RAJAH & TANN ASIA

LAWYERS WHO KNOW ASIA

The Internet of Things – A Challenge for Regulators?

IoT and the Challenge of Data Privacy

Date	2 June 2016
Prepared For	IIC TRPC
Presentation By	Rajesh Sreenivasan
Contact Details	rajesh@rajahtann.com

RAJAH & TANN

Outline

- Introduction to IoT and Use of Data
- Data Privacy Concerns Snapshot
- Collection of Personal Data
- Sufficiency of Consent (Purposes)
- Cross-border Transfer of Personal Data
- Regional Snapshot
- Regulators' Challenges

Wearables

Internet of Things

Media

"Connection of physical objects to the Internet and to each other through small, embedded sensors and wired and wireless technologies, creating an ecosystem of ubiquitous computing"

Industrial Applications

Home Automation / Smart Appliances

IoT and Big Data

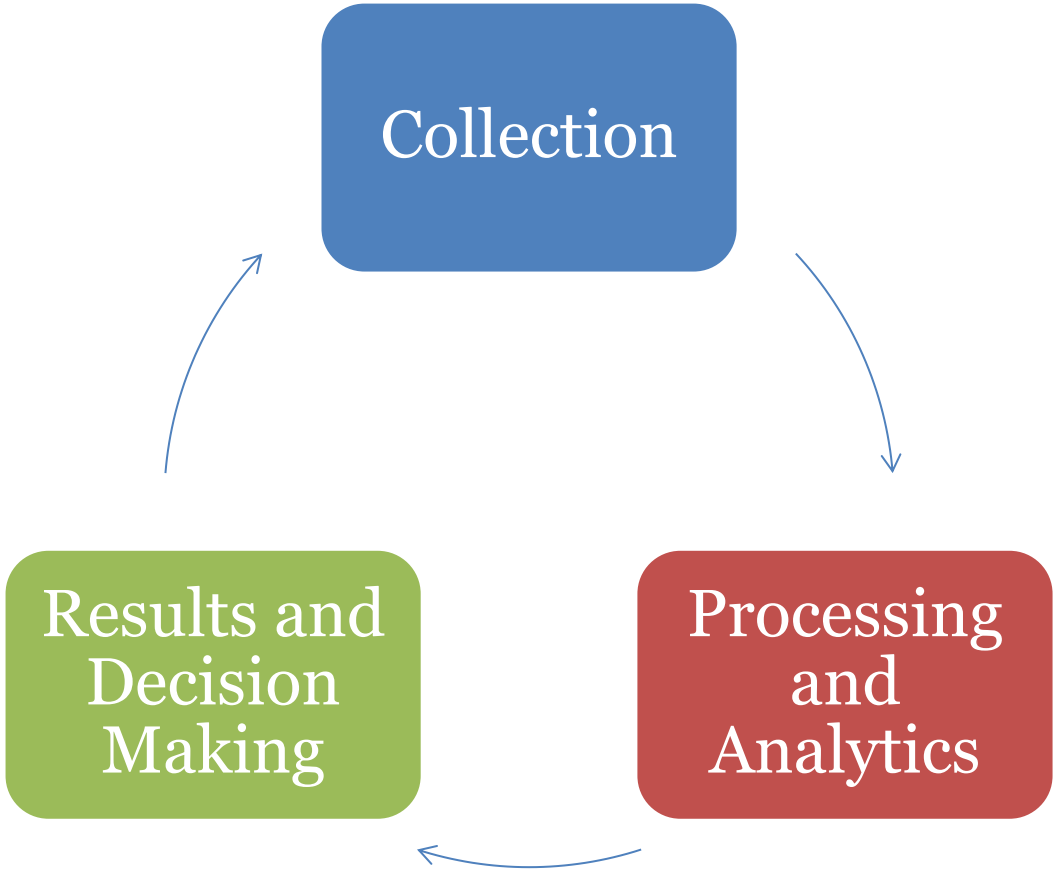
Big Data

- "**Big Data**" generally refers to the collection of large volumes of data which can be processed and mined for information

