

# **Japan's New Data Privacy Regime and How it Will Enable Cross-Border Data Flows, Innovation and Privacy Protections in the Modern Information Age**

Thursday, 11 May 2017  
Tokyo

# Welcome and Introduction

**Markus Heyder**

Vice President & Senior Policy Counselor  
Centre for Information Policy Leadership

# CIPL at a Glance

BRIDGING REGIONS

BRIDGING INDUSTRY & REGULATORS

BRIDGING PRIVACY AND DATA DRIVEN INNOVATION

## ACTIVE GLOBAL REACH

50+  
Member  
Companies

We **INFORM** through  
publications and events

We **NETWORK** with global  
industry and government leaders

5+  
Active  
Projects &  
Initiatives

We **SHAPE** privacy policy,  
law and practice

We **CREATE** and  
implement best practices

20+  
Events  
annually

15+  
Principals  
and  
Advisors

### ABOUT US

- The Centre for Information Policy Leadership (CIPL) is a global privacy and security think tank
- Based in Washington, Brussels and London
- Founded in 2001 by leading companies and Hunton & Williams LLP
- CIPL works with industry leaders, regulatory authorities and policy makers to develop global solutions and best practices for data privacy and responsible use of data to enable the modern information age



[Twitter.com/the\\_cipl](https://twitter.com/the_cipl)



<https://www.linkedin.com/company/centre-for-information-policy-leadership>



[www.informationpolicycentre.com](http://www.informationpolicycentre.com)



2200 Pennsylvania Ave NW  
Washington, DC 20037



Park Atrium, Rue des Colonies 11  
1000 Brussels, Belgium



30 St Mary Axe  
London EC3A 8EP

# Special Remarks

**Andrew Wylegala**

Minister Counselor for Commercial Affairs  
Embassy of the United States, Tokyo



# Special Opening Remarks

## **Mr. Takuya Hirai**

Member, House of Representatives/Chairman, Special Mission  
Committee on IT Strategy, Liberal Democratic Party

## **Ms. Mari Sonoda**

Secretary General  
Japan Personal Information Protection Commission

# **International Efforts by the Personal Information Protection Commission**

---

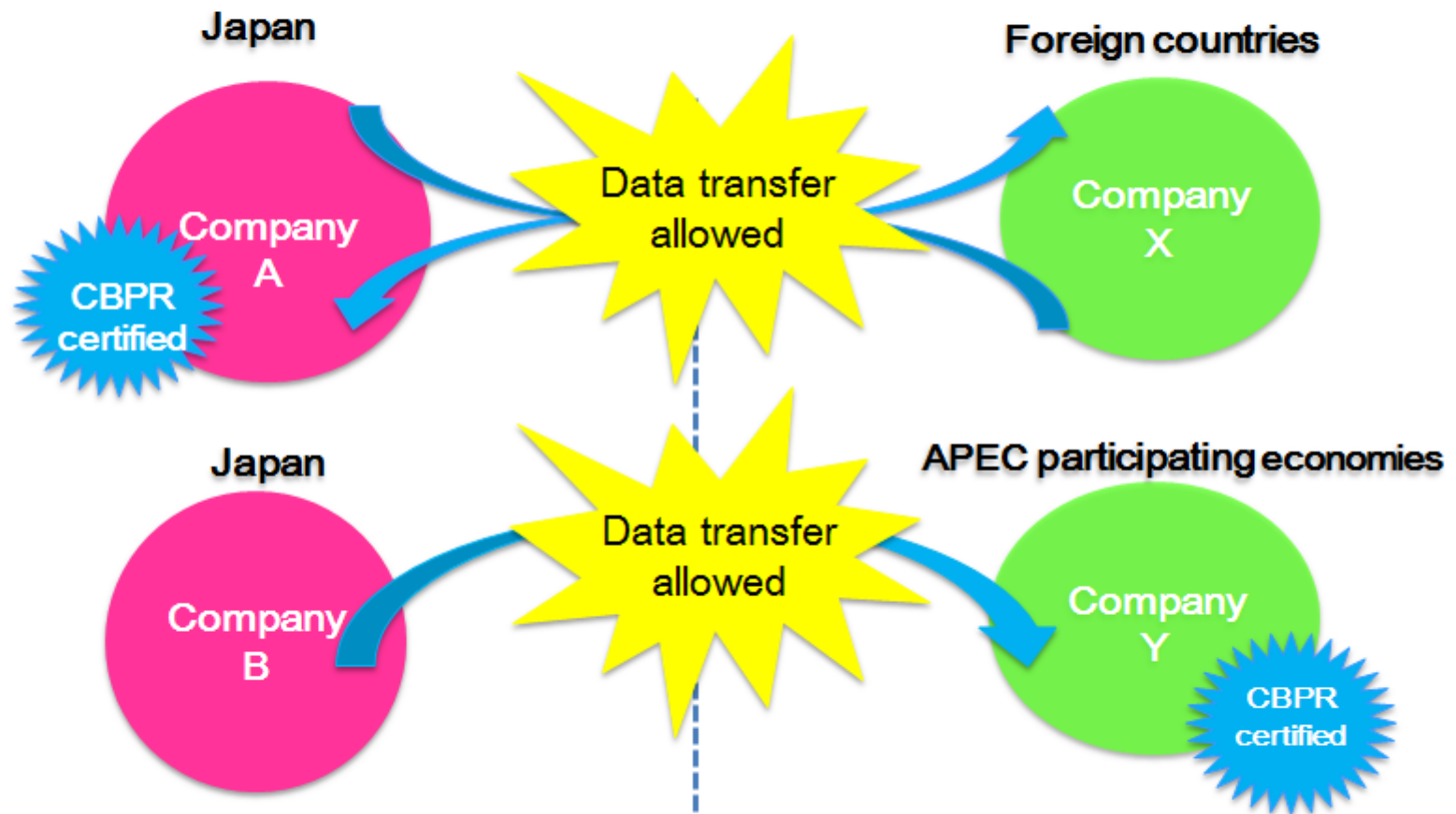
Personal Information Protection Commission  
Secretary-General Mari Sonoda

## I. Provision of personal data to a third party in a foreign country

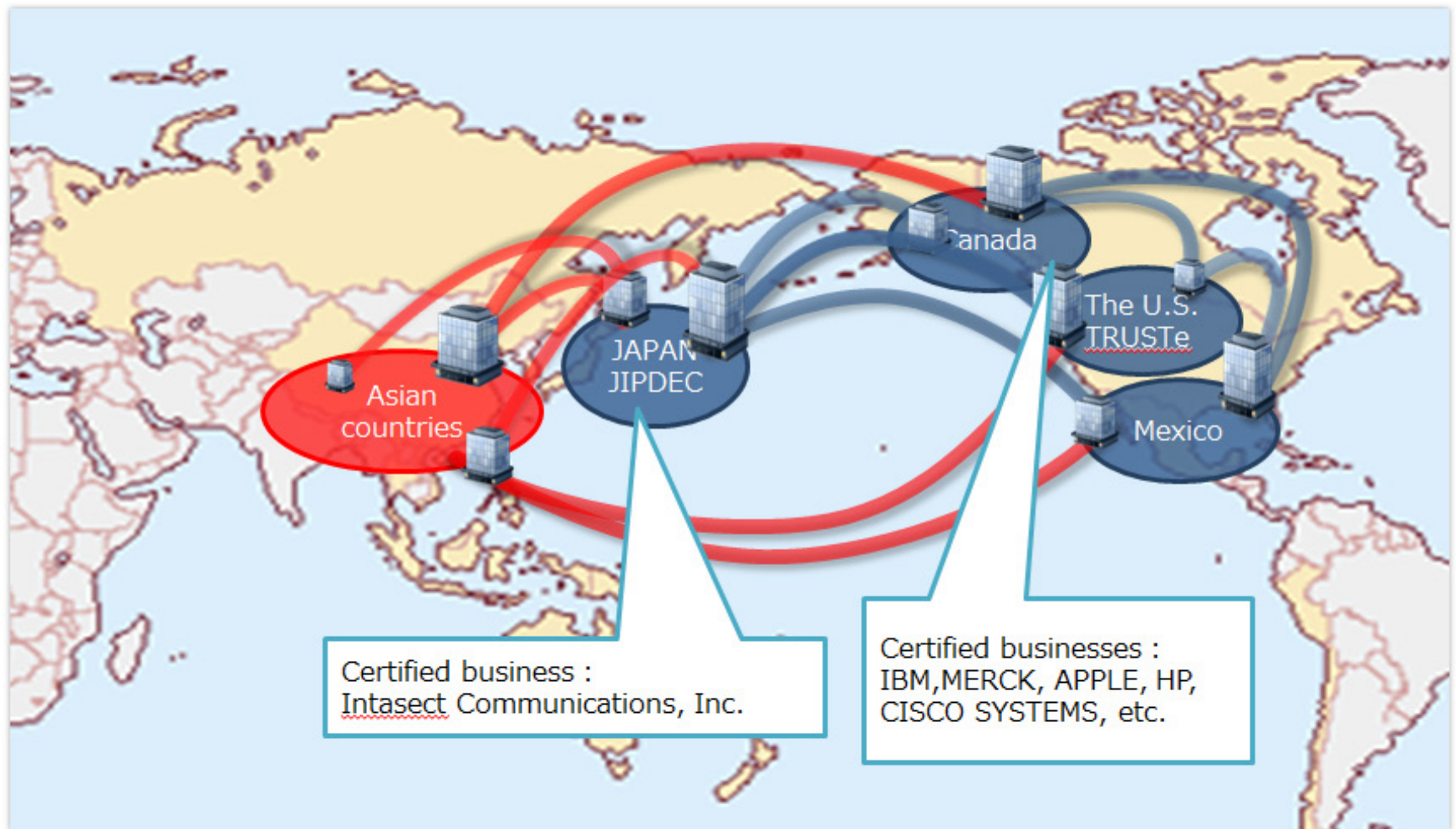
---

- In any of the following cases, personal data may be provided to a third party in a foreign country in the same way as in-country;
  - ① Cases in which there is a principal's consent to the provision to a third party in a foreign country;
  - ② Cases in which a third party in a foreign country has established and maintained a system that conforms to the standards prescribed by the PPC rules;
  - ③ Cases in which a third party is located in a foreign country or region designated by the PPC rules;

## II. The APEC CBPR system



## II. The APEC CBPR system



Pave the way for engineering the interoperability with the EU personal data cross-border transfer system.

### III. International efforts by the PPC

- ✓ “New Initiatives for Ensuring Smooth Cross-Border Personal Data Flows” (Personal Information Protection Commission Decision on July 29, 2016) was updated on November 8, 2016.

#### **「Concerning the International efforts」 (Personal Information Protection Commission Decision on November 8, 2016) (excerpt)**

##### United States

A shared recognition has been gained regarding the importance of collaborating closely and holding a regular meeting continuously. In addition, a consensus has been achieved on cooperatively practicing public relations for the APEC Cross Border Privacy Rules (CBPR) system and undertaking promotional activities to encourage the APEC member economies to participate therein together with the respective countries' stakeholders.

##### The European Union

While stressing the importance to ensure the protection of personal data and simultaneously promoting its cross-border transfer between Japan and the European Union, a consensus has been achieved on continuing to hold a cooperative dialogue between the two parties toward that goal.

# Scene Setting Remarks

**Bojana Bellamy**

President

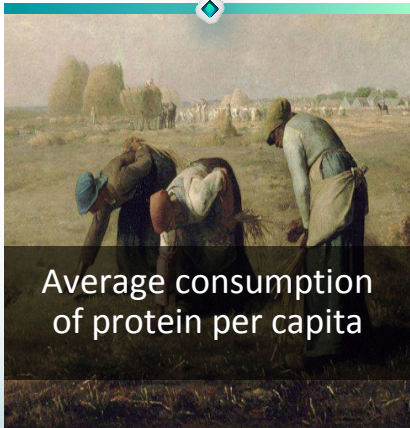
Centre for Information Policy Leadership



# The Fourth Industrial Revolution

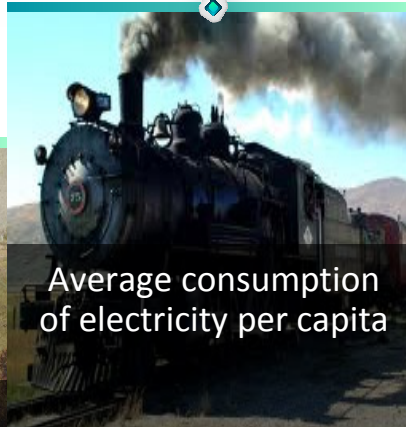
## Agricultural Society

4000 BC ~ 1763



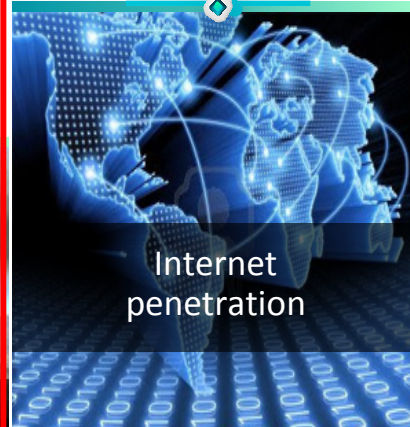
## Industrial Society

1764 ~ 1970



## Internet Society

1971 ~ 2015



## Data Society

After 2015

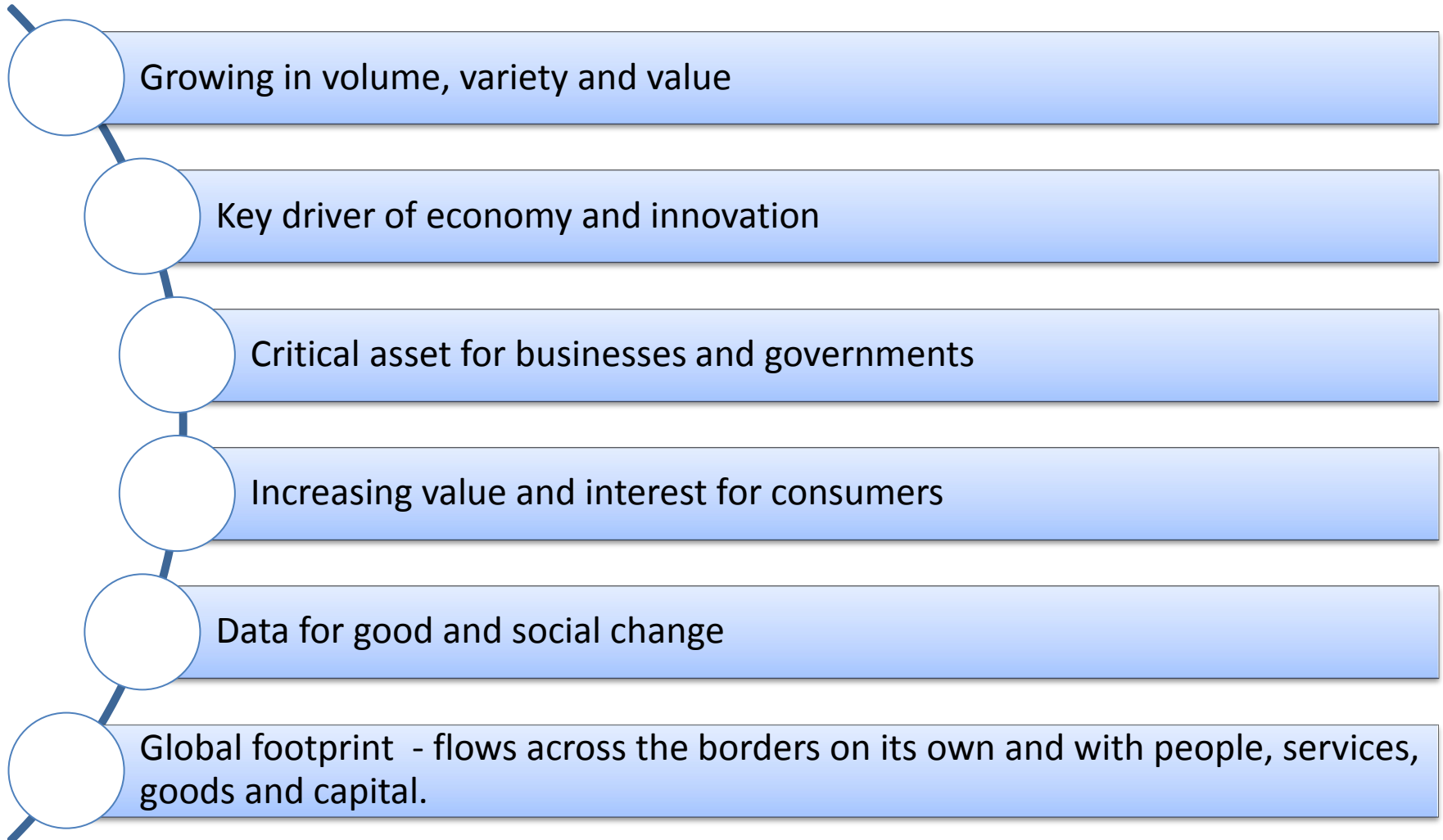


1. Always connected
2. Data processing
3. Transformation of Business Models

*Digital Economy*



# Data at the Center of the Fourth Industrial Revolution



# The new era of digital globalization

Global flows of trade and finance are flattening, while data flows are soaring



Digital technologies are changing how business is done across borders and broadening participation

## Large multinationals

Attain truly global scale with new markets and suppliers

New strategies for products, assets, organization

## Startups

>80% of tech-based startups are "born global"

Foreign customers, financing, suppliers from day one

## SMEs

Use digital platforms to find customers and suppliers abroad

50M on Facebook, 10M on Alibaba, 2M on Amazon

## Individuals

New ways to work, learn, and communicate across borders

>900M have international connections on social media



Global flows increase economic growth

**10%**

Increase in world GDP, worth \$7.8T in 2014

**\$2.8T**

GDP increase from data flows, larger impact than goods trade

**~50%**

Potential GDP boost for some countries by increasing participation in global flows

