As published in Hong Kong's e-Law Asia, June, 2001

Inter-Pacific Bar Association Addresses Privacy and Data Protection Issues in Asia

David Laverty, InternationalCounsel, Chicago

A session on privacy and data protection regulations in Asia held at this year's Tokyo conference of the Inter-Pacific Bar Association (IPBA) showcased several experts in analyzing the fragmented and often conflicting approaches to the online collection of information found in the Asia-Pacific region. The April 22-25 11th annual IPBA conference, which attracted some 730 delegates, featured 26 panels on topics ranging from corporate and commercial matters to dispute resolution, including several sessions focusing on online legal issues.

The privacy and data protection panelists included such leading figures as Alfred Buellesbach, DaimlerChrysler's chief data protection officer; Shunji Shinohara, head of legal affairs of Fujitsu Limited; Bob Lewin, President and CEO of TRUSTe, a leading privacy seal provider; as well as law firm experts addressing developments in Japan, Singapore, the PRC and Hong Kong. The panelists agreed that there are very real compliance issues for companies which collect information from customers, employees and other parties based in the Asia-Pacific region. The rules may apply, for example, to companies which ask online users for personal information such as the users' name, company information and an e-mail address, accept online credit cards and gather information through "cookies" and other means of electronic data collection.

Companies that request this information potentially have a legal compliance issue in any country where the information is collected and those to which it is transferred. Regulatory restrictions may come into play at such stages as the point of data collection (what is collected, how it is collected and how is the use disclosed?), during the use of the data (can it be used for purposes other than specified?), for transfers of the data to third parties, relating to the security and protection of the data, and may also limit the transfer of information to third countries.

Compliance Efforts – Corporate Perspectives from the EU and Japan. Alfred Buellesbach, who is in charge of DaimlerChrysler's world wide data protection efforts, offered the perspective of a global EU-based company with a sophisticated approach to the EU's privacy and data protection regime and an understanding of global compliance challenges. Despite certain similarities in existing approaches and efforts toward harmonization of legal rules for e-commerce and the Internet, DaimlerChrysler has encountered a divergence of worldwide approaches to privacy and data protection. For example, in Germany, the location of the company's headquarters, the core data protection principles of the German Federal Act on Data Protection, which require public and private entities to obtain individual consent, maintain confidentiality and provide notice and rights of access to individual information, have been supplemented by the EU Data Protection Directive, which includes additional requirements on obtaining and using as little data as possible and special restrictions regarding certain "sensitive" data. The Directive also includes well-known restrictions on transfers of data to any third countries which do not provide protection equivalent to the EU rules. Such data transfer rules has led the EU to negotiate "safe harbor" guidelines with the U.S. and others and has

broad implications, including the fact that data transferred among affiliate companies may be treated as third-party transfers.

Dr. Buellesbach noted that company compliance solutions include the implementation of standard data protection contractual provisions prior to transferring to third countries (if restricted by EU-like data transfer restrictions), the adherence to a safe harbor solution such as between the EU and the U.S. or introduction of a company-wide code of conduct (the approach chosen by DaimlerChrysler).

Shunji Shinohara of Fujitsu Limited offered the perspective of a global Japan-based company facing similar challenges but operating from a different legal tradition. Mr. Shinohara commented on the growing concern over the treatment of private data in Japan, leading to the change from ministry-approved and industry group guidelines to the introduction of a new law on personal data protection, which Mr. Shinohara reports is generally welcomed by the business community in Japan. Though not required by Japanese law to do so, Fujitsu has taken actions to protect personal data due to a belief in its importance to consumers.

In contrast to the extensive consumer-oriented focus of DaimlerChrysler, Fujitsu's international operations were largely established to manufacture or procure materials, with only a small number handling customer data. Mr. Shinohara reported that Fujitsu has thus far not encountered substantial compliance issues elsewhere in the Asia-Pacific region, though Taiwan was cited as one country with active privacy-related enforcement activities, such as through litigation.

Four Basic National Privacy/Data Protection Approaches. The panelists identified four basic national approaches to the issue: (1) statutory general data protection laws, which include Japan's new law, Hong Kong, Taiwan and New Zealand, (2) sector-specific laws (such as for medical or financial information), for countries such as the PRC and Malaysia, (3) state-approved guidelines, an approach which had been followed by Japan, though that country is moving to a statutory general data protection approach, and (4) a self-regulatory approach, as represented by Singapore (though that country includes some sector-specific restrictions). There is currently a tension between more of a regulated approach, such as is shared by the EU, and the tendency toward the kind of *laisse faire* approach found in U.S. (leading to the difficulty in balancing these approaches in the EU/U.S. "safe harbor" negotiations.)

Japan – Evolution from State-Approved Guidelines to Statutory Restrictions. Mr. Yoshikazu Iwase of Tokyo's Anderson Mori further described Japan's existing system of voluntary guidelines as well as Japan's new Basic Bill for Personal Data Protection. As background to this new law, Mr. Iwase also cited a growing public concern over privacy as well as the impact of the EU Data Protection Directive, which restricts the transfer of personal data from EU member states to third countries which do not exhibit an adequate level of protection (Japan hopes to be added to the list of countries to which such transfers may flow unimpeded).

"Business entities" covered under the new law include persons who use personal data databases, which would include law firms that maintain databases of clients and/or employees. Tracking the OECD privacy guidelines, the basic law provides that business entities must specify the purposes of data collection to the subject of the collection, must keep the personal data accurate and current, adopt adequate security safeguards against loss or leakage of information, use collected information only for the purposes described, and prevent a transfer to third parties without consent of the data provider. Business entities also must disclose the

personal data that it owns when requested to do so by a data subject, and correct any inaccuracies in such data.