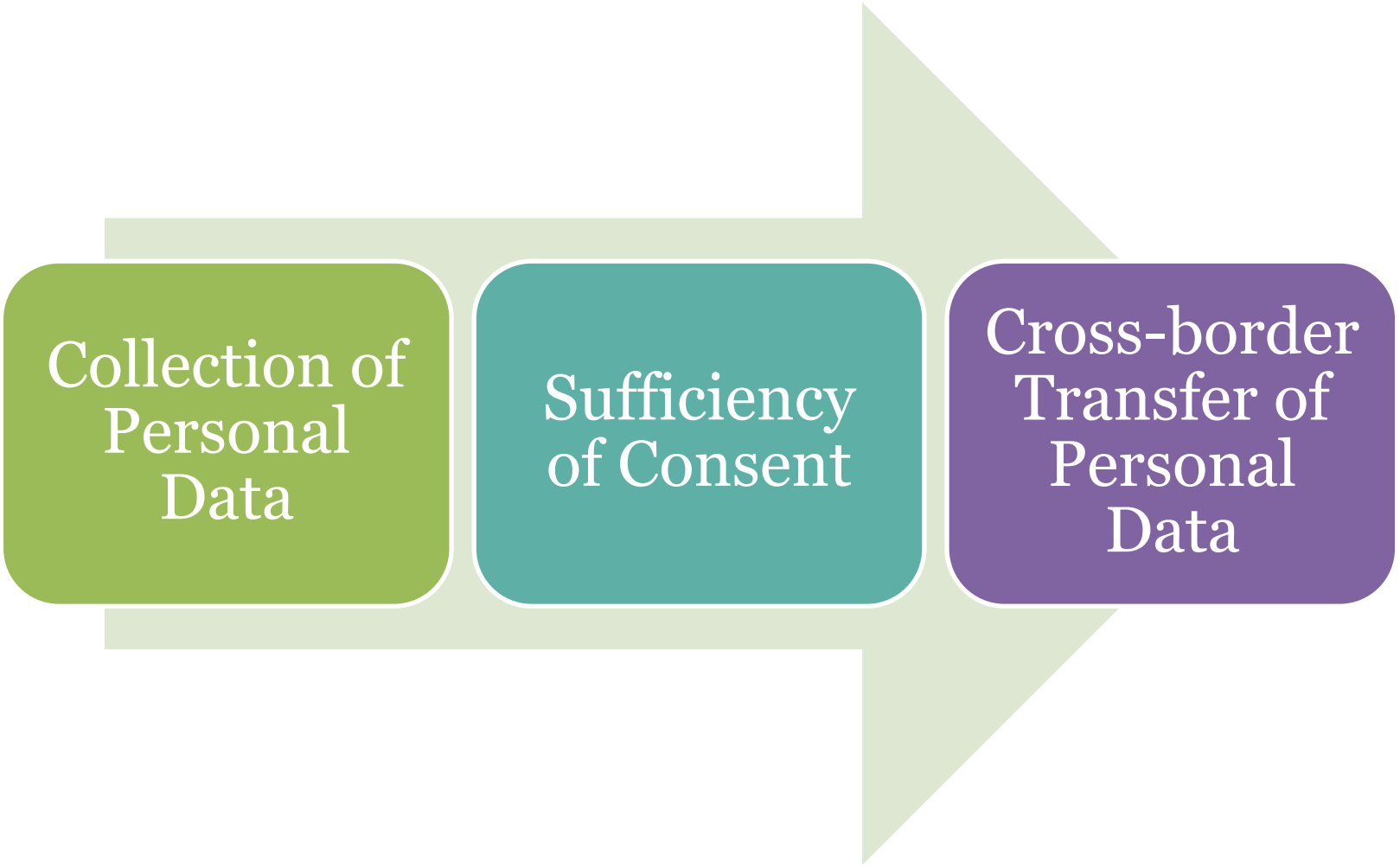
Characteristics

- Volume
- Veracity
- Variety
- Velocity

Data Collection and Analytics Process for IoT



Data Privacy Concerns



Collection of Personal Data

- **Definition:** The Personal Data Protection Act ("PDPA") defines "**personal data**" as: data, whether true or not, about an individual who can be identified – (a) from that data; or (b) from that data and other information to which the organisation has or is likely to have access.
- **General Principle:** Before collection of personal data, you must obtain the individual's **consent** for collection, use and/or disclosure of his personal data. This means the individual must be informed of the specific **purposes** for which is personal data is collected, used and/or disclosed.

