CYBERSECURITY AND PRIVACY

WORKSHOP ON THE DIGITAL ECONOMY
INSTITUTE PENTADBIRAN AWAM 26-10-2020

ASSOC. PROF. DR. SONNY ZULHUDA
INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

sonnyzulhuda.com
2 OUTLINE

• Setting Up the Context

• Key Barriers to the Digital Economy in Malaysia
  • Eliminating Barrier #1: Creating a Dynamic Regulatory Ecosystem
  • Eliminating Barrier #2: Stronger Consumer Protection
  • Eliminating Barrier #3: Enhancing Personal Data Protection
  • Eliminating Barrier #4: Data Security for Sustainability

• Challenges in Data Governance

• Moving On
The worldwide network of economic activities, commercial transactions and professional interactions that are enabled by information and communications technologies (Techtarget).

The economic activity that results from billions of everyday online connections among people, businesses, devices, data, and processes, with the interconnectedness of people, organisations, and machines that results from the Internet, mobile technology and the internet of things (IoT) is deemed a backbone (Deloitte).
<table>
<thead>
<tr>
<th><strong>4 THE ENABLING TECHNOLOGY</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Today’s Digital</strong></td>
</tr>
<tr>
<td><strong>The inter-connectivity</strong></td>
</tr>
<tr>
<td><strong>Future governance</strong></td>
</tr>
</tbody>
</table>

sonnyzulhuda.com
Behind this digital economy revolution is the massive use, sharing and exploit of data in a new intensified level of Volume, Velocity, Variety, Variability, Veracity, Visualization, and Value; a.k.a Big Data.

From automation to digitization to datafication…

6 THE OTHER SIDE OF DIGITAL ECONOMY

Phishing Webpage
“Businesses in Malaysia have adopted digital technologies less readily than the government and population.”

“…digital divide where Malaysia lags behind international peers in digital adoption by businesses.”

“Only 62% of businesses are connected to the Internet, 46% has fixed broadband and 18% have a web presence.”

“KEY BARRIERS RELATED TO DIGITAL CONNECTIVITY, ENTREPRENEURSHIP AND TAXATION

Creating a dynamic ecosystem for the digital economy to improve the infrastructure, regulations, skills and public finance.

Increasing digital transactions "and digital cash" requires overhauling regulations and increasing consumer comfort.

Ongoing tensions between data protection and its legitimate use for commercial purposes...

Lack of data sharing, often cautiously approached due to security concerns.

ELIMINATING BARRIER #1: CREATING A DYNAMIC REGULATORY ECOSYSTEM FOR THE DIGITAL ECONOMY

- Strengthening Electronic Commerce Law by upholding the legality of e-Contract, digital transaction, mobile communications, and smart contracts.

- The legitimate usage of e-contract and e-evidence depends on the integrity and retrievability of the data [s.8 of E-Commerce Act 2006]. See: *Yam Kong Seng & Anor v Yee Weng Kai* [2014] 4 MLJ 478.

- Legal recognition of electronic payment system and Financial Technology (FinTech).
 WHAT CHANGES: FINANCIAL SERVICES & DIGITISATION

• With the financial industry moving towards digitisation, new dimensions of risk management have emerged.
  • Datafication: Tendency to record not only the critical data, but also everything else.
  • More gadget, more potential security breaches
  • Same thief, new method!
  • CIA of data security: Managing the confidentiality, integrity and availability of data
  • Legal risks surrounding data: From reputation to financial detriments

“Datafication” – the process of quantifying all information around us: our location, movement, communications, usage of devices, etc. which will allow us to use such information in new ways, such as in predictive analysis. This will help us further to unlock the implicit, latent value of the information.

V. Mayer-Schonberger and K. Cukier (2013) 
Big Data: A Revolution That Will Transform How We Live, Work and Think.
WHAT REMAINS: THE NEED FOR FINANCIAL INTEGRITY AND CONSUMER PROTECTION

Financial inclusion
- Accessibility for all
- Affordability
- Technological adoption and adaptation

Financial integrity
- Security of transaction
- Security of data
- Security of financial system

Consumer protection
- Fraudsters
- Industrial exploit
- Right to privacy
- Public security, social stability, economic resilience
FINTECH DOES NOT PLAY IN LEGAL VACUUM

- **Capital Markets and Services Act 2007**
- **Financial Services Act 2013**
- **Central Bank of Malaysia Act 2009**
- **Penal Code**
- **Personal Data Protection Act 2010**

