Privacy Statutes in Asia-Pacific Jurisdictions

By Mukesh Advani (www.ubicna.com), UBIC North America, Inc.

In addition to blocking statutes that tend to restrict disclosure of information of commercial, economic or technical nature, privacy laws seek to protect personal information, which means any information that can identify a particular individual. Privacy laws seek to protect the “processing” of “personal information.” The term “processing” incorporates any action that touches data during its life cycle and includes collection, use, disclosure to others and destruction. Accordingly, the recovery of data to be used in the discovery process falls within its ambit. The term “personal information” generally means any information that can identify a particular individual. For example, emails are personal data as they can be traced to an identifiable individual. Certain types of sensitive information about an individual, such as financial, medical, religious, racial or political affiliation, is often granted even greater protection against disclosure.

Many jurisdictions in Asia-Pacific are common law jurisdictions, while others are civil code jurisdictions. Data privacy laws and regulations are already in place in many Asia-Pacific jurisdictions, including Japan, China, Hong Kong, Australia, New Zealand, Korea, Singapore, Taiwan and India. A number of Asia-Pacific nations are also currently working through the Asia-Pacific Economic Cooperation forum (APEC) to develop such rules. The combined effect of such restrictions on the corporations in terms of data they can produce in the US ediscovery could be significant.

Following is a brief analysis of such laws in some of the key Asia-Pacific jurisdictions. The information provided here is not intended to be exhaustive coverage of such laws in any jurisdiction. Rather, such laws with respect to each jurisdiction should be separately researched and analyzed for compliance with the assistance of local counsel from that jurisdiction.
UBIC

Accurate, End-to-End eDiscovery Solution & Services for Global Corporations and Law Firms

Cost Savings. Predictable Results. Reliable Support.

North America
www.ubicna.com
usinfo@ubicna.com
877.321.8242

United Kingdom
www.ubicna.com
usinfo@ubicna.com
+44-207-256-4210

Japan
www.ubic.co.jp
ubic_info@ubic.co.jp
+81.3.5463.6344

Korea
www.ubicna.com/kr
krinfo@ubicna.com
+82.2.3288.3362

Taiwan
www.ubictw.com
info@ubictw.com
+886.2.8752.3787

Secure Data Centers
With High Speed Network in
New York, Silicon Valley, London,
Tokyo, Osaka, Seoul and Taipei

UBIC carries out English and Asian Language-based eDiscovery and data forensic projects related to cross-border litigation, including anti-trust, intellectual property (IP) litigation and product liability (PL) investigations, as well as DoJ, ITC, SEC, Foreign Corrupt Practices Act (FCPA), and international cartel investigations.

Multiple languages
UBIC’s proprietary, advanced technology platform, Lit i View™, accurately handles encoding schemes and native file systems in multiple languages including Chinese, Japanese, Korean and English.

24/7 Global Support
With offices, professional staff and data centers in strategic locations around the world, UBIC’s global presence and connectivity ensures a 24/7 response capability plus data security.

Full-spectrum EDRM
UBIC offers flexible, customizable, end-to-end software solutions and services across the EDRM spectrum in support of corporate litigation strategy and crisis management.

Lit i View
Easy to use; Customizable user interface; Unified database; Compatible with other solutions; Simultaneous multi-language search and review; Advanced search techniques.

Legal Cloud Service
UBIC provides customizable service packages for preventive legal strategies (risk management, internal audit) and to address the problem of rising costs associated with prolonged investigations and litigations and the growth and dispersion of data volumes across the globe.

UBIC, Inc.
UBIC has assisted clients in more than 250 administrative and legal proceedings in the U.S. and Europe and more than 500 corporate investigations in Japan, Korea, Taiwan, Hong Kong and Singapore. UBIC North America, Inc. is a wholly owned subsidiary of UBIC, Inc., a publicly traded company in Tokyo, Japan (TSE:2158), providing eDiscovery solutions and services globally.

For more information about UBIC North America, Inc. please visit www.ubicna.com.
China
In transferring data out of the People’s Republic of China, one must be familiar with a number of national and local laws, including the State Secrets Law, the Anti-Unfair Competition Law, the Archives Law and Computer Information System Regulations. The State Secret laws are implicated when any information is deemed by the Chinese government to be a state secret, which may include civil matters when the government is involved (e.g., as an owner).

The Unfair Competition Law is for the protection of commercial secrets. A claim based upon the State Secret laws was rejected by the Ninth Circuit, and ediscovery compelled in a case in which the defendant Chinese corporation contended that disclosure of certain information will subject it to criminal prosecution in China.1

Japan
Privacy concepts are well developed in Japan. The Personal Information Protection Act of 2003 provides a structure of obligations for organizations that collect “personal information.” The statute requires disclosure to the individual of the purpose of use of data and further requires consent for transfer of “personal information.” The individual may request to review such data and must be granted an opportunity to correct, supplement or delete it. It also has notice and opt-out provisions. Currently, a corporation that violates the law may be fined or ordered to take remedial steps, and the corporation head may be imprisoned. As part of an effort to increase penalties for violations of this statute, the authorities in Japan plan to extend liability under that law to individual corporate employees.

