

# Implementing Data Protection Laws In Asia – A Balanced Approach

Stephen Lau

Advisor, HP Enterprise Services Hong Kong

&

Former Hong Kong Privacy Commissioner for  
Personal Data



*Malaysia*

*July 2010*

# What Is Privacy?

## The right to be left alone

- the interest of the person in controlling the information held by others about him, or "*information privacy*";
- the interest in controlling entry to the "personal place", or "*territorial privacy*";
- the interest in freedom from interference with one's person, or "*personal privacy*";
- the interest in freedom from surveillance and from interception of one's communications, or "*communications and surveillance privacy*".

# Personal Data Protection a Global Issue

- Increasing societal affluence (70's)
- Advances in computers, digital storage and telecommunications (80's) leading to
- Exponential growth of personal data collected, transmitted and exploited
- The internet going critical and the advent of eCommerce (90's)

# Privacy & Personal Data Protection & computers

- (a) they facilitate the maintenance of extensive record systems and the retention of data in those systems;
- (b) they can make the data easily and quickly accessible from many different points;
- (c) they make it possible for data to be transferred quickly from the information system to another;
- (d) they make it possible for data to be combined in ways which might not otherwise be practicable; and
- (e) because the data are stored, processed and often transmitted in a form which is not directly intelligible, few people may know what is in the record or what is happening to it.

- 
- 

1975 UK White Paper

# Transborder Data Flow

- Using credit card overseas
- Buying foreign securities
- Employees' records of multinational companies
- Internet

# The Internet of Information

- -B2B ( Business to Business)
- B2C ( Business to Consumer)
- Explosion of personal information collection and sharing

# Audio Clip

- <http://www.aclu.org/pizza/>

# LEGISLATION

# Privacy Laws

## **United States:**

- Federal public sector Privacy Act;
- Sectoral privacy laws;

## **Europe:**

- Both private and public sector data privacy laws;
- European Directive on Data Protection.

# United States

## *Sectoral Laws: A Sample \**

- •2002: Sarbanes-Oxley
- •2000: Children's Online Privacy Protection Act
- •1999: Gramm-Leach-Bliley
- •1996: Health Insurance Portability and Accountability Act
- •1988: Video Privacy Protection Act
- •1986: Electronic Communications Privacy Act
  
- \* This list represents only a small sample of sectoral laws in the United States.

# Privacy Laws

## **Asia Pacific**

Federal laws in Australia, New Zealand,  
Hong Kong, Japan, Korea, Malaysia

Sectoral privacy laws in Taiwan, Thailand

# HONG KONG Personal Data (Privacy) Ordinance

- to protect the individual's right to privacy with respect to personal data
- to safeguard the free flow of personal data to Hong Kong from restrictions by countries that already have data protection laws

# HONG KONG

## Personal Data (Privacy) Ordinance

- it covers both automated and manual data;
- it covers both the public and private sectors; and
- it establishes an independent statutory body which has wide-ranging investigation and enforcement powers to be exercised when and where appropriate to ensure compliance.

# Personal Data

"Data" is defined in the Ordinance as any representation of information (including an expression of opinion) in any document, and includes a personal identifier, and "Personal Data" is defined as any data:

- relating directly or indirectly to a living individual
- from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
- in a form in which access to or processing of the data is practicable.

**Privacy Laws generally  
adopt a number of  
universal personal data  
protection principles**

# Personal Data Protection Principles

- ***OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (80's)***
- ***EU Directive on Data Protection (90's)***

# Hong Kong Personal Data (Privacy) Ordinance

## Data Protection Principles

### 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 the 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.

# Hong Kong Personal Data (Privacy) Ordinance Data Protection Principles

## 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.

# Hong Kong Personal Data (Privacy) Ordinance Data Protection Principles

## Principle 4 - Security of Personal Data –

All practicable steps shall be taken to ensure that personal data held by a data user are protected against *unauthorized or accidental access, processing, erasure or other use* having particular regard to -

- (a) the kind of data and the *harm* that could result if any of those things should occur;
- (b) the *physical* location where the data are stored;

# Hong Kong Personal Data (Privacy) Ordinance Data Protection Principles

## 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.

# Balance of Rights

- **The right of individuals is not absolute.**
- **It must be balanced against societal rights.**

# Hong Kong Personal Data (Privacy) Ordinance Exemptions

The Ordinance provides specific exemptions from the requirements of the Ordinance. They include:

- a broad exemption from the provisions of the Ordinance for personal data held for domestic or recreational purposes;
- exemptions from the subject access and use limitation requirements of the Ordinance where their application is likely to prejudice certain competing public or social interests, such as: security, defence and international relations; prevention or detection of crime; assessment or collection of any tax or duty; news activities; and health.

# Main Functions and Powers of the Privacy Commissioner

- monitor and supervise compliance with the provisions of the Ordinance;
- approve and issue codes of practice giving practical guidance for compliance; with the provisions of the Ordinance;
- specify classes of data users required to provide information concerning their personal data practices for compilation of a public register of data users;
- approve the automated matching of personal data;
- promote awareness and understanding of, and compliance with, the provisions of the Ordinance;
- carry out inspections of personal data systems, including those of Government departments and statutory corporations; and
- investigate, upon receipt of complaints from data subjects or on his own initiative, suspected breaches of requirements of the Ordinance.

