

**Privacy Laws and Business Conference
Cambridge, England**

Theme: Privacy Crisis Ahead?

**Day 3~Wednesday 5th July 2006
9:40 am Session**

**Title: Privacy Crises in Hong Kong and how the
Privacy Commissioner is Dealing with them**

**Mr Chairman, Distinguished Guests, Ladies and
Gentlemen**

1 Introduction

It is uncanny the way in which events occur in life. On first reading about this conference I had no idea at the time just how prophetic its main theme would be for those of us in the privacy community in Hong Kong. In March of this year three simultaneous database leakages of significant amounts of personal data occurred in Hong Kong. They aroused considerable public concern, extensive media coverage and embarrassment for the data users concerned. The most significant data leakage occurred in a publicly funded agency the **Independent Police Complaints**

Council (“the IPCC”) which monitors and reviews the investigation of complaints filed against members of the Hong Kong Police force. However, within days of this leakage being reported the media ran stories on two other database leakages that had been brought to their attention by Internet surfers. The latter cases involved a telecommunications company based in Hong Kong - **CSL**, and a European-based international bank - **ING**. In the interests of brevity I will concentrate upon the IPCC case as this was without doubt the most serious.

I want, in the time available, to attempt five things:

- 1 Briefly overview these three database leakages in terms of the events that gave rise to them;
- 2 Comment upon the primary cause of the leakages;
- 3 Look at what the response of my Office has been;
- 4 Examine whether existing remedies under the law adequately address the issues, the crisis if you like; and
- 5 Comment upon the legislative amendments deemed necessary to instil greater respect for personal data privacy.

As the IPCC case is rather complex I can only convey an overview but I am happy to take any questions you may have at the end of this presentation. During question time you may also wish to discuss the Yahoo! incident that has emerged in China and with which my Office has been involved. That incident may develop into a privacy crisis because it involves the disclosure of data by an Internet portal (Yahoo! China) to Mainland Chinese authorities. The information disclosed by Yahoo! China to the Chinese authorities eventually led to a journalist being charged, tried, convicted and sent to prison for 10 years for sending state secrets overseas by e-mail.

As I say, I am happy to discuss this case but for the time being let me revert to the IPCC incident.

2 A Review of Recent Database Leakage Incidents in Hong Kong

The IPCC Incident

In February a local newspaper reported that a Web surfer, while searching for an address, had stumbled upon a database administered by the IPCC. This database

included the names, addresses and Hong Kong Identity Card numbers of 20,000 complainants and whether they had a criminal record. It also included the names and service numbers of police officers implicated in the complaints. What made this chance discovery even more alarming was that the 20,000 names had been placed on a publicly accessible website. It later became clear that the names had been posted on the website for a period of 2 years.

Judging the newsworthiness of this discovery correctly, the editor of the English language daily - the South China Morning Post - ran the story on the first page of its next edition. The reaction was both immediate and predictable. There was massive exposure of the story in the media which aroused public outcry and questions in our Legislative Council. On hearing of the leakage, I immediately held discussions with the IPCC and, on the basis of those discussions, commenced a formal investigation. To date we have received more than 50 complaints from members of the public who claim to be among the 20,000 whose personal data have been leaked,

some among them say that they worry about reprisal and want new identity cards.

Three database leaks in quick succession left people in Hong Kong wondering just how many other databases containing customer personal data were 'out there' in cyberspace waiting to be discovered. They did not have to wait long for an answer. In mid-March it was reported that the personal data of 300 staff of a company, the members of a choir associated with the University of Hong Kong and 60 students of a secondary college had all be found on the Web.

What do these incidents have in common?

- 1 First, they indicate that data users are not taking their compliance obligations seriously enough by ensuring that appropriate privacy protection measures are in place: both IT-based and people-based measures.
- 2 Second, they exhibit serious shortcomings in managerial control over, and responsibility for, the actions of third parties contracted to manage the

databases in question. I will explain this in rather more detail later.

