Contemporary Issues in Personal Data Privacy

Stephen Lau

President Hong Kong Computer Society

Adviser HP Enterprises Services

Former Privacy Commissioner for Personal Data of Hong Kong

JUCC 2nd Information Security Conference **May 2011**

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

The aftermath of 9/11

U.S. Patriot Act and anti-terrorism laws

Served to expand powers of surveillance, and reduce judicial oversight

Internet of Information

- The aftermath of 9/11
- **The Internet of Information**

  -B2B (Business to Business)

  -B2C (Business to Consumer)

  -Explosion of personal information collection and sharing

  -Prolific Identity theft , leading to

  -Heightened consumer wariness and expectations

Audio Clip

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

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.

Federal Trade Commission Identity Theft Survey Report (2006)

- 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%)

LEGISLATION

Privacy Laws

United States:

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

Europe:

- Omnibus (covering 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

Omnibus laws in Australia, New Zealand, Hong Kong, Japan, Korea

Sectoral privacy laws in Taiwan, Thailand

Universal 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

- 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 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.**

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)
- **The aftermath of 9/11 (00's) and**
- **Explosion of Identity theft/fraud(00's) and data breaches leading to**
- **Heightened consumer expectations**

Data Breaches

- Personal data breaches of 77M players of PlayStation Network (SONY) in April 2011
- Data include name, email address, password, and possible credit card details

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

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.

Questionable Data Collection and Uses

- Apple and Google collecting excessive personal data for their smartphones and tablets' users for locating their users (2011)

- Octopus sold personal data of its 2.4M customers in its Reward/Loyalty Program to third parties for direct marketing purpose (2010)

Emerging Issues

- Social networks
- Geographical information systems
- (streetview)
- Cloud Computing
- Genetic information

EDS

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

The cost of data breaches: Looking at the hard numbers

- All things considered, a security breach can cost you anywhere between $50 to $250 per record. Depending on how many records are at stake, individual breach costs may run into millions or even billions of dollars

Forrester Research Inc. (2007)

PlayStation Network

- Analyst estimated loss of US$1.5 Billion for SONY
- Estimated costs to credit card companies at US$300 Million for card replacement

Personal Data Protection
A Corporate Responsibility

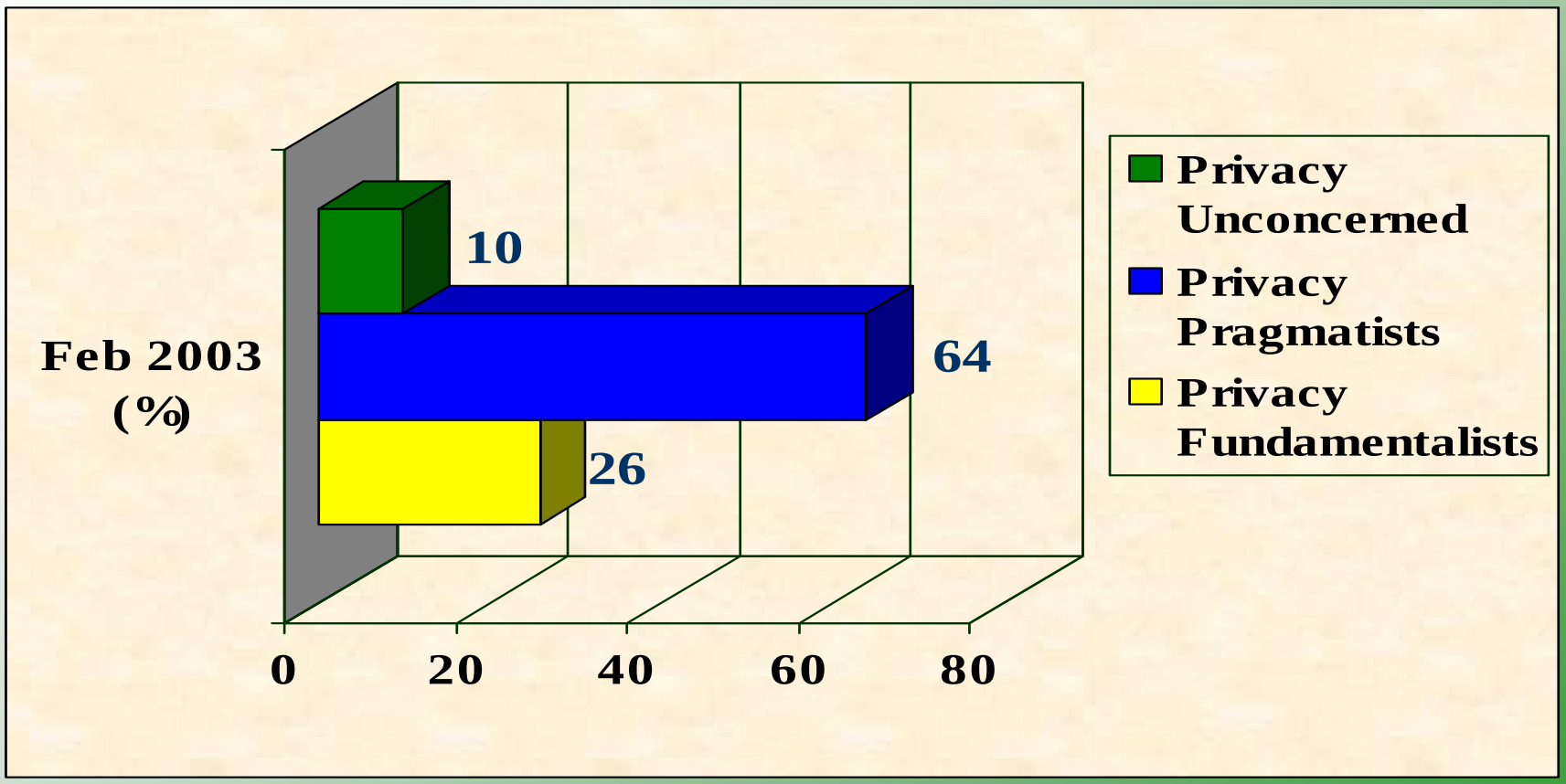
Personal Data Protection should be viewed not just as a COMPLIANCE issue, but also as a BUSINESS issue as a