# Power of the Commissioner

- Investigate complaints
- Warning notice/enforcement notice
- Compliance checking
- Inspection
- No power on criminal investigation
- No power to impose fines
- Complainant has appeal mechanism

# A Major Cultural Challenge

PRIVACY ?

DATA PRIVACY ? ?

PERSONAL DATA PRIVACY ? ?

# Asia vs the "West"



# Privacy in the Chinese context

- Culture (Confucian)
- History and power of the state
- The hierarchy of needs
- A contemporary concept

# Education and Awareness

- Logo competition
- Training courses/workshops
- Annual baseline survey on awareness/attitude
- Roadshows
- Guidelines
- TV/Radio advertisement
- Privacy Officers' Club
- Website [www.pcpd.org.hk](http://www.pcpd.org.hk)



# Cultural shift

- Organisations hold personal data of employees and clients not as **OWNER**, but as **CUSTODIAN**
- Individuals be aware of the need of personal data, there is a law to protect them, and a Commissioner with whom complaints can be lodged

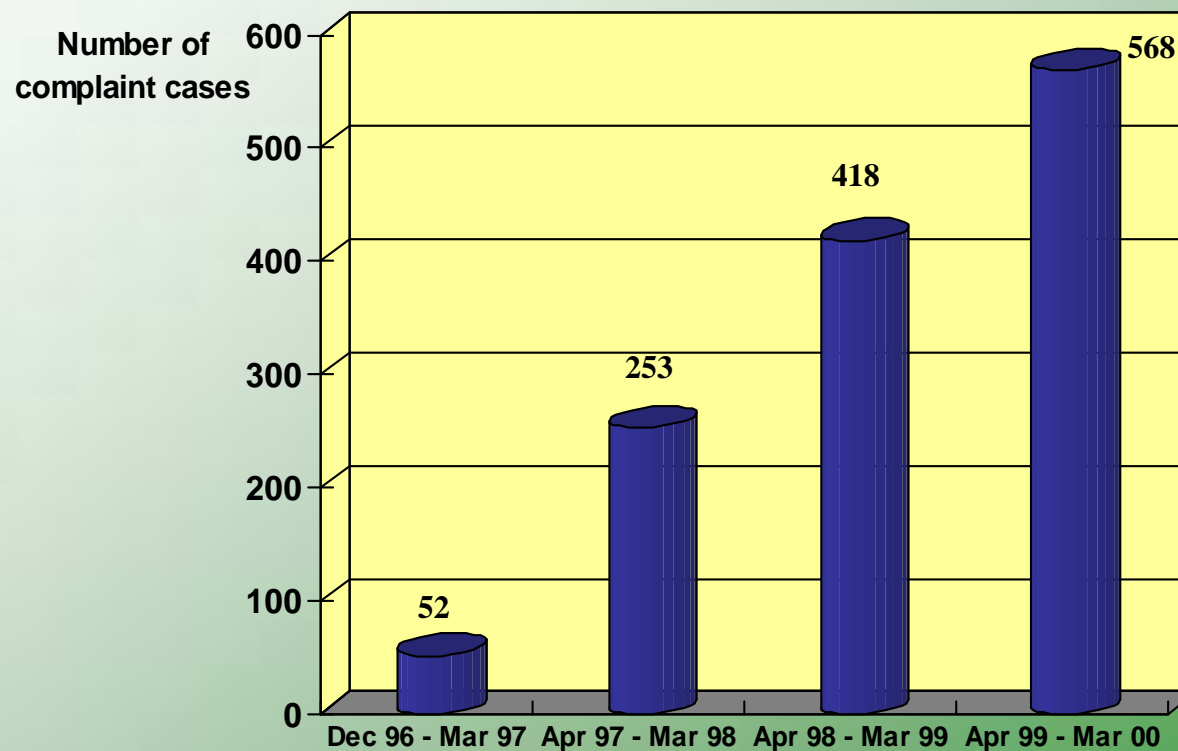
# Committees

- **ADVISORY Board**
- **Committee on TECHNOLOGY Development**

# Other challenges Then..

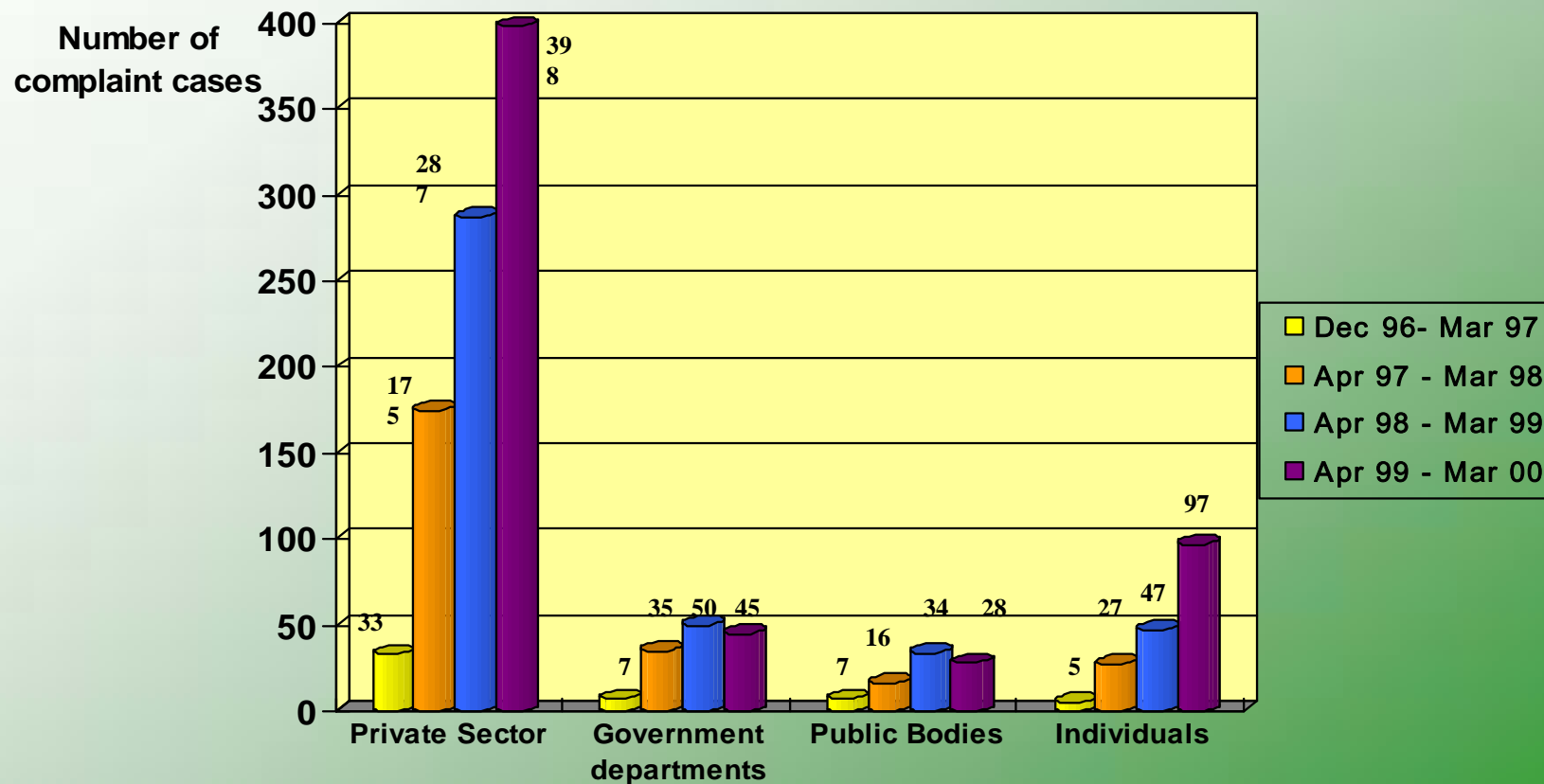
- **Staffing**
- **Up the learning curve**
- **Establish trust and confidence through professionalism, service excellence**

