Hong Kong Translation Society
Luncheon Talk

22 July 2006

Privacy and the Development of Privacy Rights in Hong Kong

Dr Chan (Elsie), Ladies and Gentlemen, a very good afternoon to you ….

1 Introduction

I would like to thank the Translation Society for providing me with this opportunity to talk about the developments of privacy and related rights in Hong Kong. In fact this has been a relatively brief passage of history that spans no more than 15 years. In that period privacy has emerged as a human right, become institutionalised and, importantly, accepted and valued by the people of Hong Kong. However, we need to learn the lessons of history and one of them is that the benefits conferred upon us by our human rights should not be taken for granted. Indeed, part

of my job and that of the Commissioner's Office is to ensure that our privacy rights are upheld and enhanced. That is by no means an easy task because there are forces 'out there' that represent very serious challenges to privacy. If those challenges are not met with robust counter-measures then privacy will wither on the vine. The gains we have worked hard to secure in the past need constant protection and nurturing. If we want to ensure that privacy rights remain an important component of human rights more generally, and if we want to ensure that future generations enjoy the same benefits, then we have to take pro-active measures if we are to guarantee the legacy.

Let me begin therefore with a story, one which perhaps people in Hong Kong may not readily identify with just yet. The story is true, and although it occurred in the United States, no one listening to it should be tempted to subscribe to the 'not invented here' syndrome. Even though the citizens of Hong Kong have a sophisticated smart Identity Card, this of itself may not be sufficient to deter ingenious criminals with access to sophisticated IT and related production technologies. In the face of

technological ingenuity assumptions regarding privacy need to be exercised with caution.

The story illustrates what happens to perfectly innocent and unsuspecting people when privacy rights are neither adequately protected nor, I might add, adequately defended.

2 The Story

Several months ago a Californian housewife received a statement from the US Inland Revenue Service stating that she owed nearly $16,000 dollars in back taxes. She had never worked in the period stated and never visited Texas where it was alleged that she had been employed.

It eventually transpired that her Social Security Number had been stolen and fraudulently used by at least 81 people, including illegal immigrants, in at least 17 states. Some of these people had stolen her identity to obtain employment, others to open bank accounts and negotiate loans. When returning from a holiday in Mexico she was detained for 4 hours by airport immigration officials because a woman using her social security number was wanted for a felony.

That is the unfortunate experience of one woman. However, she is by no means alone. Allow me to move from this specific incident to a more general and more serious one.

A major data leakage, similar to the one that occurred in Hong Kong recently, happened in February 2005 to a US company, which is one of the largest aggregators and resellers of personal and consumer data in the USA. In the leakage the identities of 145,000 people were compromised. Since then data breaches involving hacking, stolen laptops, dishonest insiders and online interceptions have resulted in the identities of 89 million US citizens being compromised. Given that the US has a population of 300 million people that figure makes up around one third of the population. But here is a really staggering figure, the financial loss incurred from such leakages and repairing the damage is estimated to have cost US$48 billion.

The costs and time involved in correcting these data leakages and re-establishing personal identities, credit, insurance and banking records are astronomic. They offer

a poignant moral to the story and that moral should serve as a caution to us all.

One lesson is that IT, while bringing untold benefits to us all, is perhaps best regarded as a double-edged sword. A simple but telling adage applies where technology is used to protect, transmit or store personal data. It is:

"If it can be done with technology, it can be undone with technology."

Therein lies the dilemma for us all as we are obligated to accept the fact that IT is assuming an ever-greater significance upon our daily lives. It is difficult, if not futile, to divorce oneself from the influence of IT. I am afraid that for most of us the choice is no choice!

3 What is Privacy?

So, what is this thing called privacy? Frankly, there is no easy answer to that question. Nonetheless, it is important that we make some attempt at clarifying its meaning and getting a broad consensus on it. It was the French philosopher Voltaire who once said:

"Define your terms, and we shall talk."

I have now to confess that privacy is a word that seems destined to defy definition. Of course, we all have our own views about privacy and that is well and good but how much common understanding is there to our definitions? Despite, the tremendous interest expressed in privacy over the past two decades, the frustrations remain. Ray Wacks, a former professor of law at Hong Kong University, in a book he wrote titled, **"Hong Kong Data Privacy Law,"** observed, and I quote:

" … that in spite of the huge amount of literature on the subject, a satisfactory definition of 'privacy' remains as elusive as ever."

There is the problem in a nutshell. Has the privacy community in the 21st century satisfied Voltaire by defining clearly the term 'privacy?' Or, is imprecision hindering our shared understanding pf privacy?