# Globalization: Then vs. now

## 20TH CENTURY

## 21ST CENTURY



**Tangible flows of physical goods**

**Intangible flows of data and information**



**Flows mainly between advanced economies**

**Greater participation by emerging economies**



**Capital- and labor-intensive flows**

**More knowledge-intensive flows**



**Transportation infrastructure is critical for flows**

**Digital infrastructure becomes equally important**



**Multinational companies drive flows**

**Growing role of small enterprises and individuals**



**Flows mainly of monetized transactions**

**More exchanges of free content and services**



**Ideas diffuse slowly across borders**

**Instant global access to information**



**Innovation flows from advanced to emerging economies**

**Innovation flows in both directions**





# Wide variety of benefits derived from data (anonymized, pseudonymized, or personal)

**For Social Good**

**To increase services  
efficiency**

**To face world  
challenges**

**To improve  
government services  
and goals**

Environmental  
protection



Pandemic disease  
information

Crime prevention



Intelligent Transport  
Systems



Pre-positioning  
Emergency Services



Smart Cities



Smart Agriculture

Healthcare



Eurostat is exploring  
ways to exploit Big  
Data for statistics

# Data Economy grows in the context of the Digital Challenge

## The Challenge

**Digital Economy is Economy itself**

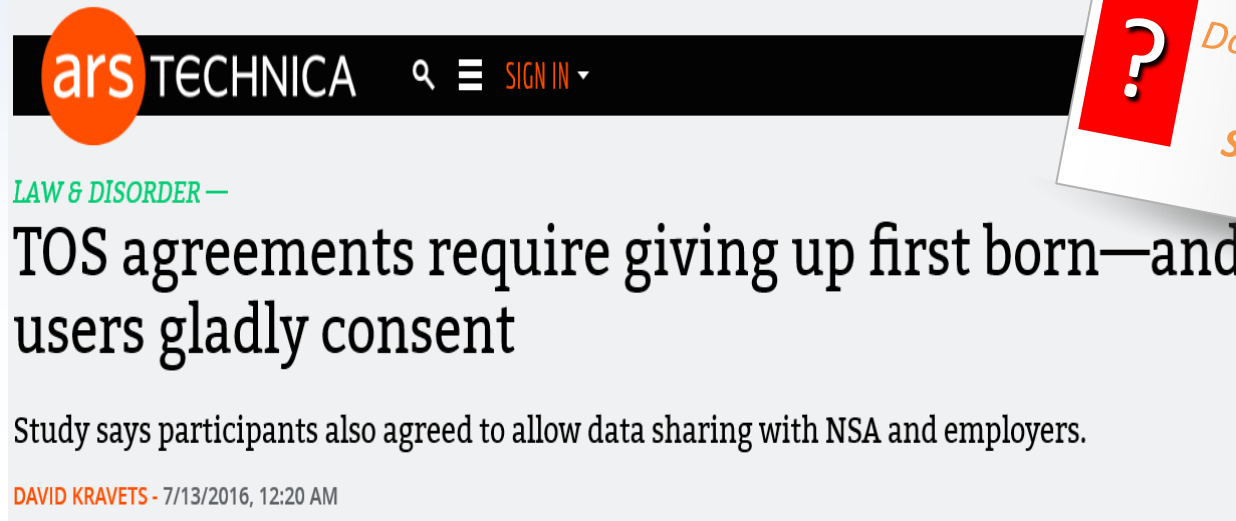
**Digital Life is Life itself**

**The rules of the game?**



**Our  
Digital  
Footprint**

# Associated problems in Transparency ...

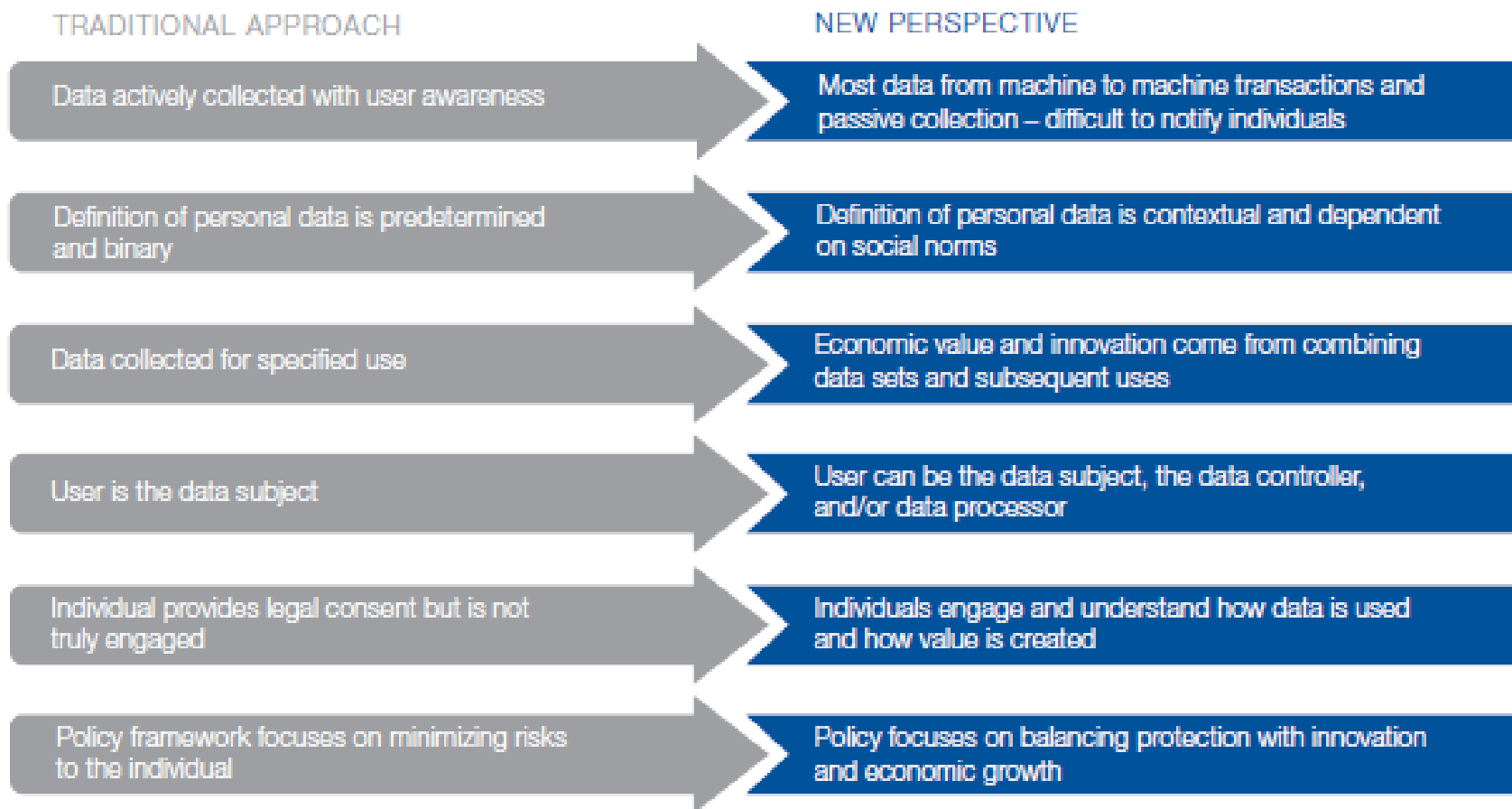


(1) 543 University students involved in the study.

(2) For readers, average TOS reading time was 51 seconds. The average adult reading speed is 250-280 words per minute (TOS should have taken 16 minutes).

# The new data-driven world challenges privacy laws, policy and implementation

Figure 2: New perspectives on the use of data



Source: World Economic Forum and The Boston Consulting Group

# New privacy framework for the trusted digital age

- Privacy Management Program
- BCR, CBPR
- Certifications / Seals
- Codes of Conduct
- Standards

**Corporate  
Digital  
Responsibility  
Accountability  
Frameworks**

**Risk  
management**

- Risks and harms to individuals
- Benefits to individuals, organisations, society

**Evolved  
interpretation  
of privacy  
principles**

**Empowering  
individuals  
beyond  
consent**

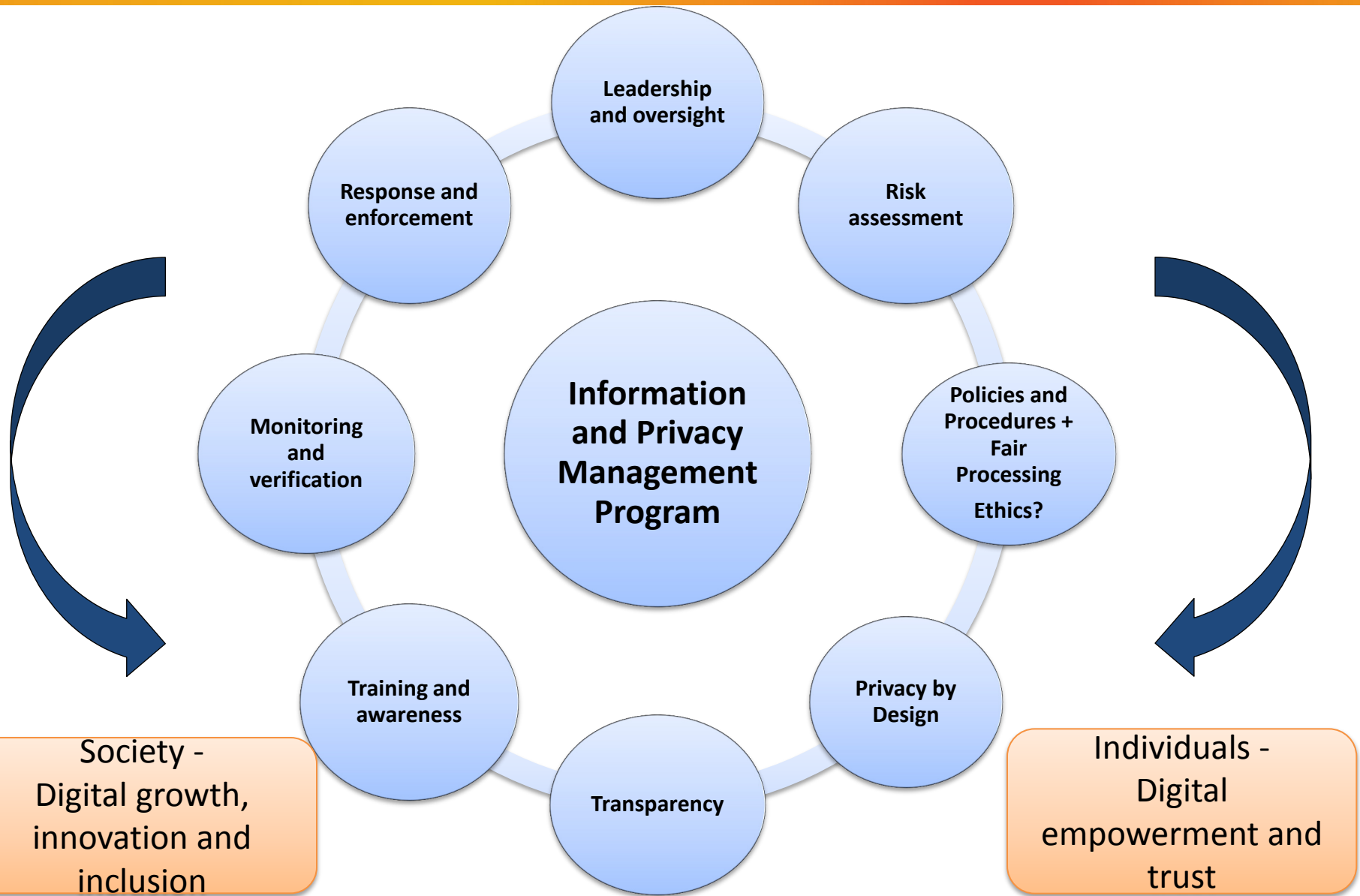
- Legitimate interest processing
- Fair processing
- Risks and harms to individuals
- New transparency

- User centric transparency
- Rights – access, correction, objection, erasure
- Complaints and redress

Smart regulation – prioritized and risk-based interpretation, oversight and enforcement by resourceful DPAs, engaging and incentivising organizations to deliver best outcomes



# Evolving Privacy Compliance into Corporate Digital Responsibility



## Session 1

# How does Japan's Amended Privacy Law Enable Cross-Border Data Flows, the Data Driven Economy, Innovation and Protection of Personal Data

### Moderator:

❖ Manuel Maisog, Partner, Hunton & Williams

### Discussion Leads:

❖ Kuniko Ogawa, Counselor, Japan Personal Information Protection Commission

❖ Kaori Ishii, Associate Professor at the Faculty of Library, Information and Media Science, University of Tsukuba

❖ Naoya Bessho, General Counsel, Yahoo! Japan

❖ Naoko Mizukoshi, Attorney-at-Law, Endeavor Law Office



# The Amended Act on the Protection of Personal Information (APPI)

Kuniko Ogawa

Counselor

Personal Information Protection Commission (PPC)

May 11 , 2017

## The Amended APPI : Changes and Challenges

1

The Act on the Protection of Personal Information was enacted in 2003  
(Fully enforced in 2005)

Changes of circumstances

As Information and Communications Technologies (ICTs) advanced, the utility of personal information became intensified and diversified beyond expectation

### 1. Enlargement of “gray areas” of personal information

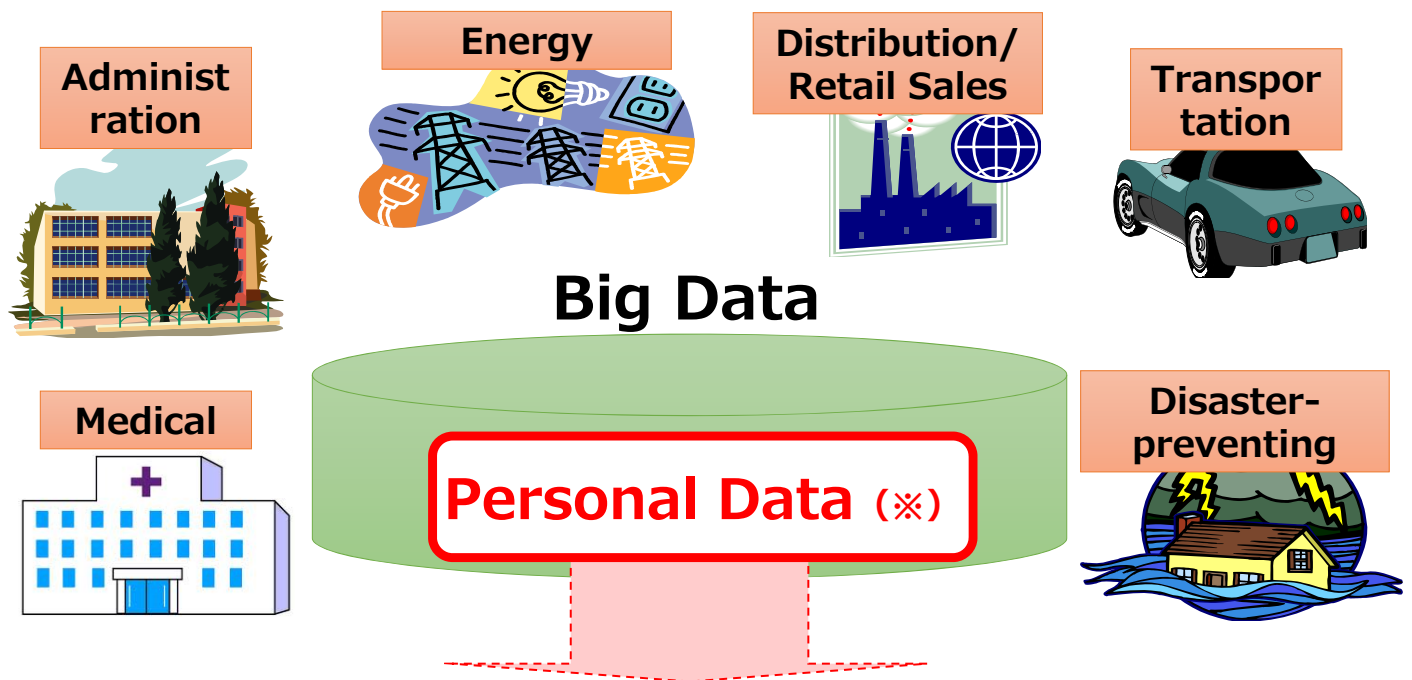
So called “gray area” was enlarged, in which judgment of personal information was difficult

### 2. Correspondence for Big Data

To realize circumstances for appropriate usage of Big Data including personal data is necessary

### 3. Responses to Globalization

As business operations are globalized, massive data flow goes beyond national border



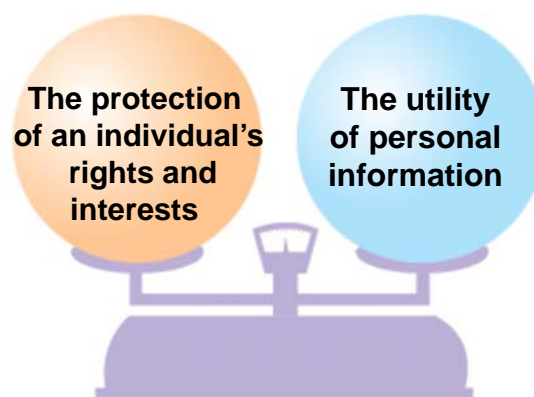
**To realize circumstances for appropriate usage of Big Data including personal data is necessary**

※ Personal data has a great deal of potential in utility of Big Data

## Purpose of The Act on the Protection of Personal Information (APPI)

3

- The APPI aims to seek the balance between **the protection of an individual's rights and interests** and **the utility of personal information**.
- Besides the overall vision for the proper handling of personal information, this Act establishes obligations, etc. that a **personal information handling business operator** shall fulfil.



### (Purpose of the Act)

Article 1 This Act **aims to protect an individual's rights and interests while considering the utility of personal information** including that the proper and effective application of personal information contributes to the creation of new industries and the realization of a vibrant economic society and an enriched quality of life for the people of Japan; by setting forth the overall vision for the proper handling of personal information, creating a governmental basic policy with regard to this, and establishing other matters to serve as a basis for measures to protect personal information, as well as by clarifying the responsibilities etc. of the central and local governments and establishing obligations etc. that a personal information handling business operator shall fulfill, in light of the significantly expanded utilization of personal information as our advanced information- and communication-based society evolves.

○The Act on the Protection of Personal Information was amended in September 2015 (To be fully enforced in May 30, 2017.)

## The outline of the amendment

### 1. Establishment of the PPC

- Aggregation of the supervising authorities to the PPC, which are currently held by the relevant regulatory ministers toward personal information handling business operators under their respective supervision.

### 2. Clarifying the definition of personal information

- (1) Clarifying the definition of personal information by stating partial bodily features etc. of a specific individual as personal information to cope with gray areas of personal information (individual identification codes)
- (2) A principal's advance consent shall be obtained in principle in cases of acquiring or providing to a third party special care-required personal information (i.e., race, creed, medical record).

### 3. Establishment of a legal framework to enhance active use of personal information

Establishment of regulations concerning "anonymously processed information" (meaning information that has been produced by processing personal information in a way to make a specific individual unidentifiable and hence disallowing reconstruction of the personal information).

### 4. Responses to globalization

- (1) Introduction of a new legal provision for transferring personal data to a foreign third party
- (2) Introduction of a new legal provision for extraterritorial application, and sharing information with the foreign enforcement authorities

### 5. Measures to Respond to a so-called "Name List Trader"

- (1) Imposing new obligations to keep and confirm a record relating to a third-party personal data provision.
- (2) An act of providing a third party with or stealing personal information database etc. for the purpose of earning illicit gains has become subject to criminal punishment as "the offense of providing personal information database".

### 6. Others

- (1) Abolition of a system wherein a business operator handling personal information of 5,000 individuals or less may be excluded from the regulated subjects.
- (2) A personal information handling business operator utilizing an opt-out procedure has become obligated to notify the Personal Information Protection Commission of certain legally required items.

## What is the PPC?

### History

- Jan 2014 The Specific Personal Information Protection Commission (SPPC) was established
- Jan 2016 The Personal Information Protection Commission was established (into which the SPPC was merged)

### Function under the Jurisdiction

- (1) Affairs related to specific personal information  
(monitoring/supervision, specific personal information protection assessment)
- (2) Affairs related to the APPI (Holding jurisdiction over the APPI)  
(Affairs related to monitoring/supervision based on the Amended APPI is to be added after its full enforcement.)
- (3) Affairs common to (1) and (2)  
(public relations/an enlightenment campaign, international cooperation etc.)

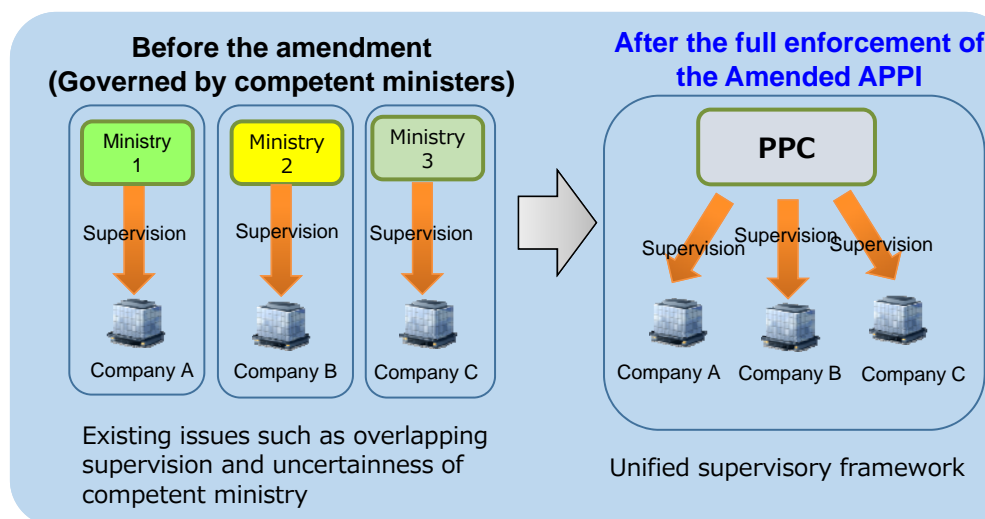
### Organizational Structure

- A collegial decision-making body comprising one chairperson and eight commissioners (Administrative commission)
- The chairperson and eight commissioners exercise their official authorities independently (with terms of five years)
- The number of professional staff of the PPC secretariat : 116 (as of 1 April, 2017)



- Centralization of regulatory authorities currently hold by respective business jurisdictional ministers to the PPC at the time of full enforcement of the Amended APPI
- Authorized to require a business operator to report or conduct on-site inspection as necessary, and in addition, to provide with guidance or advice, or to recommend or order in accordance with actual circumstances

## Supervisory framework of private business operators



## Supervisory framework of public organizations\*

- The Act on the Protection of Personal Information Held by Administrative Organs (for national administrative organizations)
- The Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, etc. (for Incorporated Administrative Agencies, etc.)
- Local government ordinance related to protection of personal information (for local government etc.)