- **Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019**
- **Islamic Financial Services Act 2013**
- **Credit Reporting Agencies Act 2010**
- **Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001**
- **Communications and Multimedia Act 1998**

- **Guidelines on Recognized Markets SC-GL/6-2015(R3-2019)**
- **SME Tax Incentives by Cradle Fund, MDEC, etc**
- **Computer Crimes Act 1997**
- **Electronic Commerce Act 2006**

**BNM Fintech Regulatory Sandbox 2016**

SONNY ZULHUDA (C) 2019

sonnyzulhuda.com
Plaintiff took legal action against defendant because the latter did not pay his debt. Defendant denied.

The evidence of the acknowledgement of debt was based on the SMS sent by defendant to plaintiff’s phone. The SMS message clearly acknowledged the debt.

Defendant argued that SMS cannot be considered as a written document.

**DECIDED:**
A message from an SMS, with all the attributes of [s.8] being present viz accessibility, intelligible and extractable for subsequent reference, *such an electronic message is as good as in writing.*
ELIMINATING BARRIER #2: STRONGER CONSUMER PROTECTION IN THE DIGITAL ECONOMY

- Enhancement of consumer protection law:
  - Amended to apply on e-commerce
  - Protects consumers against manufacturing defect, design defect and marketing defect
  - Provision against unfair terms ("a term which causes a significant imbalance in the rights and obligations of the parties arising under the contract to the detriment of the consumer" – CPA 1999 s.24A).
- Consumer-friendly Websites & E-commerce Sites
  - Fair terms for consumers (CPA 1999)
  - Clear notice of privacy protection (PDPA 2010)
- Dispute Resolution & ADR
CONSUMER PROTECTION (ELECTRONIC TRADE TRANSACTION) REGULATIONS 2012

- Disclosure of identification
- Maintenance of Business Record for 2 years
- Ratification of Errors
- Acknowledgement of Receipt
ELIMINATING BARRIER #3: PERSONAL DATA PROTECTION AND ITS “LEGITIMATE USE”

- Personal data processing is now regulated in two primary legislations:
  1. Personal Data Protection Act 2010 [Act 709]
  2. Credit Reporting Agencies Act 2010 [Act 710]

- Common Law still plays an important role:
  1. Breach of Privacy
  2. Breach of Confidence
Data user who contravenes the above Principles commits an offence and shall, on conviction, be liable to a fine not exceeding three hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.
WHEN IS A USE LEGITIMATE?

• Obtaining a Consent of data subject before or on the collection point [s.6,7 PDPA]
• Performance of contract with data subject [s.6 PDPA]
• Legitimate processing for public interests, e.g. Legal compliance, administration of justice, protecting vital interests, and exercising of law [s.6 PDPA].
• Uses falling under the partial exemptions, e.g. Crime prevention, health purpose, statistics and research, regulatory functions, etc. [s.45 PDPA].
• Uses of data after being de-identified/anonymised [s.10 PDPA].
• When the data has been deliberately made public by the data subjects themselves [s.40 PDPA]
October 2017: the personal details of some 46.2 million mobile number subscribers in Malaysia were reportedly leaked online.

June 2018: 60,000 Astro customers data have been offered for sale online. The data was being sold for RM4,500 for 10,000 records, or RM0.45 per record.

June 2018: The Ministry of Education’s School Examination Analysis System (SAPS) was taken offline, following the discovery of a security exploit that could have potentially exposed the personal details of more than 10 million citizens.
KUALA LUMPUR: Former teachers at private school took and used the students list which contained the **personal data of 188 students** such as their postal addresses, email, telephone numbers and other personal particulars to attract them to move to another school. Court decided on various issues of breach of fiduciary duty.
DATA LEAKAGE BY AN EXITING EMPLOYEE
EQUITY TRUST (LABUAN) LTD V MOHAMMAD SOFIAN MOHAMAD & ANOR [2010]

LABUAN: Court issued injunction to stop a former employee marketing staff from disclosing confidential information including clients’ listing and potential clients data to a new employer (2010)
KUALA LUMPUR: High Court ordered a university medical centre in Kuala Lumpur to pay a total of RM400,000 to a plaintiff for revealing his psychiatric medical records to a third party (2013)
JOHOR BAHRU: Court held an installation of CCTV directed towards other person’s house entrance as a breach to privacy (2011)
KEY ISSUES ON DATA PROTECTION

