Week 3

Legal Issues in Managing Information - Data Protection Policy

Outline

- Existing Data Protection (DP) Regime in Singapore
- Proposed DP Legislation in Singapore
- Backup – Ten DP Principles

Existing DP Regime in Singapore

Current Status

- Today, Singapore uses a number of ways to address DP

- These include
  - Legislative safeguards
  - Industry self-regulation
  - Reliance on common law

Legislative Safeguards (1/2)

- Singapore's regime is sectoral
  - Regulatory framework governing each industry sector will deal with DP specific to that sector
    - Financial Sector
      - Banking Act, Insurance Act
    - Healthcare Sector
      - Private Hospitals & medial Clinics Acts
    - Telecoms Sector
      - Telecoms Competition Code
  - A breach of relevant provision may invite enforcement from sector regulator

Legislative Safeguards (2/2)

- Public sector's DP policy is encompassed in IM8F & administered by MOF
- IM8F requires
  - Processes & procedures are in place within public sector agencies to ensure that data (including personal data) is properly managed & protected
  - Guidelines for cross-agency data sharing
- Public sector agencies are bound by confidentiality provisions in applicable legislation
  - Examples: IDA Act, MDA Act

Industry Self-regulation

- Examples
  - Direct Marketing Association of Singapore (DMAS) Code
  - National Association of Travel Agents (NATAS) Code
  - Various codes for medical professionals administered by
    - Singapore Medical Council
    - Singapore Nursing Board
- Other sectors
  - Model DP Code (Model Code)
    - Established by DP & Privacy Task Force in 2003
    - Adoption is voluntary
    - No active administration of Model Code
    - No monitoring of adoption by companies
      - Except for TrustSg

- A nation-wide trust mark initiative by National Trust Council (NTC) to boost e-commerce environment in Singapore
- Aims to help build confidence in e-commerce transactions especially in privacy & security
- To attain accreditation, e-merchants must comply with a stringent code of conduct administered by NTC
  - Incorporates principles of Model Code
- Code covers disclosure, privacy, fulfillment, best business practices, & protection of minors & elderly

Common Law

- To govern execution & enforcement of contracts, data can be safeguarded by using
  - Non-disclosure agreements
  - Contractual provisions

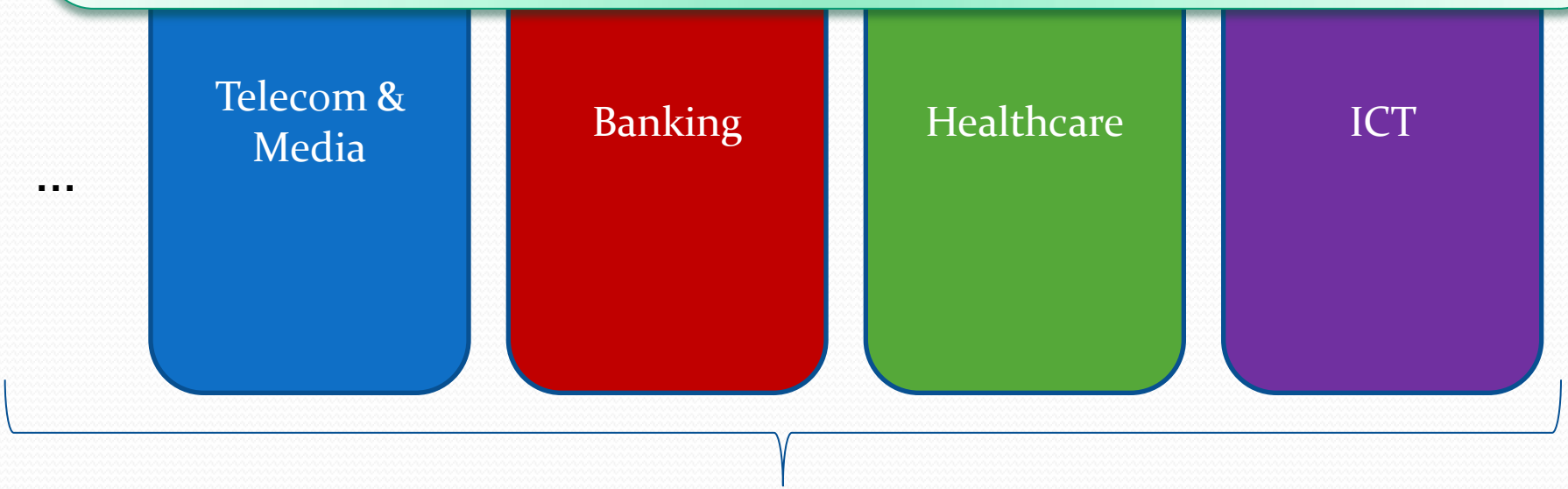
- Data can be safeguarded under laws of confidence
  - Sensitive data is protected if disclosed under circumstances importing a duty of confidence