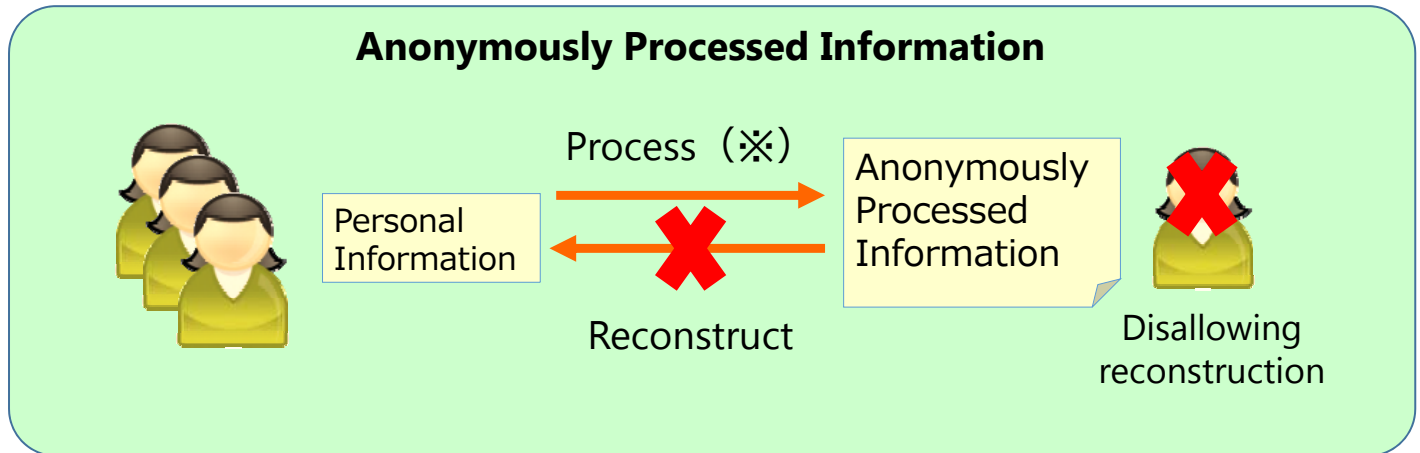
\*No change on the supervisory framework of public organizations responding to the amendment of the APPI

# Preparation for Enforcement of the Amended APPI

- The PPC has established rules as follows since January 2016.
- A total of 16 public consultations held and 2,589 comments received.
- ✓ **Cabinet order, and Commission rules to enforce the APPI (October 5, 2016)**
- ✓ **Basic policy on the Protection of Personal Information (adopted by the Cabinet on October 28, 2016)**
- ✓ **Guidelines concerning the APPI (Commission Guidelines) (November 30, 2016)**
  - Volume on general rules
  - Volume on provision to a third party in a foreign country
  - Volume on confirmation and record-keeping obligation at the time of third party provision
  - Volume on anonymously processed information
- ✓ **Action should be taken in cases where personal data breach etc. occurs (February 16, 2017)**
- ✓ **Q&A for “Guidelines concerning the APPI” and “Action should be taken in cases where personal data breach etc. occurs” (February 16, 2017)**
- ✓ **The PPC Secretariat Report on Anonymously Processed Information (February 27, 2017)**
- ✓ **Guideline to accredit accredited personal information protection organization (April 21, 2017)**
- ✓ **Public relations and enlightenment campaigns toward full enforcement of the Amended APPI**



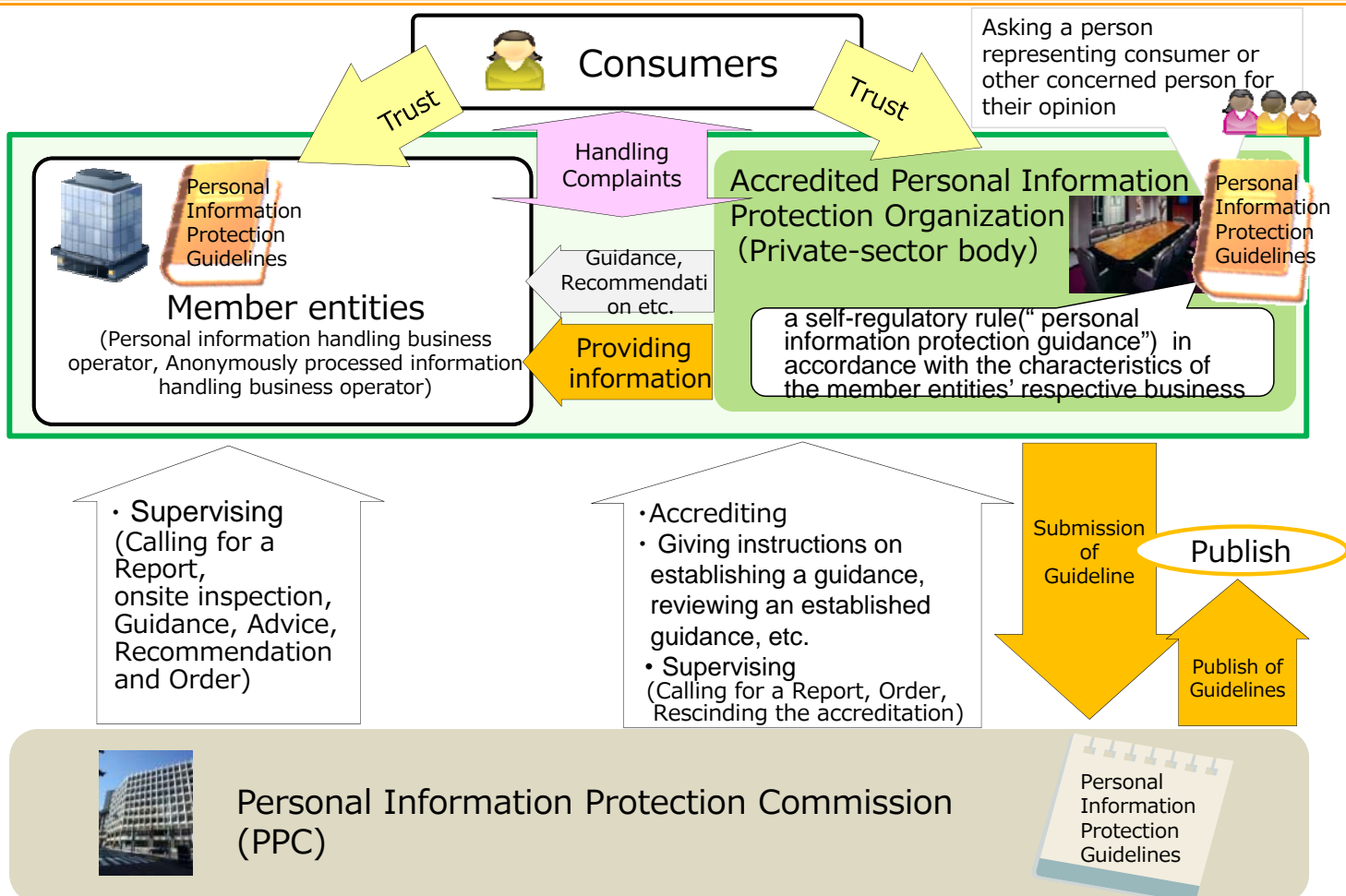
Establishment of regulations concerning **"anonymously processed information"** (meaning information that has been produced by **processing personal information in a way to make a specific individual unidentifiable** and hence **disallowing reconstruction of the personal information**), and enhance smooth circulation and utility under relaxed regulation compared with ordinarily personal information



■ **Standards in the methods of producing anonymously processed information** (PPC Rules)

- ① Deleting a whole or part of those descriptions etc. which can identify a specific individual contained in personal information (e.g. name) (including replacing, same as below)
- ② Deleting all individual identification codes contained in personal information (e.g. my number, drivers license number)
- ③ Deleting those code which link personal information and information obtained by having taken measures against the personal information
- ④ Deleting idiosyncratic descriptions etc. (e.g. age 116)
- ⑤ Besides action set forth in each preceding item, taking appropriate action based on results from considering the attribute etc. of personal information database etc. such as a difference between descriptions etc. contained in personal information database etc.

## Accredited Personal Information Protection Organization



## ➤Introducing provisions concerning globalization in the APPI

### 1 . Provision for extraterritorial application

- ✓ The APPI applies to a personal information handling business operator in a foreign country who in relation to supplying a good or service to a person in Japan has acquired personal information relating to the person (Article 75)

### 2 . Provision concerning as-needed information sharing with the foreign enforcement authorities

- ✓ In cases where a foreign business operator mishandles personal information of a citizen domiciled in Japan, the PPC may provide necessary information to the foreign enforcement authorities so as to have appropriate enforcement action taken by the foreign authorities based on their respective applicable laws and regulations.
- ✓ The PPC has joined GPEN (Global Privacy Enforcement Network)
- ✓ The PPC is institutionalizing a system aimed at sharing information with the foreign enforcement authorities

4

# Responses to Globalization②

## 3 . Personal data provision to a foreign third party

In any of the following cases, personal data may be provided to a third party in a foreign country in the same way as in-country (Article 24 of the Amended APPI);

- (1) Cases in which a third party is located in a foreign country or region designated by the PPC rules;
- (2) Cases in which a third party in a foreign country has established and maintained a system that conforms to **the standards prescribed by the PPC rules**;

“The standards prescribed by the PPC rules”

- ◆ The implementation of **action in line with the purport of the APPI** has been ensured by using **an appropriate and reasonable method** in relation to handling personal data by a person who receives the provision of the personal data
  - Examples of “**an appropriate and reasonable method**”:  
exchanging an outsourcing contract; establishing bylaws or privacy policy within a group of companies; and a personal data provider having obtained the APEC Cross- Border Privacy Rules (CBPR) certification, etc.
  - Examples of “**actions in line with the purport of the APPI**” :  
those following such standards set by international frameworks as the ones adopted by the OECD and the APEC.
- ◆ A third party in a foreign country who receives personal data has obtained a certification based on an international framework concerning the handling of personal information
  - The APEC CBPR system, under which a third-party transferee in a foreign country has been certified.

- (3) Cases in which there is a principal's consent to the provision to a third party in a foreign country.

5



## ○ Efforts by the PPC

- ① Officially joining the following international enforcement cooperation frameworks since its establishment:
  - GPEN (Global Privacy Enforcement Network)
  - APPA (Asia Pacific Privacy Authorities )
- ② Establishing an environment for smooth cross-border data transfer while protecting personal information
- ③ Actively working on issues such as establishing cooperative relationship with foreign enforcement authorities



- Having decided the International Initiatives on 29 July for ensuring smooth transfer of personal data

### “New Initiatives for Ensuring Smooth Cross-Border Personal Data Flows” (Personal Information Protection Commission Decision on July 29, 2016) (excerpt)

The Commission will for the moment, while advocating further cooperation with foreign counterparts to boost smooth cross-border transfer of personal information ensuring the protection thereof, facilitate coordination directed toward setting up a bilateral meeting on a regular basis with its counterparts in the United States and the European Union (the Brexit's effects will need to keep watching) with both of whom the Commission has held certain dialogues hitherto, with putting into perspective the possibilities of establishing a framework to enhance reciprocal and smooth data transfer.

### The United States

With sharing recognition regarding the importance of collaborating closely and holding a regular meeting continuously, a consensus has been achieved on cooperatively practicing public relations for the APEC Cross Border Privacy Rules (CBPR) system and undertaking promotional activities to encourage the APEC member economies to participate therein together with the respective countries' stakeholders.

### The European Union

Commissioner of the Personal Information Protection Commission (PPC) and Commissioner of the European Commission (EC) recognized on March 20 2017 progress that has been made regarding dialogues held hitherto between the PPC and the Directorate-General for Justice and Consumers of the EC, and agreed to further deepen such dialogues hereafter.

## ➤ Dialogues with the US

- Minister-Counselors of the US Embassy in Japan on August 8, 2016
- Senior staffer of the US Department of Commerce on September 5, 2016
- Senior staffer of the US Department of Commerce on October 19, 2016
- Senior staffer of the US Department of Commerce on February 23, 2017

## ➤ Dialogues with foreign data protection authorities etc.

- CNIL in France on January 31, 2017
- Dutch Data Protection Authority on February 2, 2017
- ICO of the UK on February 3, 2017
- PDPC of Singapore on February 3, 2017
- GIODO in Poland on March 7, 2017
- BfDI in Germany on March 8, 2017
- PCC of Canada on April 6, 2017
- ICO and DCMS on April 11, 2017

## ➤ Dialogues etc. with the EU

- Cooperative dialogues held with the European Commission (EC)'s Directorate-General for Justice
  - On April 22, 2016
  - On September 28, 2016
  - On October 20, 2016
- On November 30 and 1 December, 2016 The EU-Japan ICT dialogue etc.
- On January 18, 2017 Cooperative dialogue with the EC's Director-General for Justice
- On March 13, 2017 Seminar co-hosted by the PPC and the EC's Directorate-General for Justice
- On March 20, 2017 Cooperative dialogue with the European Commissioner for Justice, Consumers and Gender

## ➤ Dialogues with foreign embassies in Japan

- Embassy of the Federal Republic of Germany on February 17, 2017
- Delegation of the European Union to Japan on February 22, 2017
- British Embassy on February 24, 2017
- British Embassy on April 19, 2017

## APEC Cross Border Privacy Rules (CBPR) system

**Promotion of APEC CBPR System**

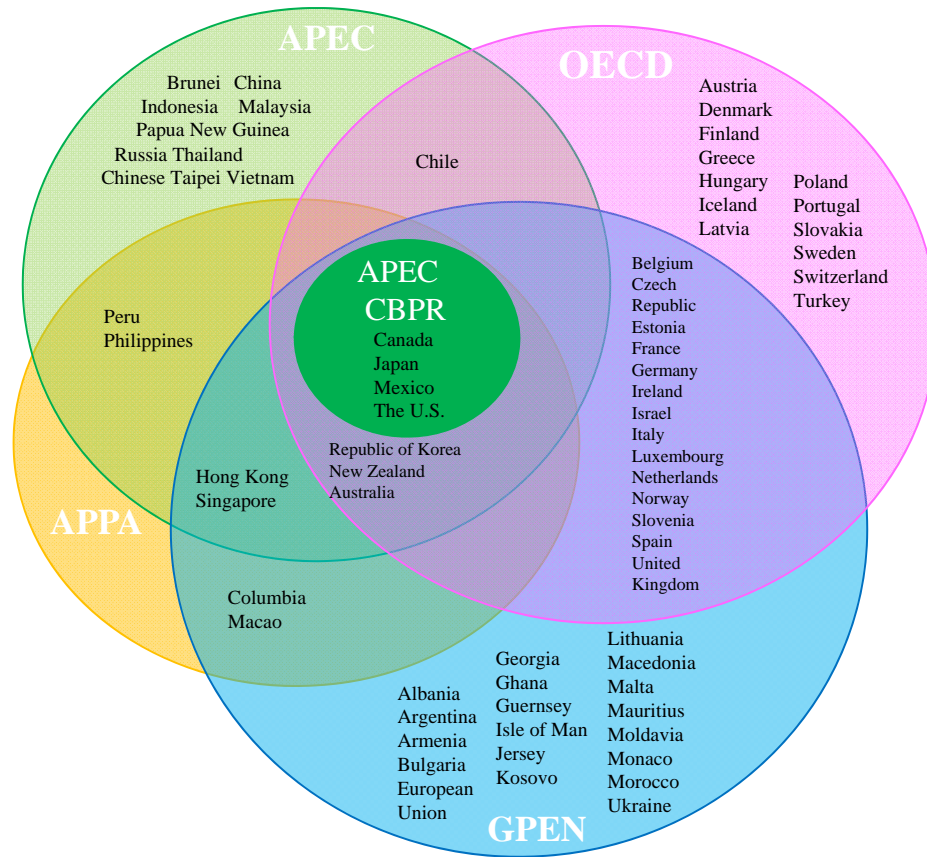
- The CBPR system is a mechanism to certify a business operator's compliance with the APEC Privacy Framework in the APEC member economies and an effective instrument to judge the business operator's level of personal information protection by international standards.
- Guidelines issued based on the Amended APPI stipulate the obtainment of a CBPR certification as an example of conditions to be satisfied when receiving the provision of personal data to a third party in a foreign country.
- As the JIPDEC has been approved as a Japan's first certification body under the APEC CBPR system (i.e., accountability agent), Japan has been advancing efforts to infiltrate and promote the CBPR system in the APEC region.

(Note) JIPDEC certified an organization under the CBPR system for the first time

**(Reference) APEC Cross Border Privacy Rules (CBPR) system**

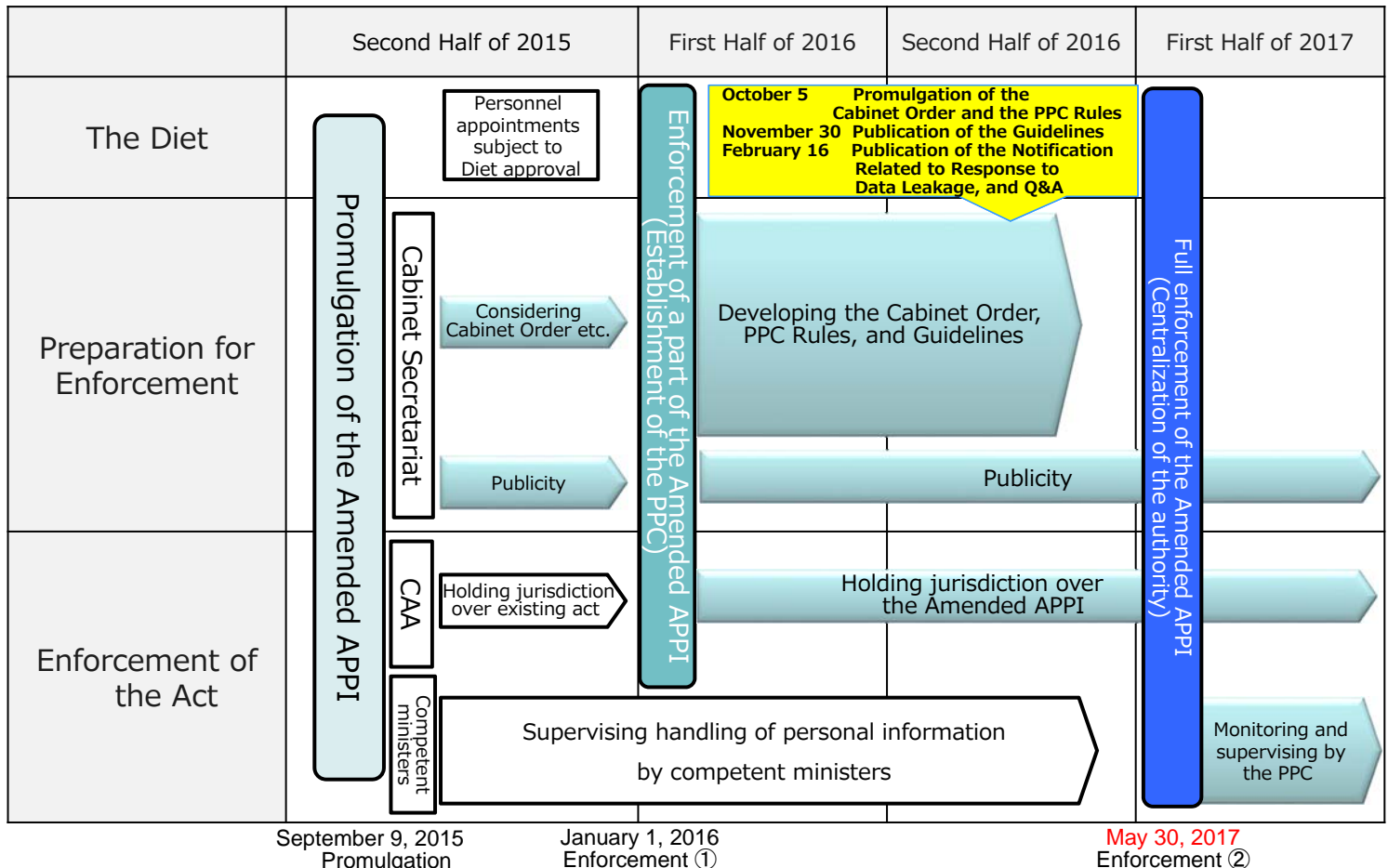
APEC Cross-Border Privacy Rules (CBPR) System is an international mechanism to certify a business operators' compatibility with the APEC Privacy Framework. To participate in the CBPR system, an economy must first satisfy the necessary conditions. The Economy then nominates one or more Accountability Agent (AA) for APEC recognition. Once at least one AA has been recognized in relation to that Economy, organizations will be able to commence participation in the CBPR system in the Economy. Applicant organizations may only participate in the CBPR system if their policies and practices are certified by the relevant AA to be compliant with the requirements of the APEC Privacy Framework.