Seeing that I am addressing an audience of people with a professional interest in languages, I wish to refer to the Chinese characters. They are 私隱. But, at best, this is unfortunate. Indeed, in Chinese society the very concept of privacy in its modern sense is relatively new. In Chinese vocabulary, the direct translation of the characters for privacy connotes the notion of secrecy, or that there is something which an individual consciously wishes to hide. Once again, clarity and consistency become lost in translation I'm afraid.

More recently my Office has addressed this issue by adopting a new logo that depicts a symbolic graphic rather than the former Chinese character, 私. I felt that character was inappropriate given our role.

So, can we make any sense of the notion of privacy at all? Yes, we can. If we stay for the time being with the generic notion of privacy then it is possible to identify four distinct privacy interests. These are:

1 **Information privacy;**

2 **Territorial privacy;**

3 **Personal privacy; and**

4 **Communications and surveillance privacy.**

I need hardly point out the significance of the last of these as recent events in Hong Kong vividly illustrate the tensions between constitutional privileges and public security.

I hope that this cursory examination of the linguistic difficulties associated with privacy has not conveyed to you that all is lost, because it isn't. For me the previous debate, although interesting, is a little academic because, as the name of my Office states, we operate in the realm of **personal data privacy.**

So, what is personal data privacy? Let me spend a little time giving definition to it.

4 What is personal data privacy?

The Ordinance that confers privacy rights and protects our personal data privacy in Hong Kong is called **The Personal Data (Privacy) Ordinance.** The law defines

personal data, and I'll paraphrase the exact legal definition, as:

" data directly or indirectly relating to the living individual from which it is practical for the identity of the individual to be ascertained, in a form in which access to, or processing of, the data is practical."

A few observations on this if I may. First of all, a dead person's personal data does not meet the criteria of the definition. Secondly, there must be a sufficiency of data to enable the individual to be identified. Thus, an ID card number alone does not necessarily constitute personal data. Thirdly, the personal data must be accessible and therefore recorded in either a physical or electronic format.

I am labouring the point here intentionally. Why? Well somewhat unfortunately my Office has become known as the PCO - the Privacy Commissioner's Office. It comes as a surprise to many of those that register complaints with us that in fact I am not the Privacy Commissioner. I am the Personal Data Privacy Commissioner. We are taking active measures to correct this misconception. However, I would

be less than candid if I did not admit that it has become something of a problem that we continue to wrestle with. We therefore find ourselves in the position of having to refuse complaints filed with us, and we do that quite regularly. This is not done on an arbitrary basis because we use various tests to establish a ***prima facie*** case. Where a 'complaint' fails those tests we are not empowered to investigate. However, once again you will note the significance of language here. Personal data privacy is but a sub-set of privacy in a generic sense and after 10 years we still need to hammer this message home.

In short, my Office is an advocate and protector of **personal data privacy rights**. No more and no less.

5 Privacy the Early Days

Let me move on. By the 1970s we began to see privacy gathering strength in Europe, which has a very rich tradition in furthering the cause. In 1973 Sweden became the first European country to pass personal data/information privacy protection laws. By the end of the 1970s a further six jurisdictions - Austria, Denmark, France, Germany, Jersey and Luxembourg - had followed

Sweden's example. In the 1980s a further fourteen jurisdictions had privacy laws. During that decade the privacy movement spread beyond Europe to Canada, Australia and New Zealand. It would seem that by the 1980s privacy had installed itself as one of the more sophisticated human rights in developed countries. Victor Hugo was correct when he observed:

"Nothing is as powerful as an idea whose time has come."

Privacy's position in Europe was strengthened by the Organisation for Economic Co-operation and Development. In 1980 an expert committee appointed by that Organisation promulgated the most influential set of privacy principles to date. Those principles are enshrined in the privacy laws of many jurisdictions including those of Hong Kong. Subsequently the European Union took up the privacy crusade with a number of important directives that have influenced privacy thinking. Most notable among these is the protection that is to be afforded personal data collected in one jurisdiction that is subsequently transferred

to another jurisdiction where there may, or may not, be similar legal protections for that data.

Very well. I have spent enough time on the Big Picture against which privacy developments have been set. Let me supplement that by now turning to the specific context of Hong Kong.

6 Privacy in Hong Kong ~ the Early Days

As you will have noted, in a global sense Hong Kong arrived on the scene none too early. However, it has made up for lost time and is now without doubt an influential voice in the Southeast Asian region today. I will say a little more about that contribution later on but for now I will concern myself with matters closer to home.