Data Collection: 2 models for IOT

Aggregate Data

- Requires data collection from large group of people
- Value is focusing on a large group of data sets within certain demographics
- Less issues with privacy

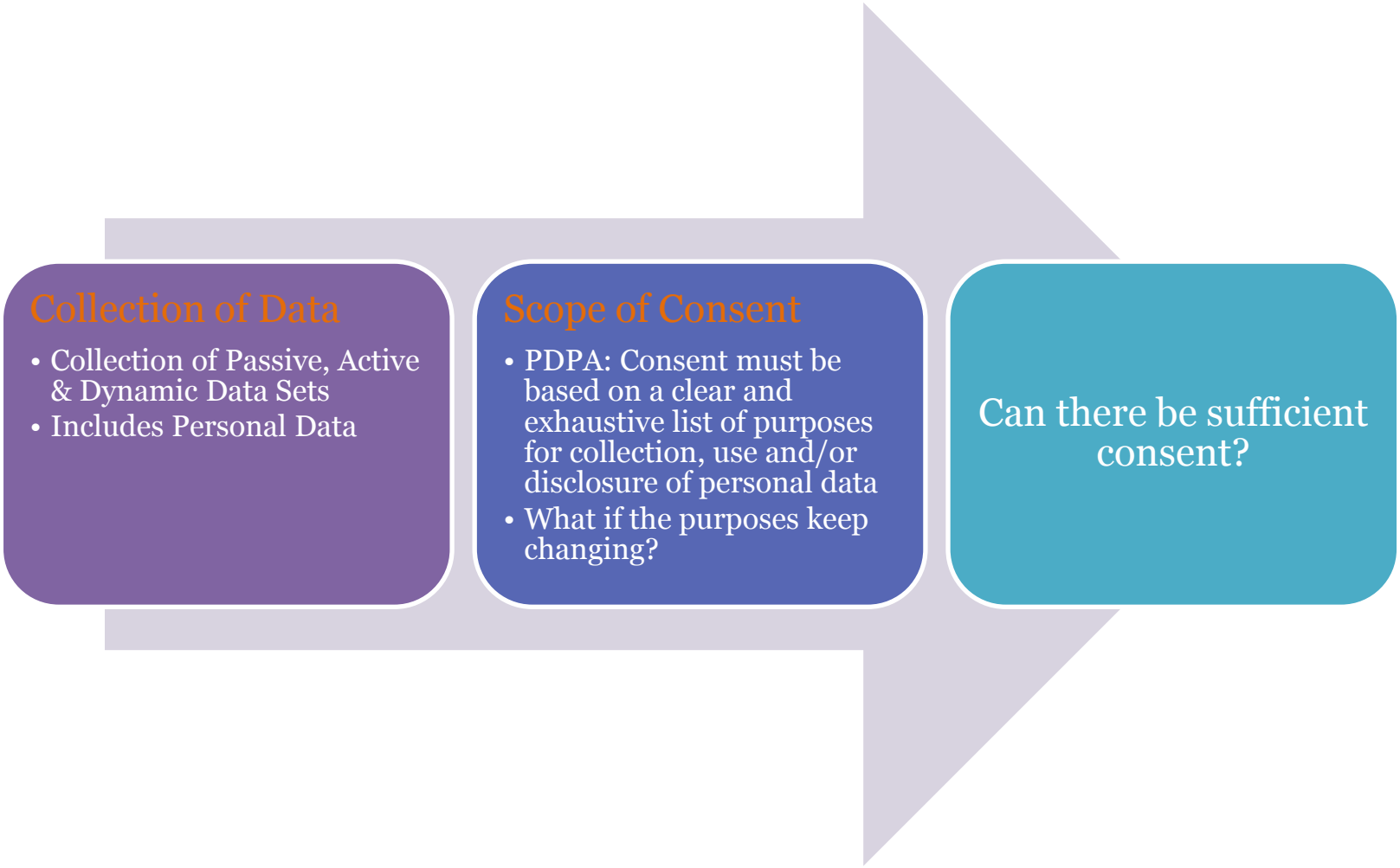
Individualised Data

- Privacy is difficult to manage
- May need disclosure of personal data to third parties to provide services

Data Collection: True Aggregate Data?