- 3 Third, the incidents are symptomatic of negligent corporate governance. This is unacceptable. In the private sector there is plenty of evidence to support the view that corporate cavalierism can be very damaging to business interests.

Not an exhaustive charge sheet but enough to be going on with for now.

On reflection one is tempted to observe, given the detail that has been uncovered during the course of our investigations into these three incidents, that what we, in the privacy community, should be lobbying hard for is the privacy-equivalent of a Sarbanes Oxley Act. There can be little that is more sobering to public servants or corporate executives than a 25 million dollar fine, or the prospect of 20 years in jail!

The knock-on effect in Hong Kong right now is that there has been a loss of public confidence, in both the ability and

commitment among data users to do their utmost to protect personal data privacy. However, as is often the case in life out of the bad comes good. Ironically it is precisely these sorts of blunders that play into the hands of regulators such as myself. I will explain what I mean in a moment but I want now to move on to look at **how** the damage was done.

3 Outsourcing and Accountability

The popularity of business process re-engineering has been mirrored by a growing reliance upon the outsourcing of non-essential corporate activities. Nowhere is this more so than in the area of IT where a network of contractors and sub-contractors has become an established part of the modus operandi. In a bid to preserve competitiveness such developments are logical, if not essential. However, acceptance of this way of doing things must be predicated on a number of imperatives.

- 1 The first of these is the belief that personal data is of strategic value to many organisations. It is entrusted to them for safe-keeping and, as such, should be accorded the respect and protection that it deserves.

- 2 A second is that the legal obligations of principals, contractors and sub-contractors should be regulated by contractual clauses that deal with the confidentiality of personal data and the absolute need to ensure compliance with privacy provisions.
- 3 The third amounts to little more than the data user placing himself in the shoes of the data subject and applying a little commonsense. For example, recourse to the precautionary measure of using anonymised or dummy data for system testing purposes.

In the IPCC incident such pre-occupations seem not to have crossed the minds of the parties involved. Indeed the IPCC appear to have had very little understanding, if any, of what its IT contractor and sub-contractors were doing with the database. An absence of contractual provisions to protect the data of the complainants against individual police officers and a lack of intimate knowledge of the practices of the contractor and sub-contractor gave rise to a situation in which the principal was blissfully ignorant

of the manner in which the personal data were being handled and processed. It came as a surprise to the principal to learn that the CDs containing the personal data which were given to an IT sub-contractor for processing had been copied to a file server using File Transfer Protocol and in the process the integrity of the data was lost when it eventually appeared on a publicly accessible website.

The catalogue of mistakes therefore included:

- carelessness;
- an absence of IT expertise on the part of the principal;
- a lack of transparency in the relationship between the principal, the contractor and sub-contractor; and,
- an almost complete absence of accountability.

Put it all together and what you have is a personal data privacy accident waiting to happen.

Once the investigation by my Office was underway I was struck by the level of public denial that characterised the

positions adopted by the respective parties. By now matters had degenerated into the ‘blame game.’

In the case of **CSL** the data leakage was also attributed to a vendor who had placed two databases containing the personal data of customers on a publicly-accessible server. The vendor obtained the customer data contained in the loyalty programme database for compiling and undertaking analyses and filing reports.

Let me summarise the salient points illustrated by all three incidents - **IPCC, CSL and ING** - in their use of either outsourcing, or the transfer of data to an indirect employee of the business.

- 1 First, there is evidence to suggest that the principal failed to ensure that the parties to which they transferred personal data complied with usage, confidentiality and disclosure instructions. Why? Because there were no such instructions.
- 2 Second, there appears to have been a complete breakdown in conveying to contractors and third

parties the importance of applying appropriate security and privacy protection measures to data once it left the electronic or physical presence of the principal. I find it difficult to believe in 2006 that this imperative is an alien concept among IT practitioners.