# Office of the Privacy Commissioner for Personal Data, Hong Kong Annual complaint caseload (1999-2000)



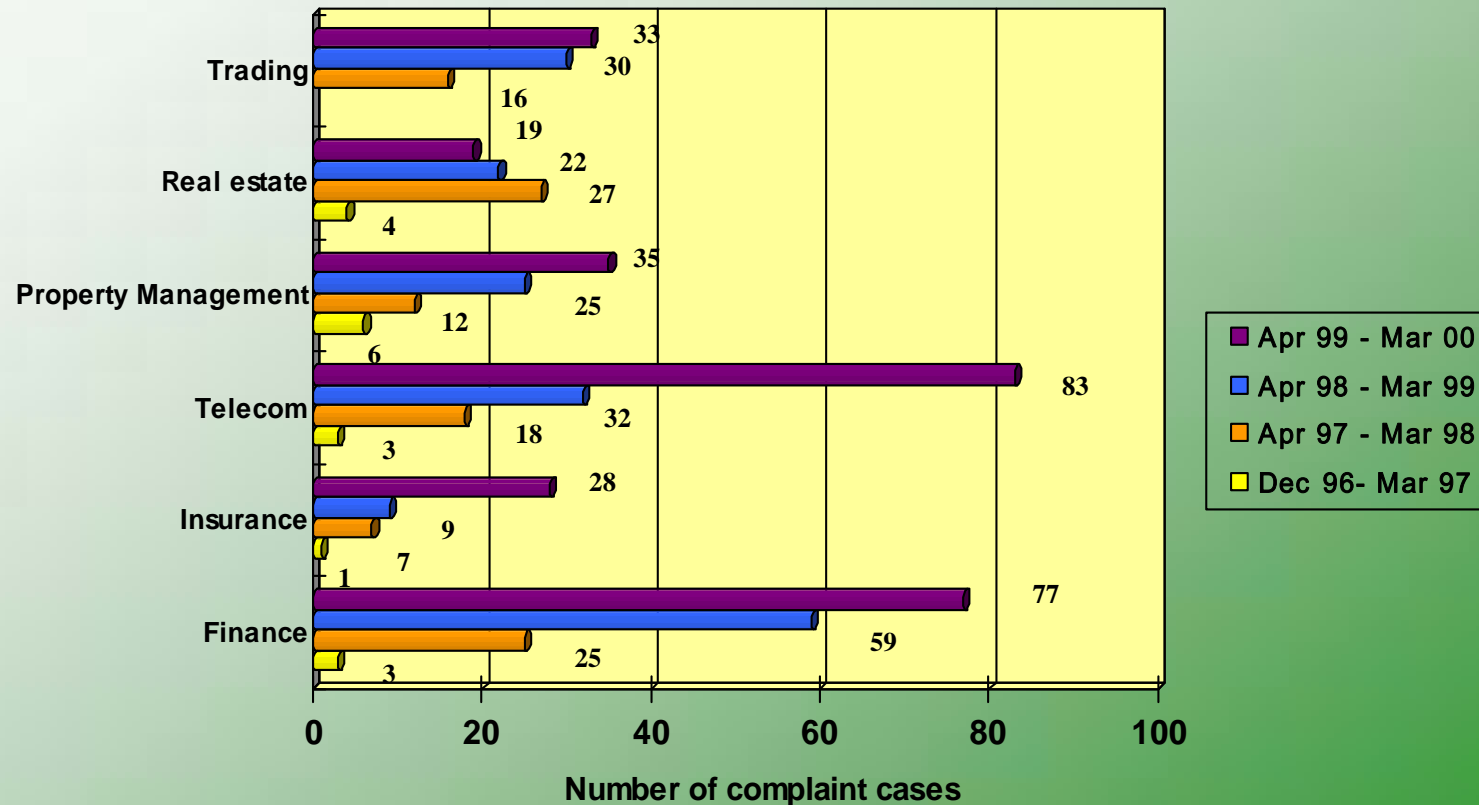
# Office of the Privacy Commissioner for Personal Data, Hong Kong

## Types of party complained against (1999-2000)



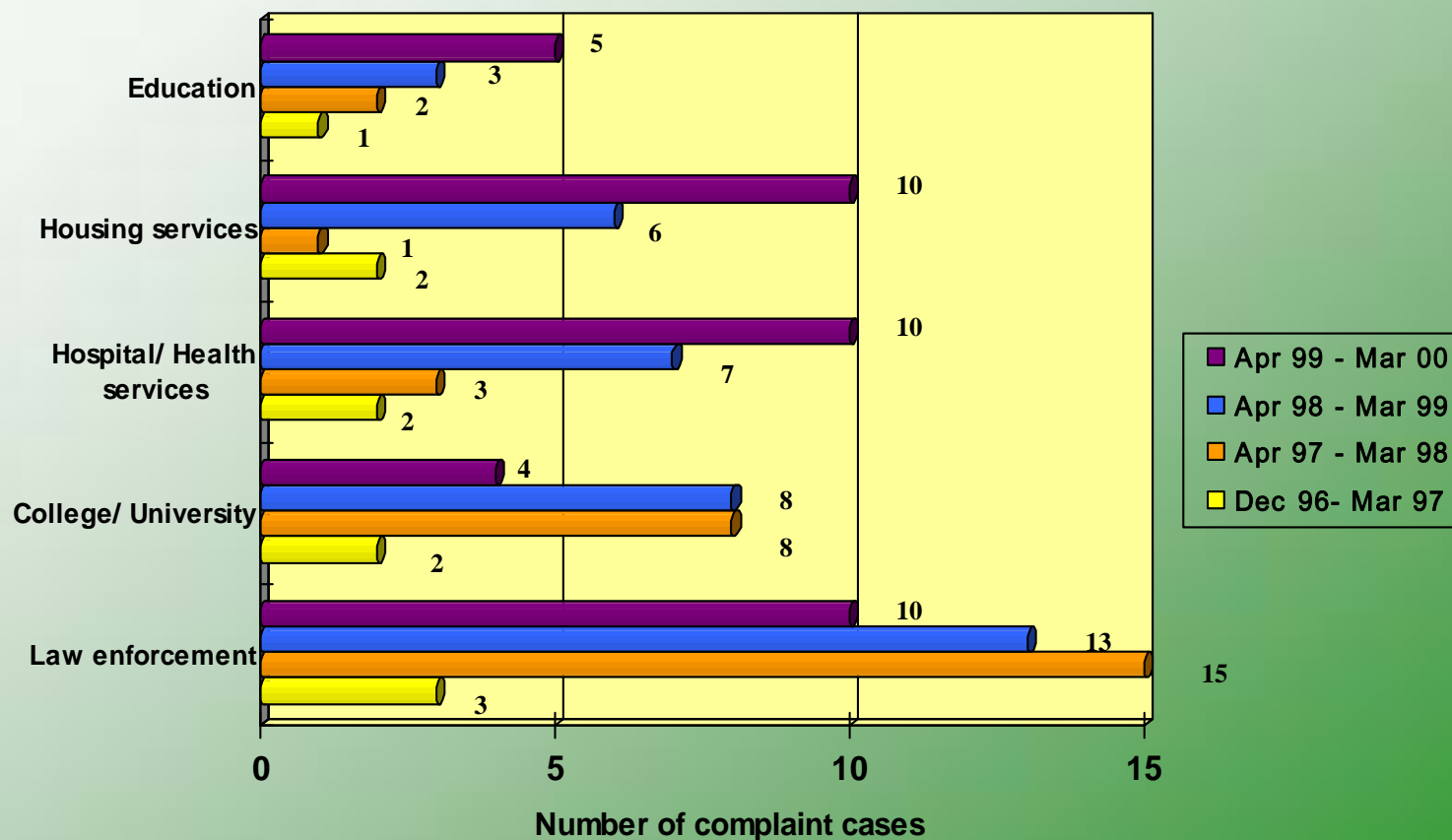
# Office of the Privacy Commissioner for Personal Data, Hong Kong