- Collection of data through IoT devices and machines make it easier for *personal data* to be collated, even when individually, the data is not personal in nature
- Data that does not appear personal in nature can easily become personal data when viewed and analysed in context with other information
- E.g. Dietary information may reveal information such as religion or ongoing health concerns

Scope of Consent (Purpose)



Competing Interests

Regulator?

IoT Service Provider
- Difficult to constantly monitor purposes for use of data
- Interest is to keep the wording as broad as possible
- Maintain flexibility in use of data

Consumer
- Want control of how personal data is being collected, used and disclosed
- IoT may result in their data being used for purposes that they never expected

Scope of Consent (Purpose)

Existing Models

- Putting in place a general one-stop-model Privacy Policy
- Listing all purposes for which the individual must give consent to receive product/services
- No real choice for individual on how his information is used
- Singapore already puts in place separate requirements for obtaining consent for marketing purposes

Reforming Process for Consent

- Need to review what purposes are necessary for provision of the product/services at hand
- Increasing challenge for individuals who want their data to be used for specific narrow purpose (e.g. providing feedback) but end up consenting to a much broader scope of purposes (e.g. marketing emails, data analytics)

Scope of Consent (Purpose)

Reforming Process for Consent

- Ongoing process (not one-time consent)
- Need to increase transparency and provide adequate notice and choice to customers
- Higher standards of notice and choice for consent need to be led by regulators as well as companies who value privacy

Potential Approaches

- Encourage privacy by design at the point of design/development of product or service
- Data minimisation (regular audits and assessments on what data is actually necessary)
- Ongoing updates on purposes for which personal data is used
- Provide choice to customers (e.g. additional rebates for opt-in for data analytics)
- **How far should regulators go to intervene in monetisation models?**

Cross-Border Transfers

- IoT enables data (including personal data) to be collected and analysed from multiple sources and locations (not restricted by geographical borders).

- Also, due to the large volume of data, cloud storage is usually required. This may not necessary be contained within a single jurisdiction.

- Cross-border transfers and usage of the data becomes inevitable. This is usually subject to certain requirements under the data protection laws of various jurisdictions

Cross-Border Transfers

- **Basic Principle:** Section 26(1) of the PDPA: "An organisation **shall not** transfer any personal data to a country or territory **except** in accordance with requirements prescribed under this Act to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under this Act."

- **General Steps Required**: Prior to the transfer of personal data, the transferring organisation must:

  (a) take steps to ensure that it will comply with the data protection obligations while it remains in its possession or under its control

  (b) take appropriate steps to ascertain and / or ensure that the receiving organisation (outside Singapore) is bound by legally enforceable obligations to protect the personal data so transferred to a standard that is comparable to the protection under the PDPA

Cross-Border Transfers: Challenges

- **Auto Upload / Transfers**: Personal data collected from IoT devices usually transferred or uploaded automatically (sometimes without individual's knowledge). Traditional forms of data controls may not be applicable in this situation. What alternatives are there?

- **Multiple Parties Involved**: Multiple parties may be involved in the transfer of the personal data. How should responsibility be allocated?

- **Differing Laws Between Multiple Jurisdictions**: How can one company manage to comply with the laws of multiple jurisdictions on protection of personal data and cross-border transfers?

Regional Overview

Since 2010, Singapore, Philippines, Malaysia, South Korea and Taiwan have enacted data protection laws in their respective jurisdictions.

Australia, Hong Kong and Japan : Strengthened or are looking to strengthen their data protection laws.

Thailand : draft data protection law in the process of being finalized and enacted.
Indonesia: draft data protection law included in 2016 National Priority Legislation Program.