Proposed DP Legislation in Singapore

Singapore' DP Framework

General DP Law

- Increasing consumer awareness of DP issues, esp. with online use
- DP regime useful for business to increase trust with local and intl customers



Sector-specific frameworks (Acts, Regulations, Mandatory Codes, Voluntary Model Codes, Trustmarks, etc.)

General DP Law

- Public Consultation Proposals

- Referenced Canada, Australia, New Zealand, Hong Kong, EU and UK models & international guidelines in formulation
- Aims to set a general baseline standard for all sectors, working concurrently with existing sector-specific regimes
- Balances consumer interests with business costs
- Considers need for technology neutrality given rapid business model innovations

Overview of DP

Personal Data	Information relating to an identifiable individual Examples of personal data: IC number, mobile phone number Example of non-personal data: Financial corporate records			
Data Life-cycle Stages	**Collection** e.g. sign-up form or roadside survey	**Use/ Processing** e.g. business analytics or telemarketing	**Disclosure** e.g. outsourcing operations or selling	**Retention/ Deletion** i.e. storage on server
DP = Protection of Personal Data against:	Collection of excessive data (more than required for purpose) & collection without consent	Use/ processing of data beyond consented purposes	Disclosure to parties without prior consent	Insecure retention/ (lack of sufficient security measures) & insufficient excessive length of retention

Overview of DP – Other Points

- Protection cover natural persons (whether living or dead)
  - Should deceased be excluded to respect their privacy?
- "Light touch" baseline legislation
  - Applies to all private sector organisations to ensure a min standard of DP across private sector
- Complaints-based regime
  - As opposed to stringent audit-based regime
  - Organisations will not be regularly audited by DPC, nor required to submit regular self-audit reports to DPC on compliance with DP rules
- Do-Not-Call Registry adopts 'opt-out'
  - Should it be 'opt-in'? National Call Registry?
- …etc

General DP Law

- Public Consultation Proposals

- Structured according to internationally consistent DP principles
- With exclusions or exemptions for specific purposes

- Accountability
- Purpose
- Consent
- Limiting Collection
- Limiting Use, Disclosure, & Retention
- Accuracy
- Security
- Openness
- Access & Correction
- Challenging Compliance

Key Exclusions & Exemptions

- General exclusions, e.g.
  - Personal data in court documents
  - Personal or domestic use
- Other exclusions on collection, use and/or disclosure, e.g.
  - For news activities
  - Clearly in the interest of the individual & consent cannot be obtained in a timely manner, such as medical emergencies
  - Relates to national security, defence, public security, such as terrorist threats
  - For research & statistical purposes, under certain conditions
  - For companies outsourcing, transfer of data solely for purpose the data was collected for

General DP Law

- **Public Consultation Proposals**

Proposed set-up of
Data Protection Commission (DPC)

Powers to investigate	Issue orders to rectify non-compliance	Impose financial penalties < $1M	Appeal to Independent Tribunal then to the Courts	Other powers e.g. referral to mediation

General DP Law

- Public Consultation Proposals: Do-Not-Call Registry

Consumers

Consumer registers phone number through website or toll-free number

Service is free

DNC Authority

DNC Authority verifies identity of consumer & updates DNC lists

3 DNC lists:
(a) Phone calls
(b) SMS
(c) Fax

Telemarketing companies

Telemarketing companies remove numbers on DNC lists from their own lists of numbers to call

Companies have on-going obligation to check/filter & pay access fees

General DP Law
- Public Consultation Responses

- MICA received a total of
  - 71 submissions from organisations & individuals,
  - Comments to specific questions from 85 individuals

for public consultation that ended on 25 October 2011

- A quick poll conducted during public consultation garnered 750 responses from the public

General DP Law

- Public Consultation Responses: Quick Poll (1/3)

1. Do you support the set up of a national Do-Not-Call Registry where consumers can request to opt-out of telemarketing calls, SMSes and faxes by an organisation?