One thing is very clear and that is that there are certain types of businesses that use extensive networks of contractors, sales agents or other intermediaries and it is these sorts of businesses that seem prone to non-compliance. Personal selling is a case in point as in many instances indirect employees or moonlighters are recruited to the job. These people require sales contact data wherever they go and whenever they need to, and so it is common practice for them to access remote servers for retrieving data. What this means is that there is a heavy duty of responsibility on the shoulders of systems administrators to ensure that security settings are robust and controls are being enforced.

4 A Measured Response

Of course there is learning in all this and I am determined that the lessons be learned to minimise the likelihood of

any recurrence. Apart from initiating a formal investigation my Office embarked upon an aggressive communications campaign designed to reassure the public that we were treating the incidents with the utmost seriousness. I think that we have gotten our views across and certainly had them widely reported. In such circumstances there is no substitute for good communications and by that I mean disseminating clear, simple and consistent messages.

So, what other measures are we taking to try and address the issues I have identified? Two initiatives are worthy of mention.

- 1 The first of these has been for us to conduct a thoroughgoing review of our law with a view to suggesting a raft of amendments. I will say more about this in a moment.
- 2 Secondly, we took the initiative to establish an IT Governance Working Group.

The primary purpose of the group is to facilitate discussions with representatives of IT professional

associations concerning the ways in which we might highlight members' responsibilities as data users, raise awareness of privacy issues and encourage the adoption of effective measures to prevent such incidents from recurring.

I am pleased to report that the second of these initiatives has borne fruit. The working group is currently promulgating privacy guidelines for IT practitioners which will be released in a few months time. This is an interim measure and will be supplemented by a Code of Practice on Electronic Storage and Transmission. In addition, we have launched an Information Security Enhancement Campaign which is a package of measures that includes educating students in the tertiary sector, offering seminars and, later this year, organising a conference on the security aspects of personal data. We hope by these means to sustain a high profile and raise awareness among data users that will ultimately result in the adoption of appropriate privacy-compliant behaviours and the implementation of effective security and privacy protocols.

The first measure i.e. changing our law will take rather longer but we hope that the publicity surrounding these data leakage incidents will result in the government attaching urgency to the legislative process.

We are of the view that these combined measures will assuage public fears and send a clear message to the community, and those in the IT industry in particular, that we are determined in our efforts to put right that which is wrong.

5 Does the law address the crisis and does the punishment fit the crime?

I am sure that it will occur to you from what I have said that there are distinct limitations to the remedies that I am empowered to apply in these circumstances: I share the public's doubt about whether the sanctions contained in the provisions of our law fit the crime.

However, I would concede that the crime is not uniform in nature. There is a distinction that should be made between genuine lapses in compliance that are the result of carelessness or systems deficiencies and deliberate attempts

at unauthorised access to personal data that are premeditated and malicious in intent.

In relation to compliance with the provisions of our law, my Office has the power to inspect personal data systems, to investigate complaints and to self-initiate investigations into any acts or practices associated with the handling of personal data. To facilitate investigations and inspections I, as the Commissioner, am empowered to send prescribed officers to enter premises with prior notice, summon any person to give evidence and to hold hearings in public or private. However, in the context of cyberspace such powers are of limited effect.

In the event of a contravention of our law being found I, as the Commissioner, may issue an enforcement notice requiring the data user to desist from such actions that led to the contravention within a specified period, if there is reason to believe that there will be a repetition of the contravention. Unless my decision is overturned on appeal, any non-compliance with the terms of the enforcement notice will oblige me to refer the matter to the police for prosecution. Over the years there have been a

minimal number of cases in which the police prosecuted and successfully obtained a conviction.

However, contraventions committed in cyberspace are altogether a different matter. Regrettably, to the dismay of many of us, there is no Interpol on the Internet.

It is evident that back in the early 1990s the spirit of legislators were inclined to place emphasis upon education, training, publicity and media relations as the means of influencing public attitudes and behaviours towards personal data privacy. That rationale rested upon an appeal to better nature and the power of persuasion. However, the occurrence of data leakages as serious as that in the IPCC case give rise to considerable doubts regarding the effectiveness of this strategy.

