Personal Data Privacy in the Asia Pacific : A Real Possibility

Jim C. Tam, Ph.D.
School of Information Technology Management,
Ryerson Polytechnic University,
Toronto, Ontario, Canada
jimtam@acs.ryerson.ca

In exploring the state of affairs in personal data privacy in the Asia Pacific, we need to examine privacy from a number of perspectives — computing, legislative, political, cultural and social. In the Asian cultures in general, the notion of confidentiality and anonymity is uncommon, and there is a relative lack of private space or protection of personal information. As a result of the patriachical structure of the societies, citizens are accustomed to routinely submitting personal information to authorities. Politically, the modus operandi of the governments in this region is that of control. In the context of this prevalent practice, personal privacy is an unfamiliar concept[1] in many of these societies.

Even though privacy is a fundamental human right recognized in the Universal Declaration of Human Rights, violation of privacy by the governments in the Asia Pacific region is fairly common[2][PRI99]. Little or virtually no recognition of privacy is made in their constitutions, either explicitly or implicitly. As a result of increased trade between Asia and the rest of the world, there is correspondingly an increased expectation on Asia Pacific governments to recognize and respect human rights including personal data privacy.

Personal data privacy legislation should be promulgated in order to ensure privacy. In order to reconcile personal privacy and free flow of information, legislation must ideally maintain a delicate balance between the two —— generalized enough to facilitate information flow[3] but specific enough to safeguard personal privacy. In a recent survey, however, only a handful of countries[4] have actual legislation in compliance with the guidelines issued by the Organization for Economic Co-operation and Development (OECD) to safeguard the rights of their citizens on personal data privacy. It is often too common a practice for governments to restrict or control the flow of information. The censorship and information filtering of Internet servers in China is a case in point[AFP00]. Even where legislation is in place, public and private corporations have been reluctant to implement guidelines or comply with the legislation due to resource restraints, cost implications and social practices.

Instead of treating protection of privacy and personal data as a fundamental human right, there is an emerging trend among the governments and businesses to treat them as a trade commodity[5] to boost the regional economy. Nevertheless, in order to promote trade with other international partners, the governments in Australia, Hong Kong, Japan, Korea, New Zealand, Taiwan, etc. have introduced a variety of measures to protect personal data and privacy. These measures include comprehensive legislation, sectoral guidelines, technological means, self-regulatory practices and procedures. In addition, these measures differ significantly in many aspects, including levels of data protection, areas of jurisdiction, applicability of pertinent laws and the kinds of technology deployed. All these differences would render the streamlined transmission of information over the Internet difficult with their respective trade partners in the other parts of the World.

At another level, surveillance is generally pervasive in Asia Pacific countries. Law enforcement and intelligence agencies have been given significant power to deviate from privacy control measures. There have been widespread violations of laws relating to surveillance of messages, interception of communications, biometrics identification and secretive state files being kept on citizens or dissidents. Furthermore, the comprehensive or sectoral laws have not kept up with the proliferation of various kinds of obtrusive technology. The central privacy enforcement agencies generally have limited power and resources, rendering the privacy control ineffective.

Further to the general contextual challenges discussed above, there are a number of specific critical issues that need to be addressed before the Asia Pacific region can enhance their data privacy control.

(1) The Asia Pacific countries rely on US computer technology. However, the US Government has been adverse to the export of privacy control technology.[6] Furthermore, it has sent "envoys to dozens of countries to demand restrictions on privacy enhancing technologies, promotion of new laws to increase wiretapping and access to financial records, and expressing opposition to laws" [BAN99].

(2) Interlegal issues in relation to cross-border information flow[7] need to be resolved. In particular, there are two major issues to be settled. First, to decide on jurisdiction, this could be the jurisdiction of a court or an authority. Second, to decide which law applies to the case at hand (*lex causae) [BIN99].* In a region with a wide variety of types of laws, this could prove to be a very complex and difficult situation to resolve.

(3) As a result of globalization and re-organization, basic "structural and organizational" changes[HUR99] have created an unprecedented number of business conglomerates. This renders the protection of the information even more difficult in many countries as the custodianship of the information is not well defined. Therefore, there is a need to formulate appropriate information management strategies on ownership, accessibility and control. In jurisdictions that have such strategies, the challenge lies in the implementation to meet statutory privacy requirements.

