Hong Kong Institute of Certified Public Accountants
IT Conference 2010: Information highway – linking Hong Kong to the Global village and how accountants can add value

Keynote Speech by Mr. Allan CHIANG,
Privacy Commissioner for Personal Data

9 am – 1pm, 27 November 2010 (Sat)
Grand Ballroom, Lower Level 1, Kowloon Shangri-la Hotel

Good morning, ladies and gentlemen. This is an important event for both accounting and IT professionals and I am honoured to be given this opportunity to speak about the importance of personal data privacy.

In this information age, the combined effects of emerging Internet technologies, increased computing power and fast, pervasive digital communications are creating new business models and tools that enable companies to collect, analyse, combine, use, transmit and store vast amounts of consumers' information in ways that are often invisible to consumers. Such practices have posed immense risks to privacy and protection of personal data.

Let me outline for you how some major technological developments are challenging privacy.

RFID

First, RFID or Radio-frequency identification which happens to be the subject of the second keynote session today. I am sure Mr. Jonson Yue will explain in detail what this technology is and its benefits. Suffice it to say that RFID is the next generation technology beyond barcodes.

RFID tags can be attached to consumer products and be read electronically from a distance quickly and easily, making them valuable for managing inventory and supply chain logistics. RFID chips can also be implanted in people for monitoring and transmitting critical health conditions.

Imagine a world of "ubiquitous computing" where RFID is part of our daily lives. As you walk down the street, the embedded RFID microchips could emit a cloud of data – from you, your clothes, your purse and other personal items. Anyone with a suitable receiving device could conceivably collect vast amounts of your personal information and build a profile of yours without your knowledge or consent.

The more troubling or scary part of the scenario is that information about the item is recorded together with information of time and location, thus creating a potential for ongoing surveillance. In other words, your every move could be tracked and monitored.

MOBILE

Before the advent of this era where more and more objects are connected to information networks, the so-called “internet of things”, we are already living in a world of mobile data processing. Today, 5 billion mobile subscriptions worldwide are powering a growing variety of computing devices, including not only mobile phones but also smart phones, PDAs, netbooks, laptops and portable gaming devices. Like RFID enabled devices, mobile devices also raise the privacy issue of location tracking.

Mobile devices are able to detect, store, and broadcast in real time their physical location. They allow subscribers access to a range of new services and applications such as locating nearby friends, finding recommended restaurants in foreign cities, “checking in” at venues to receive discounts and coupons, and obtaining up-to-date traffic reports. However, many individuals may not be aware that the location of their mobile device is constantly being recorded even if the device is not used.

Think for a minute. When you travel abroad and land from a plane, who is the first one to greet you. Not the immigration or customs officials, nor your wife or husband calling from home, but your mobile network operator. Isn’t it?

CLOUD COMPUTING

The next technology I would like to talk about is cloud computing. This is the subject of the third keynote session this morning. Again, without stealing the limelight of Mr. Edvan Chan, I would simply say that users of cloud computing store and process data on massive remote servers accessible through the Internet rather than on local computers. For consumers, examples of cloud applications include web-based e-mail, online calendars, document management sites and photo-sharing sites. As regards commercial applications, firms are increasingly relying on cloud-based computing to incorporate their most mission-critical software applications.

The basic privacy risk of cloud computing is that the user loses control over the data that have been fed into a given application, as data changes hands, crosses borders, and may be accessed and used without the user's knowledge and consent.

BEHAVIOURAL ADVERTISING

Now, let me change the subject to the collection of information about individuals for advertising purposes. Such practices are common in the physical world but are more pervasive on the Internet. In order to gain access to web sites, you may have to register and provide personal information. When you make online purchases, you definitely have to provide personal information.

In addition, many websites employ discrete ways of collecting information on individuals, for example, through the use of cookies. They aggregate data about the user and create detailed personal profiles including user preferences and interests.

As a result, they are able to make predictions about which advertisements might appeal to which consumers. Those targeted ads are then served up while a user is browsing a Web site. Such behavioural advertising is very targeted, thus explaining why the advertising revenue is more than enough to sustain a free Web site to consumers.

But behavioural advertising also raises fundamental questions about consumers' expectations and assumptions regarding their privacy. It is unclear whether consumers fully accept that they are paying for "free" information or services by disclosing their personal information. We are all aware of the infamous Octopus incident. It seems clear that many Hong Kong people do mind enterprises sharing their personal data with third parties for profit without their consent.

Now, as data-gathering technologies infiltrate more of our lives, there may be a "tipping point" where consumers would no longer be able to exercise control over the collection and use of their personal information even if they want to, because so much of their digital life has already been exposed. Indeed, as some privacy sceptics have said, "Privacy is dead or dying".