## Breakdown of complaints against private sector organizations (1999-2000)



# Office of the Privacy Commissioner for Personal Data, Hong Kong

## Breakdown of complaints against public sector organizations (1999-2000)



# Codes of practice

- **HK Identity Card Number**
- **Consumer Credit Data**
- **Human Resources management**

# Guidelines

- **Recruitment advertisement**
- **Cold calling**
- **Mobile service operators**
- **Cross marketing activity**
- **Property management**
- **Financial debt collecting**
- **Collection of finger print**
- **Data breach handling**
- **Workplace monitoring**

# Contemporary Challenges

- **Identity Thefts/Frauds**
- **Data Breaches**

# Personal Data Protection a Global Issue

- Increasing societal affluence (70's)
- Advances in computers, digital storage and telecommunications (80's) leading to
- Exponential growth of personal data collected, transmitted and exploited
- The internet going critical and the advent of eCommerce (90's)
- Explosion of Identity theft/fraud(00's) and data breaches leading to
- Heightened consumer expectations

# Identity Theft

**.The fastest growing form  
of consumer fraud in  
North America**

# Federal Trade Commission Identity Theft Survey Report (2006)

- A total of 3.7 percent of American adults indicated that they had discovered they were victims of ID theft in 2005.
- This result suggests that approximately **8.3 million U.S. adults** discovered that they were victims of some form of ID theft in 2005.

# Federal Trade Commission Identity Theft Survey Report (2006)

- Victims of ID theft are classified as belonging to one of three categories
- misuse of one or more of their existing credit card accounts (3.2M, 1.4%)
- misuse of one or more of their existing accounts other than credit cards (3.3M, 1.5%)
- misused to open new accounts or to engage in types of fraud (1.8M, 1.8%)

# Hong Kong Data Breaches

- The Hospital Authority, which manages all the public hospitals in Hong Kong, had a series of patients' data loss with loss of electronic devices including USBs . The latest incident in May 2008 involved the loss of an unprotected USB containing the personal data of 11,000 patients.

# Hong Kong Data Breaches Growing

- Banking giant Hong Kong Bank was under fire after admitting it had lost the data of 159,000 accounts from a Hong Kong branch. The data was held on an Internet server which is understood to have gone missing (May 08)
- ...followed by the loss by courier service of a digital tape containing 25,000 phone conversations with its customers. (July 08)

# UK Revenue and Customer Department

- an incident involving the loss of two compact discs holding the personal data of up to 25 million individuals. The circumstances were that on 18 October 2007 both compact discs were sent to the National Audit Office via the internal post system which is operated by a courier company. The data was being sent to the NAO in response to a request for information for audit purposes. The package containing the data was not recorded or registered, and the data are not encrypted.

# UK Revenue and Customer Department

- The personal data include names, addresses, dates of birth, child benefit numbers, National Insurance numbers and bank or building society account details.
- ...the Chairman resigned

# UK - Roll call of data breaches grows

- Since the security breach at HM Revenue and Customs in November 2007, the Information Commissioner's Office (ICO) has been notified by April 2008 of **almost 100 data breaches** by public, private and third sector organisations.
- Of the security breaches that the ICO has been made aware of by private sector organisations, 50% were reported by financial institutions. Information that has gone missing includes unencrypted laptops and computer discs, memory sticks and paper records. Information has been stolen, gone missing in the post and whilst in transit with a courier.
- The material includes a wide range of personal details, including financial and health records.

Information Commissioner's Office (ICO) UK  
23/04/08



# US - TJX

## the Discount Retail Giant

- At least 45.7 million credit and debit card numbers from customers in the United States, Britain and Canada were stolen over a period of several years from the computers of TJX, the discount retail giant disclosed in a regulatory filing in 2007.
- Apparently the thieves were able to tap into the wireless system that is used for POS card verification.