Regional Overview

Country	Data Protection Legislation?	Details
Australia	✓	Privacy Act 1988 and Australian Privacy Principles
Singapore	✓	Personal Data Protection Act 2012
South Korea	✓	Personal Information Protection Act
Malaysia	✓	Personal Data Protection Act 2010
Hong Kong	✓	Personal Data Protection Ordinance
Japan	✓	Act on the Protection of Personal Information (Law No. 57 of 2003)
Philippines	✓	Data Privacy Act of 2012
China	✓	No single act but data protection laws exist in multiple legislation and guidelines
Thailand	N/A	In the pipeline
Indonesia	N/A	In the pipeline (but other laws apply)

Regional Overview: Managing Data Privacy Issues for IoT

- Many jurisdictions in the ASEAN and APAC region have put in place privacy legislation. There are jurisdictions which have still not managed to put in place privacy specific legislation and rely on disparate laws on IT communications, e-commerce, and other sector-specific legislation.
- While many of the legislations are based on similar broad principles, the privacy legislation in place have differing standards and specific requirements.
- Even more activist or long standing regulators have not provided detailed guidance on managing personal data based on modern trends (e.g. cloud storage, IoT, data analytics).
- Companies rely on their own risk management standards when complying with data privacy legislation (if any).

Regional Overview Focus: Cross-Border Transfers

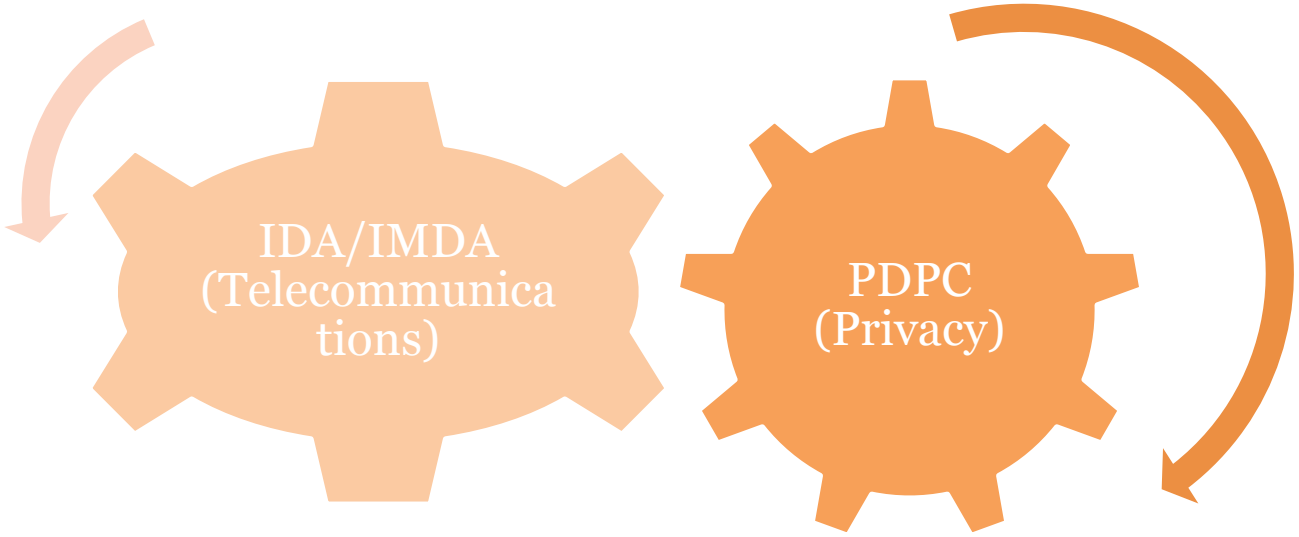
Countries with Regulations

- Singapore, Malaysia, Australia, Japan, Korea, New Zealand
- Note: Hong Kong provision on cross-border transfer restrictions not yet in force

Countries without Privacy Regulations

- Thailand and Indonesia will be coming up with new personal data protection legislation
- Other ASEAN jurisdictions do not yet have a personal data specific legislation in place
- Many MNCs follow a group-wide policy for data protection but encounter push back locally
- ASEAN region will require further coordination as part of AEC Initiative

Regulators in Singapore



iDA pdpc

Regulatory Experience Case Study: M2M Fleet Management

Service	Benefits	Data Collection
• Regulator reviewed need for license for M2M Fleet Management Service • Service provided real-time information about the vehicles (e.g. fuel consumption, vehicle positioning) to customers (vehicle owners)	• Access to information helped cut fuel consumption and improve performance (optimised servicing)	• SIM cards were activated in the production line when the vehicle is built • SIM cards configured only for automated communication between vehicles and servers

