Speech by the Secretary for Justice at Internet Law Symposium
****

Following is the Keynote Address by the Secretary for Justice, Ms Elsie Leung, at the Symposium on 'Internet Law in Hong Kong' organized by The Institute of Electrical and Electronic Engineers Hong Kong today (September 26):

Dr Chin, Mr Chiu, the Honourable Sin Chung-kai, distinguished guests, ladies and gentlemen,

Good morning,

Thank you for the opportunity to speak at this symposium today. 'Internet Law in Hong Kong' is certainly a topic that deserves attention given the increasing prominence of Internet usage in a knowledge-based economy such as ours.

The Internet is now part of daily life. About half of households and businesses in Hong Kong are connected to the Internet. We have more than 2.4 million Internet accounts. The first thing many of us do when we arrive at work is check our e-mails; youngsters spend hours 'chatting' to their friends through ICQ; e-commerce goes on around the clock; we can even pay our bills on the net or book tickets to the cinema or our favourite opera.

Naturally, the Government is keen to facilitate such beneficial applications. But at the same time, we must also protect against abuses of the technology and applications that have had such a profound affect on our lives. So, we need laws to ensure that the Internet is suitably regulated. And today, I want to discuss how the law has evolved to cope with this increasing influence of the Internet.

Policy Objectives

A fundamental point in formulating laws about Internet usage actually applies to all laws in Hong Kong. While the Department of Justice has a central role to play in safeguarding the rule of law, the Department of Justice does not formulate laws of its own. The established practice, both before and after 1997, is for Policy Bureaux to take up the responsibility for initiating legislation falling within their portfolios. In regards to the Internet, the Commerce, Industry and Technology Bureau, known as 'CITB', is the lead policy bureau. The Communications and Technology Branch 'CTB' within the CITB covers the portfolio of the former Information Technology and Broadcasting Branch, which we referred to as the 'ITBB'.

When the ITBB was set up in 1998, it adopted what could be described as a 'minimalist and facilitative approach' in dealing with IT legislation. 'Minimalist' means that we only bring in new legislation when absolutely necessary. New laws will not be introduced when existing legislation can apply equally to activities in a cyber environment. And we may not legislate if other options, such as voluntary agreements or a non-statutory code of practice, can achieve the intended policy objective. 'Facilitative' conveys our approach to work with the industry, the professions, the academic sector and the community to facilitate benevolent Internet use, with adequate safeguards to deter destructive Internet applications. Let me give you a few examples of what I mean. I will start with the application of the Personal Data (Privacy) Ordinance.

Personal Data (Privacy) Ordinance (Cap 486)

In Hong Kong, a person's personal data privacy is protected by the Personal Data (Privacy) Ordinance. This Ordinance gives statutory effect to internationally-accepted data protection principles :

* Principle 1 on 'purpose and manner of collection of personal data' requires lawful and fair collection of personal data;

* Principle 2 on 'accuracy and duration of retention of personal data' provides that personal data held should be accurate, up-to-date and kept no longer than necessary;

* Principle 3 on 'use of personal data' provides that personal data should only be used for the purpose for which they are collected unless with the consent of the data subject (ie, 'the individual who is the subject of the data');

* Principle 4 on 'security of personal data' requires the data user to take appropriate security measures;

* Principle 5 on 'information to be generally available' requires a data user to be open about the policies and practices in relation to the personal data;

* Principle 6 on 'access to personal data' provides for a data subject to have access to his or her own personal data and to request correction.

Generally speaking, its provisions apply to the collection, storage and use of personal data both online and offline. Hence, we do not need new laws to protect personal data communicated in the e-form. Data collected or processed by locally-based data users must observe the provisions in the Ordinance. Anyone who contravenes the Ordinance is liable to enforcement action by the Privacy Commissioner. An individual who suffers damage from a contravention of the Ordinance, including injured feelings, may obtain compensation from the data user concerned.