# US - Personal data loss hit record level in '07

- The San Diego-based [Identity Theft Resource Center](#) says that more than 79 million records were reported compromised in the United States through Dec. 18. That is a nearly fourfold increase from the nearly 20 million records reported in 2006.
- Another group, [Attrition.com](#), estimates that worldwide more than 162 million records were compromised through Dec. 21. Attrition reported 49 million last year.

**Associated Press / December 31, 2007**



# Privacy Concerns are adversely affecting E Commerce

- US E Commerce sales only 3.4% of total sales - \$136 billion in 2007  
(US Dept of Commerce Census Bureau, Feb 2008)
- Canada e commerce sales just over 1% of total sales - \$49.9 billion  
» (Statistics Canada, April 2007)

# TJX the Fallout

- Personal and commercial lawsuits
- A flurry of law suits at least -9 states and 6 Canadian provinces on “negligence “
- coordinating its investigation of TJX with 39 state Attorneys Generals, the FTC found TJX “failed to use reasonable and appropriate security measures to prevent unauthorized access to personal information on its computer “ (March 08)

# TJX

## the Fallout

- TJX announced in May 2007 that its first-quarter profit dipped 1% as initial costs regarding data loss offset revenue growth. It foreshadowed further costs relating to investigation, enhanced computer security and systems, along with "technical, legal and other fees" that could total 2 or 3 cents per share in the second quarter. Beyond these costs, TJX reported **it doesn't know how much the data breach will eventually cost**, including "exposure to credit card companies and banks, various legal proceedings and other expenses".

In December 2007 TJX proposed to pay up to US\$40.9 million to compensate banks that issued Visa payment cards potentially affected by the data loss if they agree not to sue it.

# Data Breach

## Hard Costs to Corporate

- Financial penalties imposed by regulators
  - Nationwide (UK) \$1.5M      Choicepoint (US) \$15M
- Other penalties imposed by regulators to demonstrate the weaknesses are addressed
- Compensation payments in commercial and class action lawsuits
- Loss of customers/ corporate partners
- Costs of crisis management, damage control, notification, review and retrofit of information systems, policies and procedures.
- Payment for credit monitoring services for affected individuals
- Legal and administrative expenses in defending litigation

# Data Breach

## Soft Costs to Corporate

- **Diminution of brand and reputation**
- **Loss of client trust**
- **Loss of competitive edge**

# Ponemon Institute Annual Study (2007) Cost of a Data Breach

- Average total per-incident costs in 2007 were US\$6.3M, compared to an average cost of US\$4.8M in 2006
- The cost of lost business increased by 30% to an average of US\$4.1M in 2007, about two-third of the average total cost per incident.

Costs include legal, investigative, administrative, customer defection, reputation management, customer support, opportunity loss

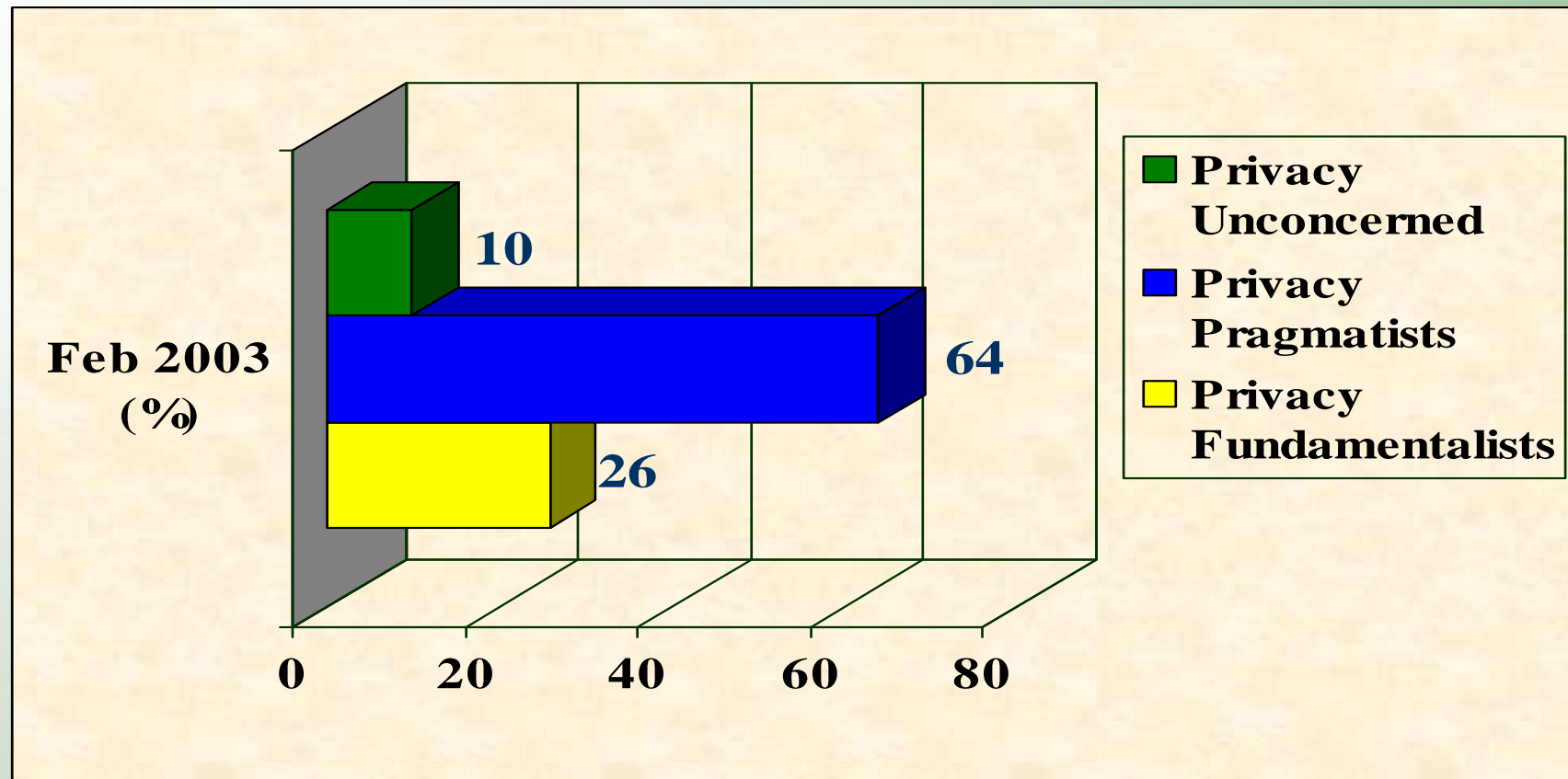
# Personal Data Protection A Corporate Responsibility