Regulatory Experience Case Study: M2M Guidelines

Regulator's Approach

- One concern: public safety and national security
- Safeguard communications between a Telco and a machine (equipment)
- Acknowledges challenges faced by service providers in keeping records of relevant information
- Regulator can regulate M2M communications by identifying and tracing the ultimate end user of equipment/machine
- Need to balance promotion of IoT and putting in place necessary controls for greater accountability

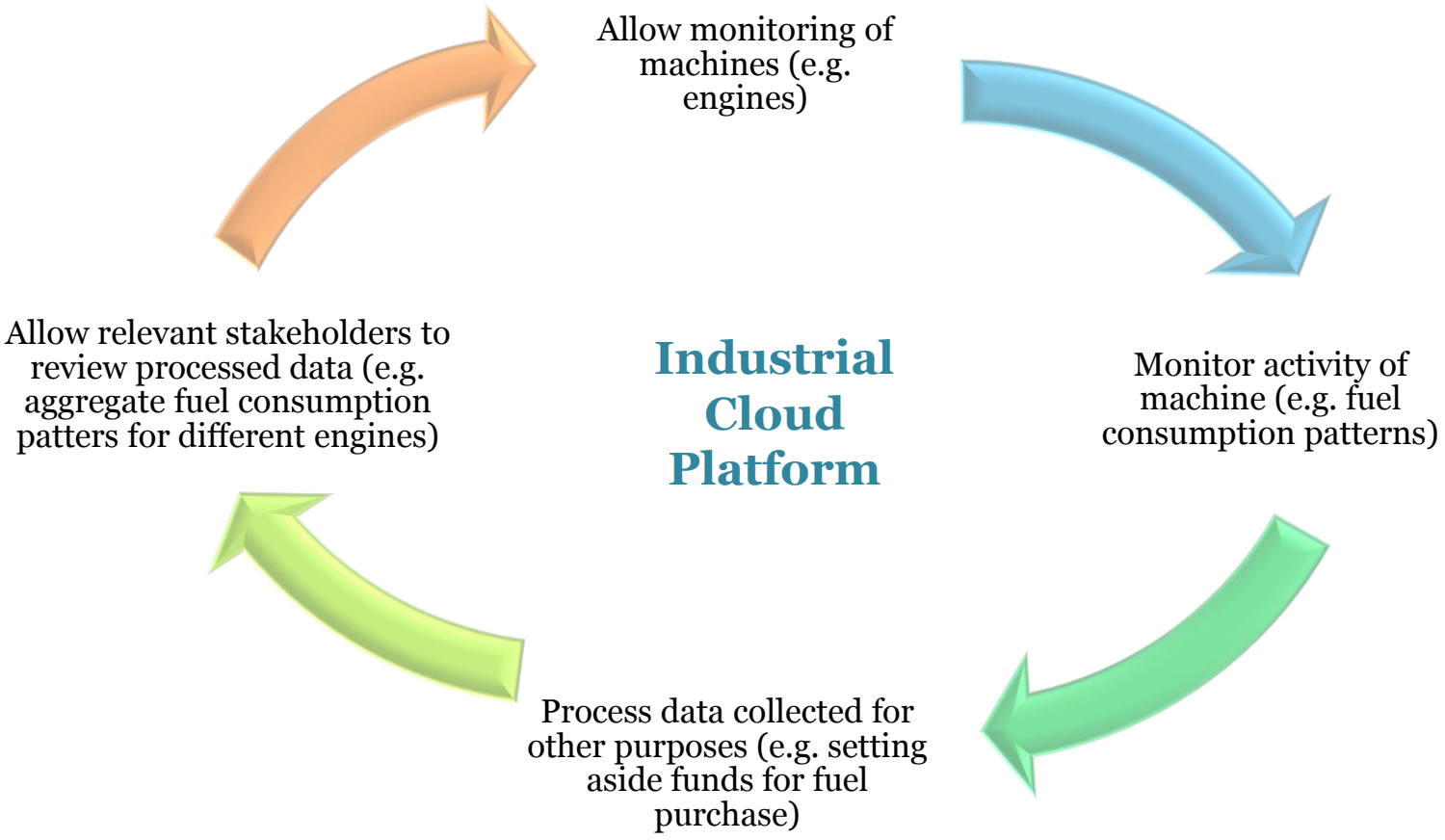
Initial Comments

- Adopt different approaches for consumer and commercial IoT applications?
- Different nature of use and risks for consumer (e.g. smart watch) and commercial applications (e.g. monitoring temperature levels in a boiler)