- **Yes (728) - 97%, No (22) - 3%**

2. Is there a need for a DP law to protect consumers' personal data against misuse?

- **Yes (740) - 99%, No (10) - 1%**

General DP Law

- Public Consultation Responses: Quick Poll (2/3)

3. Should the scope of coverage under the DP law include all forms of personal data (both electronic and non-electronic)?

- **Yes (721) - 96%, No (29) - 4%**

4. Should the scope of coverage also include personal data of deceased individuals although this may be administratively complex?

- **Yes (548) - 73% , No (202) – 27%**

General DP Law

- Public Consultation Responses: Quick Poll (3/3)

5. Do you think that a Data Protection Commission should be set-up and given the power to investigate and serve enforcement notices on organisations that have breached DP laws?

- **Yes (720) - 96%, No (30) - 4%**

6. Do you think that the financial penalty of an amount not exceeding $1 million for non-compliance with the DP law is high enough deterrent?

- **Yes (467) - 62%, No (283) - 38%**

General DP Law

- Public Consultation Responses: Overall views

- More clarity on definition of personal data

- Mixed views on various issues
  - Coverage of personal data of the deceased
  - Application of DP Act to organisations not in Singapore
  - Failure to 'opt out' as a form of consent
  - Penalty ceilings & private rights of action
  - Length of sunrise period
  - etc

General DP Law

- Public Consultation Responses: Issues pertinent to ICT firms

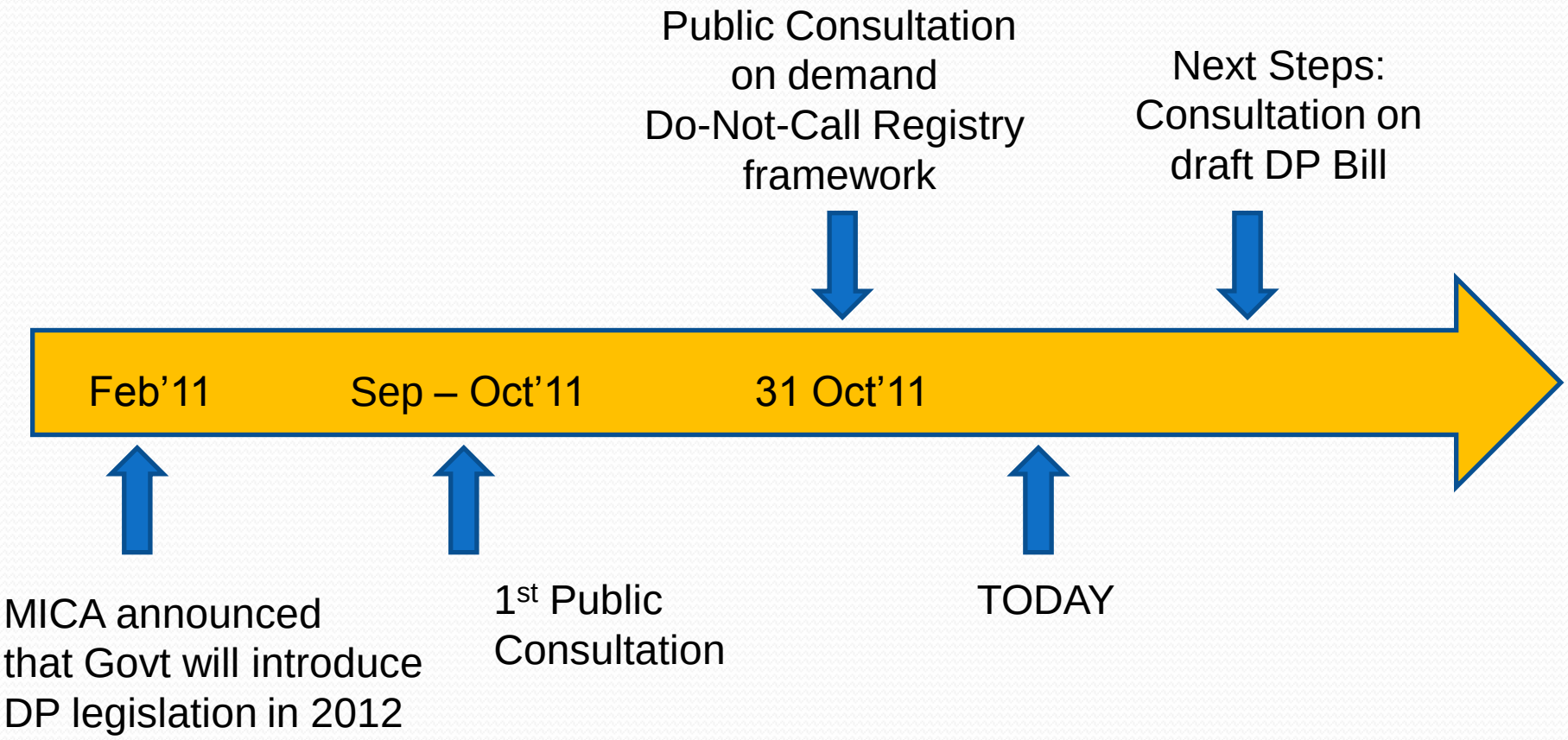
- Differentiation between data controllers & data processors
  - Mixed views on whether data processors should be treated differently from data controllers
    - Related point: Some firms asked for exclusions or different treatment for internet intermediaries
- Coverage of organisations not in Singapore
  - Mixed view on whether organisations conducting data-related activities in Singapore while not in Singapore should be covered
- Treatment of data mining & business analytics activities
  - Suggestions on allowing firms to perform analytics on data 'anonymised' through firewalls, more exemptions, etc