As I pointed out, in the 1980s privacy was on the ascendancy in Europe. However, at that time in Hong Kong it was largely the interest of a relatively small group of people.

I think two factors drove privacy developments here.

1 Firstly there was the economic or trade interest. As the European Union is one of Hong Kong's major trading partners there was a fundamental need to protect economic interests. Harmonising privacy legislation in Hong Kong with the demands of the European Union for data protection would best achieve that goal. In the process, Hong Kong would ensure that it became an EU-compliant trading partner.

2 Secondly, the human rights movement was gaining strength and this became a focal point for privacy. The movement also offered a sympathetic forum in which privacy obtained immediate recognition.

In 1994, after very extensive research and community consultation, the Law Reform Commission recommended:

"that the internationally agreed data protection guidelines be given statutory force in both the public and private sectors."

By "internationally agreed data protection guidelines" the Commission was referring to the principles laid down by the Organisation for Economic Cooperation and Development some 14 years earlier.

Although the Law Reform Commission was instrumental in placing our privacy laws on the statute book it would be wrong to convey the idea that they represented the only forces at work. In fact I think their views were influenced by at least two other developments.

1 Firstly, well before privacy assumed importance on the government's agenda in Hong Kong the UK government ratified the covenants contained in the International Covenant on Civil and Political Rights for the UK and its dependent territories, including Hong Kong.

Article 17 of the International Covenant states:

"No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour or reputation."

Closer to home Article 17 is reflected in the Basic Law's Article 39 and thus the spirit of the International Covenant's privacy provision is incorporated into our own local laws.

2 Secondly, there is evidence that in the 1990s technological, social and global economic factors played a part in bringing privacy to the fore. Let me take the first of these, technological developments, as an illustrative example.

If nothing else Hong Kong consumers have an ongoing love affair with hi-tech consumer durables. Our society exemplifies one in which new technology spreads rapidly.

For example, household ownership of PCs has mushroomed in the past 10 years. Today some 4.9 million people in Hong Kong are Internet users and 67% of households have broadband access. These developments have been matched by the explosive growth in .hk web sites. There are now in excess of 100,000 of them.

However, the enthusiasm for all things hi-tech only goes so far. Successive surveys, and our own research in particular, indicate that there are low levels of trust and confidence in the integrity of personal data both in transmission and in back-end storage. Hard experience has made many people wary of online transactions and the predicted boom in E-shopping just has not materialised. Even today only around one third of people with a bank account avail themselves of E-banking facilities.

Given this reticence we need to ask what the concerns are? A recent survey we conducted is illuminating on this point. The findings of that survey of 1000 young people indicate that nearly 80% of them regard their major concern to be the misuse of their personal data. Loss of money in online transactions was the second in their list of concerns. This gives some indication of the relative importance attached to personal data privacy.

If I were to expand upon social and global economic developments I think it would become very clear that there were, in the 1990s, a confluence of factors that provided

the right conditions for introducing privacy laws in Hong Kong.

7 The Personal Data Privacy Ordinance

Our privacy laws took effect in December 1996 when we opened for business. They are notable in the fact that they established my Office as a non governmental regulatory body - one that enjoys a high degree of autonomy. It is worth remembering that Hong Kong remains one of a handful of jurisdictions in which privacy is accorded this status. We distinguished ourselves in that respect from the outset and might well ask why that is so?

More significantly, ten years on, we remain the only privacy agency accorded independent status in Asia. While other countries, such as Japan and Korea, have personal data privacy laws the agencies in charge report directly to a Ministry or government department. To that extent they do not enjoy the same degree of independence of thought and action as we do.

In essence the law requires that my Office fulfil a number of key duties.

1 First, we exist to advocate, and uphold the privacy rights conferred upon citizens by the law. Those rights relate to the collection, use, accuracy, retention security and access to personal data. They are stated in their most succinct form in six Data Protection Principles.

2 Secondly, our regulatory function means that we have a duty to ensure compliance with the law among data users. This is a demanding task as there are millions of data users in Hong Kong and it is reasonable to conclude that many of them have a poorly developed understanding of the law e.g. SME's

3 Thirdly, it is our duty to inform and educate both data subjects and data users of their rights and obligations under the law. We attach great significance to this task because education, training and promotional activities are the best ways to influence behaviours.

4 Finally, we have a duty to safeguard the free flow of personal data to Hong Kong from restrictions by those jurisdictions that already have data protection

laws. Likewise, we have a duty to protect personal data collected in Hong Kong that is transferred to another jurisdiction where there may be no comparable privacy protections.

