SUNGKYUNKWAN JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOL.8 Fall 2014 No. 2

For more information, please contact us at :

The Glocal Science & Technology Law Institute, Sungkyunkwan University
53, 3-ga, Myeongnyun-dong, Jongno-gu, Seoul, Korea
Tel : +82-2-760-0767 Website : http://law.skku.edu
Fax : +82-2-760-0846 E-mail : ilhwan@skku.edu

CONTENTS

Symposium

Article

A Study of International Standards on Transborder Flows of Personal Information

IL HWAN KIM*

I. INTRODUCTION

In Europe, Facebook's illegal acts regarding personal information (sales of personal data, collection and storage of deleted data, etc.) have continued to receive criticism, with 22 complaints filed against the social networking site for its violation of regulations protecting personal information. Consequently, authorities in Ireland (where Facebook's European headquarters are located) launched investigations into Facebook Europe's data protection practices, issuing recommendations in October 2011 for Facebook's European head office to correct any services that may cause data protection legal violations. In response, Facebook stated that it would change its privacy policy to strengthen the level of personal data protection and enhance transparency for European users, and agreed to improve its services, by allowing users to disable the facial recognition functions and rein in the collection of data related to non-users.[1]

Since deciding to implement a new privacy policy integrating 60 personal information policies from March 2012, Google also encountered strong opposition from many countries,[2] On February 18, 2013, France's Commission Nationale de l'Informatique et des Libertes (CNIL) announced plans to impose restrictions on Google, saying "We demanded in October last year that Google change its personal data collection policy, which contravenes EU law. Despite giving them four months, the company has not taken any action or provided any answers." The French regulator added, "The data protection agencies of the EU members are scheduled to discuss detailed restriction measures starting next week." The spokesperson for the European Commissioner for Justice, Vivian Redding, told AFP, "A company that provides users with services within the EU member countries must comply with EU data protection law," adding, "It is essential that users be allowed to know how their data are used."[3] Google's privacy policy has stoked controversy over its potential abuse of monopoly position through conduct

* Professor, Sungkyunkwan University School, of Law, Ph.D

[1] Washington Post, Dec. 22, 2011.

[2] The controversy over Google's personal information collection policy began in January of 2012. On January 14 of that year, Google announced it would consolidate the privacy policies of about 60 services, including search, Gmail and YouTube, starting from March 1. In response, the EU demanded that the company delay this integration until an assessment ended, expressing concerns about the abuse of personal data. However, Google proceeded with the consolidation as planned on March 1.

[3] Chosun Il-bo, Feb. 19, 2013.

that infringes the rights and interests of users since the Federal Trade Commission of the United States expressed concerns about the integration of Google's privacy rules.[4]

Similarly, the Korea Communications Commission (KCC) recommended on February 28, 2012 that Google rework its updated Privacy Policy to be presented on March 1, pointing out that the planned update may fall short of meeting the requirements of Korea's Information and Communications Network Act. To this end, Google posted additional information on April 16 for Korean users to help them better understand its privacy policy, including the purposes of use, the types of information it collects, and the use of multiple accounts, etc. However, a comprehensive review by the Personal Information Protection Commission of Korea of Google's Privacy Policy, - that included the KCC's recommendations and Google's subsequent actions, determined that the current Privacy Policy of the Internet search engine was still likely to violate the Personal Information Protection Act and the Information and Communications Network Act of Korea.[5]

Various transnational legal instruments are in place to protect private information. Currently, Europe is at the forefront of global trend-setting in personal information protection-having enacted its comprehensive Data Protection Directive of the EU[6] as early as 1995. The EU Directive generally prohibits the transfer of personal data to any country where the level of data protection is "inadequate." Accordingly, the United States set up the "Safe Harbor Principles (2002)" prescribing when data is protected at a level that matches that of the EU so as to be exempt from the prohibition against personal data transfer prescribed under the EU Directive. Other countries also reflect the content of the Directive when enacting or amending their own personal information protection legislations.Under the current circumstances where personal information protection issues and trade issues are combined, there is a need to review Korea's measures of protecting the rights of data subjects, as personal information transfers are dramatically increasing across national borders.

[4] iNews, Feb. 29, 2012.

[5] The Personal Information Protection Commission of Korea pointed out the following about Google:first, Google states the purpose of personal data processing in an ambiguous and comprehensive manner, and accordingly allows itself to collect and use personal data excessively; second, Google may infringe upon users' right to choose, asking for a comprehensive and unilateral consent on personal data processing through the consolidation of privacy policies; and third, Google does not specify that it would delete the personal data without delay, when requested by a user. Thus, the Personal Information Protection Commission determined that Google's integrated privacy policy is likely to violate Article 3 of the Personal Information Protection Act which prescribes the "clarification of the purpose of personal information processing and minimum collection of personal information," Article 15 and 22 of the Act on "consent in personal data processing" and Article 21 and 36 of the Act which set forth the "destruction of personal information" as well as the Information and Communications Network Act. See the written decision and press release on Google announced on June 12, 2012 by the Personal Information Protection Commission.

[6] "Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data," (hereinafter, the "EU Directive").

II. INTERNATIONAL STANDARDS AND DETAILS ON PERSONAL INFORMATION PROTECTION

A. The United Nations

In the resolution adopted on December 14, 1946, the UN General Assembly resolved, "Freedom of information is a fundamental human right and is the touchstone of all the freedoms to which the United Nations is consecrated; Freedom of information implies the right to gather, transmit and publish news anywhere and everywhere without fetters." This illustrates that the UN, at its earliest stage, emphasized the free flow of information as well as freedom of information as a human right. From the late 1960s or early 1970s, however, the impact of data processing on the right to privacy started to garner attention internationally. In particular, UNESCO has take ninterest in privacy and personal data protection since the 1970s.[7] The concept of "privacy" may be most challenging to define of all the international human rights. The difficulty becomes even greater when the number of theoretical attempts still being conducted to define privacy and and continuous enactment of new laws is recognized. In short, although privacy is clearly established as a fundamental right that needs to be protected, international privacy rules have remained general and abstract.[8] Article 12 of the Universal Declaration of Human Rights of 1948 not only prescribes that privacy must be protected, but includes detailed regulations relevant to the protection of the right to privacy. For example, "the concept of individual privacy has thus been extended to include the kinship 'zone' of the family," expanding the scope of privacy protection to home and correspondence with others.[9]

When discussing protection of personal information, it is worth noting the Guidelines for the Regulation of Computerized Personal Data Files (the "UN Guidelines") adopted by UN General Assembly resolution on December 14, 1990.[10]

The UN Guidelines contain the following principles for the protection of personal data: 1) Principle of Lawfulness and Fairness-Information about persons should be collected or processed in lawful ways and should not be used contrary to the purposes and principles of the Charter of the United Nations; 2) Principle of Accuracy-Persons responsible for the collection or storage of data or those responsible for such should check the personal data on a regular basis to ensure that the data files recorded are accurate; 3) Principle of the Purpose-specification. The purpose for the collection and processing of personal data should be specified and legitimate in order to ensure that: a) All the personal data collected and recorded remain relevant and adequate to the purposes so

[7] James Michael, Privacy and Human Rights, Dartmouth, 1994, Preface.
[8] James Michael, ibid.,p. 1.
[9] James Michael, ibid.,p. 19.
[10] Resolution 45/95.

specified; b) None of the said personal data is used or disclosed, except with the consent of the person concerned; c) The period for which the personal data are kept does not exceed that which would enable the achievement of the purposes so specified; 4) Principle of Interested-person Access-An individual whose information has been collected or recorded has the right to know how information concerning him or her is being processed or used, and multiple rights of protection, such as the right to delete wrong or inaccurate information, should be provided to such an individual; 5) Principle of Non-discrimination-Personal data subjects should not be discriminated arbitrarily due to the difference in religion, race, sex life or political opinions; 6) Power to make Exceptions-Departures from the principles mentioned above may be authorized only if they are necessary to protect national security, public order and the rights and freedoms of others and to track criminals who commit crimes against humanity, provided that the purposes and grounds of such departures are expressly specified in a law or equivalent regulation promulgated legitimately in accordance with the internal legal system; 7) Principle of Security-Appropriate measures should be taken to protect the personal data files against natural dangers, computer viruses, unauthorized access, etc. 8) Supervision and Sanctions-Every country shall establish an independent authority which is to be responsible for supervising observance of the principles set forth above, and should implement penalty regulations and personal protection measures for the event of violation of the aforementioned principles; 9) Transborder Data Flows-When the legislation of two or more countries concerned by a transborder data flow offers comparable safeguards for the protection of privacy, information should be able to circulate as freely as inside each of the territories concerned; and 10) Field of Application. The present principles should be made applicable to all public and private computerized files as well as to manual files.