Personal Data Protection should be viewed not just as a COMPLIANCE issue, but also as a BUSINESS issue as a

**BUSINESS IMPERATIVE**

**BUSINESS DIFFERENTIATION and  
COMPETITIVE ADVANTAGE**

# The Business Case Public Profile on Privacy



The "Privacy Dynamic" - Battle for the minds of the pragmatists — Dr. Alan Westin

# The Business Case Build a Trusting Relationship

***“Trust is more important than ever online ... Price does not rule the Web ... Trust does.”***

Frederick F. Reichheld, *Loyalty Rules:  
How Today's Leaders Build Lasting Relationships*

## ... Or Else, it's Good Bye

- 20% of consumers immediately terminated their accounts with vendors that lost their information;
- An additional 40% considered taking their business elsewhere after receiving notifications of information mishandling.

– —Ponemon Institute, *Lost Customer Information*:

# **Build a corporate culture protecting information and respecting privacy**

- **It is essential that personal data privacy protection become a corporate priority throughout all levels of the organization**
- **Appoint a privacy officer and form a multi-departmental privacy team**
- **Develop an information and privacy protection policy based on the universal personal data protection principles and compliance with relevant privacy laws**
- **Build and sustain a culture to protect information and respect privacy through education, technology, processes and procedures**
- **Senior Management and Board of Directors' commitment is critical, with privacy compliance part of management performance evaluation**

# Make Privacy a Business Imperative

- **Gain a competitive advantage**
- **Enhance trust and consumer confidence**
- **Keep existing customers –attract new ones**
- **Minimize the risk of a privacy breach and the high costs associated with them**

# Contemporary Challenges

- Sensitive data
- Outsourcing/cloud computing
- Social media
- Workplace monitoring

# Workplace Monitoring

- Telephone monitoring
- Email monitoring
- Internet Monitoring
- Video Monitoring

**Note: workplace for domestic helper is  
HOME**

# Contemporary Issues

- The aftermath of 9/11
- The Internet of Information
  - B2B
  - B2C
- **The internet of Things**
  - pervasive RFID
  - M2M (Machine to Machine)

# THE INTERNET OF THINGS

- RFID
- Short- and long-range wireless communications
- Sensor networks

**Embedding  
intelligence into things so that  
they become smarter**

# Radio Frequency Identification (RFID)



# RFID

- Radio Frequency Identification (RFID) is a type of automatic identification system. The purpose of an RFID system is to enable data to be transmitted by a portable device, called a TAG, which is
- A tiny chip connected to an antenna.....

**Hitachi's 0.3 mm mu chip**



# RFID

....which is read by an RFID reader and processed according to the needs of a particular application.



# RFID

- The data transmitted by the tag may provide identification or location information, or specifics about the product tagged, such as price, color, date of purchase, etc.

