APEC ECSG TECHNICAL ASSISTANCE SEMINAR
DOMESTIC IMPLEMENTATION OF THE APEC PRIVACY FRAMEWORK
June 1-2, 2005 HONG KONG

PRESENTATION

"It is the best of times....it is the worst of times"

Stephen Lau
Chairman, EDS Hong Kong and
former Hong Kong Privacy Commissioner for Personal Data

Good morning, ladies and gentlemen. I am pleased and honoured to be here today at this seminar organised by APEC on the APEC Privacy Framework.

I like to begin by reviewing the impact of technology, recent and new, on data privacy, then offer some food for thought on the road forward for the APEC economies in chartering the data protection regimes, particularly to the Data Protection Authorities or their equivalents.

ICT, the marriage of information and communications technology, is creating new application and services in our daily life. The awesome growth of Internet, with over 300 million people world-wide now surfing the Internet for fun and information, provides impetus to new initiatives in electronic commerce.

Its many recognised advantages include a new channel of doing business which brings in new revenue, with cost-effective access to global markets. New and innovative businesses also are mushrooming, e.g. contents providers including data brokers with numerous databases, and specialised hardware and software vendors for Internet applications and security.

However, there is a significant road block to the seemingly unstoppable momentum in harnessing the potentials of electronic commerce. This stumbling block is to do with ensuring trust and confidence of both the consumers and the businesses. A European Union document on electronic commerce summaries this concern admirably.

"For electronic commerce to develop, both consumers and businesses must be confident that their transaction will not be intercepted or modified, that the seller and the buyer are who they say they are, and that transaction mechanisms are available, legal and secure. Building such trust and confidence is the prerequisite to win over businesses and consumers to electronic commerce. Yet many remain concerned about the identity and solvency of suppliers, their actual physical location, the integrity of information, the protection of privacy and personal data, the enforcement of contracts at a distance, the reliability of payments, the recourse for errors or fraud, the possible abuses of dominant position - considerations which are heightened in cross-border trading."

Of all these concerns related to trust and confidence, data privacy is regarded as dominant, as the Internet is multiple networks with many pathways connecting many thousands of computers. Without adequate security, access to databases by unauthorised or fraudulent users could be made and messages which could contain sensitive personal data intercepted during transmission, leading to personal data being used and disclosed for unintended, unauthorised or fraudulent purposes.

To illustrate my point, let's look at some statistics. The US Federal Trade Commissioner estimates that 10 million people were victims of identity theft in 2002. According to Gartner, 9.4 million online US adults were victimised between April 2003 to April 2004, with the losses amounting to US$11.7 billion.
Early this year, ChoicePoint, a data broker in the US, reported that the personal information of 145,000 Americans may have been compromised in its breach, in which con men posing as business looking to do background checks on their customers were given access to its credit information data base. Soon after that Bank of America divulged that back up tapes containing the financial information of government employees were lost while being shipped to a data warehouse...

Meanwhile, innovative technology marches on. Complementary to the advances in Internet technology and the growth of electronic commerce is a host of other technologies., for example, biometrics is increasingly being used to authenticate the identity of individuals ; location tracking technology with wireless technology coupled with GPS (Global Positioning System) and GIS (Geographical Information System) to improve business and customer services, locating victims in search-and-rescue-operations, and "concierge" services e.g. locating a restaurant or providing directions in an unfamiliar environment; Radio Frequency Identification (RFID) tags, which are microchips with antenna, will eventually be attached to every item of merchandise to optimise inventory control and supply chain logistics. Applying to all the data items collected by all these innovative applications the advanced data base technology with data mining techniques will allow data consolidation, analyses and projections for focussed marketing and effective business decision making.

But for data privacy, technology is a double-edged sword. It is both a protector and a nemesis of privacy. Biometric identifiers are used to uniquely authenticate an individual to protect unauthorised access of his personal data, yet biometrics can also be used for surveillance from afar through facial recognition leading to the loss of anonymity. RFID tags are planned to be used for compiling profiles of individual's buying behaviour. Finding where you are whenever and wherever by location tracking technology is the antithesis to the right of privacy, "the right to be left alone". Already concerned parties and Data Protection Authorities are voicing serious concerns on the potential and corollary erosion of personal data privacy.
Though this forum is mainly concerned with the impact on data privacy from economic activities including electronic commerce, I note in the agenda the significant reference to national security and public safety. Invariably we all realise their prominent influence, more so than ever before, is due to the tragic event of 9/11 of 2001, a date which truly changed the entire world. Its impact caused a drastic change in national policies and

priorities. In the years since 9/11, according to the international survey report by EPIC (Electronic Privacy Information Centre) and Privacy International, four trends have become apparent: the swift erosion of pro-privacy laws; greater data sharing amongst corporations and law enforcement agencies, e.g. the "Secure Flight" program; greater surveillance; and sharply increased interest in people-tracking technologies, such as face-recognition systems and national ID cards.

