

PRIVACY POLICY IN INDONESIA AND MALAYSIA: FROM DIGITAL ECONOMY TO PERSONAL DATA PROTECTION LAWS

The 3rd Asia Privacy Bridge Forum
@Seoul 27-06-2017

Dr. Sonny Zulhuda
Civil Law Department
Ahmad Ibrahim Kulliyah of Laws
International Islamic University Malaysia

Indonesia & Malaysia towards the Digital Economy

2017 (c) Sonny Zulhuda



“Digital economy is inevitable.. Indonesia is highly potential to develop digital economy that the country should not be lagging behind in its development.. We must play a role in the process.”

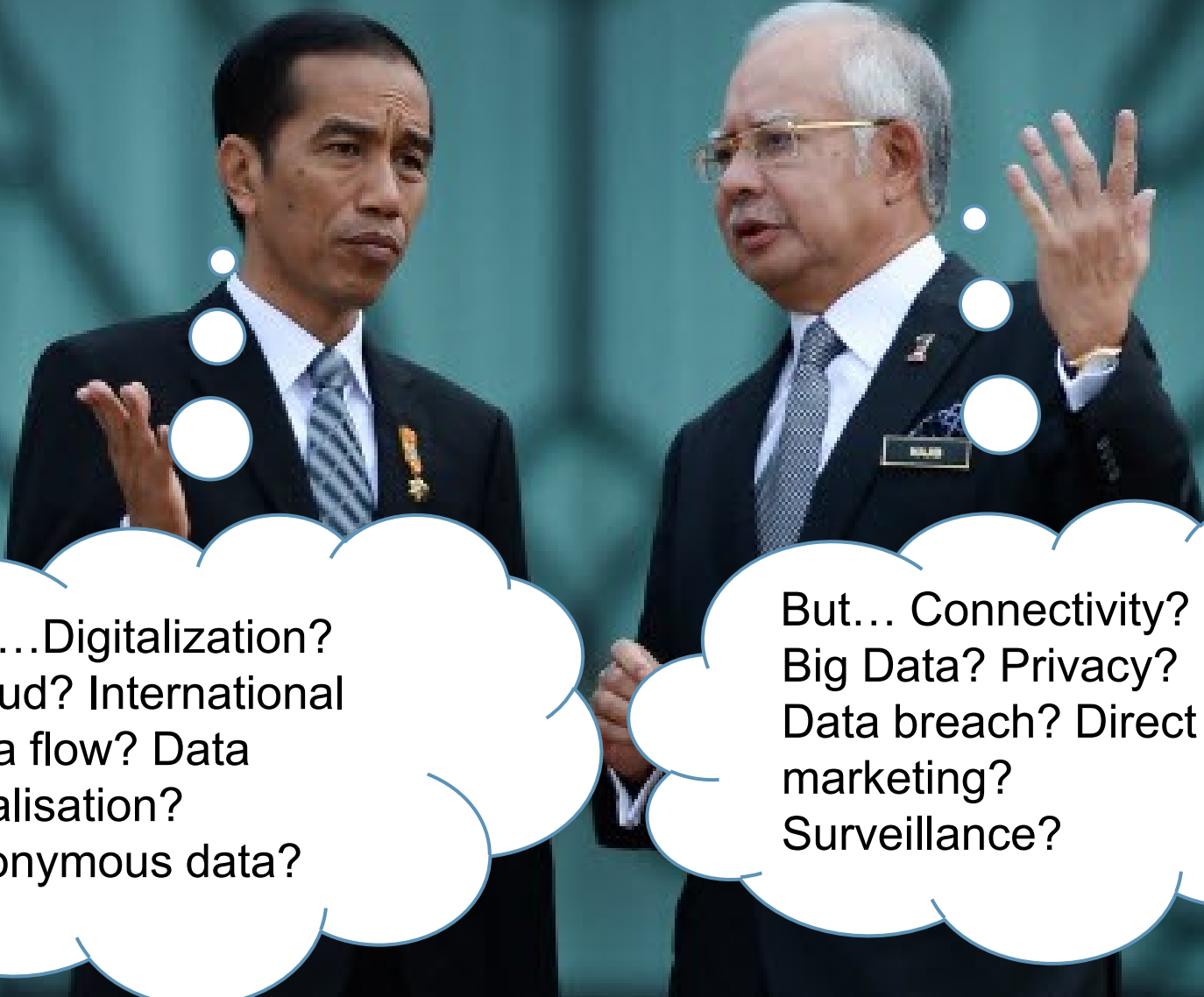
President Joko Widodo

“2017 will be the year of the Internet Economy for Malaysia. To build a vibrant Digital Economy, we need inclusivity from both the people and the capital economy..”

Prime Minister Mohammad Najib Razak

Indonesia & Malaysia towards the Digital Economy

2017 (c) Sonny Zulhuda



But... Digitalization?
Cloud? International data flow? Data localisation?
Anonymous data?

But... Connectivity?
Big Data? Privacy?
Data breach? Direct marketing?
Surveillance?

Overview of the Law

- **Malaysia**
 - Enforced Personal Data Protection Act 2010 (“Act 2010”)
 - Seven PDP Principles – applies only to commercial transactions, excludes data processing by Government
 - Enforced by a PDP Commissioner, appointed by the Minister
 - Imposes penal sanctions on various types of offences
 - What to watch: ENFORCEMENT time! 1st court case started in May on illegal processing of personal data.