Hong Kong – Another Example of Statutory General Data Protection. "Personal data" covered under Hong Kong's Personal Data (Privacy) Ordinance must have the elements of attribution (in relation to a living individual), identification (the individual may be identified from the data) and retrievability (access to or processing of the data must be possible). Observing similar principles as the new Japanese law, Yongfu Li of CMS Cameron McKenna reported that the Ordinance requires that collected data must be relevant (related to a function or activity of the "data user"), necessary for or related to the stated purpose and not excessive. The data user must specify the purposes of data collection and access/correction rights, inform data subjects of the classes of persons to whom the data may be transferred, keep the personal data accurate and not retain it longer than necessary and, in the absence of consent, must use collected information only for the purposes described or directly related purposes. Data users must adopt adequate security safeguards against loss or leakage of information, must disclose the personal data that it owns when requested to do so by a data subject, and correct any inaccuracies in such data. The Ordinance also addresses aspects of employee data, such as generally providing access to employee evaluations but denying access to pre-Ordinance evaluations for a period of 7 years.

The PRC – Limited Sector-Specific Rules in the Absence of a Privacy Tradition. Unlike Hong Kong, Mr. Li pointed-out that the PRC does not regulate privacy and data protection through general statutory provisions. Only a few express references to privacy protection appear to exist under PRC statute. For example, while Internet content providers that operate electronic bulletin board services are not to disclose web user personal data to third parties without consent, this restriction applies only unless modified by other laws. One such law requires Internet service providers to record certain customer information, including a customer's account, domain name, telephone number and even Internet log-on times, and make this information available to authorities. In fact, state access to personal information is highly valued, as evidenced by the continued existence of the lifetime "personal file" system on each individual to record whereabouts, employment, awards, punishments and other information. While minimum data protection-like limitations are established, such as certain collection, safekeeping and transfer restrictions, the system is designed for state control, not individual protection, and access by individuals is strictly prohibited. Mr. Li also reported the launch of a computerized staff management system known as "China black files" which is meant as a repository of personal data for employees which employers can access. While employee permission is required for access, detractors argue that employees will be under pressure to grant permission if they desire future employment.

Singapore – A Largely Self-Regulatory Approach. In contrast to Japan and Hong Kong, Singapore has no plans to institute statutory general privacy or data protection laws. Apart from a limited common law and contract protection of confidential information, the protection of account information under the Banking Act is among the few limited statutory privacy or data protection provisions. Wilson Wong of Allen & Gledhill reported that the Singapore government perceives only modest consumer interest in privacy and data protection as balanced against the government's interest in not restricting online business or impeding the growth of e-commerce in Singapore. Singapore has instead introduced a non-binding code of practice for Internet service and content providers. Providers who wish to comply with the code may apply to a compliance authority for the use of a compliance symbol, and complaints may be made to the authority in the event of a failure to comply with the code. Though elements of the OECD privacy guidelines are reflected in the code, the code contains many open-ended obligations even for those who

voluntarily subject themselves to compliance, such as to take "reasonable steps" to ensure confidentiality, use personal information for "legitimate purposes" and "endeavor to give the user an option" as to whether it wishes to receive third-party marketing material.

TRUSTe – A Private Sector Privacy Seal Alternative. The objective behind an online privacy "seal" program, such as that introduced by Singapore and privately-administered programs such as that run by TRUSTe, is to indicate to consumers that they can expect companies which display the seal to follow certain requirements about the way the displaying web site handles data, and that an independent third party would handle complaints and resolve disputes. TRUSTe's CEO, Bob Lewin, explained that a contract signed between TRUSTe and a company running a web site obligates the company to adhere to TRUSTe's policies and enables TRUSTe to address users' privacy concerns irrespective of the citizenship of the consumer or the location of the TRUSTe licensee. Licensees are to adhere to a set of fair information practices, with familiar principles based on the OECD privacy guidelines, such as which empower users to prevent a web site from selling, sharing or disseminating their personally identifiable information.

Mr. Lewin indicated that such a self-governance model allows industry to self-regulate yet with the outside scrutiny of a third party such as TRUSTe. Sanctions for a failure to comply with the TRUSTe standards include a potential whistle-blowing to government authorities or revocation of the privacy seal. Mr. Lewin advised that the over-2,000 web sites that display the TRUSTe seal now generate about 200 complaints per month, most of which are resolved to the user's satisfaction.

Mr. Lewin emphasized the importance of building online trust to the healthy growth of online commercial transactions, whether or not companies are compelled by law to conform to privacy and data protection requirements. Yet, since compliance with privacy laws in multiple jurisdictions is of growing importance, TRUSTe has also developed privacy seal programs which enable companies to comply with the EU Data Protection Directive and Japan's new laws.

Continued Role of the IPBA for Privacy/Data Protection in the Asia/Pacific. The IPBA's International Trade Committee will build upon the foundation of the Tokyo privacy and data protection session in preparing possible recommended guidelines for companies doing business in major Asia/Pacific countries. A working group is being formed, to include industry leaders such as DaimlerChrysler's Alfred Buellesbach as well as law firm and government representatives, with the goal of issuing recommendations in time for the IPBA's 2002 conference in Hong Kong, to be held in April of next year.

David Laverty, the author of this report, moderated the privacy and data protection session and is the new chairman of the IPBA's International Trade Committee. Persons interested in the committee's activities, including the privacy and data protection working group, may contact Mr. Laverty through the Chicago-based law firm InternationalCounsel at laverty@internationalcounsel.com or by telephone at 312 575 0601.