## Joining the international cooperative frameworks



【As of Nov 2016】

## Schedule





Thank you !

Kuniko Ogawa

[ogawa-k5pw@ppc.go.jp](mailto:ogawa-k5pw@ppc.go.jp)



# Kaori Ishii

Associate Professor in the Faculty of Library,  
Information and Media Science,

University of Tsukuba

# The concept of the amendment

- Fundamental concept has not changed.
- The important role of the Personal Information Protection Commission (PPC)
- Regulation and guidelines published by the PPC
  - The scope of personal information, the interpretation of the consent, anonymously processed information, data breach, and the conditions for disclosing personal data to a third party, etc.
- Trans-border data flow
  - Expansion of the application to foreign entities, enforcement cooperation, and certain restrictions on the trans-border flow of personal data
- Flexibility of the PPC's guidelines
  - Implicit and explicit consent
  - Emphasis on the APEC-CBPR System

# Interpretation and Development

- Interpretation
  - The need to broaden usages of personal information for the benefits of Big Data, Internet of Things, and cloud computing services
  - “Reasonable expectation of privacy” standard
- Challenges of the scope of protection
  - Anonymously processed information
- Machine learning
  - Unpredictable society
  - The issues on profiling, discriminatory decisions, lack of transparency, and impeding consent
  - Need for a broader perspective



# Responsibilities of Accountable Organizations

- JIPDEC
  - Privacy Mark System based on the Japanese Industrial Standards for personal information management systems
  - Enhancing public awareness
  - Accredited personal information protection organization in 2005
  - Accountability Agent of the CBPR in 2016
- Obligation to instruct, recommend, and take other measures
  - Handling complaints
  - Sharing information with the PPC
- Appropriate education for a better understanding of the law



# Role of regulators

- Domestic viewpoint
  - Backstop regulator
  - Looking at the substance of accredited organizations
  - Active enforcement activities
- International viewpoint
  - Enhancing the APEC-CBPR
    - Acknowledging the differences among countries
  - EU-GDPR
    - Coherent and detailed regulation
    - Subject to the assessment by the European Commission when seeking for the adequacy decision
    - Affects on third countries



Centre for  
Information  
Policy  
Leadership  
Hunton & Williams LLP

ヤフー株式会社 執行役員  
(インテリジェンス管掌)  
別所 直哉

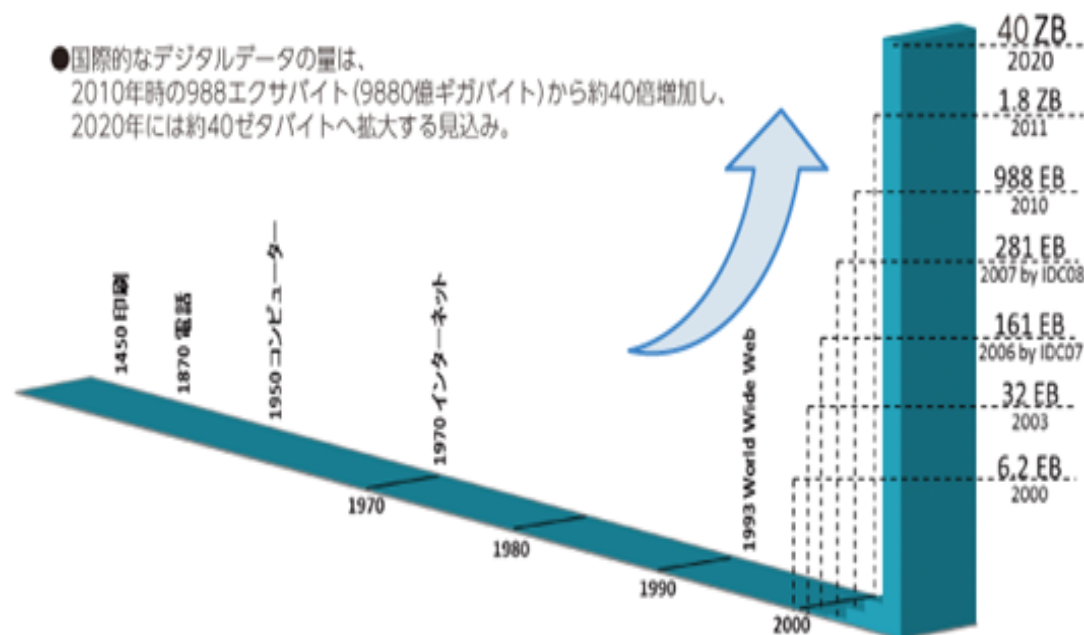
# 改正個人情報保護法と企業の取組み

---

ヤフー株式会社 執行役員  
(インテリジェンス管掌)  
別所 直哉

# これからの経済成長を支えるのは「データ」

- データは成長の源泉
- 増大するデータを利活用していくことが重要



(出典：平成26年情報通信白書)

## 改正個人情報保護法の目的

### 第1条（目的）

この法律は、高度情報通信社会の進展に伴い個人情報の利用が著しく拡大していることに鑑み、個人情報の適正な取扱いに関し、基本理念及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め、国及び地方公共団体の責務等を明らかにするとともに、個人情報を取り扱う事業者の遵守すべき義務等を定めることにより、個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする。

## 改正法への期待

- 「個人情報保護委員会」の機能に期待
  - 分野横断での統一的な取り扱い
  - 実務に配慮されたガイドラインの策定
  - 国際的な枠組みの積極的提唱
- 「匿名加工情報」の活用

## データ利活用上の企業の懸念

- 法律ではなく、一般の人々の不安によってデータ利用が進まないことが懸念
- データ漏洩で実質的な損害が発生していなくても、裁判所が認める損害賠償額が莫大（1件5,000円）



## (参考)札幌市の事例

- 札幌市が、札幌駅前の地下歩行空間で、サイネージエリアにセンサーを設置して「サイネージの閲覧人数・年代・性別」を計測する実証実験を実施（2017年2月）
  - 市民から不安視する声が多く寄せられ、中止に
- ※ 実験では、センサーに入る3メートル以内に線を引き、趣旨を説明する看板を立てていた

## プライバシーポリシー改定

- 2016年6月、Yahoo! JAPANは

→ プライバシーポリシーを改定

1. プライバシー情報の取扱いを契約条件に組み入れ
2. 利用者視点でシンプルに読みやすく
3. 詳しい説明をガイドとして表示

# プライバシーポリシー（新・旧）

## before

### 履歴情報および特性情報の取得

- お客様がYahoo!JAPANID（以下本章で「ID」といいます）を登録される際に郵便番号や性別、職業などをお尋ねします。
- また、当社は、ご利用の内容（お客様が利用されたサービス、購入された商品、ご覧になったページや広告の履歴、お客様が検索された検索キーワード、お客様がサービスと電子機器を接続し、お客様が当該電子機器を操作すること等を通じてやりとりされる情報等を含みます）、ご利用日時、ご利用の方法、ご利用環境（携帯端末を通じてご利用の場合の当該端末の通信状態、ご利用に際しての各種設定情報なども含みます）、お客様のIPアドレス、クッキー情報、位置情報、端末の個体識別情報、病気予防のためのエビデンス（根拠）情報の収集、獲得、創出のためのプロジェクトおよびその一環としてなされるゲノム解析サービスに申し込まれたお客様から提供いただいた試料を検査し、解析した結果得られるお客様の遺伝子に関する情報等（以下「遺伝子情報」といいます）などの情報を、お客様が当社や当社の提携先（情報提供元、広告主、広告配信先などを含みます。以下「提携先」といいます）のサービスをご利用になる際に取得します。
- また、当社は、カルチュア・コンビニエンス・クラブ株式会社から、株式会社Tポイント・ジャパンが発行するTポイント（以下「Tポイント」といいます）の付与を受けるための所定の手続きを行われたお客様の、購入された商品、ご利用になったキャンペーンやサービスの履歴（Tポイントをご利用になった履歴を含みます）に関する情報やカルチュア・コンビニエンス・クラブ株式会社が独自の基準で分類したお客様の興味関心分野や推定したお客様の属性に関するデータ（以下「顧客傾向データ」といいます）の提供を受けます。
- また、当社は、一定の場合を除いて、お客様がYahoo!メールにて閲覧されるメールを機械的に解析し、当該解析の結果を取得して広告の表示に利用します。

### 個人情報の取得

- お客様がIDを登録される際にメールアドレス、生年月日などをお尋ねします。
- また、ご利用いただく方を特定する必要がある場合や当社にお問い合わせをいただいた際に連絡先を確認させていただく必要がある場合に、氏名、生年月日、住所、電話番号、銀行口座番号、クレジットカード番号、運転免許証番号などの個人情報をお尋ねすることがあります。
- また、お客様と提携先などとの間でなされたお客様の個人情報を含む取引記録や、決済に関する情報を当該提携先などから取得することがあります。
- 当社が取得した個人情報は、当社のサービスまたは当社を経由してご利用いただくサービスを提供するために必要なものに限られています。

## after

### パーソナルデータの取得

当社は、以下の場合にパーソナルデータを取得させていただきます。

- (1) 端末操作を通じてお客様にご入力いただく場合
- (2) お客様から直接または書面等の媒体を通じてご提供いただく場合
- (3) お客様によるサービス、商品、広告、コンテンツの利用・閲覧に伴って自動的に送信される場合
- (4) 上記の他、お客様の同意を得た第三者から提供を受ける場合など、適法に取得する場合

# プライバシーポリシー（新・旧）

## before

## after

### ■ 履歴情報および特性情報の利用目的

- (1) ログインが必要なサービスで、同じお客様からのアクセスがどうかを確認する場合
- (2) お客様のセキュリティを確保するため、一応の時間が経過したお客様に対してIDやパスワードの入力力を促す場合
- (3) Yahoo!ショッピングなどにおいて、お客様のショッピングカートにある商品を追憶できるようにする場合
- (4) 当社や当社から広告を配信している提携先サービスの利用履歴や当社や提携先サービスへの訪問数を照会する場合
- (5) 当社や提携先が製造したコンテンツ、広告、各種サービスのご案内などをお客様に配信したり提供したりする場合
- (6) 場合当社や提携先が提供しているサービスや広告の内容を、充実させたり、改善したり、あるいは新しいサービスを検討したりするための分析・抽出等を行う
- (7) お客様がサービスをご利用になる際の環境の改善に向けた基礎資料とするために、携帯端末の通信状態等の情報を分析した結果を公表する場合
- (8) 提携先に、どのような広告や情報、サービスなどを掲載または提供していただくことが効果的であるかなどを分析して提供する場合
- (9) Tポイントの付与を受けるための所定の手続きを行われたお客様の、ご覧になったページや広告の履歴に関する情報、当社が独自の基準で分類したお客様の興味関心分野に関する情報をカルチュア・コンビニエンス・クラブ株式会社へ提供する場合、カルチュア・コンビニエンス・クラブ株式会社は、当該提供される情報を特定の個人を識別可能な情報と別に区分して管理・運用し、顧客傾向データを充実、改善するための資料として利用します。また、同社は、当該提供される情報を利用して、充実、改善された顧客傾向データを、同社が定めるT会員規約およびその他の規約に従って、郵便や電子メール等による方法での各種情報のご案内その他の目的で利用したり、お客様がご覧になった広告の履歴に関する情報を、どのような広告を掲載することが効果的であるかなどを分析し、また分析結果を当社や当社の提携先である広告主に提供したりするために利用します。なお、本号に基づくカルチュア・コンビニエンス・クラブ株式会社への情報の提供を希望されないお客様は、下記リンクからカルチュア・コンビニエンス・クラブ株式会社への情報の提供を中止することができます。
- (10) 当社、カルチュア・コンビニエンス・クラブ株式会社または株式会社Tポイント・ジャパンが共同で実施するキャンペーンを運営、実施、改善するために、Tポイントの付与を受けるための所定の手続きを行われたお客様の、当該キャンペーンをご利用になった履歴に関する情報をカルチュア・コンビニエンス・クラブ株式会社に対して提供する場合
- (11) 通信事業者、通信環境の改善のための参考資料として、携帯端末の通信状態等の情報を提供する場合
- (12) 研究開発等を行う同会社や研究機関等に、インターネットの利用状況照会の基礎資料として、お客様がご覧になったページの履歴に関する情報を分析して提供する場合
- (13) 当社が提供しているサービスの充実や改善、新しいサービスの検討、インターネット環境の改善等を目的として外部の研究機関（大学、研究所）を委嘱するがこれらに限りません）と共同研究を行うために、当該研究機関に提供する場合
- (14) 通信手帳、生年月日その他の関連する情報を、国や研究文の他の研究目的で利用することを希望する研究機関に提供する場合
- (15) お客様からのお問い合わせに対応するために、お客様のサービスご利用状況を確認する場合

### ■ 個人情報の利用目的

- (1) お客様にご自分の履歴情報の閲覧や修正、ご利用状況の閲覧を行っていただくために、氏名、住所、連絡先、支払方法などの履歴情報、利用されたサービスや購入された商品およびそれらの代金などに関する情報を表示する場合
- (2) お客様にお知らせや連絡（当社や提携先の提供するサービスや商品のご案内を含みます）をしたり、商品や商品を送付したりするため、氏名や住所、メールアドレスなどの連絡先情報を利用する場合
- (3) 当社や提携先が提供しているサービスや広告の内容を充実させたり、改善したり、あるいは新しいサービスを検討したりするためにお客様の情報を利用する場合
- (4) お客様の本人確認を行うために、氏名、生年月日、住所、電話番号、銀行口座番号、クレジットカード番号、運転免許証番号、配達記録付郵便物の配達結果などの情報を利用する場合
- (5) お客様に代金を請求するために、購入された商品名や数量、利用されたサービスの履歴や期間、回数、請求金額、氏名、住所、銀行口座番号やクレジットカード番号などの支払に関する情報などを利用する場合

### パーソナルデータの利用目的

当社は、以下のことを行うためパーソナルデータを利用させていただきます。

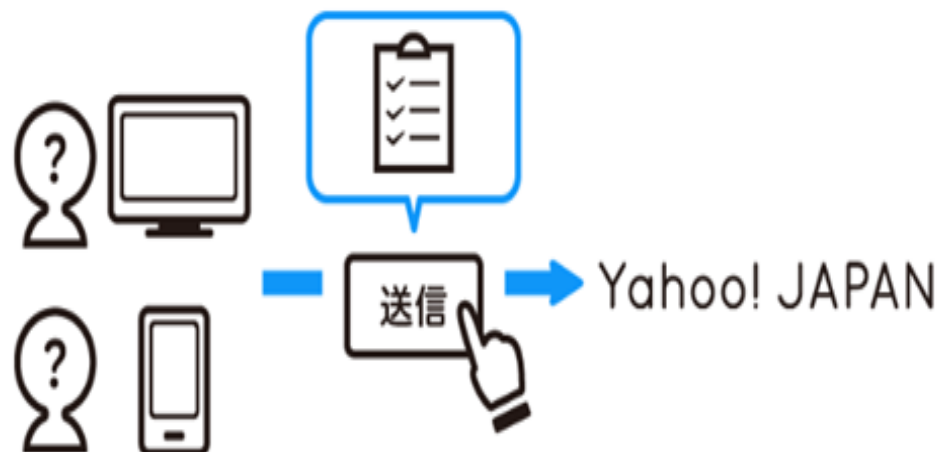
- (1) お客様に適したサービス等をご提供するため
- (2) お客様からのお問い合わせに対応するため
- (3) 商品の配送、代金請求、ポイント付与等をするため
- (4) お客様にサービス等に関するお知らせをするため
- (5) サービス等を安全にご提供するため。これには、利用規約に違反しているお客様を発見して当該お客様に通知をしたり、サービス等を悪用した詐欺や不正アクセスなどの不正行為を調査・検出・予防したり、これらに対応することが含まれます
- (6) サービス等の改善および新たなサービス等を検討するため
- (7) サービス等のご利用状況等を調査、分析するため

# プライバシーガイド

## パーソナルデータを取得する場合

### 端末操作を通じてお客様にご入力いただく場合

Yahoo! JAPAN IDをご取得いただく際に、登録情報を入力し、送信していただく場合が代表的な例です。このほか、[アンケート調査](#)にご協力いただく場合など、お客様がお使いの端末を操作して情報を入力し、「送信」や「登録」ボタンをクリックまたはタップするなどして入力情報がYahoo! JAPANに送信されるような場合に、Yahoo! JAPANは情報を取得させていただきます。





# プライバシーガイド

## パーソナルデータの活用例について

### パーソナライズ

個々のお客様に最適なコンテンツをはじめとするサービス等を提供する場合（おすすめの商品やサービス等を表示したり、ご案内したりする場合を含みます）に、お客様の居住地、性別、生年月などの情報や、お客様のサービス等のご利用履歴（検索キーワード、閲覧されたウェブページ、ご利用になったアプリ、購入された商品など）を分析して、Yahoo! JAPAN独自の基準で推定したお客様の興味関心に関する情報を利用させていただきます。たとえば、Yahoo!ニュースでは過去に閲覧したニュース記事等を分析して関心が高いと推定される記事を表示し、Yahoo!ショッピングでは商品の閲覧履歴や購買履歴等を分析しておすすめ商品情報を表示します。



Yahoo! JAPAN

## データ利活用において重要なこと

- 利用者がコンテキストを理解できること
- 利用者の理解（期待）を裏切らないこと

→ 利用者の信頼の下でのデータ利活用を



## Session 2

# Cross-Border Data Flows and the APEC Cross-Border Privacy Rules System

### Moderator:

❖ Jacobo Esquenazi, Global Privacy Strategist, HP, Inc.