As I mentioned earlier, we do not rely solely on legislation. We depend heavily on some non-legislative means to guard against risks to e-privacy. The Privacy Commissioner's Office has been monitoring e-developments closely. Notes and guidelines have been published with a view to promoting self-awareness among individual net users and elevating the compliance level of data users. For example, there are guides for individual users on 'Internet Surfing with Privacy in Mind' and 'Personal Data Privacy and the Internet'. Companies using the Internet can refer to the management handbook 'E-Privacy : A Policy Approach to Building Trust and Confidence in E-business'. These notes and guidelines do not have legal status, but they help protect privacy in relation to personal data in the e-world.

Control of Obscene and Indecent Articles Ordinance (Cap 390)

The Control of Obscene and Indecent Articles Ordinance - the 'COIAO' - is another law that applies equally to information communicated through 'traditional' modes or via the Internet. The COIAO is by nature a sensitive law. On the one hand it seeks to restrict the publication, circulation and display of obscene and indecent materials; on the other it strives to safeguard the freedom of expression and the freedom of publication. The COIAO covers printed material, sound recording, films, video-tapes, disc and electronic publication.

However, legislative control alone cannot solve the problem of indecent articles. It is simply impracticable - more likely impossible - to monitor all the information transmitted through the Internet. The Government has adopted a co-regulatory regime with the industry and with parents.

In October 1997 the Hong Kong Internet Service Providers Association promulgated a Code of Practice setting out the appropriate action that an Internet service provider should take to prevent network users from transmitting or hosting obscene materials on the Internet. In June this year, the Government sponsored the Association to launch an Internet Content Rating System project. Through this project, webmasters declare their website content on a voluntary basis, while Internet users are able to decide whether they or their children should browse a particular website based on the declarations made by the webmasters.

Electronic Transactions Ordinance (Cap 553)

While we leverage and capitalise on existing laws as far as practicable, the Government has taken the initiative to introduce laws specifically for the purpose of facilitating the use of electronic transactions, including those conducted over the Internet. For example, the Electronic Transactions Ordinance enacted in January 2000. Its provisions are modelled on the UN Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce.

This Ordinance provides a clear framework to facilitate and promote e-business, which in turn can enhance Hong Kong's competitive edge. The Ordinance gives electronic records and digital signatures the same legal status as that of their paper-based counterparts. The Ordinance also removes the uncertainty and fear associated with the security of e-transactions. A voluntary recognition scheme for certification authorities has been set up under the Ordinance to enhance public confidence in the use of digital signature in electronic transactions. A digital certificate issued by a certification authority identifies the subscriber of the certificate and addresses the basic issues of authenticity, integrity, non-repudiation and confidentiality of the data used in e-transactions. The Postmaster General is a certification authority recognised under the Ordinance. Two commercial certification authorities have also been recognised under the Ordinance.

It is important to note that the recognition scheme for certification authorities under the Ordinance is operated on a voluntary basis. That said, anyone dealing with a company not certified by such a voluntarily registered certification authority will still enjoy legal protection, because the e-transaction taking place will be covered by contract and common law applicable to paper-based transactions. The Ordinance accepts the use of electronic records as legally admissible evidence. It provides that encrypted messages and digital signatures meeting statutory requirements will be accepted prima facie as sufficient evidence.

The Government has closely monitored developments since enactment of the Electronic Transactions Ordinance. We have taken heed of comments and suggestions received during a public consultation exercise held in early 2002. We have formulated a set of proposed amendments that are contained in the Electronic Transactions (Amendment) Bill 2003 introduced into the Legislative Council in June this year. There are three major proposed amendments :

- First, to facilitate electronic transactions not involving government entities, we propose to adopt a technology-neutral approach in the use of electronic signatures to satisfy signature requirements under law. Such an approach will enable the legislative framework and future development of e-business to better keep pace with technological advancements. We propose to amend the Ordinance so that a signature requirement under law can be met by any form of

electronic signature if it is reliable and appropriate for the purpose and agreed by the parties concerned. We also propose to clarify the use of electronic signatures in the formation of electronic contracts;

- Secondly, we propose to remove unnecessary legal impediments to electronic transactions and e-government that may be created by legal provisions containing references to, or the requirements of, serving documents on parties concerned by post or in person. These legal provisions were enacted at a time when electronic transactions were not prevalent. There is now no justification to exclude electronic means. We therefore propose to accept the service of these documents by electronic means in specified cases. The list of specified cases will initially include specified provisions in the Landlord and Tenant (Consolidation) Ordinance, the Rating Ordinance and the Government Rent (Assessment and Collection) Ordinance. This list will be expanded over time through an ongoing process; and

- Thirdly, we propose to streamline and improve the operation of the voluntary recognition scheme for certification authorities under the Ordinance.