- Automatic Processing of Data
- Trans-border Data Transfer
- Data Breaches Notification
- Data Governance and Transparency
- Industry Self-Regulation
- It's About Public Trust
STRENGTHENING DIGITAL ECONOMY THROUGH DATA GOVERNANCE AND TRANSPARENCY

• Data Processing as Governance and Board Room Agenda: sec 133 PDPA
• Open privacy policy: sec 7 PDPA
• Special Data Protection Officer? (PDP Regulations 2013 – Reg 4)
• Audit Requirements: s. 101 & 104 PDPA.
• The involvement of a third party (Data Processor): s. 7,9,12 PDPA.
### ELIMINATING BARRIER #4: DATA SECURITY FOR A SUSTAINABLE DIGITAL ECONOMY

<table>
<thead>
<tr>
<th>Act Description</th>
<th>Legal Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criminalising acts that compromise data security (cybercrimes, sabotage, breach of secret)</td>
<td>Computer Crimes Act, Penal Code, Sedition Act</td>
</tr>
<tr>
<td>Governing Critical Information Infrastructure</td>
<td>ISMS standards</td>
</tr>
<tr>
<td>Security of Personal information through Privacy Governance</td>
<td>Personal Data Protection Act</td>
</tr>
</tbody>
</table>
AUDIT, ENFORCEMENT AND PROSECUTION OF DATA PROTECTION ABUSES

• More than 18,000 issues referred to since Nov. 2013, including 140 complaints and reports;
• 82 cases followed up by the PDP Commissioner (by end of 2015);
• Banking sector, property and services are the top three sectors with most cases/reports.

Complaints relate to
  • un-consented processing and disclosure of personal data;
  • unauthorised use of data by exiting employees;
  • poor security of data record;
  • un-consented direct marketing;
  • data retained unnecessarily;
  • unauthorised sale of data.
<table>
<thead>
<tr>
<th>No</th>
<th>Sector</th>
<th>Offence(s)</th>
<th>Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Tourism (Hotelier)</td>
<td>Processing personal data without the Commissioner’s Certificate – s.16(4) &amp;</td>
<td>MYR10,000 fine or 8 months imprisonment for each of the offence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Processing personal data without the consent of data subject – s.5(2)</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Education (Private university)</td>
<td>Processing personal data without the Commissioner’s Certificate – s.16(4)</td>
<td>MYR10,000 fine or 3 months-imprisonment</td>
</tr>
<tr>
<td>3</td>
<td>Service sector (Employment agency)</td>
<td>Processing personal data without the Commissioner’s Certificate – s.16(4)</td>
<td>MYR10,000 fine</td>
</tr>
<tr>
<td>4</td>
<td>Education (Private University)</td>
<td>Processing personal data without the Commissioner’s Certificate – s.16(4)</td>
<td>Compound RM10,000</td>
</tr>
<tr>
<td>5</td>
<td>Service (Job agency)</td>
<td>Processing personal data without the Commissioner’s Certificate – s.16(4)</td>
<td>MYR10,000 fine</td>
</tr>
</tbody>
</table>
MORE AND MORE DATA BREACH?
CHALLENGES OF DATA PROTECTION TODAY

• Ready data vs Synchronised data (location, IP address, face recognition, social networking preferences)
• Data privacy vs Conflicting interests (public health, open data, security)
• Locally stored vs Cloud storage
• Within the country vs Cross-border
• Own definition vs GDPR definition (PDPO, Breach notification duty, standardisation, PIA)
• Reactive Measures vs Preventive Action (Analytical/Predictive)
• Governing data = Managing trust
Basic: * Building internal data culture and awareness of ALL stakeholders * Continuous training program

Governance: * Appoint leaders and owners of compliance measures. * Centralised, Decentralised, Hybrid leadership. * Organisational & Operational ownership

Baselining & Benchmarking: * Define data security & privacy goals * Define the measures to achieve goals (Core & elective measures) * Define timeframe, team, budget, plan, etc.

Documentation & Audit: * Document all the measures & processes * Conduct audits including adequacy audit and compliance audit across departments and divisions

Implementation: * Continuous monitoring for compliance (due diligence) * PDCA Framework * Keeping up with outsiders (Regulators, Data User Forum, Consumers Associations, Workers Union, press, etc.)
THANK YOU!

DR. SONNY ZULHUDA
sonny@iium.edu.my
http://sonnyzulhuda.com