- **Indonesia**
 - Currently no comprehensive Act, but derives its norms from the broad Information and Electronic Transaction Act (Law No. 11 Year 2008) (“Law 2008”)
 - A subsidiary law under the Law 2008: Imposing duties on the Controller of Electronic System and Electronic Transaction (By-Law No. 82 Year 2012) (“By-Law 2012”)
 - Recently enforced the Ministerial Regulation No. 20 Year 2016 on the Protection of Personal Data by Electronic Processing (“Regulation 2016”) – Restricted scope: It regulates electronic system controller rather than data user. Only civil and administrative sanctions.
 - What to watch: A more comprehensive DRAFT PDP BILL on its way!

The Challenges of Digital Economy

(And how the PDP laws address them)

1. Personal data is a commodity
2. Data processing is getting automated
3. Cloud is a default choice
4. Trans-border data flow is inevitable
5. Data due diligence is a norm
6. Data breach gets sophisticated
7. Industries fight back with self-regulation
8. Bottom rule: Trust in the digital economy

#1. Personal Data is a Commodity. Who is affected, and who is in Charge?



- Is Digital Economy a “Free Economy”?
- Who controls the data?
 - Individuals
 - Government
 - Businesses
 - “Data user/controller” vs “Electronic system controller”
- Malaysian 2010 Act applies on commercial transactions, excludes the Government;
- Indonesia’s Regulation 2016 emphasises on the duties of “Electronic system controller” but applies extra-territorially.

#2. IoT: Data processing gets automated

- In Europe: duty to inform about “the logic involved in that automated decision-taking”.
- Both Malaysian and Indonesian laws are silent about a specific obligation when there is an automated decision-taking.
- Nevertheless, they provide for an enforceable right of data subject to get an access or information about their data processed by the data controller.



#3. Cloud is a default choice

- Under Malaysian 2010 Act:
 - Data user's own cloud = assumes a primary duty; while a data processor's cloud = a secondary duty
 - Control over Data Processor by:
 - Data security requirements under s. 9(1)(2)
 - Contractual obligation – s. 9(2)(a)
 - Subject to inspection by the Commissioner – s. 101

- Under Indonesian 2016 Regulation:
 - Duties of “Electronic system controller” includes obtaining consent, giving notice & choice, having a certified system, local retention of data and written breach notification.

#4. Trans-border data flow is inevitable

- Under Malaysian 2010 Act: data export control:
 - S.129(1) – “white list” countries
 - Alternatively: Data user to exercise reasonable precaution and due diligence to assess risks – s.129(3)(f)
- Under Indonesian By-Law 2012 and Regulation 2016: Data localisation obligations:
 - Both data center and disaster recovery center must be located in Indonesia.
 - Also, e-transactions data has to be kept within the local jurisdiction.

#5. Data due diligence is a norm



Due diligence is:

putting appropriate & preventive measures

+

efforts to monitor such measures.

- A statutory duty of data due diligence under the Malaysian 2010 Act
 - On data security risks analysis – s.9(1)
 - On organisational data governance – s.133(1)
- Risk-based governance under the Indonesian 2016 Regulations and 2012 By Laws.
 - Educational activities, preventive measures, disaster management training, etc. under reg. 5.
 - Risk Management, audit and system governance under section 13-14 of the 2012 By law.

#6. When data breach takes place

Malaysia:

- No breach notification duty
- Commissioner may issue enforcement notice
- Disputes can be taken to and resolved by the Tribunal
- Aggrieved parties can alternatively take action in court for both civil and criminal remedies.

Indonesia:

- The By-Law 2012 imposes a breach notification duty (in writing) to the data subjects. Authorities must also be notified if the breach causes serious damage.
- The Regulation 2016 also imposes breach notification duty to the data subjects.
- Disputes to be resolved through mediation, or other alternatives.
- Civil remedies and administrative sanctions can be given.

#7. Industry fights back: Self-regulation

- With an array of various potential liabilities under Malaysian 2010 Act, it is best for the industries to put up a Self-regulatory mechanism – a bottom-up rather than top-down approach
- A common rule of game for specific industries can be pre-defined by the “Data User Forum” where all players of a particular sector can sit and discuss.
 - Data User Forum – s. 21 PDPA
- They can come up with a specific Code of Practice. Already registered 3 Codes of Practice: Electricity Sector, Insurance and Takaful Sector, and Banking Sector.
 - Code of Practice – s. 23 PDPA
- No similar provision exists in Indonesian laws

#8. Back to Basic: Importance of Trust

- **64%** believes managing people's data is a corporate differentiating factor
- **84%** say breaches of data privacy and ethics causes them to lose trust in companies
- **90%** thinks that breaches of data privacy have negative impact on stakeholder trust in the next 5 years

PwC 20th 2017 Global CEO Survey
From 1,379 CEOs interviewed in 79 countries

- How to build a trust? “PDP as a Design” *lessons from the Uberisation*
- Data protection is not only about complying with laws – it is about constructing the trust and helping your business.
- Data protection law as a design: privacy policy, transfer guarantee, cloud agreements, etc. to help create the trust in digital economy.

Next: International Collaboration

Agenda

- Malaysia and Indonesia are the backbone for ASEAN – the ASEAN Economic Community (AEC), established in 2015, has as one of its e-commerce objectives the development of a “coherent and comprehensive framework for personal data protection.”
- Also, we have to collaborate globally, as the threat of data breach is ubiquitous, global, and borderless. Not to forget the borderless effect of other laws e.g. the GDPR.
- Data privacy agencies are to emulate the international work-frame from the worldwide data security agencies.

THANK YOU

고맙습니다

Dr. Sonny Zulhuda

sonny@iium.edu.my

<http://sonnyzulhuda.com>