The UN Guidelines set the minimum standards to guarantee privacy and the human rights of a person who provides his or her own information in a computerized data file, and to help each country reflect these standards in their national legislation. The guidelines also contain principles for data protection prescribed in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (the "OECD Guidelines") and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention No. 108") and, in effect, highlight the aspect of human rights protection. This may be because the guidelines were drafted in 1988 by the United Nations Sub-Commission on the Prevention of Discrimination and the Protection of Minorities, an organization consisting of humanrights experts, that makes recommendations on human rights issues to the UN Commission on Human Rights, as an auxiliary organization of that Commission.[11] Member countries should follow the UN Guidelines when they pass

[11] Gwang Hyun Lee, A Study of International Cooperation for the Protection of Personal Information,

legislation to regulate computerized personal data files, although the UN Guidelines have no binding force. Member countries may refer to the Guidelines and select implementation measures and procedures to suit their own situations.

B. Significance of the OECD Guidelines

It is the Organization for Economic Cooperation and Development (OECD) which first urged its member countries to take legislative measures to reflect the international trend on personal data protection. Since each country regulates and protects personal data in ways suitable to their own situations, the OECD sought to have personal data protection laws adjusted to help facilitate international circulation of personal information. Thus, the OECD initiated its efforts to secure smooth circulation of information among countries, to coordinate the interests of countries and protect personal information.The OECD held an international symposium on transborder data flows and the protection of privacy in Vienna in 1977, where it presented basic guidelines based on the investigation of the practices and problems of personal information protection in transborder data flows.[12]

In 1980, the OECD developed the Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, which was later adopted in September the same year. Though the OECD Guidelines are not legally binding, they contain the shared opinions of the international community in regard to the collection and management of personal information, and prescribe general guidelines that member countries should observe. Reflecting the principles of technology-neutrality to accommodate technological development of the future, the principles are consulted by member countries for national legislation. Discussions were focused on development of technologies and methods that can promote the smooth implementation of such principles on the Internet.[13]

All OECD members, regardless of differences in laws and policies, have a common interest in harmonizing the protection of privacy and individual freedom with free flows of data. Thus, the purpose of the guidelines was to have member countries enact legislation in a way that can accommodate both the demand for personal information protection and the demand for transborder flows of data. Although the OECD Guidelines are not legally binding, they have served as the foundation for many national data protection laws as they contain principles on personal data processing applicable to both

doctoral dissertation at Korea University, 2009, p. 98 and p. 112.

[12] For discussions on transborder flows of personal data until the end of the 1990s, *see* KISA, A Study of Policies on Transborder Flows of Personal Information, 2000.

[13] The Global Privacy Enforcement Network (GPEN) is an international network established in accordance with an OECD recommendation. Member countries of the GPEN share privacy-related issues and experience, and strengthen international cooperation in the protection of personal information.

the public and private sectors and regardless of the type of processing.[14] Since the OECD adopted the OECD Guidelines in 1980, it has also adopted the Guidelines for the Security of Information Systems in 1992, Guidelines for Cryptography Policy in 1997 and Guidelines for the Security of Information Systems and Networks-Towardsa Culture of Security in 2002, (a revised version of the 1992 Guidelines).

C. European Union Data Protection Directive

In July 1990, the Commission of the European Communities (EC) submitted to the Council of the EC the "Commission Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data" for the purpose of protecting personal information within the region and as a result, general rules on the protection of personal data were created.[15] Subsequently, the European Parliament and the Council of the EU commonly adopted the EU Directive setting out the rights and freedoms of individuals as well as the basic principle of the right to privacy set based on the Council of Europe Convention No.108 of 1981. The EU Directive, as a general regulation on personal information handling, aims to protect the basic rights and freedom of the people of member states, safeguard the right to privacy regarding the processing of personal data and promote the free flows of personal data between EU member countries.[16] In addition, as it is applicable to both the public and private sectors, it is more detailed and concrete than the OECD Guidelines and contains strong policies protecting personal information. Directives of the EU are binding on EU member states with direct effect, although the member states have some discretion in their individual implementation.[17]

D. Other Relevant International Organizations and Their Activities

1. The International Working Group on Data Protection in Telecommunications (IWGDPT)

In the IWGDPT, to which Korea holds membership, personal data protection authorities from each country discuss current legislation and technological issues regarding privacy in the field of information and communications, aiming at improving the protection of personal information and privacy in telecommunications and media.[18]

[14] However, Article 3 of the OECD Guidelines allows the exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties; the application, to different categories of personal data, of different protective measures; or the application of the Guidelines only to automatic processing of personal data.

[15] Robert M. Gellman, "Can Privacy Be Regulated Effectively On a National Level? Thoughts on the Possible Need for International Privacy Rules," 41 Vill. L. Rev. 129. 1996. p. 156.

[16] Paul M. Schwartz & Joel R. Reidenberg, Data Privacy Law, MICHIE Law Publishers, 1996, p. 13.

[17] In Hyun Cho, A Study of the Protection of Personal Information in the Constitution, Doctoral dissertation at the Graduate School of Myongji University, 2009, pp. 90-91.

[18] The IWGDPT was founded in 1983 and holds meetings twice a year.

Since its foundation, the IWGDPT has discussed the adequacy of a period of keeping telecommunications data for investigative purposes, a proposal to extend the length of time call history is retained (telecommunications traffic data), and measures to protect privacy in the mobile communications environments (RFID, home network and wireless Internet), etc.[19]

2. The International Conference of Data Protection and Privacy Commissioners (ICDPPC)

(1) Significance of the ICDPPC

The ICDPPC, an association of data protection authorities for the protection of personal information, is an international organization for cooperation aimed at monitoring the personal data protection practices of nations and protecting such data.The ICDPPC was initiated as a conference to exchange information between personal data protection authorities of the EU. Since 2001, however, it has evolved into an international organization (consultative body) as the scope of participation expanded. Personal data-related agencies of more than 80 countries including the UK, Australia and Canada are registered members. The Korea Internet and Security Agency (KISA) obtained full membership at the annual Conference held in Poland in 2004 while the Personal Information Protection Commission of Korea became a full member in 2012.[20]

(2) Major Objectives of the ICDPPC[21]

The ICDPPC is an important forum leading the international community's discussions on the protection of personal information, It's members propose common solutions for issues related to personal data protection. Joining the ICDPPC is a very complicated procedure. According to ICDPPC rules, "The data protection authority must be guaranteed an appropriate degree of autonomy and independence to perform its functions," requiring the authority be empowered, both in a legal and practical fashion, to undertake action independently. The ICDPPC evaluates the data protection authorities of each country, and grants accreditation and membership only to those who qualify. So far, 87 agencies from 54 countries such as the UK (Information Commissioner's Office) and Canada (Office of the Privacy Commissioner) have been accredited by the ICDPPC.

[19] Dal Chun Kang et al, An Analysis of Relief of Privacy-related Damages and Counseling Cases, research material, KISA, 2005, pp. 29-31.

[20] The Personal Information Protection Commission of Korea joined the ICDPPC in 2012 at the ICDPPC conference held in Uruguay from October 22 to 26.

[21] (Visited on Nov. 20, 2013).

<http://www.google.co.kr/url?sa=t&rct=j&q=20080107_oecd_%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8_8%EA%B0%9C%EC%9B%90%EC%B9%99_%EA%B5%AD%EB%82%B4%EB%B2%95&source=web&cd=3&ved=0CDYQFjAC&url=http%3A%2F%2Feyesray.tistory.com%2Fattachment%2Fcfile9.uf%4018306D364DB960791A15C4.pdf&ei=2JwKT9HCN8KHmQXC4PSDAg&usg=AFQjCNGQxGYb43LWpdsVM1bZzm38XtpUTg&cad=rjt>.

Credentials required for accreditation by the ICDPPC are: ①The data protection authority must be a public body established on an appropriate legal basis; ②The standards and procedure under which the authority operates must be compatible with the principal international instruments, such as the OECD Guidelines (1980); ③The authority must have a minimum level of legal powers necessary to perform its functions, such as the right to request data submission, conduct investigations and demand the implementation of laws (rights to redress and accuse). In addition, the authority should perform the following major missions; ④provide public agencies or private businesses with legal advice; ⑤handle privacy-related issues; ⑥have functions to monitor whether public agencies and private businesses comply with laws regarding the protection of personal data; ⑦offer education and promotion on the protection of personal information; and ⑧engage in international cooperation in regard to transborder flows of data.[22]

(3) Activities of the ICDPPC[23]

As a forum for data protection authorities, the ICDPPC determines the necessary credentials for personal data protection agencies and grants accreditation to those which have such credentials. It continues to work for protection of personal information, proposing resolutions on related global issues and holding regular meetings every September.