# RFID

- Tags can be embedded in product packaging

(Like Gillette razor blades)



# Unique Features of RFID Systems

- TAGs contain amongst various information an unique identifier ( eg identifying an individual can of coke as distinct from the tradiitional BARCODE which labels all cans of coke)
- RFID radio waves can travel thru solid objects such as walls, briefcases, wallets
- RFID tags can be as small as a dot

# Unique Features of RFID Systems

- RFID tags can be embedded into or affixed to virtually any physical items
- Tag information can be read/transmitted, silently and invisibly, from a few metres (passive tags) to hundreds of metres (active tags)

## Main two-way wireless technologies\*

	Data rate Per second	Range	Cost !
Mobile WiMax	15Mb	5km	\$8 in 2008
3G cellular (HSDPA/LTE)	14Mb	10km	\$6
2G cellular (GSM/CDMA)	400k	35km	\$5
Wi-Fi	54Mb	50-100m	\$4
Bluetooth	700k	10m	\$1
Zigbee	250k	30m	\$4
UWB	~400Mb	5-10m	\$5
RFID	1-200k	0.01-10m	4 cents

•Typical performance; actual figures vary  
! Approx. device-chip cost at high volume

Sources: William Webb; Cambridge Consultants; OECO  
Pyramid Research; Nokia; TI; CSR; Ember; Hitachi

# THE INTERNET OF THINGS

- 2006 1 billion RFID chips were sold
- 2007 estimated to rise to 1.7 billion

IDTechEx

“By 2025 Internet will need to accommodate a trillion devices, most of them wireless”

David Clark, MIT

# RFID Applications

- Transportation – passports, payment cards, frequent travelers for border crossings
- Tracking – products, inventories, automobiles, library books, currency, people movement, etc

# Benefits of RFID

- Better supply chain management
- Improve fraud detection and prevention
- Better security
- Better product planning and customer services
- Improve efficiencies and productivities

# Wonderful!!! BUT.....



- [privacy\\_spychips.video.wmv](#)

# Emerging Issue

- The aftermath of 9/11
- The Internet of Information
- The internet of Thing
  - -Pervasive RFID
- The Internet of people
  - -**Invasive RFID**

# **THE INTERNET OF THINGS and PEOPLE**

**The Internet of things**

**Embedding intelligence into things so  
that they become smarter**

**The Internet of people**

**Embedding intelligent things into  
intelligent beings**

**Smarter??**

# Internet of People



SPAIN - Baja Beach Club

# Internet of People

## Baja Beach Club

- Claimed to be the first time (2004) chips have been placed in human as a mean of identification
- Rice-grain-sized chip implanted under the skin in the upper left arm
- Through identification by a scanner, the individual can jump the entrance queue, admit to the VIP area, pay for drinks as an in-house debit card

# Internet of People Verichips

- Approved by the US Food and Drug Administration for RFID body implants

1.2mm by 12mm  
in size ( rice grain)



# THE INTERNET OF PEOPLE

- **Infant protection** - offering hospital a means to prevent infant abductions and accidental mother-baby switching
- **Patient protection** - providing rapid, secure patient identification in emergency situations, especially important for patients with chronic illnesses
- **Wander prevention** - installed many long-term facilities and helping provide residents with mobility in specified areas while preventing them from wandering off

# THE INTERNET OF PEOPLE

- **Instant medical records**

The implantable chip can seamlessly retrieve stored medical records data-based information within milliseconds. With the chip scanner within close proximity of the chip, the individual's medical history can be retrieved to communicate accurate information when necessary - particularly for diabetic, emergency care, cardiac care or memory-impaired individuals.

# WHY?



# The Internet of People

- **Serious ethical and privacy considerations:**
  - issues about informed consent
  - moving towards a potentially nefarious tool to track citizens (scope creep/slippery slope)
  - Being rushed to the marketplace without understanding the privacy implications and consequences
  - Inherently and Potentially risky

# Coming On Stream...

- An implantable capsule that measures ethanol ( alcohol) concentration in the blood, for use by alcoholics who volunteer for monitoring as an alternative to prison
- A tiny chip that would fit into a person's ear and monitor vital signs such as body temperature, blood pressure, heart-rate

# 'chip the foreigners'

- This subcutaneously human tracking VeriChip could be used to register guest workers, verify their identities as they cross the border, and "be used for enforcement purposes at the employer level"

VeriChip Corporation

# Guiding Principles of Balance

- The right of individuals to privacy is not absolute. It must be balanced against societal right
- Balance between safeguarding personal data privacy and facilitating continued development of information and communications technology
- Any change to privacy law should not undermine national competitiveness and economic efficiency

# Guiding Principles of Balance

- The need to avoid putting onerous burden on business operations and individual data users
- Due account should be given to local situation and culture
- The privacy law should remain flexible and relevant in spite of technological changes

# Recognising

- Tension between citizens' privacy rights and government in personal data handling
- Tension between individuals' privacy rights and business organisations in personal data handling

# Resolving through

- A balance approach with
  - Informed consent
  - Informed choice

Supported by an adequate law

# TERRA INCOGNITA

- **The aftermath of 9/11**
  - National security and privacy
- **The Internet of Information**
  - Personal information sharing and identity theft and privacy
- **The internet of Things**
  - -Pervasive RFID and privacy
- **The Internet of people**
  - -Invasive RFID and privacy

# The Internet of Things

- “To promote a more widespread adoption of the technologies underlying the Internet of Things, principles of informed consent, data confidentiality and security must be safeguarded. Unless there are concerted efforts involving all government, civil society and private sector players to protect these values, the development of an Internet of Things will be hampered, if not prevented”

»

ITU Report

**THANK YOU**