Privacy in Asia :
Building on the APEC Privacy Principles

Hyun-joon Kwon
Korea Internet & Security Agency
2013. 9. 4

Contents

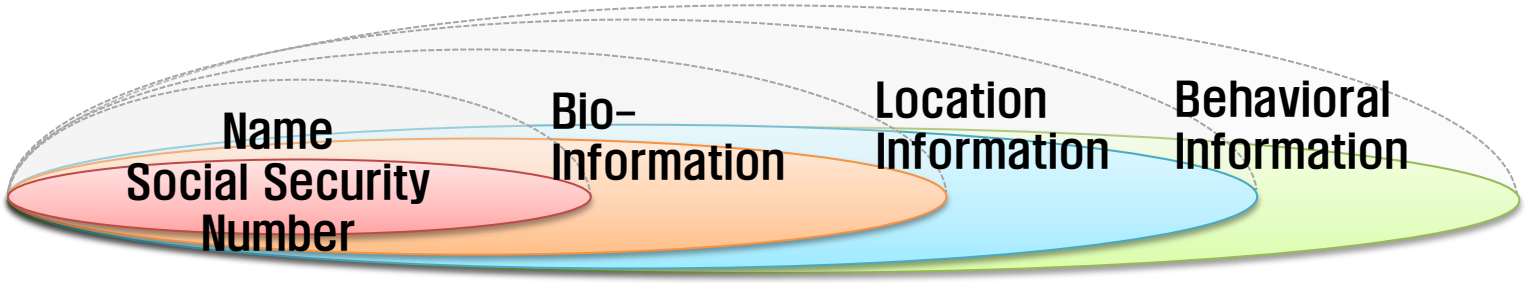
1 PI Protection Framework in Korea

Expansion of the concept of Personal Information

The scope of personal information expands as smart society emerges

– Expands FROM the biographical, physical, economical and social information (typical information)

TO behavior, location, preference, taste information as well as records of visiting website, etc. (atypical information)



Personal Information Flows mostly on Internet

Development of ICT technology – cloud computing, etc. and decrease of the price of H/W

→ Provide environment that can use large amount of personal information with low costs

Expansion of SNS, online community, and blogs

→ rapid increase of kinds and quantity of personal information released online

→ Voluntary disclosure of name, preference, and interest in SNS

(Facebook, Twitter, and etc)

Flow volume of personal information : offline < online

→ Customized services & advertisements based on the analysis of personal information are now a trend of major business models of global Internet enterprises

※ 95% of the sales in Google was from advertisement (refer to Google IR, 2012)

Laws on Personal Information Protection in Korea

Special Law	ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION AND INFORMATION PROTECTION, ETC. ACT ON THE PROTECTION, USE, ETC. OF LOCATION INFORMATION	USE AND PROTECTION OF CREDIT INFORMATION ACT ACT ON REAL NAMES FINANCIAL TRANSACTONS AND CONFIDENTIALITY	MEDICAL SERVICE ACT FRAMEWORK ACT ON HEALTH EXAMINATION ACT ON WELFARE OF PERSONS WITH DISABILITIES	FRAMEWORK ACT ON EDUCATION ELEMENTRARY AND SECONDARY EDUCATION ACT EARLY CHILDHOOD EDUCATION ACT	Many special laws on ..... Passport, Taxation, Police, Customs, Etc. .....
	Personal Information in **ONLINE COMMERCE**	Credit & Financial Information	Health Information	Student Information	
General Law	Personal Information Protection Act				

Government Framework of PI Protection Policy

Korea Communications Commission	Financial Services Commission	Ministry of Health & Welfare	Ministry of Education	.....
Personal Information in Online Commercial Service	Credit, Financial Information	Health Information	Student Information	

Ministry of Security and Public Administration

Coordination & Planning

Definition : Personal Information

ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION AND INFORMATION PROTECTION, ETC. (“Network Act”)

Chapter 1. General Provisions
Article 2. (Definitions)

6. The term **"personal information"** means the information pertaining to an **individual alive**, which contains **information identifying a specific person** with a name, a national identification number, or similar in a form of code, letter, voice, sound, image, or any other form (including information that does not, by itself, make it possible to identify a specific person but that **enables to identify such person easily if combined with another information**);