During the September 2005 meeting in Montreux, Switzerland, ICDPPC adopted a declaration and three resolutions with particular significance for international cooperative efforts to protect private data. In the Montreux Declaration, the Commissioners appeal to the UN and every government in the world, respectively, to prepare a legal binding instrument to promote universal recognition of the importance of personal data protection, and to promote the adoption of legal and institutional instruments that can effectively protect personal data of their peoples according to the basic principles of data protection.The Resolution on the Use of Personal Data for Political Communication states that data subjects should be granted right of access, and the right not to receive messages, etc., and that adequate remedies and sanctions should be provided in case those rights are breached. The Resolution on the use of biometrics in passports, identity cards and travel documentssuggests three principles, mentioning the reality where biometric data are utilized widely in the public and private sectors for the

[22] Visited on Nov. 20, 2013.
<http://www.google.co.kr/url?sa=t&rct=j&q=20080107_oecd_%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8_8%EA%B0%9C%EC%9B%90%EC%B9%99_%EA%B5%AD%EB%82%B4%EB%B2%95&source=web&cd=3&ved=0CDYQFjAC&url=http%3A%2F%2Feyesray.tistory.com%2Fattachment%2Fcfile9.uf%4018306D364DB960791A15C4.pdf&ei=2JwKT9HCN8KHmQXC4PSDAg&usg=AFQjCNGQxGYb43LWpdsVM1bZzm38XtpUTg&cad=rjt>.

[23] Dal Chun Kang et al, op. cit., p. 28.

purposes of fighting terrorism, etc.[24]

3. Asia-Pacific Economic Cooperation (APEC)

(1) Significance of APEC

Asia-Pacific Economic Cooperation (APEC) is a regional forum promoting economic growth of all member states by strengthening economic and technical cooperation between countries located in the Asia Pacific region. It is a gathering for discussions and identifying measures related to a wide range of issues that Pacific Rim member countries are faced with, including promotion of electronic commerce, counter-terrorism, and prevention of infectious diseases. Member states take individual or collective action to open their markets and facilitate economic growth, which are then discussed in a series of Senior Officials Meetings (SOM) and the summit meetings. APEC working-level activities and projects are managed by APEC senior officials and executed by four major committees-the Committee on Trade and Investment, the SOM Steering Committee on Economic and Technical Cooperation, the Economic Committee, and the Budget and Management Committee. Sub-committees, expert groups, task groups and special project teams act on behalf of these four major committees. The Electronic Commerce Steering Group (ECSG), in particular, is an APEC Senior Official's Special Task Force, which promotes electronic commerce within the APEC region.[25]

(2) Development of the APEC Privacy Framework (APF)

APEC member economies shared the view that the active electronic commerce within the region requires consumer confidence and trust in the privacy and security of online transactions and information networks. Thus, members naturally reached agreement on the need for efforts to develop and implement technologies and policies which help bolster consumer trust and the growth of e-commerce. One of the efforts is to strike a balance between effective protection of data privacy and the free flow of information. APEC developed the APEC Privacy Framework (APF), aiming to enhance consumer confidence through appropriate protection of personal information, and promote electronic commerce through the building of such trust.[26]

After several members agreed to develop an APEC privacy recommendation based on the findings of a privacy policy survey conducted on APEC members by the United States in August 2002. the seventh APEC ECSG meeting in 2003 formed a privacy subgroup to push ahead the establishment of an APEC privacy guideline. Consisting of a total of nine countries, including Korea, the United States, Australia, Japan, China, Hong

[24] Dal Chun Kang et al, op. cit., pp. 28-29.

[25] Soon Jung Byun, The Trend of APEC ECSG Discussions on the Protection of Personal Information-Based on the Establishment of the APEC Privacy Framework -, KISA, June 2006, pp. 1-3.

[26] *See* KISA, A Study of Impacts of APEC CBPRs on Korea, 2007.

Kong, Canada and Thailand, the subgroup developed the APF based on a draft he eight principles prescribed in the OECD Guidelines, after gathering the opinions of each member state by email, phone, and related seminars. It then submitted the APF to the APEC Ministers' Meeting (October 2004) and had it finally approved and adopted in November 2004.

4. Asia Pacific Privacy Authorities (APPA)

(1) Significance of the APPA

The Asia Pacific Privacy Authorities (APPA) Forum is a new name for the Privacy Agencies of New Zealand and Australia Plus Hong Kong and Korea (PANZA+). Originally, PANZA+ was an extended version of PANZA with the increased participation of Hong Kong and Korea. In the 24th PANZA+ Forum in 2005, however, members agreed to change the forum's name to the APPA, aiming to extend the forum's scope to the Asia Pacific region, as they believed that "+" was an inappropriate way to refer to Hong Kong and Korea.[27]

(2) Activities of the APPA

During the 24th Forum (2005), participants discussed the draft of the APPA Statement of Objectives developed by the Privacy Commissioner of New Zealand. It also agreed that any Asia Pacific country, with an already-established privacy-related authority, such as the Privacy Commissioner, or which had plans to implement privacy legislation or an authority, would be eligible for membership in the APPA. However, discussions on such issues as whether to allow participation of non-Asia Pacific countries(for example, those located in South America), the necessary credentials for APPA participant authorities, how to apply for participation, and the scope of participant countries were left to the following APPA meeting.[28]

In Korea, the KCC and KISA hosted the 29th APPA Forum in June 2008 with "Internet Trust & Privacy" as its theme. Members in the 31st APPA Forum in Hong Kong in June 2009 shared their privacy-related legislation, technological trends and business cases and discussed major privacy issues.[29]

[27] Dal Chun Kang et al, op. cit., pp. 29-30.

[28] Dal Chun Kang et al, op. cit., pp. 29-30.

[29] Dong Wook Kim, The Study of Internet Governance Structure and Policy Guideline, Research Report,Vol. 09-69, Korea Information Society Development Institute, Nov. 2009, p. 86.

III. STANDARDS ON TRANSBORDER FLOWS OF PERSONAL DATA FROM THE PERSPECTIVE OF COMPARATIVE LAW

A. Overview: Establishing a Global Standard for the Combination of Personal Data Protection and Trade Barrier Issues

Among international guidelines on the protection of personal information, the OECD Guidelines (1980) and its eight principles are the most important. Currently, Europe is leading the trend of data protection globally, and in particular, the EU Directive is regarded as most crucial. Considering data protection a part of human rights protection, not a sub-standard of consumer protection or electronic commerce, the EU prohibits the transfer of personal data to countries whose level of data protection is deemed inadequate. In response, and as mentioned previously, the United States established the "Safe Harbor Principles (2002)" to match the level of data protection of the EU and is exempted from restrictions, such as the aforementioned prohibition of transborder flow of personal data. The EU Directive also serves as reference for other countries when they enact or revise their own data protection legislation.

B. Relevant Details in the OECD Privacy Protection Guidelines

It was the OECD which demanded its member states take legislative measures, such as guidelines, in response to the international trend of personal data protection. The OECD Guidelines represent the international community's agreement on the collection and management of personal data, despite not being legally binding. The Guidelines set forth principles that are technology-neutral enough to accommodate technological development in the future. They also provide important guidance for member countries in taking steps to see these principles appropriately implemented in their territories. Discussions concentrate on the technologies and methods through which the principles can be implemented smoothly on the Internet.[30]

The Preface to the OECD Guidelines points out that due to the development of automatic data processing, the issue of privacy protection in relation to personal data has reached a serious level, mentioning that most of the OECD members have introduced or will introduce privacy protection laws. It also raises a necessity "to develop Guidelines which would help to harmonize national privacy legislation and, while upholding such human rights, would at the same time prevent interruptions in international flows of data," because "disparities in national legislations could hamper the free flow of personal data across frontiers."

[30] In regard to this, *see* KISA, Discussions and Proposal for Enforcement of Privacy Laws of OECD Countries, 2006.

The OECD Guidelines set forth basic principles of international application about free flow and legitimate restrictions.[31] Pursuant to the principles: ①Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data; ②Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data are uninterrupted and secure; ③A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection; ④ Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.[32]

C. The EU and the Council of Europe

1. Relevant Details in the EU Directive

(1) Major Details of the EU Directive

The objectives of the EU Directive are to "protect the fundamental rights and freedoms of natural persons" and "their right to privacy with respect to the processing of personal data" (Article 1(1)) and to "neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1" (Article1(2)). As such, the EU Directive calls for the harmonization and balance of personal data protection and transborder flows of personal data, as Article 1(1) prescribes the protection of privacy in relation to personal data while Article 1(2) provides that members should not restrict nor prohibit transborder flows of personal data between member countries.[33]

Chapter II, which covers Articles 5 to 21, prescribes general rules on personal data processing: first, personal data must be collected and processed for specified, explicit and legitimate purposes; second, personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; third, personal data must be processed fairly, and the data subject must be provided precise and

[31] GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, KISA, 2005, p. 4.

[32] For more details, *see* KISA, A Study of Measures of Legislative Amendments in regard to Transborder Flows of Personal Information, 2012, pp. 18et ss.

[33] Tae Hyun Kim, A Constitutional Review of Personal Data Protection Policies, Doctoral dissertation at the Graduate School of Kyung Hee University, 2003, pp. 103-104.

sufficient information regarding the collection of the relevant data; and fourth, personal data must be processed pursuant to the data subject's will, and if not for lawful purposes, in accordance with specified legal provisions.