DATA PROTECTION PRINCIPLES

Ladies and gentlemen, such declarations of the death of privacy have been over-exaggerated. As the Privacy Commissioner for Personal Data, I act in collaboration with my counterparts worldwide to protect privacy in relation to personal data. The Personal Data (Privacy) Ordinance, which has been in force since 1996, provides the legislative framework in this regard. Although the Ordinance is presently under review to ensure that the provisions provide adequate data protection in light of rising human rights expectation and rapid developments of information and communications technology, the 6 Data Protection Principles, which form the backbone of the Ordinance, have stood the test of time. I will briefly go through these 6 principles here.

Principle 1 – [Purpose and manner of collection] This provides for the lawful and fair collection of personal data and sets out the information a data user must give to a data subject when collecting personal data from that subject.

Principle 2 -- [Accuracy and duration of retention] This provides that personal data should be accurate, up-to-date and kept no longer than necessary.

Principle 3 -- [Use of personal data] This provides that unless the data subject gives consent, otherwise personal data should be used for the purposes for which they were collected or a directly related purpose.

Principle 4 -- [Security of personal data] This requires appropriate security measures to be applied to personal data.

Principle 5 -- [Information to be generally available] This provides for openness by data users about the kinds of personal data they hold and the main purposes for which personal data are used.

Principle 6 -- [Access to personal data] This provides for data subjects to have rights of access to and correction of their personal data.

I appeal to you that these Data Protection Principles must be adhered to in the development and adoption of new information and communications technologies so that any privacy-invasive risks could either be minimized or eliminated altogether.

First, personal data protection should be made an integral part of any project or system that involves personal data from planning to execution.

During the planning stage, *privacy impact assessment* should be carried out to identify any potential issue that a project may have on personal data and privacy protection and how it may be avoided or mitigated prior to any actual design.

Even if the final design has taken care of all the issues identified in the *privacy impact assessment*, given the changing nature of the

business environment, regular *privacy compliance assessments* should be carried out throughout the lifetime of the project to ensure continuous compliance with the *data protection principles*.

I would like to quote three recent IT-related cases to illustrate the importance of embedding privacy into the key fabric of technology itself.

FINGERPRINT RECOGNITION SYSTEM

The first case related to the use of fingerprint recognition system to record employee attendance in a local furniture company. While it provided a convenient and perhaps speedy solution to a mundane task, the use of biometric personal data like fingerprints for the purpose of attendance recording was too privacy-intrusive a measure.

We have to bear in mind that unlike a password or PIN which can be reset, fingerprints are very personal and private because they are unique information about an individual's physical self. The integrity of such data must be safeguarded to protect the individual's identity against theft or misappropriation.

Furthermore, the internal rules of the company provided for immediate dismissal for those employees who did not use the fingerprint system. The disparity in bargaining power between the employer and the employee would cast doubt on whether a fair consent had been given by the employees in the circumstances. A

privacy impact assessment would have picked up these potential controversies before the scheme had the chance to take off.

GOOGLE STREET VIEW PROJECT

The second example I'd like to mention refers to Google's Street View Project this year. It isn't so much a fault at the design stage, but at its execution. Google admitted that it had inadvertently collected Wi-Fi payload data while snapping pictures for the Street View project. It was revealed later that the intention was only to collect Wi-Fi station names and not the payload data.

The project manager, while selecting the software, overlooked the fact that the software was also capable of capturing the payload data. Such an execution error would not have been detected in a *privacy impact assessment* but should have been picked up in a subsequent *privacy compliance assessment.*

WHOLE BODY IMAGING

The third example refers the use of whole body imaging scanners to improve airport security. This is a programme of the U.S. Transportation Security Administration and, as reported widely in the media recently, has generated much controversies because it is tantamount to a "digital strip search".

By using backscatter or millimeter-wave scanners, metal and/or plastic weapons, explosives and drugs hidden underneath clothing

could be revealed in a image of the naked body. This obviously raises privacy concerns but these can be resolved by well thought-out privacy protection policies. First, the scanner image should be viewed in a remote location by a trained security official who does not interact with the scanned passenger before or after the scans, or has any personal information about him or her.

Secondly, there must be a complete prohibition against any retention or transmission of the images in any format. More importantly, to address the concern that the scans produce anatomically detailed and identifiable images of the naked body, “privacy filters” could be applied to the scanned image before it is viewed. These filters either obscure the personal details of the body or transform the raw image into an outline in which only potential threat items are highlighted.

Although the U.S. authorities have yet to adopt these privacy filters, it should be clear that when privacy protection principles on collection, use and disclosure of personal data are implemented together with appropriate privacy-enhancing technology, increased airport security could be delivered without compromising privacy.

CONCLUSION

To conclude, I submit that all information and communication technologies are, from a privacy perspective, essentially neutral. What matters are the choices made in their design and use. As Privacy Commissioner, I would advocate embedding privacy at the early design stages of information technologies so that otherwise

privacy-intrusive technologies could be turned into privacy-enhancing technologies, embracing the data protection principles of minimizing personal data use, maximizing data security, and empowering individuals.

In a world of ubiquitous data availability that we live in, this win-win approach can also transform privacy issues into lasting privacy solutions – ensuring that privacy, far from dying, is alive and kicking.

Thank you very much.