, informed and unequivocal consent would be required.	**POLAND** - (a) Yes. (i) Yes. The consent should be provided in written form.	**RUSSIA** - (a) Consent or a court decision is a prerequisite to any personal data processing in Russia, but is not sufficient in itself to legitimize cross-border transfers: government permission is also required. (i) The general requirement is for opt-in consent.
SOUTH KOREA - (a) Yes. (i) There is no specific provision, but as a matter of principle under the Civil Code, consent must be positive – i.e., it should be opt-in.	**SPAIN** - (a) Yes, pursuant to Article 34(e) of the Data Protection Law. (i) Yes (Article 34(e))	**THAILAND** - (a) Yes. (i) Consent may express or implied.
UK - (a) Yes. (i) DPA is silent as to whether consent must be opt-in. However, the Information Commissioner has indicated that there must be some active communication between data controller and subject, and data controller must be able to produce clear evidence of data subject's informed consent.	**UNITED STATES – FEDERAL** - N. A.	**UNITED STATES – NEW YORK & CALIFORNIA** - N. A.

Question 3(c): ***. . . where necessary for the conclusion or performance of a contract between controller and a third party in the interest of data subject?***

AUSTRALIA – Yes.	**CANADA – FEDERAL** - No.	**CANADA – ONTARIO DRAFT LEGISLATION** - No.
CANADA – QUEBEC - No.	**CHINA** - N. A.	**FRANCE** - Yes. Article 69-6° of Draft Law No. 1.
GERMANY - Yes.	**HONG KONG** - See above. Transfer of personal data out of jurisdiction on this ground is arguably permissible (provided that the data subject would have consented to such a transfer had he been consulted), if it is to avoid or mitigate anything which would adversely affect the data subject's contractual rights or benefits.	**HUNGARY** - No.
ITALY - Yes, the transfer of data is permitted if it is necessary for the conclusion or performance of a contract made in the interest of the data subject (Art. 28, paragraph 4, b).	**JAPAN** - N. A.	**MALAYSIA** - Yes.
MEXICO – FEDERAL - Yes, under the proposed FPDPL.	**POLAND** - Yes.	**RUSSIA** - No, this is not sufficient justification in itself for cross-border transfers: consent or a court decision, plus government permission must always be obtained.
SOUTH KOREA - There is no specific provision. Totality of circumstances will have to be reviewed to determine whether the data subject consented to data transfer for the purpose of performance of contract.	**SPAIN** - Yes (Article 34(g)).	**THAILAND** - Yes. This qualifies within exception (4) of the Thai Privacy Bill.
UK - Yes. DPA Schedule 4 Section 3.	**UNITED STATES – FEDERAL** - N. A.	**UNITED STATES – NEW YORK & CALIFORNIA** - N. A.

Question 3(c): ***. . . where necessary for the conclusion or performance of a contract between controller and a third party in the interest of data subject?***

AUSTRALIA – Yes.	**CANADA – FEDERAL** - No.	**CANADA – ONTARIO DRAFT LEGISLATION** - No.
CANADA – QUEBEC - No.	**CHINA** - N. A.	**FRANCE** - Yes. Article 69-6° of Draft Law No. 1.
GERMANY - Yes.	**HONG KONG** - See above. Transfer of personal data out of jurisdiction on this ground is arguably permissible (provided that the data subject would have consented to such a transfer had he been consulted), if it is to avoid or mitigate anything which would adversely affect the data subject's contractual rights or benefits.	**HUNGARY** - No.
ITALY - Yes, the transfer of data is permitted if it is necessary for the conclusion or performance of a contract made in the interest of the data subject (Art. 28, paragraph 4, b).	**JAPAN** - N. A.	**MALAYSIA** - Yes.
MEXICO – FEDERAL - Yes, under the proposed FPDPL.	**POLAND** - Yes.	**RUSSIA** - No, this is not sufficient justification in itself for cross-border transfers: consent or a court decision, plus government permission must always be obtained.
SOUTH KOREA - There is no specific provision. Totality of circumstances will have to be reviewed to determine whether the data subject consented to data transfer for the purpose of performance of contract.	**SPAIN** - Yes (Article 34(g)).	**THAILAND** - Yes. This qualifies within exception (4) of the Thai Privacy Bill.
UK - Yes. DPA Schedule 4 Section 3.	**UNITED STATES – FEDERAL** - N. A.	**UNITED STATES – NEW YORK & CALIFORNIA** - N. A.