### Discussion Leads:

❖ Shinji Kakuno, Director, International Affairs Office, Japan Ministry of Economy, Trade and Industry (METI)

❖ Tsuzuri Sakamaki, Counselor, Japan Personal Information Protection Commission

❖ Yoichi Iida, Director for International Research and Policy Coordination, Global Strategy Bureau, Japan Ministry of Internal Affairs and Communications (MIC)

❖ Suhee Kim, Deputy Director, Personal Information Protection Policy, Ministry of the Interior, Korea

❖ Masataka Saito, Director, Accredited Personal Information Protection Organization Office, JIPDEC

❖ Josh Harris, Director of International Regulatory Affairs, TRUSTe

❖ Jane Horvath, Senior Director of Global Privacy, Apple

❖ Keith Enright, Director, Global Privacy Legal, Google

# **The Importance of Promoting APEC/Cross-border Privacy Rules System**

May 11th

Shinji Kakuno

International Affairs Office

Ministry of Economy, Trade and Industry

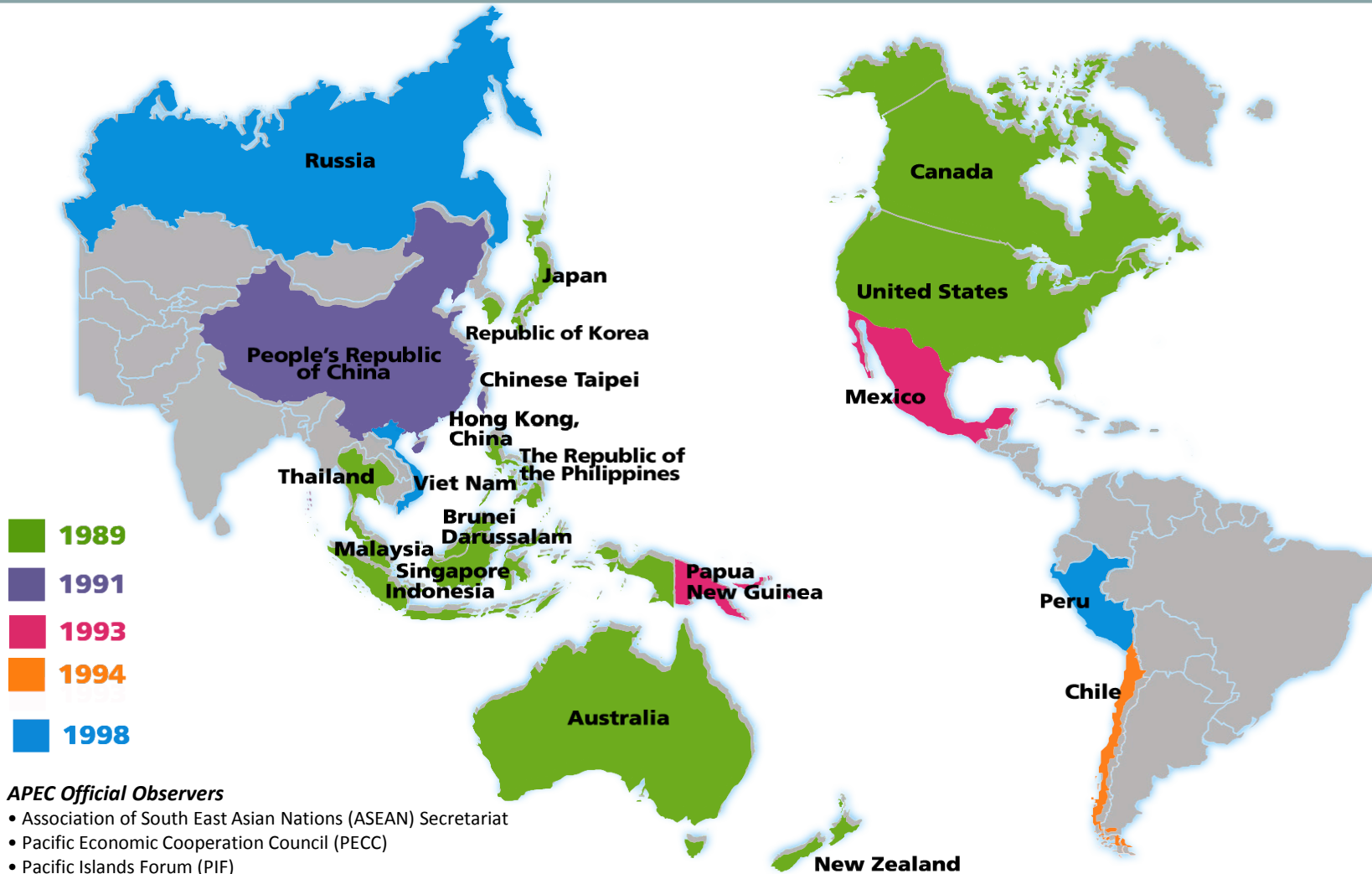
# Contents

---

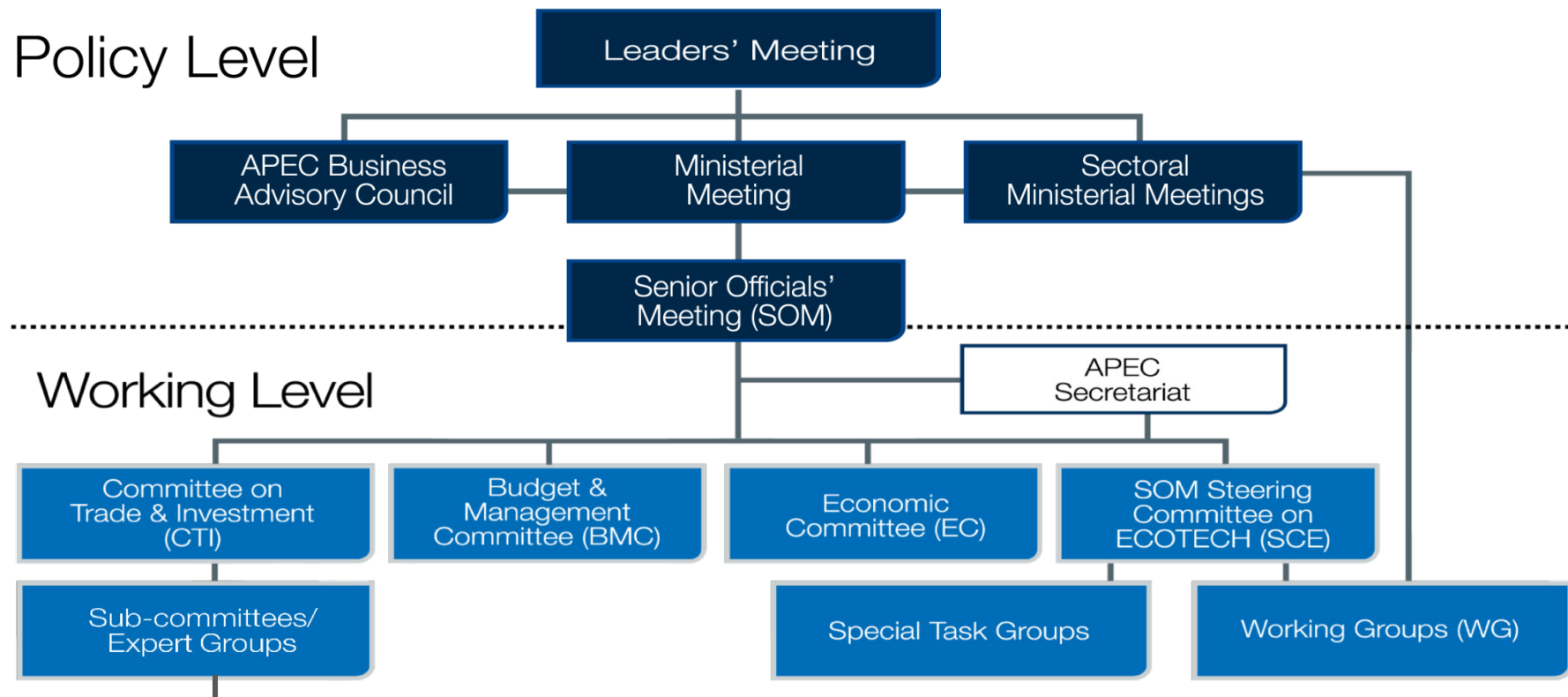
- Overview of APEC and Cross Border Privacy Rules (CBPR) system
- Current Status of the System
- Importance and Benefit of the System
- Challenges and Expectation to the System

# About APEC

- 21 countries and regions have participated in this forum and account for 55% of world GDP, 44% of world trade and 40% of world production.



# Organizational Structure of APEC



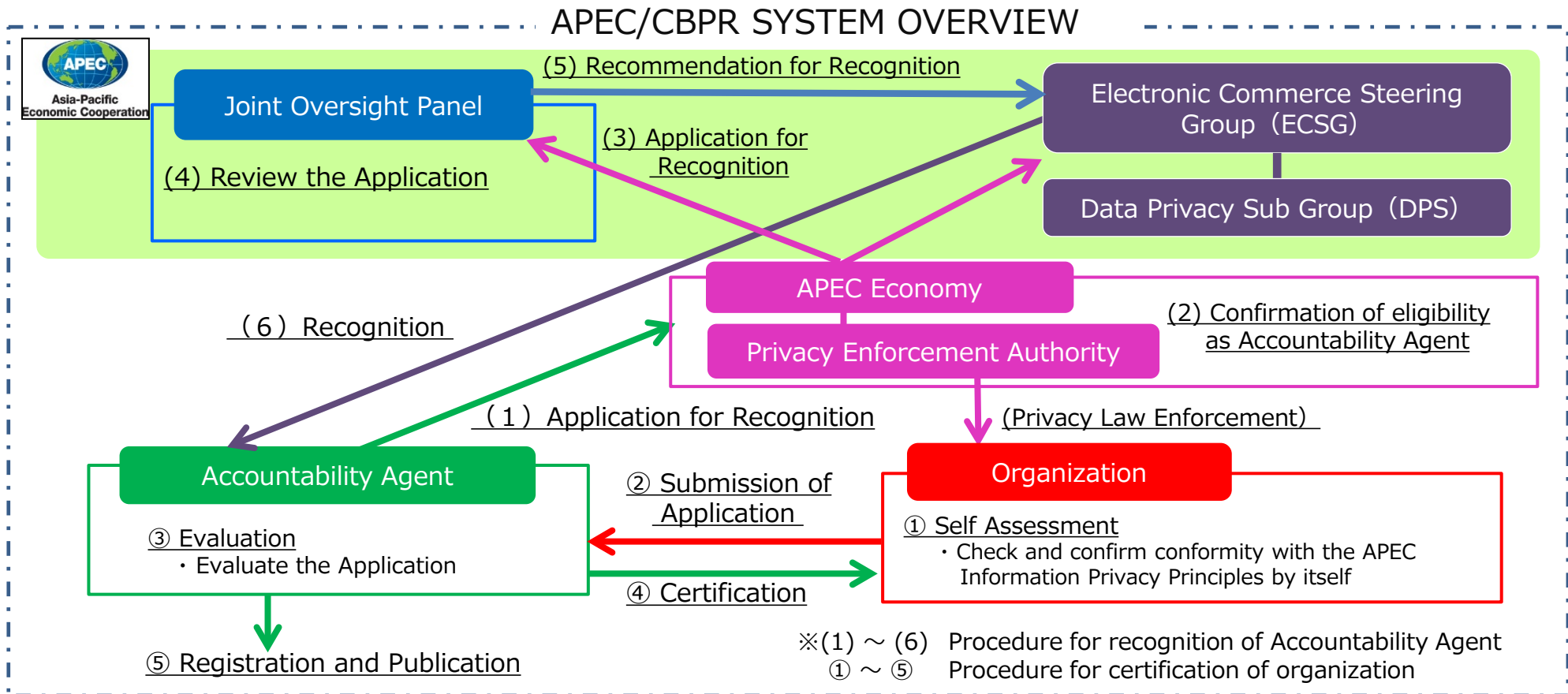
- Sub-Committee on Standards and Conformance
- Sub-Committee on Customs Procedures
- Market Access Group
- Group on Services
- Investment Experts Group
- Intellectual Property Rights
- Business Mobility Group
- **Electronic Commerce Steering Group (ECSG)**

## ECSG

- Established in 1999 as a special task force of SOM, following the APEC Blueprint for Action on Electronic Commerce and in 2007 aligned with CTI.
- Under ECSG, the Data Privacy Subgroup (DPS) is formed, which deals with personal data protection issues, such as development and management of Cross Border Privacy Rules System (CBPRs).

# Basic Scheme of CBPRs

- APEC system for certifying the conformity of company's personal information protection system with APEC Privacy Framework.
- Privacy protecting framework and rules of the applicant organization are evaluated by recognized Accountability Agent.



# Current Status of CBPRs

- Participating Economy: the U.S., Mexico, Japan and Canada
- Recognized Accountability Agents; TRUSTe (the U.S.) and JIPDEC (Japan)
- Certified Organizations; 19 in the U.S. (incl. Apple, Cisco Systems, HP, IBM and Merck) and 1 in Japan
- On December 20, 2016, IntaSect Communications, Inc. was certified as CBPRs compliant, which was the first case in Japan. We hope this could further stimulate other APEC economies' intention to joining in CBPRs.  
(As of May 1st)



# Importance of Promoting CBPRs

- It is widely recognized that the free flow of information is a fundamental principle to promote the global economic and social development.
- At the same time, the importance of data protection and respecting and promoting privacy is recognized.
- More and more countries introduce own personal information protection measures and some of them make it difficult to transfer personal information from these countries to other.
- Therefore, we need to establish and promote the system of protecting personal data based on the international privacy guideline or framework to ensure the cross-border transfer of personal information. APEC/CBPRs is one of such systems.

# Recognition for CBPRs' Importance in APEC

- The importance of CBPRs was recognized by APEC Leaders and Ministers by being referred in the APEC PERU 2016 Leaders' Declaration and Ministerial Joint Statement.

## APEC PERU 2016

### ○LEADERS' DECLARATION

We recall the APEC Leaders 2011 Honolulu Declaration and recognize the importance of implementing the APEC Cross-Border Privacy Rules (CBPR) System, a voluntary mechanism whose participants seek to increase the number of economies, companies, and accountability agents that participate in the CBPR System.

### ○APEC Ministerial Meeting JONT STATEMENT

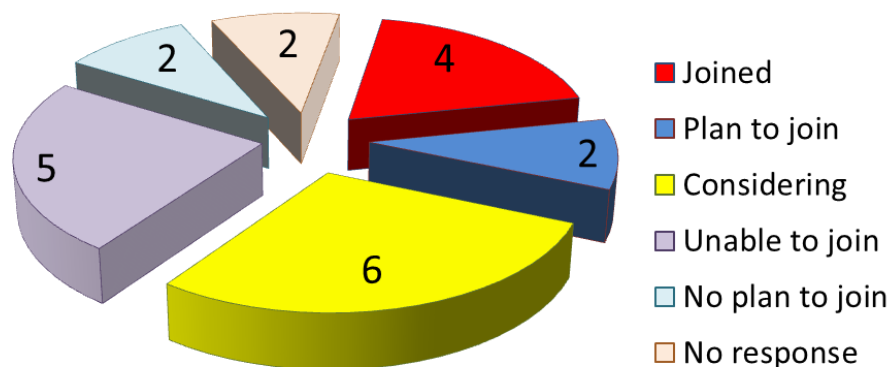
We recognize the importance of the APEC Cross Border Privacy Rules (CBPR) System, a voluntary mechanism whose participants seek to expand participation, and we support enhanced cooperation in this area, including through promoting capacity building.



# Increased Interest in CBPRs

- A survey on the readiness for joining CBPRs conducted by APEC last year, intentions of APEC economies for joining in CBPRs were as follows:
  - 2 (KOR and PHL) have plans to join
  - 6 (AUS, HKG, RUS, SGP, CT, and VNM) are considering
- So far, Korea had already submit the application for participating in CBPRs last December (the application is now under the review). Furthermore, in the last APEC/ECSG meeting in February, Chinese Taipei, Singapore and the Philippines had expressed their interests in participating in CBPRs.

Intention for Joining in CBPRs

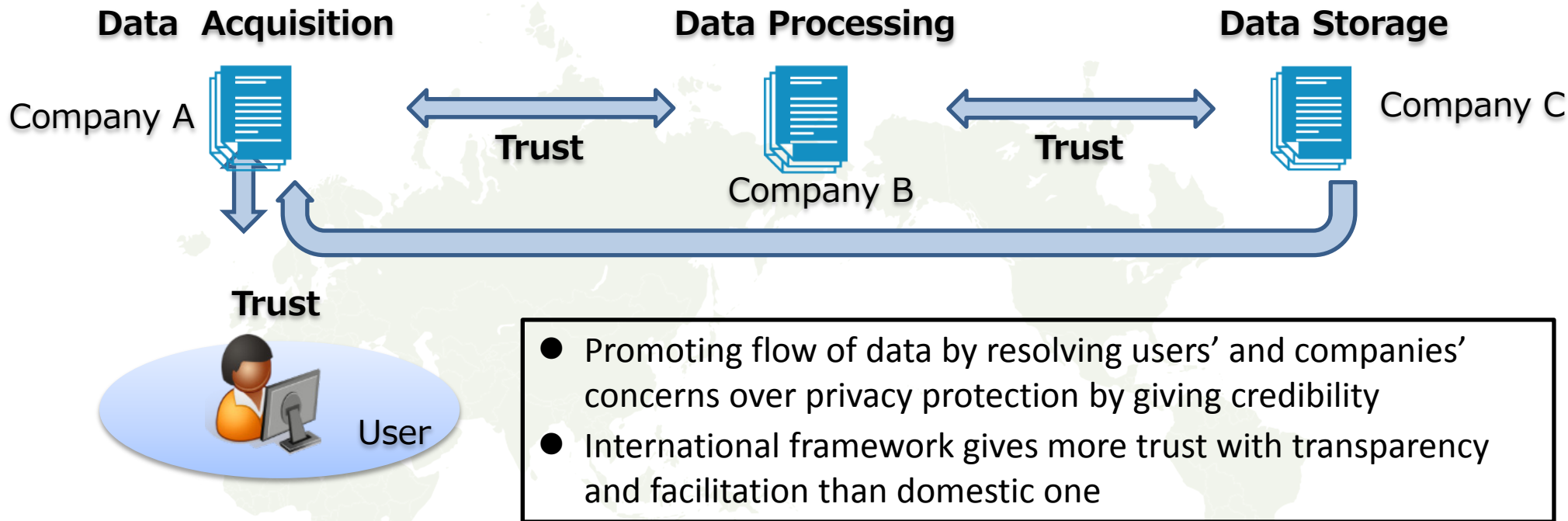


Source: SURVEY ON THE READINESS FOR JOINING CBPRs 2016 (APEC/Vietnam)

**Japan supports other APEC economies' efforts to participate in CBPRs by sharing experiences and lessons learnt from implementing CBPRs.**

# Benefit of Obtaining CBPR Certification (1)

Gaining “Credibility” necessary in Business to Acquire, Process and Storage of Data based on the International Recognized Privacy Framework



**APEC/CBPR system, based on international privacy framework, could be a global standard of privacy protection system**

In other business domains, respective international ecosystems are already established, such as ISO14001 (Environment Management System), ISO9001 (Quality Management System), ISMS (Information Security Management System), etc.

## Benefit of Obtaining CBPR Certification (2)

**As a conditions for cross-border transfers of personal data under the Amended Act on the Protection of Personal Information (coming into effect from May 30, 2017)**

- In any of the following cases, personal data may be transferred to a third party in a foreign country in the same way as in-country;
  - Principal's consent,
  - A third party is in a country designated by PPC\*rules or
  - **A third party has a personal information Protection system conforming with the standards prescribed by PPC rules**



\*PPC; the Personal Information Protection Commission

### **One of the standards;**

The third party's obtainment of a certification based on an international framework (incl. CBPR) concerning the handling of personal information.

# Challenges and Expectation to CBPRs

## **Number of Participating Economies**



For more effective implementation of CBPRs,  
the increase of participating economies is necessary

## **Number of Organizations obtaining CBPR**



For more effective implementation of CBPRs, the increase of organizations  
obtaining CBPR certification is necessary

## **Limitation of CBPRs (recognized only in APEC)**



Expectation to the globalization of the system beyond the APEC  
including interoperability with GDPR and establishment of global system



# Thank you !

May 11th

Shinji Kakuno  
International Affairs Office  
Ministry of Economy, Trade and Industry

# C IPL Japan Workshop Panel

## Cross-Border Data Flows and the APEC Cross-Border Privacy Rules System

11 May, 2017

Yoichi IIDA  
Global ICT Policy Strategy Bureau  
Ministry of Internal Affairs and Communications

# Discussions on Free flow of information in International Fora

---

Free flow of information and privacy protection are parallel priorities in policy talks.

## G7 ICT Ministers' Declaration (2016.4)

We continue to support ICT policies that preserve the global nature of the Internet, promote the flow of information across borders and allow Internet users to access online information, knowledge and services of their choice. We oppose data localization requirements that are unjustifiable taking into account legitimate public policy objectives.

## G20 Hangzhou Summit (2016.9)

We support ICT policies that preserve the global nature of the Internet, promote the flow of information across borders and allow Internet users to lawfully access online information, knowledge and services of their choice. At the same time, the G20 recognizes that applicable frameworks for privacy and personal data protection, as well as intellectual property rights, have to be respected as they are essential to strengthening confidence and trust in the digital economy.