Personal Information in Network Act

Chapter 1. General Provision
Chapter 2. Promotion of Utilization of Information and Communications Network
Chapter 3. Utilization of Electronic Documents through Electronic Document Relay
Chapter 4. Protection of Personal Information

- Collection, Use, and Provision of Personal Information

- Management and Destruction of Personal Information

- Rights of Users

Chapter 5. Protection of Users in Information and Communications Networks
Chapter 6. Securing of Stability of Information and Communications Networks
Chapter 7. Telecommunications Billing Services
Chapter 8. International Cooperation
- Transborder Data Flows of Personal Information
Chapter 9. Supplementary Provisions
Chapter 10. Penal Provisions
Addenda

Recent Changes of PI in Network Act (1)

By 2014, implement a clean internet environment without RRN

- **After the revised Network Act is enforced, new collection of RRN is prohibited (Article 23-2)**
  ※ Exception: ① Authentication agency, ② Commanded by law, ③ Official notification by KCC
- **Previously collected numbers need to be destroyed within two years of the law's enforcement**
- **If there is a legal basis, limited use and collection will be allowed**

Use an expiration system to minimize unnecessary storage of personal information

- **Take necessary actions such as destroying of personal information of those who have not used the service for a certain period (Article 29)**
  - Personal information expiration: Less than 3 years when the contract between a supplier and a user is concluded
  - Exception to the expiration period: When a special period is defined in another law, and it is unavoidable to fulfill the responsibilities according to the law

Recent Changes of PI in Network Act (2)

Notice use history of PI to guarantee the right of user to make his/her own decisions on PI

- **Notice to data subjects about the use history of their PI periodically (Article 30-2)**

  - **Target: ① Business with more than 1 million average daily visitors in the last three months of the previous year**

    ② ICT business with the revenue of more than 10 Billion won

  - **Types of information to notice**

    · PI collected and used according to the privacy policy

    · A person who is provided with PI, objectives and PI items

    · A person who is consigned handling of PI, objectives of consignment

  - **Notice period and methods: periodic notice at least once a year (e-mail, paper, telephone, transmission, etc.)**

Transborder Data Flows of Personal Information in Network Act (1)

Article 63 (Protection of Personal Information Transferred to Abroad)
(1) Any provider of information and communications services or similar shall **not** execute an international contract **in violation of this Act** with respect to personal information of users.
(2) A provider of information and communications services or similar shall, when it intends to transfer personal information of a user to abroad, **obtain consent of the user.**
(3) A provider of information and communications services or similar who desires to obtain consent under paragraph (2) shall **notify** the relevant user of all the following matters **in advance**:

1. **Items** of the personal information transferred;
2. **The state** to which the personal information is to be transferred, the **date and time** of transfer, and the **method** of transfer;
3. The name of the person to whom the personal information is to be transferred (referring to the name of a legal entity and the **contact information** of the person responsible for management of information, if the person is a legal entity);
4. **The purposes** of use of the person to whom the personal information is to be transferred, and **the period of time** for possession and use of the personal information.

Transborder Data Flows of Personal Information in Network Act (2)

Article 63 (Protection of Personal Information Transferred to Abroad)
(4) A provider of information and communications services or similar shall, when it transfers personal information to abroad with consent under paragraph (2), **take protective measures**, as prescribed by Presidential Decree.

Presidential Decree of Network Act
Article 67 (Protective measures in Transborder data flows of personal information)
(1) In cases where personal information is transferred to abroad in accordance with Act article 63(4), protective measures are all the following:

1. technical and administrative measures for the protection of personal information in accordance with Presidential Decree article 15
2. measures for processing complaints and mediating disputes in connection with the personal information intrusion
3. other necessary measures for the protection of personal information

(2) Any provider of information and communications services or similar shall consult with the person to whom the personal information is to be transferred about all the matters under subparagraphs of paragraph (1), and reflect them in the contract.