News Round-Up

Issues from Around the Globe

BY THOMAS J. SMEDINGHOFF (BAKER & MCKENZIE)

CONTRACTS

Germany - ACCEPTANCE OF OFFER BY AUTO-REPLY: The Regional Court of Cologne held that an order confirmation, which was generated by means of an automated e-mail-reply-mechanism regarding an order of goods over the Internet, constitutes a sufficient declaration of will by the offerer. Whether the declaration constitutes a legal acceptance depends, according to the court, on the circumstances of the case, but this can be assumed if the declaration states the immediate execution of the order (LG Köln, Decision of April 16, 2003).

COPYRIGHT

Germany - PARLIAMENT VOTE ON COPYRIGHT BILL. On April 11, 2003, the German Upper House adopted the "Bill on Copyright in the Information Society," which implements the EU Directive 2001/29/EC. The Copyright Bill still has to pass the German Lower House. It makes a number of amendments to the German Copyright Act (*Urheberrechtsgesetz*) regarding the digital use of works of authorship. See link to Bill at http://dip.bundestag.de/btd/15/008/1500837.pdf.

E-TRANSACTIONS

New Zealand - ELECTRONIC TRANSACTIONS: The Ministry of Economic Development released a discussion paper on the Electronic Transactions Act. See paper at http://www.med.govt.nz/irdev/elcom/transactions/regulations/discussion/index.html.

Vietnam - E-COMMERCE SITE: The Vietnam Chamber of Commerce and Industry (VCCI) launched a national e-commerce gateway. See article at http://db.vnpt.com.vn; see gateway at http://www.vnemart.com.

INTELLECTUAL PROPERTY

Global - USTR 2003 SPECIAL 301 REPORT: The Office of the United States Trade Representative (USTR) released its annual Special 301 Report on the adequacy of intellectual property protection in 74 countries. It identifies the Ukraine as a priority foreign country, and puts Argentina, the Bahamas, Brazil, the European Union, India, Indonesia, Lebanon, the Philippines, Poland, Russia, and Taiwan on the priority watch list. See Report at http://www.ustr.gov/reports/2003/special301.htm. See Executive Summary at http://www.ustr.gov/reports/2003/execsummary.pdf.

PRIVACY

Global - PASSENGER PRIVACY: Europe and the US are continuing negotiations on passenger record access. See analysis at http://www.epic.org/privacy/intl/passenger_data.html#analysis.

Japan - PRIVACY BILL: The Lower house passed The Private Information Protection Bill. See article at http://news.tbs.co.jp/headline/tbs_headline-e744013.html.

United States - DATA-MINING PROJECTS UNDER SCRUTINY: At a House Subcommittee meeting, leaders supported two data-mining projects that will collect data from United States residents as a means of detecting risks of terrorism. The Subcommittee will hear privacy issues regarding data-mining at the end of May 2003. See http://www.pcworld.com/news/article/0,aid,110614,00.asp and http://dc.internet.com/news/article.php/2110391.

SECURITY

Global - ITU SECURITY STANDARD: The International Telecommunication Union (ITU) released a new specification language incorporating biometrics, security, and banking standards. See press release at http://www.itu.int/newsroom/press_releases/2003/14.html.

continued on page 20

Country Index. . .

from page 19

SPAM

United States - ANTI-SPAM LAWS: The governor of Virginia signed two bills that impose criminal penalties against chronic spam offenders and allow prosecutors to seize profits, computers and other assets. See press release at http://www.governor.state.va.us/Press_Policy/Releases/2003/Apr03/0429b.htm. See article at http://www.washingtonpost.com/wp-dyn/articles/A56764-2003Apr29.html.

United States – OPPOSITION TO FEDERAL SPAM LEGISLATION: At the Federal Trade Commission (FTC) forum, forty-four states and the District of Columbia announced that they are against the federal CAN Spam Act and the Reduction in Distribution of Spam Act because of concerns that weaker federal law will pre-empt stronger state anti-spam legislation. The forum is the first serious evaluation of blacklists by the federal government. See press release at http://www.ftc.gov/opa/2003/04/spamforumagenda1.htm. See article at http://www.washingtonpost.com/wp-dyn/articles/A60659-2003Apr30.html.

TRADE

Singapore - FTA SIGNED: Singapore and the US signed a Free Trade Agreement (FTA) which will eliminate trade tariffs and benefit e-commerce, intellectual property protection, and information technology. The accord mirrors the United States' Digital Millennium Copyright Act. See Agreement at http://www.ustr.gov/new/fta/Singapore/final.htm. See joint statement at http://app.sprinter.gov.sg/data/pr/2003050603.htm. See articles at http://asia.cnet.com/newstech/industry/0,39001143,39129251,00.htm and http://dc.internet.com/news/article.php/2202701. ❑

Thomas J. Smedinghoff is the North American Practice Group Coordinator for the E-Commerce Law Practice Group at Baker & McKenzie. This report is summarized from Baker & McKenzie E-Law Alerts, available at www.bakernet.com/ecommerce.