## G20 Digital Ministers' Declaration (2017.4)

We reaffirm support for ICT policies that preserve the global nature of the Internet, promote the flow of information across borders, and allow Internet users to lawfully access online information, knowledge and services of their choice. At the same time the G20 recognizes that applicable frameworks for privacy and personal data protection, as well as intellectual property rights, have to be respected as they are essential to strengthening confidence and trust in the digital economy.

# Promoting Data Driven Society and Data Flow

Digitalization and Data-driven society bring new values in various aspects;

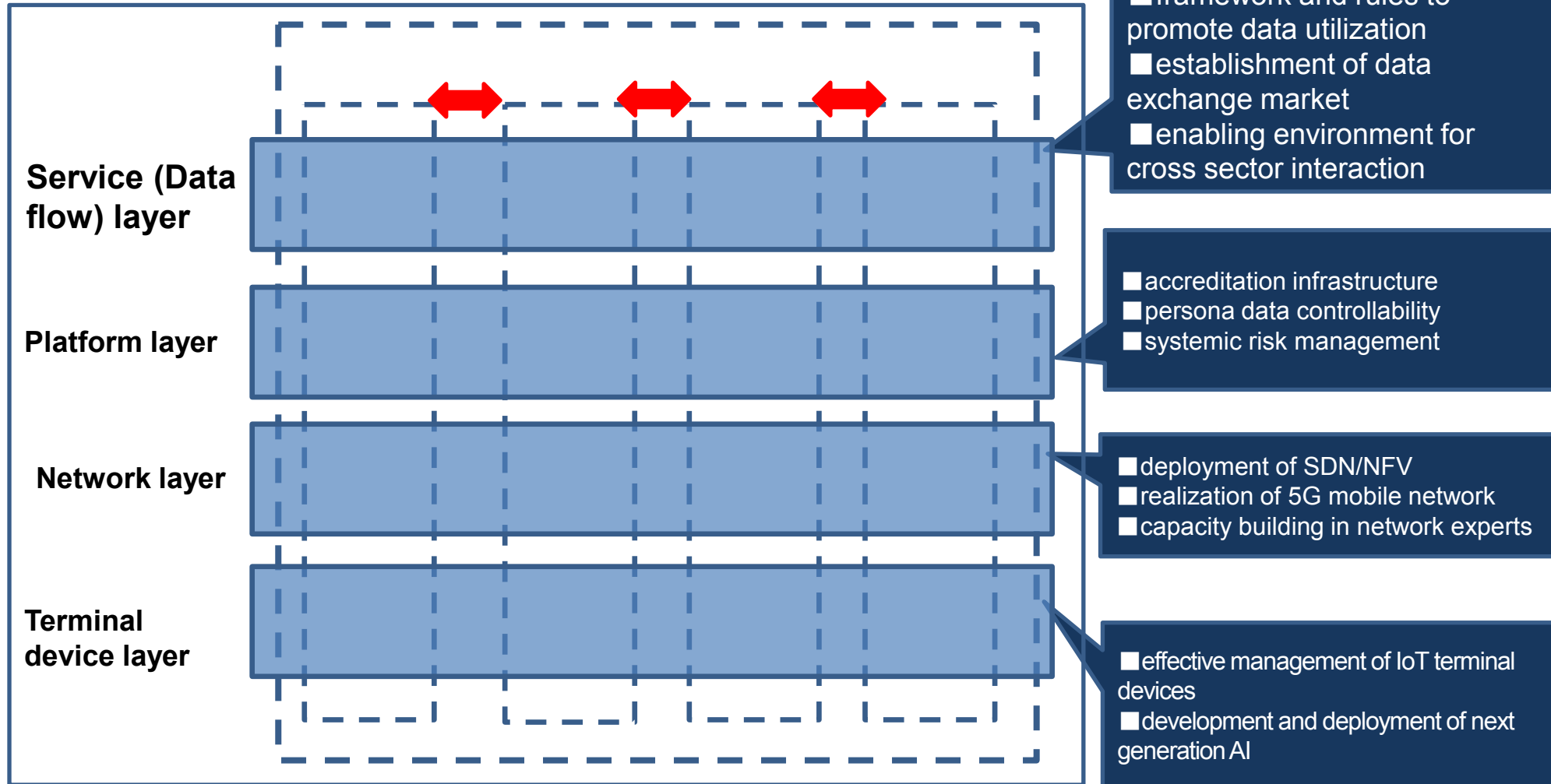
- boosting economic growth via innovation  
GDP increase appx. 30 Trillion Yen (260-270 Billion US\$) estimate in White Paper 2016
- transforming society  
improving quality of life through realizing Society 5.0
- developing diversified culture  
Multi-lingual contents, conserving digitalized cultural heritages

Digital Data ; Source of various new values

Free flow and full utilization of data are critically important for reaping the benefits of digitalized society.

# Structure of Digitalized services and promoting measures ~ MIC's perspective

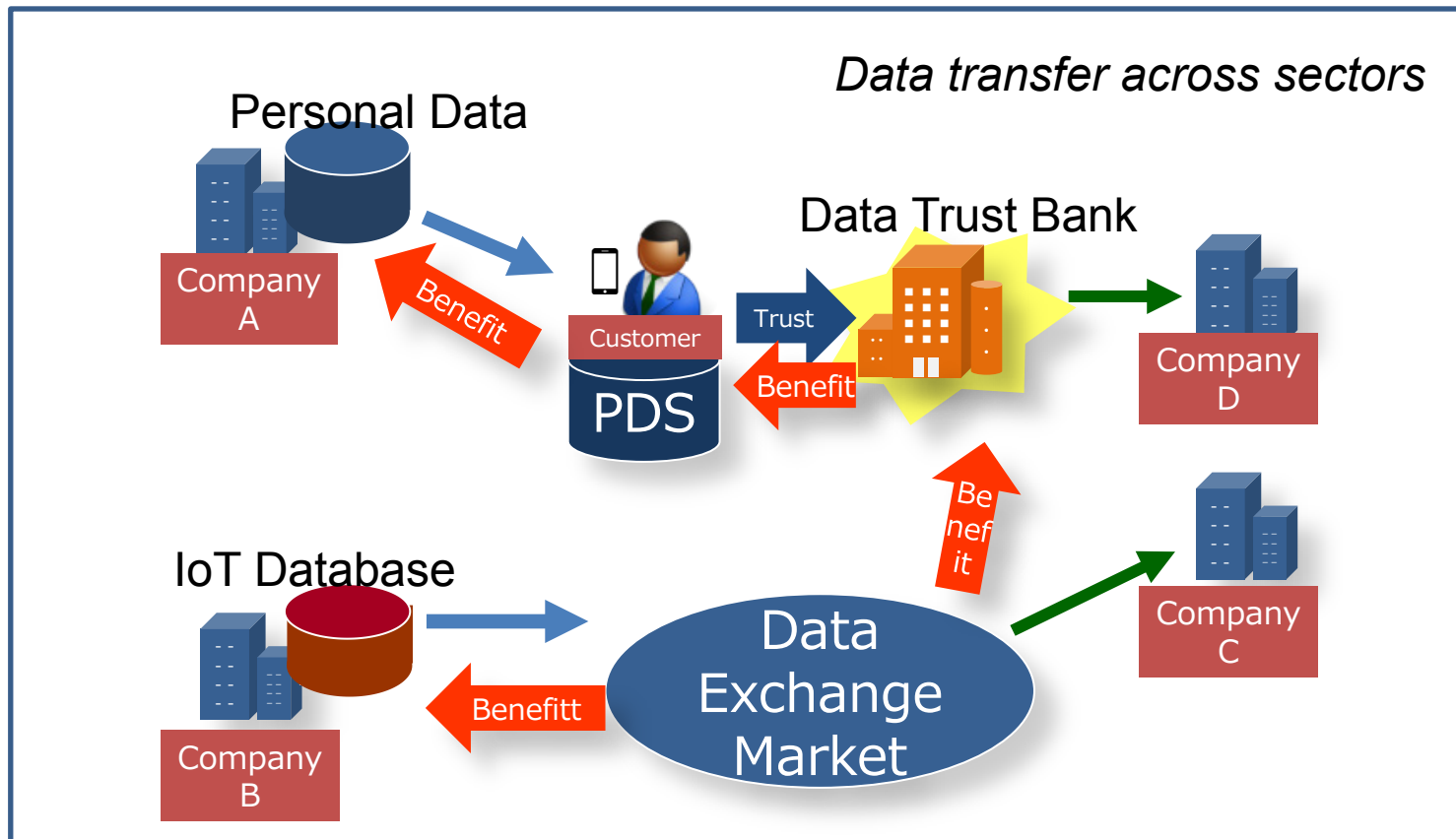
Data flow needs to be facilitated by improvements in rules, exchange mechanisms and enabling environment



# Concept of Data Exchange Market and Data Trust Bank

- to find possible framework and rules to promote data utilization
- to find conditions for establishment of data exchange market
- to find ways to improve enabling environment for cross sector interaction

## Data Exchange Market and Data Trust Bank (Concept)





# Omotenashi Cloud Service Field Trial

Learn how to use personal data for customized services for foreign visitors



Volunteer Tourists from Foreign countries



Provide personal data and participate

Wifi access



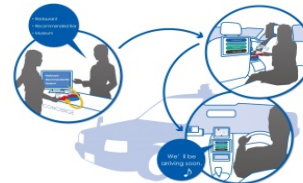
Registration service



Navigation



Smart mobility service



I D etc.

Customized  
Information service

Disaster Info.  
Server

Translation  
Server

Local Info.  
Server

Olympic/Paralimpic  
Info. Server

Personal ID  
DB

連携

Personal  
DB

Info.

共通クラウド基盤

FY 2016  
3 areas



Challenges;  
How to judge credibility.  
Complex procedure required.

FY2017  
extended  
( under planning)



Cross-border transition  
Of personal data may be  
Required, if foreign service  
companies join.

# The Overview of APEC/CBPR System

JIPDEC  
11 May 2017

- In January 2016, JIPDEC was recognized as AA (Accountability Agent) of APEC/CBPR System for the first time in Japan.
- In June 2016, JIPDEC started its operation as AA of APEC/CBPR System.
- On Dec 20<sup>th</sup>, 2016, IntaSect communications inc was examined and certified by JIPDEC for the first time in Japan.  
([https://english.jipdec.or.jp/protection\\_org/cbpr/list.](https://english.jipdec.or.jp/protection_org/cbpr/list.))
- Currently, we receive inquiries regarding application procedures and conducts individual consultation to business entities.

- CBPR certification in Japan is included in the work of **Authorized Personal Information Protection Organizations** stipulated in the **Act on the Protection of Personal Information**. Authorized Personal Information Protection Organizations recognized by the Government certify qualified applicants under the Act.
  - JIPDEC is recognized by the Government (Ministry of Economy, Trade and Industry; and Ministry of Internal Affairs and Communications) as an Authorized Personal Information Protection Organization.
- To apply for APEC/CBPR certification, business entities are required to become **Target Entities** of Authorized Personal Information Protection Organizations of JIPDEC.

Specifically, either one of the following requirements must be met: (1) they must become enterprises certified by a personal information protection certification system that JIPDEC operates, or (2) they must become members of a business program organized in JIPDEC for promoting the protection and utilization of electronic information. Also, they need to agree to comply with JIPDEC's **Personal Information Protection Guideline**.



- Accountability agent (JIPDEC, in Japan) is responsible for the review of self-assessment which is CBPR System certification process.
  - Applicant organizations are responsible for developing their own privacy policies and procedures, and can participate in CBPR System only if the appropriate Accountability Agent certifies that the policies and procedures comply with CBPR requirements.
  - Accountability Agent **monitors** certified companies as needed and confirms whether there are no change of personal information handled, etc. (Receiving the notification of change is also possible.)
  
- **It processes complaints** and submit anonymous case notes and complaint statistics to APEC.
  
- It should be noted that, depending on the results of monitoring and complaint processing, it will request additional reviews, suspend the certification, or cancel the certification. (Penalties)

<p>period to improve</p>	Public	cancellation	Grave	<ul style="list-style-type: none"> <li>- When there is a false statement to a written application to CBPR certification.</li> <li>- When personal information handling is not improved even if the reply deadline to warning and improvement guidance, etc. has passed.</li> <li>- When an incident or accident about personal information handling happens by intent or gross negligence.</li> <li>- Other (When JIPDEC evaluates that the certification should be canceled.)</li> </ul>	SPECIAL AUDIT
	Public	suspension	Grave	<ul style="list-style-type: none"> <li>- When there is a risk that an incident or accident about personal information handling happens by intent or gross negligence.</li> <li>- When personal information handling is not improved even if the reply deadline to warning and improvement guidance, etc. has passed.</li> <li>- Other (When JIPDEC evaluates that the certification should be suspended.)</li> </ul>	
	Non-public	improvement guidance (recommendation)	Grave	<ul style="list-style-type: none"> <li>- When a medium-sized incident or accident about personal information handling happens.</li> <li>- When personal information handling is not improved even if the reply deadline to warning, etc. has passed.</li> <li>- Other (When JIPDEC evaluates that there should be improvement guidance.)</li> </ul>	
	Public	warning	Minor	<ul style="list-style-type: none"> <li>- When a small (minor) incident or accident about personal information handling happens.</li> <li>- Other (When JIPDEC evaluates that there should be warning.)</li> </ul>	review
	Public	monitoring	Confirmation	<ul style="list-style-type: none"> <li>- Confirms published matters on CBPR certified companies' web sites, etc.</li> <li>- Confirms published matters in the news and articles, etc.</li> </ul>	

Red : Obligations of AA

\*In addition, there should be the notification to relevant authorities (cooperation).




- A certified entity can announce to the public that its business activities are compliant with the **APEC Information Privacy principles** in handling personal information, which would be an advantage in conducting business transactions (business-to-business, and business-to-consumer).
  - It does not certify that a company is observing a domestic law. It certifies that the company is handling personal information in compliance with CBPR when businesses go across national borders.
- Accountability Agent (AA), for certified entities, processes **complaints and consultation cases within the APEC region** on a case-by-case basis.
  - When issues arise, AA addresses them for certified entities, while a corresponding government institution (the Personal Information Protection Commission in Japan) handles those of uncertified entities.
- Other
  - The Japanese Government recommends that Japanese companies use CBPR certification as one of the requirements for overseas trustees to whom they outsource handling of personal information.

- Becomes Target Entities of Authorized Personal Information Protection Organizations of JIPDEC which is AA.
- Flow from application to registration
  - The procedure includes **1. Application, 2. Review (documentation and on-site), 3. Board of review, 4. Registration.**

procedure	Main documents submitted by Applicant	What Authorized Personal Information Protection Organizations do
application	1. <b>Intake Questionnaire</b> 2. Application form	1. Confirm documents 2. Check about the compliance with CBPR regulations 3. Charge the review fee 4. Accept application form
Review (documentation)	1. Regulations (Japanese/English) 2. Publicized documents (Japanese/English) 3. Internal regulations, etc. needed to review (Japanese)	1. Hearing (Interviews overall handling about personal information) 2. Documentation review
Review (on-site)	(Attendance and Explanation)	1. Check the operation situation of applicant on-site (Check mainly security, etc.)
Board of review		1. Hold Board of review and determine the certification 2. Charge the management fee of the certification
registration		1. Confirm the payment of the management fee of the certification 2. Issue the certificate 3. Registration of organization name/Publication of the name on web site.

- Intake Questionnaire is intended to describe the applicant's answers to 50 questions about the handling of personal information, in accordance with the APEC principles.

(Supporting documents, etc. are also needed)

 Asia-Pacific Economic Cooperation	
APEC 越境プライバシールールシステム 事前質問書	
基本情報	2
通知	5
通知に関する規定の条件	7
取得の制限	8
個人情報の利用	9
選択	11
選択手続に関する規定の条件	13
個人情報の完全性	14
セキュリティ対策	15
アクセス及び訂正	18
アクセス及び訂正手続に関する規定の条件	18
責任	22
一般	22
個人情報が移転された場合の責任の維持	23

Page | 1



# Contents of Intake Questionnaire (2)

Item	Description
<b>General Information</b>	<ul style="list-style-type: none"><li>• Name of Organization, List of subsidiaries and/or affiliates governed by privacy policy to be covered by certification, Contact Point</li><li>• Types of personal information (Customer/Prospective Customer, Employee/Prospective Employee, Other)</li><li>• Economies to collect personal information (APEC participating countries and regions)</li><li>• Economies to transfer personal information (the same above)</li></ul>
Item	Things to confirm
<b>Notice</b>	In accordance with the APEC principle, (1) Ensuring that individuals understand your policies regarding personal information that is collected, to whom it may be transferred and for what purpose it may be used. (2) Ensuring that individuals know when personal information is collected, to whom it may be transferred and for what purpose it may be used, on condition that the collection is the minimum one.
<b>Collection Limitation</b>	Ensuring that collection of personal information is limited to the stated purpose for which it is collected, in accordance with the APEC principle.
<b>Uses of Personal Information</b>	Ensuring that the use of personal information is limited to fulfilling the purposes of collection and other compatible or related purposes, in accordance with the APEC principle.
<b>Choice</b>	Ensuring that individuals are provided with choice in relation to collection, use, and disclosure of their personal information, in accordance with the APEC principle.
<b>Integrity of Personal Information</b>	Ensuring that the personal information controller maintains the accuracy and completeness of records and keeps them up to date, in accordance with the APEC principle.
<b>Security Safeguards</b>	Ensuring that when individuals entrust their personal information to an organization, their personal information will be protected with reasonable security safeguards to prevent loss or unauthorized access to personal information or unauthorized destruction, use, modification or disclosure of information or other misuses, in accordance with the APEC principle..
<b>Access and Correction</b>	Ensuring that individuals are able to access and correct their information, in accordance with the APEC principle.
<b>Accountability</b>	Ensuring that you are accountable for complying with measures that give effect to the APEC principles. Taking reasonable steps to ensure the information is protected, in accordance with the principles, after it is transferred.

- **We will conduct an individual consultation to business entities which is considering applying for CBPR certification.**

Please feel free to contact us.

- E-mail [nintei-inq@tower.jipdec.or.jp](mailto:nintei-inq@tower.jipdec.or.jp)
- Web [http://www.jipdec.or.jp/protection\\_org/index.html](http://www.jipdec.or.jp/protection_org/index.html)

APEC／CBPR 認証  
申請ガイドブック

平成 28 年 6 月

一般財団法人日本情報経済社会推進協会

Please use "APEC/CBPR certification application guide book" by downloading it.

**THANK YOU VERY MUCH.**





## Session 3

# Applying New Legal Requirements to Big Data and Analytics, Machine Learning and AI

### Moderator:

- ❖ Bojana Bellamy, President, Centre for Information Policy Leadership

### Discussion Leads:

- ❖ Susumu Hirano, Professor of Law, Faculty of Policy Studies/Graduate School of Policy Studies, Chuo University
- ❖ Kuniko Ogawa, Counselor, Japan Personal Information Protection Commission
- ❖ Satoshi Narihara, Senior Researcher, Policy Research Department, Institute for Information and Communications Policy (IICP), Japan Ministry of Internal Affairs and Communications (MIC)
- ❖ Harvey Jang, Director, Global Privacy and Data Protection, CISCO
- ❖ Dr. J.J. Pan, Chief Privacy Officer and Director of Public Policy, Acxiom Asia Pacific Corp.



# AI R&D Guidelines — Preliminary Draft —

May 11, 2017

Dean, Grad. Sch. of Pol'y Stud.,  
Prof. Faculty of Pol'y Stud., CHUO UNIV., Tokyo  
Susumu HIRANO\*

(\*) <<http://c-faculty.chuo-u.ac.jp/~cyberian/>>

## Conference toward AI Network Society

Core-member

[Study items]

Social, economic, ethical, or legal issues caused by AI networking

- Issues and institutional matters related to AI research and development principles  
(→ Subcommittee on **AI R&D Principles**)
- Matters related to the evaluation of impacts and risks caused by AI Networking  
(→ Subcommittee on **Impact and Risk Assessment**)

Subcommittee on **AI R&D Principles**

Chair-person

Me

Subcommittee on **Impact and Risk Assessment**

**(1) Principle of Collaboration**

To pay attention to interconnectivity and interoperability among AI Systems.