In addition, personal data must be kept up to date, when such data is required to be adequate, relevant and accurate having regard to the purposes for which they were collected and reprocessed, and every reasonable step must be taken to ensure that data which were inaccurate or incomplete at the time of collection are erased or rectified. If it is necessary for the purposes for which data are collected, data must be kept in a form which does not permit identification of the data subject. Member States should lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

(2) Transfer of Personal Data to Third Countries[34]

Chapter IV, which covers Articles 25 and 26, sets forth provisions on transfer of personal data to third countries. In accordance with the provisions, the Member States shall provide that the transfer of personal data to a third country may take place without prejudice to compliance with the national provisions, and the third country in question shall ensure an adequate level of protection. In addition, the adequacy of the level of protection afforded by a third country shall be assessed and notified to the member states, and a transfer of personal data to a country which does not ensure an adequate level of protection matching that of the EU is prohibited. The adequacy of the level of protection afforded by a third country must be assessed in the light of all the relevant circumstances before a data transfer. Particular consideration shall be given to the nature of the data, the duration of the proposed processing operation or operations, the data providing country, and legal environments and privacy policies of the data receiving country. The Commission shall inform other Member States of cases where it considers that a third

[34] Article 26 of theEU Directive: "1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on the following conditions: 2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses. 3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2. If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2). Member States shall take the necessary measures to comply with the Commission's decision. 4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision."

country does not ensure an adequate level of protection, and the Member States shall take the measures necessary to prevent any transfer of data to the third country in question.

However, Member States shall provide that a transfer of personal data to a third country which does not ensure an adequate level of protection may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer;

(b) the transfer is necessary for the performance of a contract between the data subject and the controller;

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party;

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims;

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

These provisions illustrate that data transfer is allowed only when a non-European third country implements an adequate level of personal data protection with exceptions as described in (a) to (f) above. Thus, the third country in question should have in place professional rules and security measures to ensure that the purposes and features for which personal data are collected and used as well as the rules of law, both general and sectoral, are complied with at an adequate level of protection.[35]

Therefore, among the provisions under the EU Directive, those on data transfer to third countries are most problematic in the transactions with non-European regions, including the United States. It is because the EU Directive may hamper electronic commerce, if based on the European recognition that "the U.S.'s level of personal data protection falls short" of the standard required by Europe.

[35] For more details, see Gyu Chul Im, Personal Data Protection of the EU, Asia-Pacific Public Law Review, Issue No. 11, 2003, pp. 219et ss.

(3) Trends in Amendment of the EU's Legal Framework on Data Protection

(a) Amendment Direction and Features

The EU has protected personal data, mainly based on the EU Directive (Directive 95/46/EC)[36] and the "Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector" (Directive 2002/58/EC)[37] adopted in 1995 and 2002, respectively. The EU Directive, in particular, adopts an extended scope of application, by defining personal data as "any information relating to an identified or identifiable natural person" and having the Directive applied to all types of personal data processing, "whether or not by automatic means."[38] In addition, the EU Directive prescribes not only a high level of detailed requirements for the legitimacy of personal data processing but multiple principles for transfer of personal data to third countries, including an adequate level of protection. Thus, the Directive, as an important reference material and standard, has exerted great influence on the member countries as well as other states, especially those in trade relations with EU members, in cases where they enact or amend their national laws on data protection.

Under the legislative system of the EU, however, a directive is not directly applicable in member states but provides a basic framework which each member state should observe in their legislation of domestic laws.[39] Therefore, a directive is implemented by a national law enacted by each member country which may choose its own details and form of the directive suitable to its national situation. This was the case for the EU Directive of 1995, when it was implemented within the member states. Thus, as to the EU Directive, it became necessary to prepare data protection legislation that applies consistently within the EU, strengthens the enforcement system, develops new principles and standards for personal data protection as the digital and trade environments change, and improves the procedure under which personal data is transferred.

[36] Directive of the European Parliament and of the Council on the Protection of Individuals with Regards to the Processing of Personal Data and the Free Movement of Such Data.

[37] Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector.

[38] Article2 (a) , 2 (b) and Article 3 (1) of the EU Directive of 1995.

[39] Pursuant to Articles 288 to 291 of the Treaty on the Functioning of the European Union (TFEU), legal acts of the EU are divided largely into legislative acts and non-legislative acts. Regulations, directives or decisions adopted in accordance with the legislative procedure prescribed in Article 289 of the TFEU shall constitute legislative acts, while other legal acts, such as recommendations, opinions, delegated acts or implementing acts shall constitute non-legislative acts. Among legislative acts, a directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods (Article 288 TFEU). For legal acts of the EU, *see* Hyung Bok Chae, Legal Acts in the Lisbon Treaty and the Reform of the Enactment Procedure, World Constitutional Law Review, Vol. 16, Issue No. 3, 2010, pp. 909 et ss.

Against this backdrop, there had been discussions on revising the EU Directive since 2009. In the process, the Commission announced on November 4, 2010 a strategy to revise the EU Directive to strengthen personal data protection and guarantee free flows of personal data. And in January 25, 2012, presented the Proposal for a Regulation of the European Parliamentandof the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data[40] ("EU General Data Protection Regulation").

The EU General Data Protection Regulation would replace the EU Directive[41] if it is adopted as planned in 2014[42] by the European Parliament and the Council of Ministers. As a regulation, the EU General Data Protection Regulation, if ratified, will be directly and comprehensively applicable in all member countries[43] (even without a measure to convert it into national law).

Other than the difference inform as a regulation, the EU General Data Protection Regulation is sharply distinguished from the EU Directive in comprehensive character: Through a massive amount of provisions constituting 11 Chapters and 91 Articles, it sets out the principles related to personal data processing, *Inter alia*, it provides that personal data must be processed in a transparent manner in relation to the data subject and under the responsibility and liability of the controller or processor and must be limited to the minimum necessary in relation to the purposes for which they are processed; it strengthens and elaborates on the data subject's rights, prepares various means to promote the exercise of those rights, and reinforces the duties of the controller; it more clearly prescribes the Commission's right to decide an adequate level of protection regarding the transfer of personal data; and it suggests and provides very detailed standards for the independence and rights of supervisory authorities.[44]

(b) Details of the Amendments to Provisions on Transfer of Personal Data to Third Countries

Any transfer of personal data which is undergoing processing or is intended for

[40] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

[41] Article 88 (1) of the EU General Data Protection Regulation.

[42] Article 91 of the EU General Data Protection Regulation (Entry into force and application)

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

2. It shall apply from [*two years from the date referred to in paragraph 1*].

[43] Article 288 of the TFEU prescribes as follows: "A regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States."

[44] *See* Il Hwan Kim and Seok Han Hong, A Study on the EU's Enforcement Frameworks on Personal Data Protection, SungKyunKwan Law Review, Vol. 24, Issue No. 4, December 31, 2012, p. 9- ; In SeonHaam, A Study of the EU's Legislations on Personal Data Protection, The Justice, Vol. 133, 2012, pp. 5 et ss.

processing after transfer to a third country or to an international organization may only take place if the conditions laid down in the EU General Data Protection Regulation are complied with by the controller and processor. A transfer may take place where the Commission has decided that the third country or the international organization in question ensures an adequate level of protection, and such transfer shall not require any further authorization. When assessing the adequacy of the level of protection, the Commission shall give consideration to the following elements:

① the rule of law, relevant legislation in force, both general and sectoral; the existence and effective functioning of one or more independent supervisory authorities in the third country or international organization in question responsible for ensuring compliance with the data protection rules, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Union and of Member States; and

② the international commitments the third country or international organization in question has entered into.

The Commission may decide that a third country or an international organization fails to ensure an adequate level of protection, in particular in cases where the relevant legislation, in force in the third country or international organization, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred. In the event, any transfer of personal data to the third country or the international organization in question shall be prohibited. The Commission shall publish in the Official Journal of the European Uniona list of those third countries and international organizations where it has decided that an adequate level of protection is or is not ensured.[45]

2. Related Details in Personal Data Protection Principles of the Council of Europe Convention No.108

The contracting parties to Convention No.108 should take necessary measures to ensure that their domestic laws follow the principles prescribed in the Convention in regard to personal data of every person in their own territories. Such principles set out in the Convention deal with fair and lawful collection and automatic processing of personal data, storage of data for specified and legitimate purposes and prohibition on use in a way incompatible with those purposes and preservation for no longer than is required. In

[45] KISA, op. cit., pp. 31-32, supra note 31; In SeonHaam, op. cit., pp. 17-18.

addition, these principles also set forth the quality of data which shall be adequate, relevant, accurate and not excessive; confidentiality of sensitive data; information of the data subject and the guarantee of rights to access and rectify such data. Convention No. 108 has provisions on the free flow of personal data between the parties to the Convention. Transborder flows of personal data should not be interrupted simply in the interest of personal data protection, unless the following exceptions occur, as outlined in Convention No.108: (a) when the protection of personal data by the other Party is not at an equivalent level; (b) when personal data is transferred to the territory of a non-Contracting State, not to a Contracting State. Prescribed as basic principles for data protection by Convention No. 108, the substantive law regulations are the common key principles that are most pivotal in the Convention. Each party should ensure that these principles are implemented through their own domestic laws. The principles aim to guarantee minimum protection for data subjects in all contracting parties, in regard to automatic processing of personal data. The application of those principles allows transborder flows of data between parties to the Convention and prevents free flow of personal data across borders from being hampered. Furthermore, such application can ultimately harmonize domestic laws of the contracting parties and consequently lessen the possibility of conflict of domestic laws and jurisdictions.[46]