- Regulations should not only apply to telcos as they may not have involvement/visibility on machines being used
- Limits of reach of local telcos (e.g. use of roaming SIM card in imported equipment)

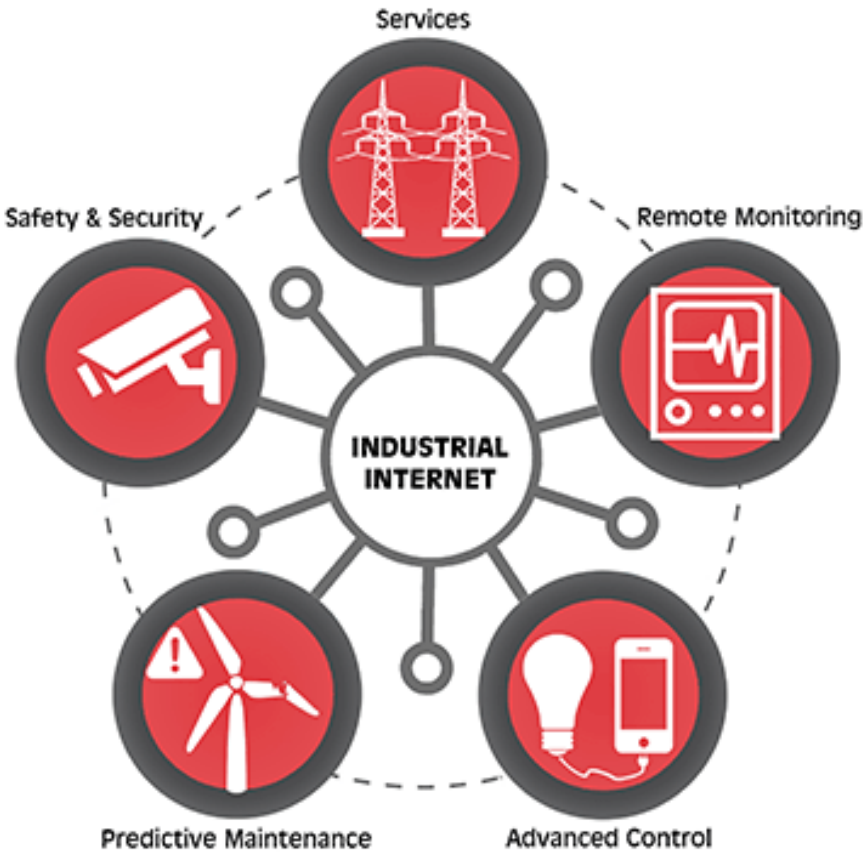
Regulatory Experience Case Study: M2M Guidelines (Cont.)

Comments	Comments
• Is there a need to change the relationship between the corporate customers, retailers and ultimate end users? (i.e. keep clear record of ultimate end user) • Difficulty of enforcing regulations on multiple stakeholders	• Lighter regulatory approach where M2M applications are limited to particular functions? • Regulator to engage and meet with other ministries to understand and help their concerns • Multi-agency discussion required (burden not put on telecommunications regulator and players alone)