**(2) Principle of Transparency**

To pay attention to the abilities to verify and explain behaviors of AI Systems.

**(3) Principle of Controllability**

To pay attention to controllability of AI Systems, and make efforts to provide relevant information properly.

**(4) Principle of Security**

To pay attention to security of AI Systems.

**(5) Principle of Safety**

To consider that AI Systems will not harm lives or bodies of users or third parties through actuators or others, and make efforts to provide relevant information properly.

**(6) Principle of Privacy**

To consider that AI Systems will not infringe privacy of users or third parties.

**(7) Principle of Ethics**

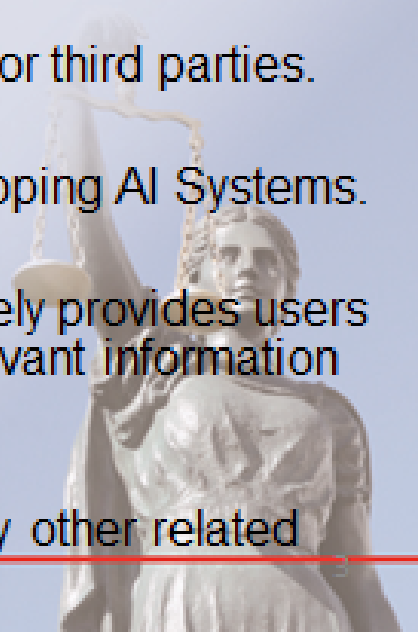
To respect human dignity and individuals' autonomy in developing AI Systems.

**(8) Principle of User Assistance**

To consider that AI Systems can assist users and appropriately provides users with opportunities to choose, and make efforts to provide relevant information properly.

**(9) Principle of Accountability**

To make efforts to accomplish accountability to users and any other related stakeholders.



## I. Principles Relating to Networked AI Systems' Functions

1. Principles chiefly for promoting the healthy progress of AI Networking and thereby increasing the benefits of Networked AI Systems

### **(1) Principle of Collaboration**

2. Principles chiefly for restraining the risks of Networked AI Systems

### **(2) Principle of Transparency**

### **(3) Principle of Controllability**

### **(4) Principle of Security**

### **(5) Principle of Safety**

### **(6) Principle of Privacy**

### **(7) Principle of Ethics**

3. A Principle which supplements those indicated in 1 and 2 above

### **(8) Principle of User Assistance**

- ## II. A Principle Which the Developer Is Expected to Fulfill for Stakeholders concerning Each Principle Listed in Section I

### **(9) Principle of Accountability**



Thank you for your attention 😊



中央大学

CHUO UNIVERSITY

— Knowledge into Action —





# Benefit of Big Data and Protection of Personal Data

Kuniko Ogawa

Counselor

Personal Information Protection Commission (PPC)

May 11 , 2017

## The Amended APPI : Changes and Challenges

1

The Act on the Protection of Personal Information was enacted in 2003  
(Fully enforced in 2005)

Changes of circumstances

As Information and Communications Technologies(ICTs) advanced, the utility of personal information became intensified and diversified beyond expectation

### 1. Enlargement of “gray areas” of personal information

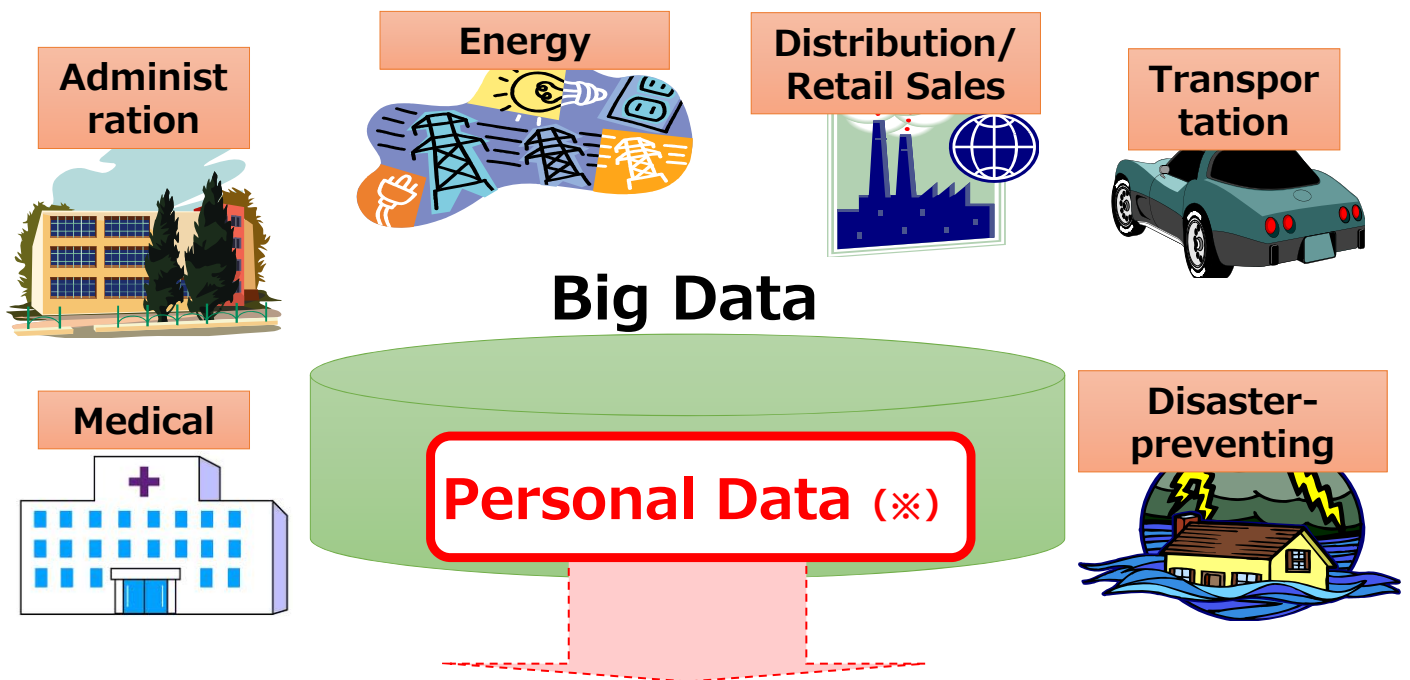
So called “gray area” was enlarged, in which judgment of personal information was difficult

### 2. Correspondence for Big Data

To realize circumstances for appropriate usage of Big Data including personal data is necessary

### 3. Responses Globalization

As business operations are globalized, massive data flow goes beyond national border



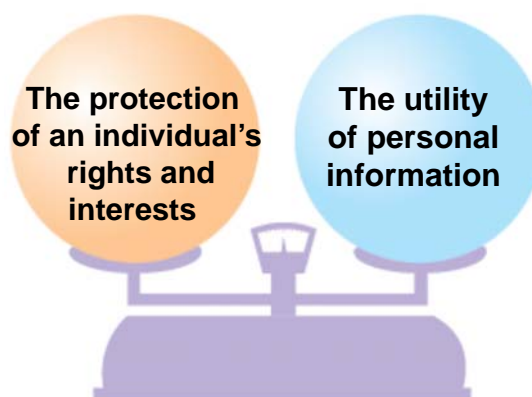
**To realize circumstances for appropriate usage of Big Data including personal data is necessary**

※ Personal data has a great deal of potential in utility of Big Data

## Purpose of The Act on the Protection of Personal Information (APPI)

3

- The APPI aims to seek the balance between **the protection of an individual's rights and interests** and **the utility of personal information**.
- Besides the overall vision for the proper handling of personal information, this Act establishes obligations, etc. that a **personal information handling business operator** shall fulfil.



### (Purpose of the Act)

Article 1 This Act **aims to protect an individual's rights and interests while considering the utility of personal information** including that the proper and effective application of personal information contributes to the creation of new industries and the realization of a vibrant economic society and an enriched quality of life for the people of Japan; by setting forth the overall vision for the proper handling of personal information, creating a governmental basic policy with regard to this, and establishing other matters to serve as a basis for measures to protect personal information, as well as by clarifying the responsibilities etc. of the central and local governments and establishing obligations etc. that a personal information handling business operator shall fulfill, in light of the significantly expanded utilization of personal information as our advanced information- and communication-based society evolves.

○The Act on the Protection of Personal Information was amended in September 2015(To be fully enforced in May 30, 2017.)

## The outline of the amendment

### 1.Establishment of the PPC

- Aggregation of the supervising authorities to the PPC, which are currently held by the relevant regulatory ministers toward personal information handling business operators under their respective supervision.

### 2. Clarifying the definition of personal information

- (1) Clarifying the definition of personal information by stating partial bodily features etc. of a specific individual as personal information to cope with gray areas of personal information (individual identification codes)
- (2) A principal's advance consent shall be obtained in principle in cases of acquiring or providing to a third party special care-required personal information (i.e., race, creed, medical record).

### 3. Establishment of a legal framework to enhance active use of personal information

Establishment of regulations concerning “anonymously processed information”(meaning information that has been produced by processing personal information in a way to make a specific individual unidentifiable and hence disallowing reconstruction of the personal information).

### 4. Responses to globalization

- (1)Introduction of a new legal provision for transferring personal data to a foreign third party
- (2)Introduction of a new legal provision for extraterritorial application, and sharing information with the foreign enforcement authorities

### 5. Measures to Respond to a so-called “Name List Trader”

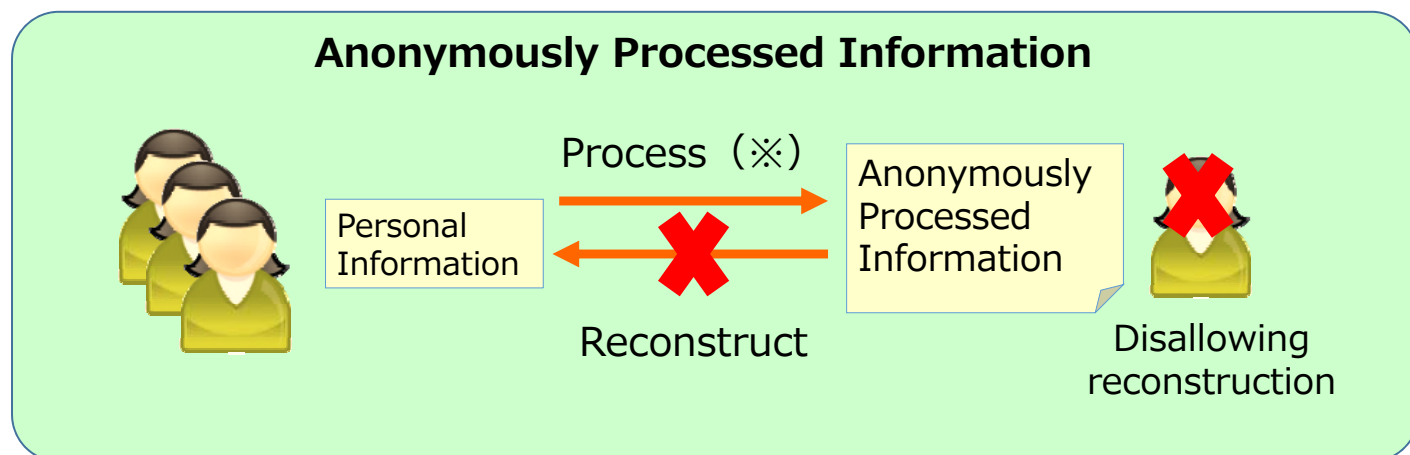
- (1)Imposing new obligations to keep and confirm a record relating to a third-party personal data provision.
- (2) An act of providing a third party with or stealing personal information database etc. for the purpose of earning illicit gains has become subject to criminal punishment as “the offense of providing personal information database”.

### 6. Others

- (1)Abolition of a system wherein a business operator handling personal information of 5,000 individuals or less may be excluded from the regulated subjects.
- (2) A personal information handling business operator utilizing an opt-out procedure has become obligated to notify the Personal Information Protection Commission of certain legally required items.

## Establishment of new legal framework of anonymously processed information 5

Establishment of regulations concerning “**anonymously processed information**”(meaning information that has been produced by **processing personal information in a way to make a specific individual unidentifiable** and hence **disallowing reconstruction of the personal information**), and enhance smooth circulation and utility under relaxed regulation compared with ordinally personal information



### ■ Standards in the methods of producing anonymously processed information (PPC Rules)

- ①Deleting a whole or part of those descriptions etc. which can identify a specific individual contained in personal information (e.g. name)(including replacing, same as below)
- ②Deleting all individual identification codes contained in personal information (e.g. my number, drivers license number)
- ③Deleting those code which link personal information and information obtained by having taken measures against the personal information
- ④Deleting idiosyncratic descriptions etc. (e.g. age 116)
- ⑤Besides action set forth in each preceding item, taking appropriate action based results from considering the attribute etc. of personal information database etc. such as a difference between descriptions etc. contained in personal information database etc.

For producing **anonymously processed information**, an appropriate processing needs to be done in accordance with standards prescribed by the PPC (**Standards prescribed by the PPC is a minimum standard**).

With regard to specific processing method based on characteristics of data and attribute of business, it is expected to be **appropriately developed by self-regulation of accredited personal information protection organizations or industry organizations etc.**

① **Deleting descriptions etc. which can identify a specific individual**

Deleting a whole or part of descriptions etc. which can identify a specific individual such as a name, address, date of birth or gender, or replace them with other descriptions etc.

② **Deleting individual identification codes**

Deleting a whole individual identification codes (face authentication data, fingerprint identification data, individual number or driver's license number etc. ), or replace them with other descriptions etc.

③ **Deleting codes linking mutually plural information**

Deleting management ID for seeking decentralized management etc. of obtained personal information in terms of security control (**including the case using telephone number or email address as an ID**), or replace them with other codes

④ **Deleting idiosyncratic descriptions etc.**

Deleting descriptions etc. relating to unusual fact or which have significant difference from other individuals (**Example: 116 years old**), or replace them with other descriptions etc.  
\* "idiosyncratic descriptions etc." means the descriptions etc. which can identify a specific individual due to its idiosyncraticness.

⑤ **Other action based on the attribute of a personal information database etc.**

Further processing is necessary in **the case remaining the condition which can identify a specific individual or restore the original personal information** due to the characteristics of personal information database etc. even though the above-mentioned ①-④ process was taken

\* Cases mentioned in the Guideline: Movement history which can identify home or workplace, purchase history of merchandise which consumer is extremely limited, Disparity in the said personal information database

## The PPC Secretariat Report on Anonymously Processed Information 7

### Publication of the PPC Secretariat Report on Anonymously Processed Information

(February 27, 2017)

- Stating matters and aspects which are reference for considering voluntary rules related to producing anonymously processed information or actually producing anonymously processed information to an accredited personal information protection organization or a group of business operators

### Main Contents of the Secretariat Report

#### ○ **What is anonymously processed information?**

Explaining definition of anonymously processed information and restrictions etc. (rules of handling) for handling of anonymously processed information

#### ○ **Processing to anonymously processed information**

- Explaining specific method of measures prescribed by processing standards of anonymously processed information and describing desirable matters for considering when producing anonymously processed information
- Presenting for reference general processing examples by categorizing information into **that belonging to an individual (a name, address) and history (purchase history)**, and in accordance with expected risk and basic aspects in each item of information

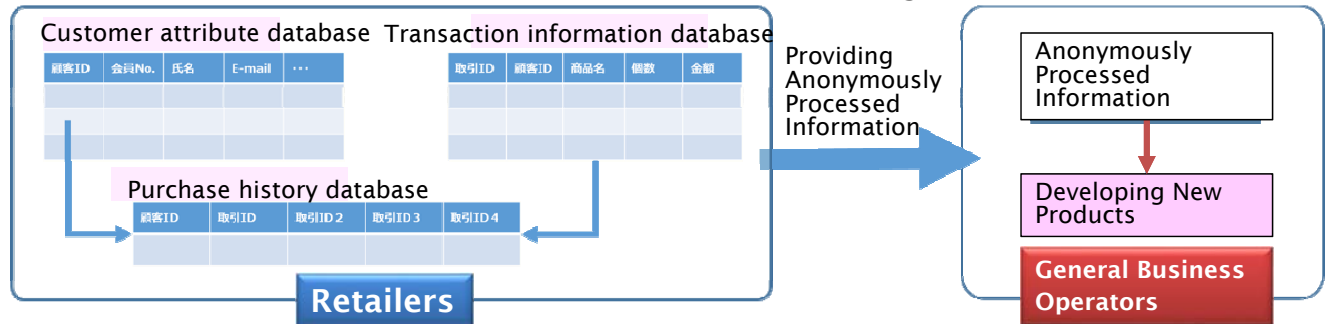
#### ○ **Use case and example of processing of anonymously processed information**

Introducing specific processing method, with expected use case in mind, of the case on purchase history, ridership history, movement history and electric usage history responding to matters and risks to be considered in respective item of information



## ○ Case of purchase history (ID-POS data)

- Processing purchase history (ID-POS data) held by retailers and providing a general business operator with processed data
- The said business operator utilizes consumer attribute and purchasing trend included in provided anonymously processed information for developing new products

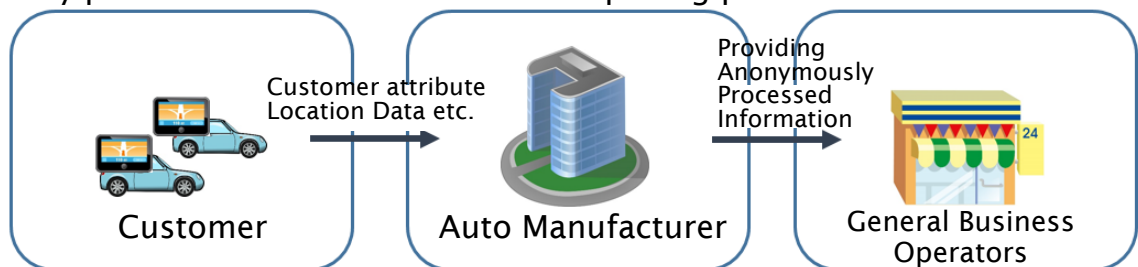


Item	Example of Processing
① Member ID	Deleting or Replacing
② Name	Deleting
③ Date of Birth	Replacing with year of birth
④ Gender	No processing
⑤ Address	Replacing with resident area
⑥ Telephone No.	Deleting
⑦ Retailer	No processing
⑧ Merchandise	Deleting information on merchandise which is extremely limited