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*

CMO Council Survey Consumer Concerns on Personal Data Security

- Security concerns rising for more than 50% of consumers
- 40% have actually stopped a transaction online, phone or in a store due to security concern
- More than 30% strongly consider taking their business else if personal data compromised
- 25% firmly said they would .....

Chief Marketing Officer Council

August 2006 www.cmocouncil.org

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

The Internet of Things

- 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
- 2009 1.98 billion
- 2010 2.31 billion

IDTechEx

"By 2025 Internet will need to accommodate a trillion devices, most ol 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

Wonderful!!!
BUT……

- privacy spychips.video.wmv

RFID
animals

RFID animals

- **Livestock**
  RFID ear tags, tag readers and software provide accurate, economical solutions for identifying and tracing livestock through all stages of their lifecycle.

RFID animals

- **Companion Pets**
  If lost or stolen, companion pets are easily tracked and identified. Rice-grain size implantable microchips provide a secure and reliable means of pet identification. Every month, some six thousand lost pets in the U.S. are reunited with their owners, thanks to this technology.

RFID animals

- Recent research suggests that in future, the largest market for RFID will not be the retail or consumer packaged goods industry, as some might think, nor perhaps transport or defence. No, the largest market for RFID will be in animals, food and farming, because adopting RFID will benefit the food supply chain, including livestock disease control and the merchandising of prepared food.

IDTechEx

TERRA INCOGNITA

- 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.

THE INTERNET OF PEOPLE

- ALzheimer's Community Care in Florida,US using the implant of a RFID chip under the skin of the right forearm into Alzheimer's patients with consent (patient or family member). When scanned in an emergency room will link to the patient's medical record.

WHY?


STOP VERICHIP!
PEOPLE ARE NOT PETS
CHIPPING PEOPLE IS WRONG
Violated.
STOP VERICHIP!
Violated.
STOP HUMAN BRANDING
"Yes" to MedicAlert
"No" to VeriChip!
RFID
"Yes" to MedicAlert
"No" to VeriChip!
Dignity?
"Yes" to MedicAlert
"No" to VeriChip!
STOP VERICHIP!
"Yes" to MedicAlert
"No" to VeriChip!

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

FDA letter to VERICHIP CORP

"The potential risks to health associated with the device are:

- Adverse tissue reaction
- Migration of implant transponder
- Compromised information security
- Failure of implanted transponder
- Failure of inserter
- Failure of electronic scanner
- Electromagnatic interference
- Electrical hazards
- MRI incompatibility

FDA letter to VERICHIP CORP

"The potential risks to health associated with the device are:

- Adverse tissue reaction
- Migration of implant transponder
- Compromised information security
- Failure of implanted transponder
- Failure of inserter
- Failure of electronic scanner
- Electromagnatic interference
- Electrical hazards
- MRI incompatibility

But APPROVE TO MARKET.....

Coming On Stream…

- Implant for congestive heart failure, to measure pressure and fluid inside a patient's heart and wirelessly send the data to an external unit. Regular monitoring will provide alert to abnomalities at an early stage

Coming On Stream…

- **Intra-body wireless communications**

  Allows several devices inside the body to relay information without interference.

  EG for diabetic patient , an implanted gloucose-level reader in one part of the body to communicate with an implanted insulin pump elsewhere

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

Coming On Stream…

- An **edible** RFID chip which could be used for examining the digestive track or check whether a patient has taken his medication.

'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

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 and People

- “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