Technical and administrative measures for the protection of personal information – **Presidential Decree Art. 15**

Article 15 (protective measures for personal information)

(1) Internal PI management plan.
- CPO, PI processor education, PI management Organization, etc

(2) Measures for unauthorized access control
- Access Control for PI D/B processing system
- Intrusion firewall & Detection System for PI D/B processing system
- Separation internal NW of PI D/B processing system from Internet (only for the entity with one Mil. Users/one day or 10 Bil. Won/1 year)
- password management policy
- other necessary measures for unauthorized access control

(3) Protective measures for forgery of the PI D/B access record and back-up

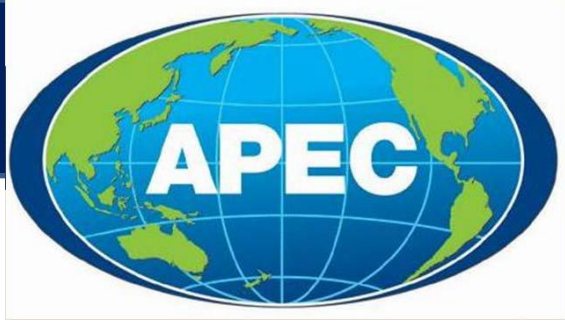
(4) PI data encryption, encryption for transmission, etc.

(5) Necessary measure for computer virus, spyware, etc.

(6) KCC shall provide ministerial ordinance for detailed standards of protective measures

2 Enforcement of CBPRs in Korea

What is APEC?



- Established in 1989 to promote economic growth, cooperation, trade and investment in the Asia-Pacific region

- Comprised of 21 member economies : Australia, Brunei Darussalam, Canada, Chile, People's Republic of China, Hong Kong, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, The Philippines, Russia, Singapore, Chinese Taipei, Thailand, The United States, Viet Nam

- APEC operates on the basis of non-binding commitments, open dialogue and equal respect for the views of all participants.

APEC Privacy Framework

- The Data Privacy Subgroup developed the APEC Privacy Framework in 2004
- The Framework is consistent with the core values of the OECD's 1980 Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data
- The Framework is a set of **nine principles** to assist APEC economies in developing privacy approaches that maximize privacy protection and the continuity of cross-border information flows