3. Related Issue: U.S.-EU Safe Harbor Framework

As illustrated above, the EU Directive generally prohibits any transfer of personal data to a country which does not ensure an "adequate" level of protection. It was likely that the EU could restrict the movement of personal data to the U.S. as its data protection regulations do not meet the "adequacy" standard required by the EU Directive. Therefore, through two years of negotiations, the U.S. and the EU agreed on the Safe Harbor Framework on July 27, 2000. The number of companies participating in the Safe Harbor program increased from about 40 in 2001 to 194 in May 2002 and 310 in March 2003.[47] The Safe Harbor principles provide the followings regarding protection of personal information: ①Notice; ②Choice; ③Onward Transfer; ④Security; ⑤Data Integrity; ⑥Access; and ⑦Enforcement.[48] As measures for the U.S. Department of Commerce to satisfy the EU Directive's "adequacy" requirement in regard to transfer of personal data to a third country, the Safe Harbor principles were proposed to maintain the existing system where personal data protection is left to regulation by sector and self-regulation, and to set a new standard for personal data protection, without amending domestic laws. There are fundamental differences between the U.S. and the EU in their approaches to privacy protection: the U.S. supports the industries in their voluntary

[46] Gwang Hyun Lee, op. cit., pp. 128et ss.

[47] US Department of Commerce webpage. www.commerce.gov.

[48] For more details, seeLegislative Information & Digital Library Management Office of the National Assembly, Overview of the U.S.-EU Safe Harbor Framework, National Assembly Library, 2000.

establishment of personal data protection policies,[49] whereas the EU takes an aggressive approach, actively intervening in the data protection by personal data controllers.[50] Thus, believing that these differences could cause trade conflicts and hamper transborder transactions of personal data, the U.S. sought to resolve the issues through negotiations with the EU. In accordance with the Safe Harbor Framework, if organizations or related companies in the U.S. report to the U.S. Department of Commerce their plans to comply with the Safe Harbor principles and receive the department's renewable certification, they are regarded as having taken adequate steps to protect data and allowed to receive data transferred from EU countries. The decision by businesses or organizations to join the Safe Harbor program is not mandatory but voluntary.[51]

IV. CONCLUSION

As personal data is transferred to other nations, multi(supra)-national companies and global business operators such as Facebook and Google, there is a need for measures to protect the right of data subjects to make decisions on their own personal information to avoid cases where such rightsare infringed upon. In other words, additional protection mechanisms are necessary in today's information society, where personal data is transferred or processed globally.

Personal data is transferred across borders by global or multinational companies and also in accordance with various trade agreements. It is increasingly likely that such data can be obtained through security breaches outside the country, making it important to conduct fact-finding surveys to prevent the personal information of Koreans from being leaked overseas through hacking, etc. Measures need to be taken to protect personal information against unauthorized transborder flows by new technologies (including cloud computing and RFID), to monitor and respond to data leakage overseas and security breaches, to amend relevant laws and regulations such as security guidelines, and to build a coordinated system with international organizations.

Global business operators need to be monitored for compliance with the Personal Information Protection Act of Korea and related laws when they transfer personal data outside Korea. It is necessary to ensure that academics, industries and

[49] *See* Il Hwan Kim, A Critical Review of the Roles and Rights of Privacy-related Authorities of the U.S., Studies on American Constitution,Vol. 22, Issue No. 3, 2011, pp. 40et ss.

[50] Hwa Soon Cho, Global Governance in Cyber Space, The Korean Journal of International Studies,Vol. 46, Issue No. 1, pp. 179 et ss.

[51] The U.S. responded to the Safe Harbor Framework, as the Department of Commerce publicly announced the principles and relevant FAQs on November 4, 1998. The purpose was to provide a clear framework for the protection of personal information by reducing ambiguity in terms of data transfer, promote international commercial transactions andmaintain and guarantee the "adequacy" by managing the Safe Harbor in an adequate condition.

specializedinstitutions review on a regular basis the risks of transborder flows of personal information in order to improve the level of data protection amidst the changes in global environments and the evolution of services. Appropriate regulatory frameworks are also needed, through revision of laws and regulations on the collection and use of personal information in the process of using global services, and guidelines provided. Last but not least, it is essential to review whether the Personal Information Protection Commission of Korea, an external independent organization, or other related state agencies appropriately supervise global companies and their compliance with Korean laws.

KEYWORDS

Transborder Flows, Right to Privacy, Personal Data Protection, OECD Privacy Protection Guidelines, Safe Habor Framework

Manuscript Submitted on Nov 5, 2014
Review Begun on Nov 10, 2014
Accepted for Publication on Dec 10, 2014

Personal Information Protection and its Enforcement Mechanism in Japan

Hiroshi Miyashita*

I. INTRODUCTION

The Japanese privacy protection regime may be described as spaghetti with its twisted and complicated mechanism. This may be because privacy is not a product of logic or theory but a reflection of social norms and culture on privacy. The right to privacy has been regarded as a privilege of the Western concept, which later extended to the East.

When the right to privacy invented by Samuel Warren and Louis Brandeis, NitobeInazo pointed out the differences of privacy cultures between Japan and the U.S; "American husbands kiss their wives in public and beat them in private; Japanese husbands beat theirs in public and kiss them in private."[1]

One cannot learn accurately the Japanese privacyprotection regime without taking into the cultural aspects of privacy account when particularly compared with the Western legal systems. As I will show some examples, privacy as a cultural value has a vital force in Japan, though the scope of this article is limited and narrow because of my focus on the existing Acts and its implementation.[2] Firstly, I will introduce the basic legal regime on the protection of personal information in Japan. Secondly, I will illustrate some distinctive aspects of the Japanese enforcement. And finally, I will examine the current status of the Act and underlying challenges under the Japanese privacy laws.

II. LEGAL REGIME OF PERSONAL INFORMATION PROTECTION

A. Privacy Laws

1. Main Acts

The legal regime of personal information protection is not simple. There are 3 main Acts on the Protection of Personal Information for private sectors and public sectors.

* Associate Professor of Law, Faculty of Policy Studies, Chuo University.

[1] INAZONITOBE, BUSHIDO, THE SOUL OF JAPAN: BUSHIDO (Shokwabo; Tokyo 1900).

[2] I have written more dynamic analysis on the Japanese privacy developments. See Hiroshi Miyashita, The Evolving Concept of Data Privacy in Japanese Law, 1 INTERNATIONAL DATA PRIVACY LAW, p. 229 (2011).

The Act on the Protection of Personal Information (hereafter "Basic Act") in 2003 covers the general policies and the private sectors.[3] Cabinet Office used to have coordinated powers, but after September 2009, newly established Consumer Affairs Agency is now in charge of the Basic Act.

The Act on the Protection Personal Information Held by Administrative Organs and the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies both covers the public sectors (hereafter "Public Sector Acts").[4] The former Act held by Administrative Organs renewed the original Act on the Protection of Personal Information Pertaining to Electronic Data Processing Held by Administrative Organs in 1988. Ministry of Internal Affairs and Communications has responsibility of Public Sector Acts.

2. Supplementary Acts

In addition to these three main Acts, the Act on Establishment of the Information Disclosure and Personal Information Protection Review Board provides the procedures of investigations upon request from objector by the Review Board. The Act on the Preparation for Related Acts for the Enforcement of the Act concerning the Protection of Personal Information Held by Administrative Organs prescribes the amendments of related administrative laws. The total 5 Acts on the protection of personal informationenacted on May 30, 2003. The main 3 Acts have only minor amendments after their enactments.

3. Cabinet Order and Cabinet Decision

The important legal documents are Cabinet Order No. 506 & 507 and Basic Policy by the Cabinet Decision. The Cabinet Order is the supplementary explanations for the Basic Act enacted on December 2003, and partially amended in 2008.[5] Basic Policy on the Protection of Personal Information based on the Basic Act in 2004 (partial amendments in 2008 and 2009) is the comprehensive direction of the protection of personal information by the government, the local governments and the business.[6]

4. Guidelines

In practice, the most important instrument is the guidelines set by each Ministry.

[3] English translation is available from http://www.caa.go.jp/seikatsu/kojin/foreign/act.pdf (last visited March 1, 2014).

[4] English translation on the Act held by administrative organs is available from http://www.japaneselawtranslation.go.jp/law/detail/?vm=04&re=01&id=131 (last visited March 1, 2014). There are 44 administrative organs and 206 incorporated administrative agencies as of March 2013.

[5] English translation on Cabinet Order No 506 & 507 is available from http://www.caa.go.jp/seikatsu/kojin/foreign/cabinet-order.pdf (last visited March 1, 2014).

[6] English translation on Basic Policy is available from http://www.caa.go.jp/seikatsu/kojin/foreign/basic-policy-tentver.pdf (last visited March 1, 2014).