So, what is the nature of the crisis that the strategies we deploy, and the legislation we resort to, must address? I think I can answer this question best by reflecting upon the evolution of privacy in Hong Kong. Our legislation in its original form was deliberately framed in technology-neutral language. You won't, for example, find reference to the

Internet or spam in the provisions. This gives insights to the legal intent of the law drafters. It seems to me that they felt the sorts of challenges to privacy that are largely the product of the application of IT should be dealt with by dedicated legislation, which is what may be happening. For example, anti-spam legislation is currently being contemplated and may come into effect later this year.

Now, that sort of thinking may have been well grounded in the early or mid-1990s. The era was characterised by a lower household ownership of PC's. The Internet to all practical intents and purposes had not been invented and IT was considerably less pervasive in people's lives. However, that picture has changed dramatically especially in an intensely populated metropolis such as Hong Kong. It is the sheer scale and nature of IT change in particular that has given rise to the crisis in privacy. The IPCC incident both exemplifies this, and is a by-product of it. In essence the crisis derives from the fact that legislation has not anticipated the massive and pervasive influence of IT upon our lives and, by extension, upon our privacy.

6 Changing behaviours: legislative amendments

Today data mining techniques, digital compression, the increased power of PCs, a plethora of Internet-based services and reduced costs of data warehousing have had an impact that was difficult to predict 12 years ago. One illustration of these advances is the number of databases containing our personal data. I doubt anyone in the audience can hazard a guess as to how many databases contain their personal data today. To some extent that is a measure of the pervasiveness of technology. One thing is for sure, the number of databases containing your personal data and mine will only increase. The temptation to collect more and yet more data is for most, if not all data users, simply irresistible. I am convinced that the prevailing view is that one just cannot have too much data and IT has played a large part in driving that mentality.

It is in this context that our privacy law is currently set, a context that is markedly different from the one in which it was conceived. If anything events have overtaken us because our law just did not anticipate a world in which immense banks of information on a growing proportion of the world's population would characterise the landscape. Of course, such IT developments have given rise to many

benefits and I would not want to under-estimate them. Equally so, they have given rise to unacceptable if not criminal behaviours. It is those behaviours that must be addressed because they represent the crisis and a formidable challenge to us all.

In Hong Kong personal data privacy rights have, in a relatively short space of time, come to be understood and valued. We know this from the findings of successive surveys we have commissioned. However, if the public perception is that the law no longer effectively dissuades those who would deliberately or accidentally violate our privacy rights then it no longer remains good law.

It is with these sorts of arguments in mind that I am chairing a working party to consider proposing comprehensive changes to our law. The more important of these have, I think, been vindicated by recent data leakages and are what the public expects of us. The spate of data leakages and contraventions have made a review of the Ordinance an imperative. It is to be hoped that our lawmakers will look carefully at the existing provisions and

deliberate on how they might be revised to effectively meet the challenges of contemporary privacy issues.

Unfortunately, we do not live in an ideal world characterised by a culture of respect for privacy. The real world is one in which investigating complaints continues to be successful. While the law does not provide a panacea for all privacy problems, the amendments proposed would offer the individual hope, protection and redress, subject to adequate resources being devoted to compliance. If data users and others, aided and abetted by IT, continue to violate our personal data privacy rights then the force of law should be brought to bear upon them.

In conclusion, my view has always been that a privacy commissioner's office is very much involved in the business of promoting attitudinal shift and behavioural change. If conventional strategies, which may have been underwritten by a tradition of voluntarism, are no longer working and if we do not address privacy crises in a robust manner, contraventions such as those illustrated will proliferate. In so doing, they will erode privacy rights. They will also erode people's faith in such rights. And

finally, people will lose faith in privacy regulators who are charged with the duties of protecting them of such rights.

I have travelled a long way to say what I have just said because this conference brings together people who are dedicated to work for privacy rights across the world without national borders.

I am grateful that I had the opportunity to talk to you and I am grateful that you listened to me.

God bless you.

END