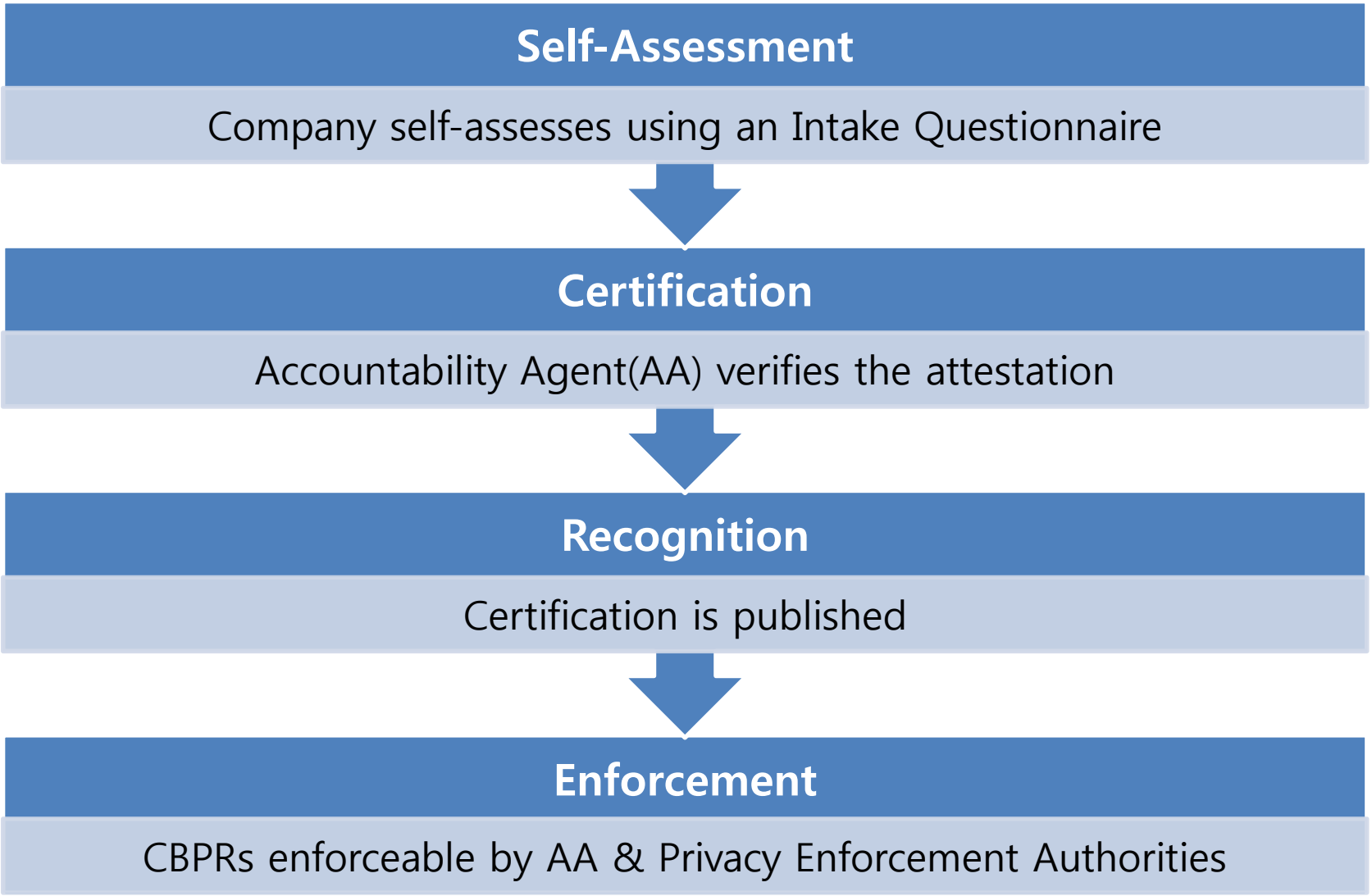
APEC & OECD Principles

APEC (9 Principles)	OECD (8 Principles)
• Preventing Harm	• Collection Limitation
• Notice	• Data Quality
• Collection Limitation	• Purpose Specification
• Use	• Use Limitation
• Choice	• Security Safeguards
• Integrity	• Openness
• Security Safeguards	• Individual Participation
• Access and Correction	• Accountability
• Accountability	

APEC CBPRs

- The Framework states that international implementation of 9 principles may be achieved through Cross Border Privacy Rules (CBPRs)
- CBPRs are a set of voluntary rules developed by an organization and member economies
- The organization then commits to apply these rules to its activities involving transfers of personal information across borders

A Four Step Approach of CBPRs



CBPRs Questionnaire

- Questionnaires assessed by a third party(Accountability Agent)
- Questionnaires consisted with 50 questions
- Questionnaires based on the APEC Privacy Framework
- Questionnaires comprised of several sections, each corresponding to a specific APEC Privacy Principle

Notice	• 4 Questions	Integrity of PI	• 5 Questions
Collection Limitation	• 3 Questions	Security Safeguards	• 10 Questions
Use of PI	• 6 Questions	Access and Correction	• 3 Questions
Choice	• 7 Questions	Accountability	• 12 Questions

Criteria of Accountability Agency

- Conflicts of Interest
- Program Requirements
- Certification Process
- On-going Monitoring and Compliance Review Processes
- Re-Certification and Annual Attestation

Enforcement of APEC CBPRs

- Self-regulatory code(voluntary rules) of conduct backed by government Enforcement
- Companies that want to participate will apply to an APEC recognized trustmark called an “Accountability Agent”
- Using standardized requirements based on the APEC Privacy Framework, the Accountability Agent will review and then certify the company for participation
- Company’s privacy policy will be “APEC Certified”

CBPRs and Domestic Laws

- CBPR System does not displace domestic laws or responsibilities of domestic regulators

- Participation in the CBPR System does not replace organizations' domestic obligations:

  - Organizations continue to be required to comply with legislative requirements

- THE CBPR SYSTEM AND DOMESTIC LAWS AND REGULATIONS -

'The CBPR System does not displace or change an Economy's domestic laws and regulations. Where there are no applicable domestic privacy protection requirements in an Economy, the CBPR System is intended to provide a minimum level of protection.'

From APEC CBPR System – Policies, Rules and Guidelines (11p)

Enforcement of CBPRs in Korea?

- CBPRs is the mechanism which facilitates electronic commerce and protects privacy

- KCC(Korea Communications Commission), taking charge of protection of personal information in Electronic Commerce section, is considering to participate CBPRs

- Before participating CBPRs, experts' opinions about comparative analysis of privacy level between Network Act and CBPRs are required

  ※ Network Act is applied in online commerce and this act is regulated by KCC

Thank you!

olddongja@kisa.or.kr