At this juncture perhaps I could ask you to reflect on a few questions that arise from what I have said so far.

~ Why is it that the advocacy of privacy rights in some Asian economies has been either muted or fallen on deaf ears?
~ Why have advocacy and social forces in some jurisdictions failed to produce the visible results that are evident in Hong Kong?
~ Why does Hong Kong continue to be different in this respect?

You may like to think on these questions.

8 The Pioneering Years

Let me make brief mention of our progress to date; a 10-year report card if you like. I regard the first eight years or so of our existence as something akin to a **pioneering**

phase. When the law came into being, in December 1996, few people had much of an understanding of what personal data privacy was about.

As I have indicated, privacy is a concept that is not easy to promote because it is rather nebulous. People have very different views of privacy and the value individuals attach to it. At the one extreme you have the privacy purists, at the other, those that deride privacy or attach little significance to it. The task for us therefore is to take a rather imprecise concept and give it a meaning and value that can readily be understood by most. And that is what we have tried to do. I don't think we have completely succeeded but then I don't think we ever will because we are in a race without a finishing line.

So, given our duties, the imprecision of privacy as a concept, grass roots ignorance and the complexities of the law, what have we been able to achieve in the pioneering phase of our development?

1 Firstly, we have managed to create **awareness and put personal data privacy on the mental map** that

all of us carry around. What makes me so confident in making this claim? In the first instance I would point to the publicity that privacy-related issues attract in the media these days. Insofar as the print media is concerned not a single day goes by without the mention of some story or disclosure about a privacy-related matter.

Added to that, our own surveys conducted by Hong Kong University indicate that there has been, over the years, a growing awareness of personal data privacy and related issues, for example, online security.

2 Secondly, I believe we have started out on our journey to create **a culture in Hong Kong that respects privacy and the personal data of the individual**. We have taken roadshows out to shopping malls, held competitions and devised educational entertainment shows for primary school children in our endeavours to build respect for privacy. It may take us a whole generation to create the value we want privacy to assume in the community but we are committed to the task.

3 Thirdly, I think that, in the main, we have been successful in **conveying to data users their obligations under the law**. Of course, there are outcrops of resistance and we have a lot of work to do in the area of small companies. Nonetheless, I think that most large corporate data users now realise that good privacy practices make for good business practices and in turn they make for good corporate governance.

4 Fourthly, I think we have been very successful in **influencing the public sector of the need to lead by example** in terms of their personal data privacy policies. Today, every government department that I know of that collects personal data has an officer who assumes responsibility for compliance. I think it important that the public sector take a lead in the sphere of exemplary personal data privacy practices quite simply because many departments collect massive amounts of personal data, some of it very sensitive data.

5 Finally, we have also been successful in networking with the private and public sector through our outreach programmes that involve training workshops, seminars and our Data Protection Officers Club, which has nearly 250 members.

Regionally we have worked on the development of a major privacy initiative called the APEC Privacy Framework. We are also active participants in a regional forum called APPA - Asia Pacific Privacy Authorities. These affiliations have given my Office a regional profile and although I don't want to sound immodest I can assure you that Hong Kong is a privacy regimen that commands respect in the Asia Pacific region.

Any credit I claim, I claim on behalf of all those who have worked in my Office and other privacy-related agencies in Hong Kong. I am determined to strengthen Hong Kong's position as we move forward into what I call the **consolidation phase** of our development. I'll talk a little more about this in a moment. Before I do so let me tell you a little bit more about the approach that my Office has

traditionally taken to the way in which we approach our work.

9 The Way we Operate

The way we operate has not necessarily emerged as the product of conscious endeavour. I think it has emerged out of custom and practice after a spell of trial and error. However, it is important because it is instructive and gives consistency and continuity to what we do. And that is important when we are offering legal advice and making rulings in specific cases.

In principle, we always try to ensure that our work is characterised by **four things**.

1 First, we are **guided by fairness** because we do not want to antagonise or alienate any section of the community. We may not be able to please all of the customers all of the time but then not even Coca Cola does that!

It is almost inevitable that there will be tensions between competing community interests and that is a

word that applies to the relationship between data subjects and data users at times. In those situations we try to place ourselves in the position of the respective parties so that we can strike a balance that is the product of consensus.

2 Secondly, this mentality is carried forward into the manner in which we deal with complaints. It should be remembered that my Office is a regulator and we can, if we want, use the stick rather than the carrot. Traditionally we have tended to err on the side of conciliation and brokering an acceptable deal rather than coercing or punishing the parties. In short, we have gone for mediation over confrontation.