As of October 2013, there are 40 guidelines in 27 different business sectors.[7] Data controllers and processors are supposed to follow the guidelines based on the specific business sector (e.g. University must observe the guidelines on the educational sector) because, as discussed later, each Ministry has enforcement powers.

5. ID Number Act

Most recently, the Act on the use of numbers to identify the specific individuals in the administrative procedures, known as ID Number Act or My Number Act (hereafter "ID Number Act"), was passed in the Diet on May 24, 2013 in order to promote administrative efficiency in the identification numbers on social security and taxation.[8] This ID Number Act is the special law of the Basic Act and the Public Sector Acts.

6. Ordinance

In addition to these national levels, every local government (1,719 as of January 2014) has its ordinance of the protection of personal information.

As you may realize, it is not easy for the beginners to understand the picture of the legal regime of the protection of personal information in Japan. Yet, both in reality and theory, the Basic Act is the most fundamental source of the privacy regime in Japan, on which this article focuses.

B. Overview

1. Purpose and basic philosophy

The Japanese privacy regime is firmly rooted in OECD privacy guidelines in 1980. Though the Act is clearly based on OECD privacy guidelines, there is no word of "privacy" in laws. Instead, the purpose of the Basic Act is "to protect the rights and interests of individuals while taking consideration of the usefulness of personal information." This purpose embodies the ideal of the Constitution that "All of the people shall be respected as individuals" (Art. 13).[9] One can recognize this context in the Basic Act which provides "personal information should be handled cautiously under the philosophy of respecting the personalities of individuals" (Art. 3).

[7] English translation on Guidelines Targeting Economic and Industrial Sectors Pertaining to the Act on the Protection of Personal Information by Ministry of Economy, Trade and Industry is available from http://www.meti.go.jp/policy/it_policy/privacy/0910english.pdf (last visited March 1, 2014).

[8] English information is available from http://www.cas.go.jp/jp/seisaku/bangoseido/english.html (last visited March 1, 2014). See also Hiroshi Miyashita, Japan appoints new independent commission for the supervision of ID numbers, Privacy Laws & Business International Reports, Vol. 127, pp. 10-12 (2014).

[9] "All of the people shall be respected as individuals. Their right to life, liberty, and the pursuit of happiness shall, to the extent that it does not interfere with the public welfare, be the supreme consideration in legislation and in other governmental affairs." (Article 13, The Constitution of Japan)

Although the Act did not mention to the right to privacy, the Supreme Court, passive to use the right to privacy, frequently protected the right to privacy as a part of the right to personality from the "the legal protection or right not to disclose private life without good reason"[10] to "the freedom not to disclose and not to be made public one's personal information to a third party without good reason."[11]

2. Exemptions

Along with the purely private use of personal data by the individuals, the Cabinet Order exempts the small business, namely business which processed no more than 5,000 personal data in the past 6 months, from the obligations in the Act. Yet, the fundamental philosophy of Article 3 always applies to every individual and one can seek the remedy by judicial branch even in data breach cases by small enterprises.

Full exemptions apply to the constitutional privileges such as mass media for news, writers for writings, academic institutions for academic research, religious organizations for religious activities, and political organizations for political activities (Art. 35& 50).

3. Scope

The Acts provide the concept of personal information as "information about a living individual which can identify the specific individual by name, date of birth or other description contained in such information" (Art. 2). There is no specific categories of sensitive data in the Acts, which can be often seen in the ordinances. Yet, the Act requires the special treatment to some personal information (Art. 6) and the Basic Policy assigns medical, financial and credit, telecommunications as this special treatment.

4. Obligations

Every 8 basic principle is provided in the Basic Act as well as the Public Sectors Act;Use Limitation Principle&Purpose Specification Principle (Art. 15, 16 & 23), Collection Limitation Principle (Art. 17), Data Quality Principle (Art. 19), Security Safeguards Principle (Art. 20, 21 & 22), Openness Principle&Individual Participation Principle (Art. 18, 24, 25, 26 & 27), Accountability Principle (Art. 31).

[10] Judgment of Tokyo District Court on September 28, 1964, HanreiJiho Vol. 385, p.12 ("After the Banquet" case).

[11] Judgment of the Supreme Court on March 6, 2008, Minshu Vol. 62 No. 3, p. 665 ("Juki-Net" Case). This decision is not understood as admission of the right to control one' personal information according to the law clerk (chosakan) explanations. *See* Tamami Masumori, EXPLANATIONS ON THE SUPREME COURT CASES IN 2008, p.141 [増森珠美『最高裁判所判例解説民事篇平成20年度』]On the contrary, since 1970s, most of the constitutional scholars defended the right to control one's personal information. *See e.g.*, Koji Sato, *The Constitutional Position on Privacy-A Comparative Studyof Japan and the United States*, HogakuRonso vol. 86 No. 5 p. 12 (1970). [佐藤幸治『プライバシーの権利(その公法的側面)の憲法論的考察』]

5. Rights and interest

Most controversial provisions of the Basic Act is the right to disclose, correct and delete of data subject because the Act intentionally did not use "right" in its language. In the draft of the Act, the authors excluded the "right" from the Basic Act (Article 25-27), but put "right" in the Public Sectors Act (Article 12, 27 & 36). This is because the human rights can be exercised only against the public intrusions so that it is no longer the human rights issues in the disputes between private parties.[12] As the original intent, the Basic Act uses "request" (motome), not "right" (kenri) in the private disputes. The controversial lower court decision did not admit the right to disclosure of the data subject due to the linguistic difference between the Basic Act and the Public Sector Acts and the enforcement mechanism.[13] Yet, it is appropriate to understand that this decision was wrong in reading the original intent of the Act, which substantially embraces the right of data subject.[14]

The right to erasure in an internet era is more controversial as to whether the embarrassing posts of one's past events can be erased or not. The lower court started to examine the search engine cases; on 15 April 2013, Tokyo District Court ordered Google to delete suggested terms which associate a plaintiff with crime. The court held that "Google libels the plaintiff and invades his privacy by suggesting search terms." In addition, the court pointed out "the plaintiff suffers damage of defamation and privacy infringement because of the increased number of searches on the Internet."[15] In conclusion, the court admitted the injunction and awarded 300,000 yen as compensation for damage. On the other hand, on 30 May 2013, in a similar case, another bench of the Tokyo District Court did not admit the right to erase personal information on the search engine, saying that "the contents of the webpage from the results of the search engine does not constitute defamation and privacy infringement on socially accepted grounds."[16] Both cases brought to the higher courts.[17] The right to be forgotten in the Internet era can also be traced back to the famous decision of 1994 where the Supreme Court of Japan

[12] The Supreme Court held the view that the Constitution does not directly apply to the privacy parties, but the general regulations in Civil Code may solve in certain context. *See* Judgment of Supreme Court on December 12, 1973, Minshu Vol. 27 No 11, p. 1536 (Mitsubishi Jushi Case).

[13] Judgment of Tokyo District Court on June 27, 2007, HanreiJiho Vol. 1978 No. 27.

[14] *See e.g.*, ITSUOSONOBE ET. AL., EXPLANATIONS ON THE PROTECTION OF PERSONAL INFORMATION, p.168 (2005 revised edition) [園部逸夫編『個人情報保護法の解説〔改訂版〕』]; SHIZUO FUJIWARA, DETAILS ON THE ACT ON THE PROTECTION OF PERSONAL INFORMATION 98 (2003) [藤原静雄『逐条個人情報保護』]; KatsuyaUga, Recent Case Analysis ([2008]13), HanreiJiho Vol. 1990, p. 164 (2008) [宇賀克也「最新判例批評」]. On the contrary, there are negative views on admitting "right" of data subject under Article 25.

[15] Unpublished decision. *See* Asahi Newspaper, April 16, 2013, p. 38.

[16] Unpublished decision. *See* Asahi Newspaper, May 31, 2013, p. 37.

[17] The case of admitting erasure was revised by the Tokyo Court of Appeal on January 15, 2014 (unpublished decision). *See* Asahi Newspaper, January 16, 2014, p. 33.

held that one's embarrassing past, including facts relating to criminal record, could not be in public if the legal interest of not being publicized outweighed the public interest.[18] The Court took into account the person's later life as well as the historical and social importance of the event, the significance of the parties, and the meaning of using the person's real name.

6. Data transfer

Data transfer to the thirdcountry is not provided in the Act. Yet, commonly used Article 23 of the Basic Act prohibits data transfer without consent of the data subject except for 4 cases such as the cases necessary to protect life, body or property, or necessary for public health and sound growth of children.

7. Enforcement

As I will examine later, the most distinctive aspect of the Japanese legal regime is enforcement mechanism. There is no independent supervisory authority except for the ID Number Act, and, instead, the competent Minister system was adopted for the Basic Act. Data subject has multiple channels to make complaints of data breach cases through the data controller (Art. 31), authorized personal information protection organization (Art. 42), National Consumer Affairs Center (Basic Policy), or local governments (Art. 13).

The penalty of the data breach is maximum 6-month prison or 300,000 yen fine in private sectors and 2-year prison or 1,000,000 yen fine in public sectors. Since the ID numbers deal with sensitive information on social security and taxation, the law sets maximum 4-year prison or 2,000,000 yen fine.