(4) There is a need to raise the awareness of the general public regarding the issues related to privacy protection in order to:

- ensure the confidentiality of their own personal information;
- safeguard their privacy on the Internet,
- be aware of various web site privacy practices; and
- make appropriate choice in disclosing their information on the Web.

The public needs to be familiarized with various privacy protection technologies such as cryptography programs, anonymous communication tools, remailers, proxy servers, digital cash , smart cards, Platform for Privacy Preferences (P3P) and various kinds of infomediary.

(5) There is a need to assess the suitability of the prescriptive EU Model or the specific sectoral/self-regulatory US model for privacy control in the Asia Pacific? In essence, what kind of privacy control framework needs to be put into place that will encapsulate the many dichotomical issues faced by countries in the region?

In summary, personal data privacy control in Asia Pacific is a complex one due to the diversity in cultures, kinds of governments, differences in legislation and types of business practices. In order to safeguard data privacy, a pragmatic framework should be formulated, balancing the critical issues mentioned above and individuals' needs in their societies. In particular, individual citizens in Asia Pacific should be more proactive in controlling personal information and ensuring anonymous communications. In their diverse relationships and interactions, individuals should be accorded with various "zones of opacity and transparency"[HUR99], in which varying amounts of personal information can be withheld or disclosed at will.

References

[AFP00] Agence France Presse (2000). China to release new regulations for Internet Services Providers, 10 Jan 2000.

[BAN99] Banisar, David(1999). Privacy and Data Protection around the World, Electronic Privacy Center, Privacy International. http://www.privacyinternational.org/

[BIN99] Bing, Jon(1999). Data Protection, Jurisdiction and the Choice of Law, Norwegian Research Center. http://www.pco.org.hk/conproceed.html/

[CPO99] Computer Privacy (1999). White House announces New Encryption Policy, 16 Sept 1999. http://www.computerprivacy.org/action/archive/06101999

[GRE97] Greenleaf, Graham(1997), *Towards an Asia-Pacific information privacy convention*, Privacy Law and Policy Reporter Vol. 2 No 7.

[HUR99] Hurley, Deborah, (1999). A whole world in one glance: Privacy as a key enabler of individual participation in democratic governance. http://www.pco.org.hk/conproceed.html/

[KIR80] Kirby, Michael (1980). Australian Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Council of the OECD, 23 September 1980.

[KYN99] Kyoto News (1999). Japanese Parliament Approves Wiretap, IP Bills, 12 August 1999.

[PRI99] Privacy International (1999). Privacy and Human Rights 1999. http://www.privacy.org/pi/reports

Footnotes

[1] The cultural differences in dealing with different situations depend on many factors: traditional, social, political, religious and family. Quite often, trade-offs or compromises are made depending on competing public and private interests.

[2] Japan Parliament approved the Wiretap Bill on August 12, 1999. China announced new regulations for Internet Services Providers on Jan 10, 2000. In a 1986 interview, Lee Kwan Yew, ex-prime Minister of Singapore, justified the use of surveillance for social and political control as a necessary means for economic progress.

[3] Restrictions on these flows could cause serious disruption in important sectors of the economy, such as banking, import/export and insurance. For this reason, countries such as Australia, Hong Kong, Japan, New Zealand, South Korea and Taiwan, have used the comprehensive law approach to safeguard personal data privacy whereas others like Malaysia, Singapore, etc have adopted the sectoral or self-regulatory approach.

[4] Japan became the first Asian country to pass The Act for Protection of Computer Processed Personal Data in December, 1988. Taiwan introduced The Law Governing Protection of Personal Data Processed by Computers in July, 1995. In Hong Kong, The Personal Data (Privacy) Ordinance was enacted in September, 1995.

[5] Moreover, suggestion has been made to deal with personal data protection as a trade matter to be taken up in the World Trade Organization (WTO).

[6] The Clinton Administration announced New Encryption Policy restricting the use of privacy control technology by foreigners.

[7] Australian Guidelines on the Protection of Privacy and Transborder Flows of Personal Data was adopted by the Council of OECD in 1980.