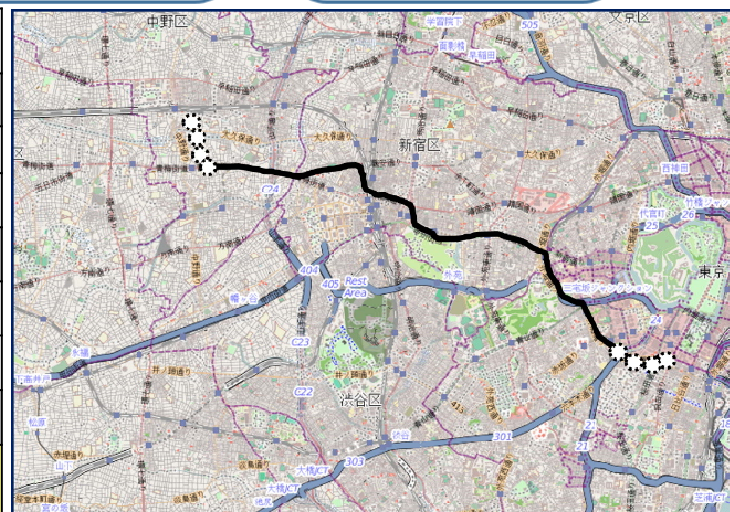
## ○ Case of movement history

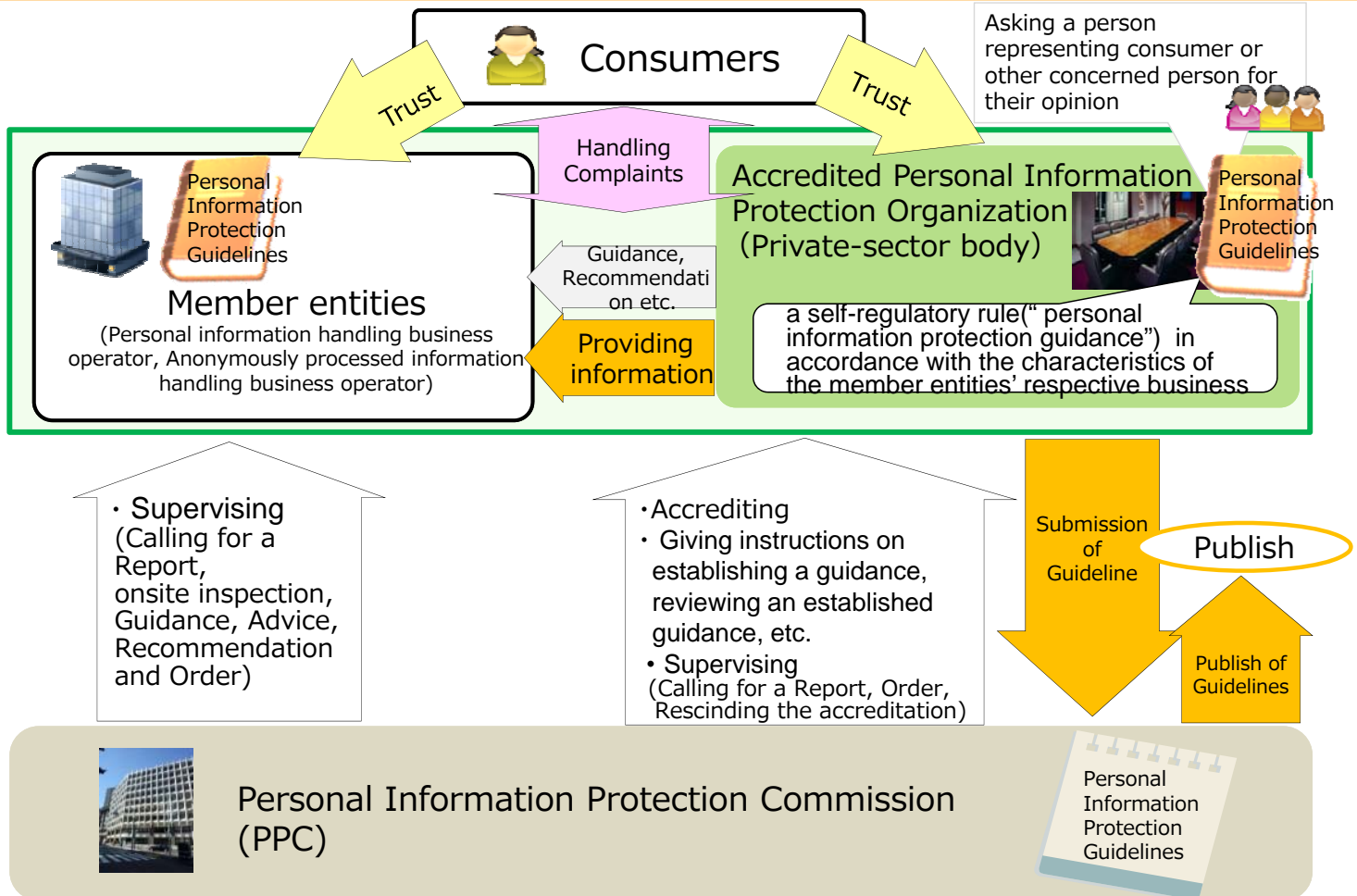
An auto manufacturer processes location information obtained through data communication module, and provide a general business operator (retailer) with processed information

The general business operator utilizes consumer attribute and moving history data included in provided anonymously processed information for store opening plan etc.

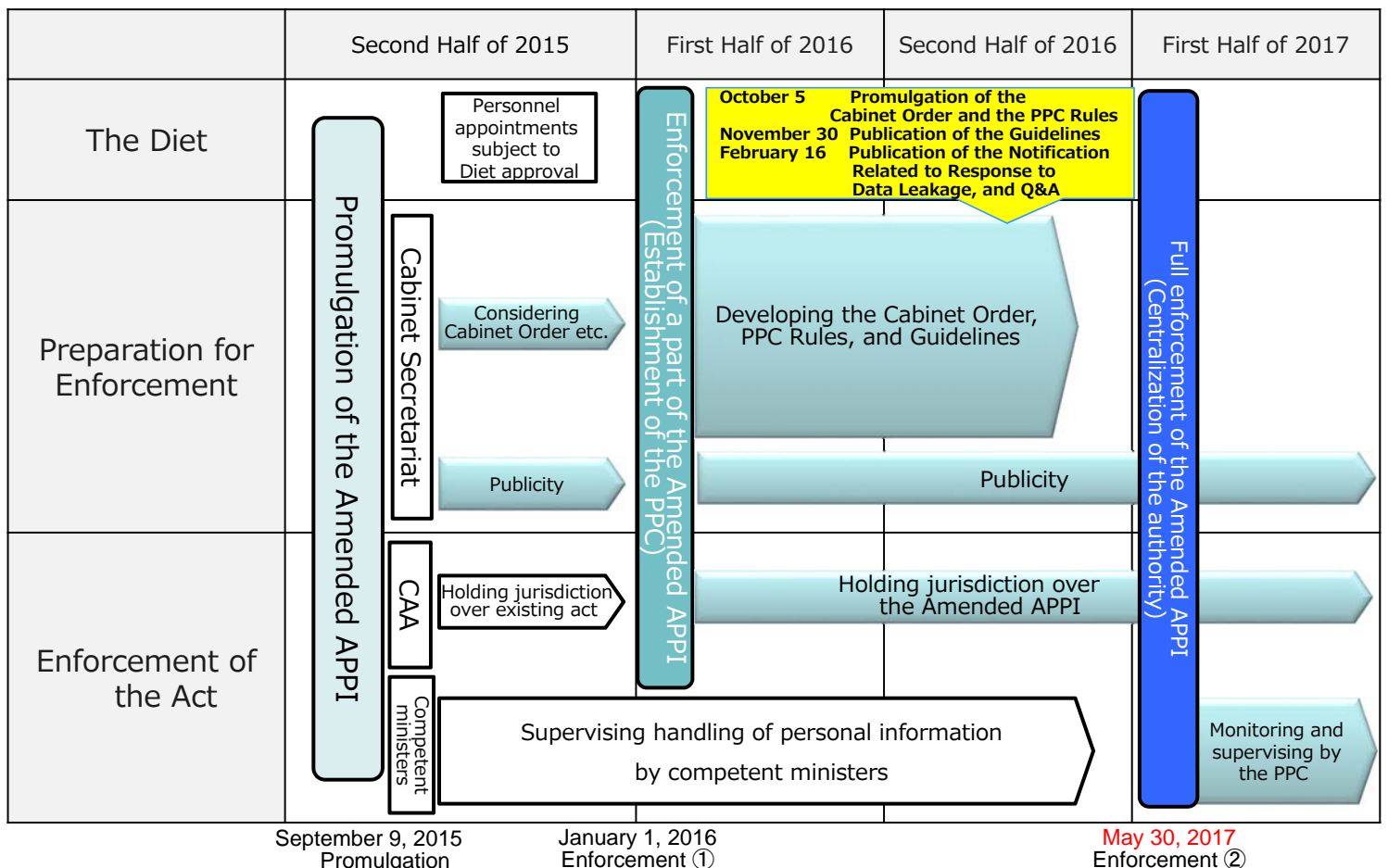


Item	Example of Processing
① Name	Deleting
② Gender	No processing
③ Date of birth	Replacing with year of birth
④ Telephone No.	Deleting
⑤ Address	Replacing with resident area
⑥ Type of vehicle	Replacing with category of vehicle
⑦ VIN	Deleting
⑧ Location Data	Deleting starting and ending point (for a few minutes) of each moving history





## Schedule







Thank you !

Kuniko Ogawa

[ogawa-k5pw@ppc.go.jp](mailto:ogawa-k5pw@ppc.go.jp)

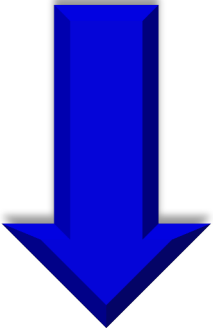


# Discussions toward AI Network Society

Senior Researcher, Policy Research Department, the Institute for Information and Communications Policy (IICP), the Ministry of Internal Affairs and Communications (MIC) of Japan

Satoshi NARIHARA

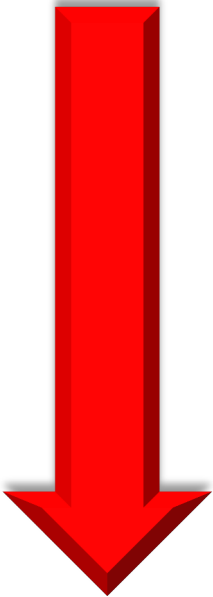
# Studies concerning AI Networking (Chronology)



January, 2015 (announcement)

**Study Group concerning the Vision of the Future Society Brought by Accelerated Advancement of Intelligence in ICT**

June 30, 2015      **Report 2015**



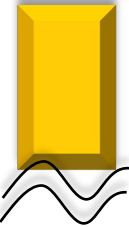
January, 2016 (Announcement)

**Conference on Networking among AIs**

April 15      **Interim Report “Wisdom Network Society (WINS)  
Produced by the Networking among AIs”**

[April 29 and 30      G7 ICT Ministers’ Meeting in Takamatsu, Kagawa]

June 20, 2016      **Report 2016 “Impacts and Risks of AI Networking”**



October, 2016 (Announcement)

**Conference toward AI Network Society**

# AI Networking

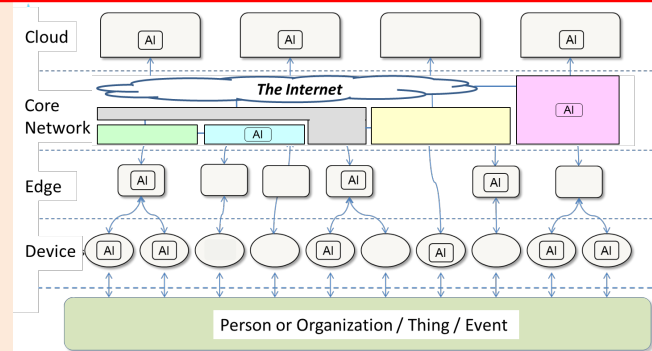
## Stages in progress of the AI Networking

(1) **An AI System would function independently**, via the Internet or other information-and-communications networks, **without collaborating with other AI Systems**.

(2) **Networks of plural Networked AI Systems would be formed** where **plural Networked AI Systems mutually collaborate and cooperate**.

- Various AI Systems with different usage appear on the network
- Multiple AI Systems collaborate and work in harmony with one another
- AI Systems with the function to coordinate multiple AI Systems also appear

AI Systems penetrate in each layer of the networks, and collaborate and cooperate with one another



(3) **Humans' latent capabilities would be augmented by the Networked AI Systems** including sensors or actuators as their components **through linking with humans' bodies or brains**.

- Networked AI Systems incorporating sensors collaborate with human bodies and brains  
-> Improvement in sensory organ capabilities
- Networked AI Systems incorporating actuators collaborate with human bodies and brains  
-> Improvement in human body capabilities

(4) **Humans and Networked AI Systems live symbiotically** and coordinate seamlessly in all kinds of situations in humans' societies.

# G7 ICT Ministers' Meeting in Takamatsu, Kagawa (April 29 & 30, 2016)

Based on discussions of the Conference on Networking among AIs, Ms. Sanae TAKAICHI, Japan's Minister for Internal Affairs and Communications, proposed that G7 countries should take the lead to progress international discussions and considerations toward the formulation of "AI R&D Guidelines," as a non-regulatory and non-binding international framework consisting of the Principles expected to be paid attention to in R&D of AI System to be Networked. The participated countries agreed to her proposal.

\*A tentative proposal on AI R&D Guidelines including eight principles was distributed prior to the proposal from Minister TAKAICHI.



## Proposal of Discussion toward Formulation of AI R&D Guideline

Referring OECD guidelines governing privacy, security, and so on, **it is necessary to begin discussions and considerations toward formulating an international guideline consisting of principles governing R&D of AI to be networked ("AI R&D Guideline")** as framework taken into account of in R&D of AI to be networked.

### Proposed Principles in "AI R&D Guideline"

#### 1. Principle of Transparency

Ensuring the abilities to explain and verify the behaviors of the AI network system

#### 2. Principle of User Assistance

Giving consideration so that the AI network system can assist users and appropriately provide users with opportunities to make choices

#### 3. Principle of Controllability

Ensuring controllability of the AI network system by humans

#### 4. Principle of Security

Ensuring the robustness and dependability of the AI network system

#### 5. Principle of Safety

Giving consideration so that the AI network system will not cause danger to the lives/bodies of users and third parties

#### 6. Principle of Privacy

Giving consideration so that the AI network system will not infringe the privacy of users and third parties

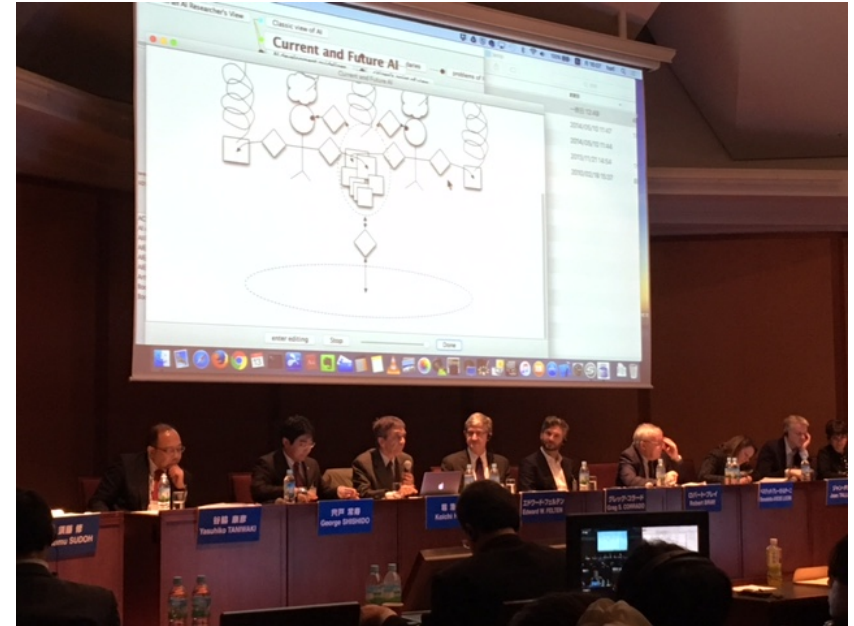
#### 7. Principle of Ethics

Respecting human dignity and individuals' autonomy in conducting research and development of AI to be networked

#### 8. Principle of Accountability

Accomplishing accountability to related stakeholders such as users by researchers/developers of AI to be networked

# International Forum toward AI Network Society (Mar. 13 & 14, 2017, Tokyo)



In the Forum, stakeholders of industry, academia, civil society, and public sector mainly from U.S., EU and its member countries, Japan and OECD exchanged opinions on social, economic, ethical, and legal issues over AI Networking, including the formulation of “AI R&D Guidelines”.

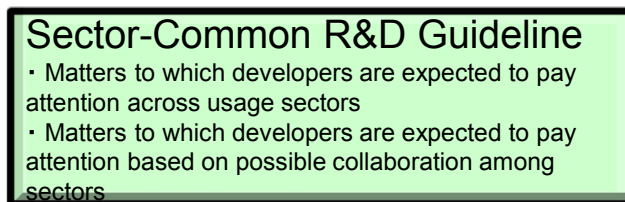
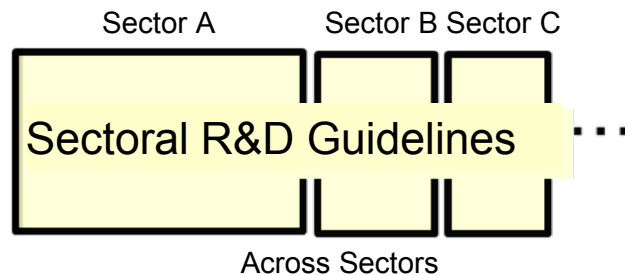
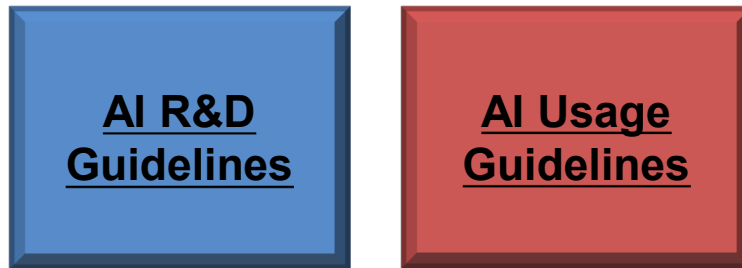
## Main Directions of Consensus through Discussions in the Forum

- Consensus building through global discussions
- Establishment of “Human-centered Society”
- Governance of AI Networking



# Basic Structure of AI R & D Guidelines

It is necessary to form an international consensus on social, economic, ethical, and legal issues over Networked AI Systems through open discussions, and to internationally share guidelines and their best practices among stakeholders as a non-binding soft law.



## Draft of AI R&D Principles

- ① Principle of **Collaboration**
- ② Principle of **Transparency**
- ③ Principle of **Controllability**
- ④ Principle of **Security**
- ⑤ Principle of **Safety**
- ⑥ Principle of **Privacy**
- ⑦ Principle of **Ethics**
- ⑧ Principle of **User Assistance**
- ⑨ Principle of **Accountability**

# Announcement of Next Forum

---

On coming October, the OECD and MIC of Japan will jointly hold international forum on AI.

## 1. Date

26 (Thu) and 27 (Fri) October 2017 (To be determined)

## 2. Venue

OECD, Paris

## 3. Purpose of the Forum

- To exchange views and opinions on benefits and risks of AI as well as social, economic, ethical, and legal issues brought about by AI among OECD member countries
- To introduce draft “AI R&D Guidelines” for international discussion

Thank you for your attention

[s.narihara@soumu.go.jp](mailto:s.narihara@soumu.go.jp)



## Applying New Legal Requirements to Big Data

acxiom. +

Dr.JJ Pan  
Asia Pacific Privacy Officer  
2017/05/11

# Reality.....

- \*Inevitability of Data

- \*Trust Deficit

- \*Accountable & Ethical Use of Data



# ESSENTIAL ELEMENTS OF ACCOUNTABILITY

## Managing Risk and Fairness to ALL Stakeholders

- Corporate commitment to internal policies
- Mechanisms to put those policies into effect
- Internal monitoring to assure mechanisms work
- Individual participation – transparency; consent
- Standing ready to demonstrate to a regulator on request, and remediation where necessary



# Operationalizing Ethical Data Use

## Accountability & Measurement

- **Line of business accountability**
  - Leadership required to be accountable for the operational compliance of their products, solutions, services
- **Individual employee accountability**
  - Achieve excellence - each employee accountable for applying rules, issue spot, report problems
- **Client Credentialing: Legitimate entity, legitimate interests**
  - on-site inspection possible
- **Vendor Screening and Accountability Program**
  - You are your vendor's keeper
- **Privacy Impact Assessment**
  - Understanding and applying the rules to business processes is complex – yet critical
  - Computer Code is the Conduct
- **Assurance Reviews**
  - Fair Information Practices – annually
  - Functional Area/Line of Business Audits

## ACXIOM BEST-IN-CLASS DATA PRIVACY AND SECURITY





THANK YOU

axiom. +

# Closing Remarks

**Bojana Bellamy**

President

Centre for Information Policy Leadership

**Centre for Information Policy Leadership**

[www.informationpolicycentre.com](http://www.informationpolicycentre.com)

**Hunton & Williams Privacy and Information Security Law Blog**

[www.huntonprivacyblog.com](http://www.huntonprivacyblog.com)

**FOLLOW US ON LINKEDIN**

[linkedin.com/company/centre-for-information-policy-leadership](https://linkedin.com/company/centre-for-information-policy-leadership)



**FOLLOW US ON TWITTER**

**@THE\_CIPL**