All these factors, the trust and confidence issue with the need and growth of electronic commerce and the free flow of information, the inevitable applications of new technologies in our economic activities giving rise to potential negative implications on data privacy, all shrouded and made murkier in the aftermath of 9/11, are the reasons why we are gathered here today, under the auspices of APEC to charter a privacy framework with a set of data protection principles for compliance within the APEC economies. It is timely, it is essential, and it is commendable.

Let me now move on and give some food for thoughts for your deliberation over the next two days with some observations I gathered from my years as a privacy commissioner. These observations might be obvious to you, but still could serve as a reminder.

1. The right to privacy, as the case for any human right, is generally not regarded as absolute. Though important, it is only one of the societal values out of many in a progressive and democratic society. Its consideration is usually a balancing act, on a case by case basis, involving other rights of perceivably equal importance, may they be national interests and security, economic interests, or community interests. . Its weighting on the value scale is also influenced by the prevailing political climate, cultural values and consequential impact on society as a whole. So data privacy sometimes is favoured, sometimes not, and that is the reality.

2. having said that, as a privacy commissioner or a data protection authority backed by a legal or regulatory framework and guided by data protection principles, we must do all we can to uphold the principles and the law, because this is our mandate, this is our responsibility to present privacy as sacrosanct, as an absolute and immovable right , just as I would expect our opponents, may they be the intelligence agencies, to do all they can to protect national security interests, to fight terrorism, to preserve public safety, or the business organisations to do all they can to maximise their economic interests . With such a firm attitude and conviction, if data protection principles are to be breached via exemptions or exceptions for the overall good, we can face up to our conscience and our duty in that we did all we should, all we could.

3. . But this should not be the end of our resolve. We should then negotiate on the option of choice where appropriate, particularly the choice which preserves our anonymity. The provision of choice should be regarded as a powerful right of our citizens who have individual perception of the relative importance of privacy. Some couldn't care less about cookies tracking their preferences as a consumer on the internet, others scream blue murder when they receive just one simple direct

marketing brochure from merchants unknown. The power and comfort of a choice provided to a citizen should never be underestimated, the choice of continuing with his conventional library card and not using a smart identity card doubling as a library card for fear, real or otherwise, his reading habits might be tracked, or the choice of having a remote sensing cash card to going through a toll road and not having to use a registered card where his movements might be tracked.

4. Sadly in many situations choice is not an alternative, particularly when personal data are being used, being matched, being profiled without the benefit of notice and awareness, typically in the pursuit of overriding security interests. Therefore for exemptions, which are de-facto breaches of the data protection principles, the data protection authority must insist upon transparency of the criteria for access and use of personal data, the independent and adequate oversight and review mechanisms., and unequivocal accountability and redress mechanisms corresponding to the consequential harm for invasion of data privacy. But be real careful here. Too many over-riding exemptions to the established principles would be derogatory and a mockery with respect to the integrity and wisdom upon which the principles were nurtured.

5. Finally, even with a well-written law with satisfactory compliance to the principles, we must be rigorous and vigilant yet pragmatic to promote and enforce the provisions of the law. Real or perceived weakness and negligence in the promotion and enforcement of the law would lead to the loss of confidence and trust in the eye of the community. In other words, we would be regarded as ineffectual, a lame duck authority.

Those are the few points I wish to make as some food for thought for this forum.

I like to conclude by making a quotation, which I stumbled upon and quoted in Sept 2002 when I was the concluding speaker to provide a summary of the proceedings of the annual data protection commissioner's conference held that year in Cardiff. It is a very well-known quotation, but I think never yet been applied in the context of data privacy. Remember that Sept 2002 was just a year after 9/11 in 2001. Last night I re-appraised the aptness of the quotation for now, the year 2005, and my sentiments still prevail. The quotation is from Charles Dickens, the opening lines of "A Tale of Two cities"

> "It was the best of times, it was the worst of times, it was the age of wisdom, it was the age of foolishness, it was the epoch of belief, it was the epoch of incredulity, it was the season of Light, it was the season of Darkness, it was the spring of hope, it was the winter of despair, we had everything before us, we had nothing before us".

Ladies and gentlemen, with the concerted efforts and wisdom of the people in this room and many other equally enlightened colleagues out there, all striving towards upholding and balancing our rights and values in a civilised society, I have every confidence that, in front of us, is the age of wisdom, the season of light, the spring of hope and we have everything before us". Thank you.