C. Implementation Status

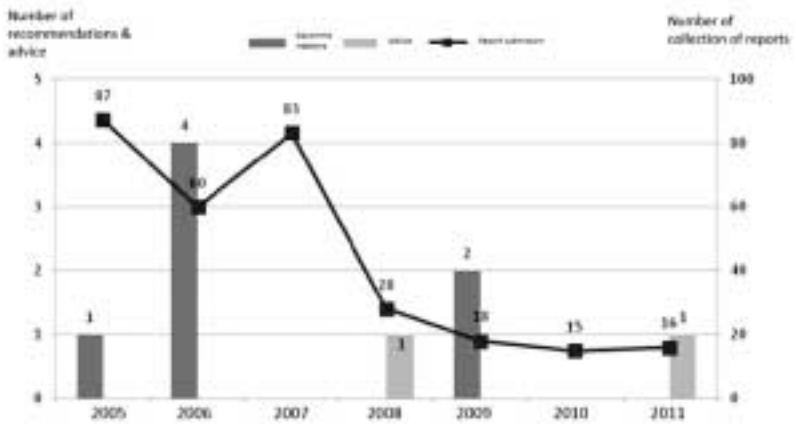
Data breach cases are almost always on the media and reputational damage is the most significant impact for business and public institutions. In private sector, 319 data breach cases were reported to Consumer Affairs Agency from each Ministry in FY 2012.[19] The number of data breach cases has decreased from 1,556 when the Act put into effect in 2005. Most of the cases are relatively small data breach incidents (67 percent of the cases are leakage of no more than 500 persons), but most of the relevant companies notified the incidents to the data subject (82 percent of the cases were reported to the data subjects). National Consumer Affairs Center and the local governments dealt with 5,623 cases of complaints including mediation (174 cases).

[18] Judgment of the Supreme Court on February 8, 1994. Minshu Vol. 48 No 2, p. 149.

[19] Consumer Affairs Agency, Implementation Status of the Protection of Personal Information in FY 2012, September 2013 [消費者庁「平成24年度個人情報の保護に関する法律施行状況の概要」]. Only Japanese version is available from http://www.caa.go.jp/seikatsu/kojin/24-sekou_3.pdf (last visited March 1, 2014).

In private sector, each Ministry enforces its guidelines in its business sector under the coordination of Consumer Affairs Agency (e.g. Financial Services Agency enforces law in the case of bank data breach). Each Ministry has power to collect reports (Art. 32), to make advice (Art. 33), to recommend and order (Art. 34).

In FY 2012, there were 8 cases of collection of reports on incidents by Financial Services Agency (7 cases) and Ministry of Economy, Trade, and Industry (1 case). As the graph shows, since 2005 when the Act put into effect, there is no case of criminal penalty nor order issued by Ministry. This was because business which had data breach incidents followed the instructions by Ministry so that there was no further order and penalty.



In public sector, there was 818 data breach cases in Administrative Organs and 1,816 cases in the Incorporated Administrative Agencies. Just mishandling of letters and faxes are more than half (54.6 percent) in Administrative Organs and loss or mishandling of letters is the biggest cause of the incidents (67.1 percent) in Incorporated Administrative Agencies. From 2005 to 2012, the number of data breach is rather increasing from 320 to 818 in Administrative Organs and from 885 to 1,816 in Incorporated Administrative Agencies. This is because mailing incidents and human error do occur in dealing personal information. After these incidents and error, it is important to notify the breach to the data subjects in many of the cases by Administrative Organs (61.1 percent) and Incorporated Administrative Agencies (96.6 percent) in FY 2012. There was 1 criminal prosecution on the case of National Tax Administration Agency in FY 2012.

Apart from the data breach cases, data subject requested disclosure and correction of their personal files in more than 111,000 cases by Administrative Organs and more than 7,900 cases by Incorporated Administrative Agencies in FY 2012. Data subject can object to the decision on disclosure, correction or deletion by each Ministry to ask review by the committee of Review Board which consists of 15 independent commissioners, approved by the Diet, with 3 sections (281 objection cases in FY2012). Judicial remedies are also available for data subjects. These decisions vary from the request of record on

entrance examination and bar examination to access to personal data held by self-defense force or prison.[20]

III. ENFORCEMENT MECHANISM OF PERSONAL INFORMATION PROTECTION

A. Soft Power Enforcement

Japan is understood as having "one of the weakest data privacy laws in Asia"[21] because of no independent enforcement authority. This evaluation may be true on the surface of the text of the Acts. It is also true that independent supervisory authorities in European countries have been playing crucially important role in enforcement of data protection laws. Yet, it is not appropriate to say that enforcement is not effective just because of no independent supervisory authority. One should carefully observe the enforcement mechanism with social norms and cultural value of privacy and its consequences.

It is widely understood that the risk of loss of social trust and business reputational damage is regarded as much more significant than paying a fine.[22] In addition the risk of reputational damage, the business often cares about the stock market after the data breach incidents. One example is Sony PlayStation Network security breach case where 77 million users around the world faced the risk of identity theft and fraud in April 2011. Firstly, Sony made public apologies at press conference and in their homepage. Secondly, Sony voluntarily gave users the free downloads of certain contents and free services of Play Station Plus for 30 days without any orders from Ministry or courts. These measures can be regarded as regaining the social trust and reputation of Sony from users and society. The consequence of this incident is not sanction by Ministry; instead Ministry of Economy, Trade, and Industry, after investigation, just pointed out the late submission of the report on security breach to the Ministry and asked improvement of security measures as the administrative instruction based on the Basic Act.[23] Without penalty by the Ministry, Sony lost 4 percent interest in the stock market just one night as the consequence of security breach.[24]

[20] Database of findings of the Review Board and decisions by the courts in Japanese are available from http://koukai-hogo-db.soumu.go.jp/.

[21] Graham Greenleaf, *Independence of Data Privacy Authorities (Part Ⅱ): Asia-Pacific Experience*, 28 Computer Law & Security Review, p. 121, 126 (2012).

[22] Miyashita, *supra note* 2, at 233. *See also* the recent empirical study on the importance of trustworthiness and reputation, YohkoOrito, Kiyoshi Murata &YasunoriFukuta, *Do Online Privacy Policies and Seals Affect Corporate Trustworthiness and Reputation?*, 19 INTERNATIONAL REVIEW OF INFORMATION ETHICS, p. 52(2013).

[23] Ministry of Economy, Trade and Industry, Instruction based on the Act of the Protection of Personal Information against Sony Computer Entertainment, May 27, 2013.

[24] Nikkei Newspaper, April 28, 2011, p. 11.

To add a few more examples, there are the security breach case by the local bank where the president of the bank resigned without any penalties but recommendation by Financial Services Agencies[25] and the voluntary compensations cases where the securities sent 10,000 yen gift cards for 50,000 customers with apologies due to the selling of personal information by the former employee[26] and the insurance company paid the total 500,000,000 yen as compensation for leaking estimated 32,000 personal information.[27] These business practices can be seen before the Act was implemented; Yahoo BB sent 500 yen gift cards because of leakage of personal information of more than 4,500,000 users in 2004.[28] Throughout the practices of data breach cases, it is difficult to deny that soft power enforcement mechanism as social norms and cultural value of protection of personal information has been working and functioning well in Japan.

One can learn the different attitude of law enforcement if compared with the UK case where Information Commissioner Office fined £250,000 monetary penalty to Sony in the same case.[29] These differences are not all-or-nothing and both soft power and hard power are compatible. The key is which types of enforcement may be effective for the certain society consistent with the certain social norms and cultural value of privacy. Therefore it may be wrong to say that hard power enforcement by the independent supervisory authority is the only source to measure the effectiveness of enforcement.

B. Trustmarks

Another feature of soft power mechanism in Japan represents trustmarks. Japan Information Processing Development Cooperation (hereafter "JIPDEC"), an authorized organization by Ministry of Economy, Trade and Industry and Ministry of Internal Affairs and Communications, has been operating trustmark known as "PrivacyMark" since April 1998.[30] As of March 2014, more than 13,000 companies are certified by PrivacyMark. The goal of PrivacyMark system is to enhance consumer awareness and to promote the proper handling of personal information. Its fee depends on the size of business from 300,000 yen to 1,200,000 yen and the additional fee for renewal of the 2 year effective period. Good motivation for the companies lies in a de facto condition to

[25] Financial Services Agency, *Administrative Decision on Michinoku Bank*, May 20, 2005. *See also* Nikkei Newspaper, April 23, 2005, p. 39.

[26] Financial Services Agency, *Administrative Decision on Mitsubishi UFJ Securities*, June 25, 2009. *See also* Nikkei Newspaper, May 20, 2009, p. 4.

[27] Financial Services Agency, *Administrative Decision on Alico Japan*, February 24, 2010. *See also* Nikkei Newspaper, October 7, 2009, p. 4.

[28] The court also took into account the voluntary compensations and deducted its amount from the total compensation. Judgment of Osaka District Court on May 19, 2006, HanreiJiho Vol. 1948, p. 122.