South Korea
The Act on the Protection of Promotion of Information and Communication Network Utilization and Information Protection Act of 2001 protects the personal information of consumers held by certain industries. The number of industries subject to this law is in the process of being greatly expanded by the responsible government ministry. The statute requires deletion of data when it is no longer needed for its intended purpose of processing.

The 2011 Act on the Protection of Personal Data requires nearly all businesses and government agencies to provide data breach protection, mandates the use of privacy assessments before establishing certain new databases, and establishes a right to file class actions in court over alleged violations of the law. The legislative intent behind the Act is to prevent damage caused by leakage and/or misuse of personal data. Under the new law, covered entities must report incidents of leaked personal data to government privacy and law enforcement authorities, and notify affected individuals.

Australia
Australia Privacy Act 1988 regulates the export of personal information from Australia. National Privacy Principle 9 (NPP 9) covers “trans-border data flows” and provides that an organization in Australia may lawfully transfer personal information out of Australia where the individual has consented, where similar privacy regimes are believed to exist in the State of import, and in certain other circumstances.

Australia also has enacted a statute (Foreign Proceedings Act 1984), under which the attorney general may “by order in writing” prohibit production of any document located in Australia to a foreign court or authority and doing of any action in Australia, which might facilitate such transfer.

New Zealand
The New Zealand Privacy Act of 1993 is one of the most comprehensive privacy statutes outside Europe. It applies to the handling of all personal information collected or held by government agencies and most businesses. The

The New Zealand Privacy Act of 1993 is one of the most comprehensive privacy statutes outside Europe.
legislation identifies “personal information” as information about an identifiable living person, irrespective of whether it is on a computer or a paper file. The legislation is based on 12 Information Privacy Principles similar to the National Information Principles in the Australian Privacy Act.

Taiwan
The Computer-Processed Personal Data Protection Law of 1995 protects the processing of personal data in certain kinds of industries, such as the financial industry. Personal data is defined broadly to include “the information regarding a natural person’s name, birthdate, identification number, physical features, fingerprint, marital status, family, education, occupation, health, medical history, financial standing, social activities as well as other information sufficient to identify the natural person.” It also creates restrictions on cross-border transfer of personal information. There is no single privacy oversight body to enforce the law. The Ministry of Justice enforces the Act for government agencies. Compliance with such laws in the private sector is enforced by the concerned government agency for that sector. An example of such enforcement is arrest by the Criminal Investigation Bureau of several people for selling lists of more than 15 million voters and personal data of up to 40 million individuals.

Singapore
There is a voluntary privacy framework, the Model Data Protection Code for the Private Sector, which applies to any recipient to whom personal data is transferred, in or outside the country. Singapore’s Banking Law prohibits disclosure of “customer information” by any bank. There are other sector-specific laws regulating the protection of personal data, such as the Official Secrets Act and the Infectious Diseases Act.

Hong Kong
The Personal Data (Privacy) Amendment Bill was introduced into Hong Kong’s Legislative council on July 13, 2011, following public outcry from several highly publicized scandals involving the sale of personal data without the knowledge or consent of individuals. The Bill seeks to regulate direct marketing and sale of personal data and requires full disclosure of the purpose for which data may be used. The individual may refuse to provide consent to the release of such data, and the entity must wait for minimum 30 days after the notice is provided and provide an opt-out mechanism for this purpose. Under the Bill, non-compliance with any of its provisions will be a criminal offense. Personal Data (Privacy) Ordinance (Cap. 486), 1995, has a provision for the onward transfer of personal data that requires that there be a reasonable belief that any personal data transferred outside Hong Kong without consent is transmitted only to a recipient operating under similar privacy laws.
India

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, were issued in April 2011 to implement India’s 2008 IT Security Act amendment. The rules oblige organizations to notify individuals when their personal information is collected via letter, facsimile or email. They require covered organizations to make a privacy policy available, to take steps to secure personal information, and to offer a dispute resolution process related to the collection and use of personal information. In addition, Article 21 of the Constitution has been interpreted by the Indian courts to include a right of privacy.

Notes
1 Richardmark Corp. v. Timber Falling Consultants, 959 F.2d 1468 (9th Cir. 1992).

This article is an excerpt from a UBIc, Inc., White Paper that also examines the conflict between the US ediscovery laws and the privacy laws and regulations in the Asia-Pacific region. The Paper discusses US Court attempts to reconcile this conflict, and also recommends best practices for navigating the minefield that exists as a result of such a conflict. To access the full White Paper, visit www.acc.com/ab/pan-pacific-data_mar13.