IoT Ecosystem – Data Chain Effect

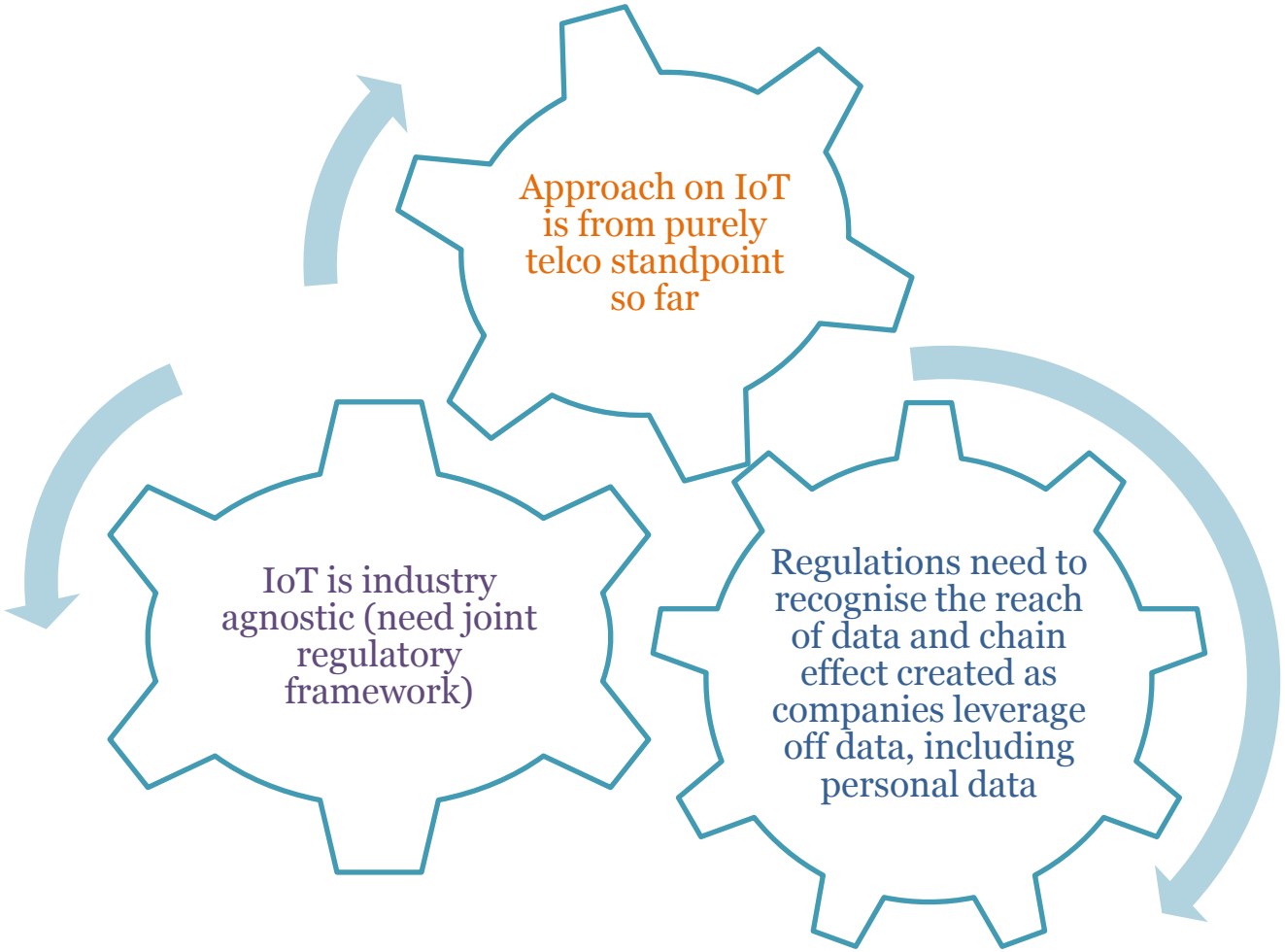


IoT Ecosystem – Industrial Internet



- Covers all industries (currently focusing on automotive, aviation, chemical, F&B, healthcare, industrial manufacturing, oil and gas, power and utilities, transportation)
- Combining developments in big data analytics with developments in engineering
- Using data for predictions to optimise efficiency

Refining Regulatory Approach



Disclaimer

The material in this presentation is prepared for general information only and is not intended to be a full analysis of the points discussed. This presentation is also not intended to constitute, and should not be taken as, legal, tax or financial advice by Rajah & Tann. The structures, transactions and illustrations which form the subject of this presentation may not be applicable or suitable for your specific circumstances or needs and you should seek separate advice for your specific situation. Any reference to any specific local law or practice has been compiled or arrived at from sources believed to be reliable and Rajah & Tann does not make any representation as to the accuracy, reliability or completeness of such information.