Sample feedback on

Exclusion of Public Sector

- "Public sector does not need – & should not be – exempted. If necessary, a Privacy Act for government (as in Canada) should be enacted with equally stringent standards."
- "The proposed carving out of such a big sector out of the Singapore legislation will negate our efforts to be "equivalent" to the EU's standards as required by Article 25 of their DP."
- "… we should, to avoid misunderstanding, openly declare that Singapore Government is already compliant & a leader in this field – having adopted the standards (and more!) of the Model Code for many years! "
- "National security & law enforcement exceptions can in any case be incorporated into the proposed DP Act."

Proposed DP Regime for Singapore



Backup – Ten Data Protection Principles

Data Protection Principles (1/5)

Principle 1 — Accountability

- An organisation is responsible for the personal data under its control and must designate an individual or individuals to be accountable for it.

Principle 2 — Identifying Purposes

- The purposes of collection must be identified at or before the time of collection.

Data Protection Principles (2/5)

Principle 3 — Consent

- The knowledge and consent of the individual are required for the collection, use, or disclosure of personal data.

Principle 4 — Limiting Collection

- Only the personal data necessary to fulfil the pre-identified purposes shall be collected.

Data Protection Principles (3/5)

Principle 5 — Limiting Use, Disclosure, and Retention

- The use and disclosure of personal data is limited to the purposes for which it was collected. Personal data shall be retained only as long as necessary to fulfil those purposes.

Principle 6 — Accuracy

- Personal data shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

Data Protection Principles (4/5)

Principle 7 — Safeguards

- The security safeguards must be appropriate to the sensitivity of the personal data.

Principle 8 — Openness

- An organisation's personal data management policies and practices must be readily available.

Data Protection Principles (5/5)

Principle 9 — Individual Access and Correction

- An individual must be able to be informed of the existence of, access, challenge and seek amendment to his personal data. He must be provided with reasons if access is denied.

Principle 10 — Challenging Compliance

- An individual must be able to direct challenges on an organisation's compliance to that organisation's designated representative.

Week 3 (02 Feb 2012)

- Information Classification
- Singapore Infocomm Security Masterplan
- Guest speaker: Mr. John Yong

  Director, Infocomm Security & Assurance

  IDA