These proposed amendments will no doubt be scrutinised by legislators in a Bills Committee to be set up later. We believe that when enacted, the Bill should help promote e-business in Hong Kong and bring Hong Kong to the forefront in terms of legislation on electronic transactions.

Computer Crimes Ordinance

The advent of the Internet has also given rise to the advent of cyber crime. People who may not normally have engaged in criminal activity can do so now from the comfort of their own home and PC, hopeful that their activities will go undetected in the millions upon millions of megabytes of information flowing around the world wired wide. In September 2001, thousands of computers across Asia were hit with the Nimba computer worm. This Nimba worm, written to take advantage of the damage done by the Code Red attacking, gave rise to fears of cyber-terrorism. The virus caused an estimated US$1.96 billion worldwide in clean up costs. In Hong Kong alone more than 1,000 computers were infected, with HK$30 million a day in lost productivity.

Clearly, we must confront the dark side of computer misuse to allow the Internet to reach its full potential. As I mentioned, existing laws such as the Personal Data (Privacy) Ordinance and the COIAO, can cover offences committed in either the physical or the cyber world. In addition, specific legislative provisions covering computer-related crimes were enacted through the Computer Crimes Ordinance in 1993. These include:

* unauthorised access to a computer by telecommunications under the Telecommunications Ordinance;

* criminal damage relating to the misuse of a computer under the Crimes Ordinance; and

* access to a computer with criminal or dishonest intent under the Crimes Ordinance.

We believe that the Computer Crimes Ordinance remains broadly adequate to deal with illicit acts such as hacking, the spreading of computer viruses and criminal damage of computer data.

However, we remain worried about the rising number of computer-related crimes. Indeed, statistics between 1998 and 2002 give us cause for concern, with the number of cases increasing

dramatically from 38 in 1998 to 272 in 2002.

For the 272 cases in 2002 there were 26 cases of unauthorised access to computer by telecommunication; 138 cases of access to computer with criminal or dishonest intent; 16 cases of criminal damage; 45 cases of obtaining property by deception including e-shopping fraud; 19 cases of obtaining services by deception; 6 cases of e-banking related theft; and 22 cases of other offences such as publishing of obscene articles etc.

In our further efforts to combat computer-related crime, the Government has decided to : (1) strengthen the existing regulatory regime; (2) increase the involvement of the community in the prevention and detection of computer-related crimes; and (3) improve co-ordination and institutional arrangements to prevent cyber attacks and promote cyber security. Work has already been started on some administrative measures and the relatively straightforward legislative amendments.

Draft Criminal Jurisdiction Ordinance (Amendment of Section 2(2)) Order

I would now like to mention the issue of territorial jurisdiction in combating cyber crimes. Computer-related crimes have no territorial borders, and this is a crucial issue that must be addressed.

In November 2002, the Government introduced into the Legislative Council some proposed amendments to the Criminal Jurisdiction Ordinance to address the traditional jurisdictional problems associated with cross-border computer related crimes. The amendments, if and when approved, will enable Hong Kong courts to exercise jurisdiction over computer-related crimes committed or planned outside Hong Kong but that are connected to, or intended to cause damage in, Hong Kong. The amendments are now with the Legislative Council. And we hope they will soon receive due attention of our Legislative Councillors.

Closing Remarks

Ladies and gentlemen, I have just outlined initiatives taken by the Government to facilitate, and suitably regulate, the use of the Internet in co-operation with the industry and the community. The Honourable Sin Chung-kai, Mr Stephen Mak and a number of my colleagues from the legal sector will also explore this and other areas in more detail. I am sure this symposium will provide you all with very useful insights into Internet-related laws in Hong Kong.

I would like to thank Dr Chin of the IEE, Mr Philip Chiu, the Chairman of the Organising Committee, all members and advisers of the Organising Committee, and all supporting organisations, for asking me to join you today for this important and informative event.

Thank you very much.

End/Friday, September 26, 2003
NNNN