3 Thirdly, we are **unabashed self-publicists** insofar as our work is concerned. We have limited resources and this forces us to be ingenious if we are to drive our message home. We use a variety of techniques to convey, often in a simplified form, explanations of our decisions in order to maximise exposure of our reasoning - exposure that we cannot afford in terms of more conventional advertising campaigns.

This is consistent with our view that we must sustain a high profile for our work in the community. In the battle for share of mind we have to acknowledge that there are many other social causes competing for public attention e.g. air quality and equal opportunities.

Our efforts have paid off because we do get extensive media coverage and this has ensured that privacy issues are 'up there' with other important social issues.

4 Finally, over the years, we have developed a very solid network of international relationships which enable us to benefit from the experience gained in other jurisdictions and to share research findings with them. There is much to learn from our counterparts overseas and we should not assume that we have a monopoly on good ideas.

If anything, networking is becoming more important because many privacy-related issues are of a global nature and therefore affect all of us.

10 The Way Forward

Let me conclude by fleshing out the way forward as we press on with the consolidation phase of our development.

I suppose that if we were completely successful we would put ourselves out of business. By which I mean that there would be no contraventions of our privacy laws and no intrusions upon our privacy in a more generic sense. That sentiment reflects the ideal world and I am afraid that is not the world we will ever find ourselves in. Our world is one characterised by contraventions of our privacy laws, and the number of violations are increasing. More significantly perhaps, they are growing in magnitude and seriousness in terms of their consequences for data subjects.

I mentioned earlier that our initial phase of development was what I termed the **pioneering phase** in which we worked to put privacy on the map. That has given way to a **consolidation phase**. Of course, we will continue with many of our duties and obligations but we will try and leverage earlier gains as we move forward. We will build on our strengths by focusing on a number of major privacy

initiatives that address developments that are of increasing concern. Those developments would include:

~ checking the excesses of the surveillance society;
~ the growing application of biometric technologies, that is, technologies that record a unique personal identifier e.g. a fingerprint; and
~ database security.

Given these priorities we now have to ask whether we need to change the way we have been operating in order to more effectively address future problems.

I will outline our intentions briefly to give you some indication of what lies ahead for us.

My intention is to redouble efforts to effect an attitudinal shift on the part of data users in terms of the respect they give to privacy rights. The implication of this is that we will have to increase our investment in compliance if we are to avert the sort of problems that emerge from database leakages. Those problems became very public

recently with the Independent Police Complaints Commission incident.

It is therefore my intention to significantly strengthen our compliance work. The team we hope to put in place will primarily be involved in two activities. Firstly, they will verify the personal data privacy policies and procedures of data users against their declaration on a data users register. A register of data users is one of our Office's current projects and will ultimately become a key information platform supporting compliance work.

Secondly, the team will proactively conduct compliance inspections on-site, notably of IT systems, database security and privacy protocols. I would like my Office to have the powers to enable us to gain access to premises to conduct those inspections unannounced. I hope in this way to send a powerful message to data users that lax, or non-existent, privacy practices will not be tolerated.

In order to put these initiatives in place my Office will shortly conclude a review of Hong Kong's privacy laws. The intention is to seek amendments designed to

streamline our operations and strengthen privacy protections. In the light of recent high profile privacy cases we will need to consider whether current sanctions fit what seem to be increasingly serious contraventions.

If in the past we have tended to err on the side of the carrot rather than the stick, this ethos is another thing we need to reappraise. If, after nearly 10 years of privacy legislation, data users persist in practices that demonstrate blatant irresponsibility concerning their legal obligations to protect personal data then it is time to evaluate other options.

I hope this review of the development of privacy, and personal data privacy in Hong Kong in particular, has provided you with a better understanding of the work of my Office.

I would like to conclude by posing some questions. In the best interests of protecting the individual's personal data privacy:-

1 Should the remit of my Office be extended beyond the realm of personal data privacy to afford more comprehensive protection of our privacy?

2 Should the Privacy Commissioner, as is the case in some other jurisdictions become the overseer of freedom of information?

3 Given that technology is both a friend and foe of privacy, how should we respond to it as an increasingly domineering feature in our life?

The CEO of a renowned computer software company recently observed:

"No one has any privacy any more."

You see, there are those who have a vested interest in ensuring that particular vision of the world comes about. How can we best influence that vision so that in 10 or 20 years time privacy protections remain robust rather than a thing of the past?

In the next decade we will have to address these questions and the issues they raise. Unless we do, privacy rights in Hong Kong, and elsewhere for that matter, will not make the transition from consolidation to maturity.