[29] Information Commissioner Office, Sony fined £250,000 after millions of UK gamers' details compromised, January 24, 2013. Available from http://ico.org.uk/news/latest_news/2013/ico-news-release-2013 (last visited March 1, 2014).

[30] English information is available from http://privacymark.org/index.html (last visited March 1, 2014).

tender the government contract in order to secure the level of protection of personal information. Accredited companies must notify the data breach cases to JIPDEC. Revocation process was discussed when the printing company which leaked 8,640,000 personal information in March 2007, which finally notified improvement request to the company.[31] No other serious revocation case was publicized so far. Again, trustmark is self-regulation, it does work because of the risk of reputational damage and social distrust in the case of misuse.

Trustmark scheme draws attention outside Japan in data transfer. JIPDEC launched mutual recognition between Korean Association for ICT Promotion and Dalian Software Industry Association (54 mutual recognition as of June 2010). In fact, 29.7 percent of the Japanese companies have practice of data exchanges with foreign entities, and nearly half of the companies (49.4 percent) indicated the need of regulations on data transfer and outsourcing.[32] APEC (Asia-Pacific Economic Cooperation) has been seeking the Cross-Border Privacy Rules, where Japan formally expressed participation in June 2013 by making use of trustmark experiences. And TRUSTe also was recognized as Accountability Agent in this cross-border rules so that trustmark scheme is likely to be a promising bridge in APEC regions. Furthermore, EU is interested in trustmark as the Proposed Regulation of EU Data Protection clearly included privacy seal and certification.[33] Article 29 Working Party of Data Protection also joined APEC meetings to seek interoperability between APEC and EU in the future.

C. Authorized Organizations

The third characteristics of the Japanese enforcement mechanism is the authorized personal information protection organizations (Art. 37). 39 organizations are authorized by different Ministries as of October 2013 based on the criteria of appropriate operation, technical knowledge and fair mind (Art. 39). The authorized organizations is to support the autonomous effort of handling personal information properly and to make public their guidelines. The authorized organizations have the delegated powers from the Ministers to investigate, collect reports and issue recommendations and orders. In FY 2012, the authorized organizations resolved the 613 complaints, collected 28 reports, and issued 116 instructions and 2 recommendations.[34] These numbers are even higher than

[31] JIPDEC, Decision of "Request" to Dai Nippon Printing Co. in the Data Breach Case, March 23, 2007 [日本情報処理開発協会「個人情報保護の事故で大日本印刷株式会社に『要請』処分」]. This decision indicated revocation if the company did not follow the requested measures.

[32] Consumer Affairs Agency, Study on the Implementation Status of Businesses on the Protection of Personal Information, March 2012 at 110 & 112. [消費者庁「個人情報の保護に関する事業者の取組実態調査(平成23年度)」]

[33] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and the Free Movement of Such Data, January 25, 2012, Art. 39.

[34] Consumer Affairs Agency, supra note 19, at 13.

those by competent Ministers, and thus the role of the authorized organizations is very important under the Japanese enforcement mechanism.

IV. LAW REFORM: BIG DATA AND INTERNATIONAL HARMONIZATION

A. Law reform

Since the Acts on the protection of personal information put into effect, there were 3 major chances to discuss amendments of the existing laws. Firstly, in June 2007, the Quality-of-Life Policy Council discussed major issues relating to the Act and decided not to amend it on 29 June 2007; this opinion was then submitted to the Prime Minister.[35] At that time, the major topic of the review was what was called "overreaction," meaning the excessive protection of personal information. For example, cases were reported in which local governments did not release personal information following an earthquake even when this was necessary so that efficient assistance could be given to the elderly and the disabled. The Act explicitly admits information sharing in the necessity of protection of life, body and property of person. Thus, the government decided not to change the Act itself because of misunderstanding of the law. Instead, the government amended the Basic Policy and Cabinet Order to address "overreaction" issues.

Next chance to discuss the possible amendments to the Acts came in 2011. Consumer Commission after the Act was transferred from the Cabinet Office to Consumer Affairs Agency had a discussion on the current status of the Act. The Special Committee on the Protection of Personal Information Report, submitted to the Consumer Commission, presented the important issues, but turned out to be the need of further discussions without any amendments.[36] The report touched the controversial characteristics of the right to disclosure, correction and deletion and the establishment of the independent supervisory authority, but did not reach the final conclusion.

Finally, the head of IT Strategy within the Cabinet, on 20 December 2013, approved the "Plan to Review the System on the Use of Personal Data" to reform the Basic Act. It aims to submit the amendments to the Diet in 2015, for the first time after the Act was enacted. The reform plan includes the establishment of an independent supervisory authority for theentire subject taking into account the functions of the existing competent Minister system and the Special Personal Information Protection Commission for the ID numbers. This reform plan, though very quick and short schedule, will hopefully be

[35] Quality-of-Life Policy Council, Summary of Opinions on the Protection of Personal Information, June 29, 2007. [国民生活審議会「個人情報保護に関する取りまとめ」]English translation is available from http://www.caa.go.jp/seikatsu/kojin/opinion.pdf (last visited March 1, 2014).

[36] Consumer Commission, Special Committee on the Protection of Personal Information Report, July 2011. [消費者委員会「個人情報保護専門調査会報告書」] Only Japanese version is available from http://www.cao.go.jp/consumer/iinkai/2011/067/doc/067_110826_shiryou3.pdf (last visited March 1, 2014).

based on the basic philosophy of the right to privacy as fundamental right along with the international trends.

B. International Harmonization

Privacy is local, but information flow is global. The task of privacy regulations is more and more difficult. Yet, it is impossible or meaningless just to adjust the languages of the privacy laws, which may be consistent with the Western models. This is because privacy is not just the legal product but a kind of social ideals. One can not ignore the cultural value of privacy, and Japan clearly faced this challenges of cultural differences of privacy.

On the other hand, some of the scholars understand the necessity of international harmonization of privacy laws. Professor Masao Horibe pointed out that it is difficult to get them to understand the Japanese legal regime in the international fora due to the cultural differences, but the Japanese government must take seriously the continual examination of international harmonization, particularly in the face of EU Data Protection Directive.[37] He also implied that the current Japanese data protection regime might not necessarily ensure "an adequate level of protection" under Article 25 of EU Data Protection Directive.[38]

Japan participated OECD, APEC, APPA and Privacy Commissioners' meetings to have dialogue with foreign privacy officers, and most recently, the Japanese delegates attended the ad hoc meeting on Convention 108 of Council of Europe. Many businesses are interested in the developments of EU Data Protection Reform. Some Ministries have studied the Asian legal developments in Korea, Taiwan, Singapore, Malaysia, Thailand and Philippine.

Cultural differences on privacy is not the excuse for non-compliance of international standards. Rather, it is the source of experimentation toward best privacy protection and each region may be laboratories of privacy ideals. Louis Brandeis, the founding father of the right to privacy, insisted that "state may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country."[39] The laboratory of privacy protection may also be enhanced as long as the regional or national experimentations work and function. Sharing best practices from the

[37] Masao Horibe, *International Harmonization of Privacy and the Protection of Personal Information*, in NEW CHALLENGES ON PRIVACY AND THE PROTECTION OF PERSONAL INFORMATION 29 (Masao Horibe ed., 2010). [堀部政男「プライバシー・個人情報保護の国際的整合性」堀部政男編『プライバシー・個人情報保護の新課題』]

[38] Masao Horibe, *Worldwide Developments of Discussion on Privacy and Personal Information Protection and Japan*, Joho-Shori Vol.54 No.11, p. 1113 (2013). [堀部政男「プライバシー・個人情報保護論議の世界的展開と日本」]

[39] *New State Ice Co. v. Liebmann*, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting).

laboratories is the real promotion of the international standards of privacy protection. "To stay experimentation in things social and economicis a grave responsibility."[40]

KEYWORDS

Personal Information Protection, Enforcement Mechanism, Privacy, ID Number, Soft Power

Manuscript Submitted on Oct 20, 2014
Review Begun on Nov 10, 2014
Accepted for Publication on Dec 10, 2014

[40] *Id.*

ICT Policy and Legal Is.sues to International Collaboration & ICT Development in Bangladesh

Khaled Mahmud*
Dr. Md. MahbubulAlamJoarde**

ABSTRACT

Information and communications technologies (ICT) enable individuals and business to engage in continuous transactions through successful communications. Progress of ICT opens the door of immense global opportunities as well as gives rise to varieties of legal and regulatory issues.The issues range from the validity of electronic contracts and security to concerns over cyber fraud and wrong use of intellectual property rights. Running business in this global market, there has to have some common ground or standards where both other parties, especially countries can agree on. The promotion of harmonized law reforms would quicken sound development of e-Commerce and ensure consumer protection beyond boundaries is a way to address the issues. This paper is the first one in the series of four studies. It focuses on why and what is required to form harmonized ICT policy in Bangladesh. This study also tried to capture Bangladeshi citizen's perspective on ICT policy need. As a developing country, Bangladesh has progressed a lot and there is a long path ahead. Adoption and proper utilization of ICT policy will lead to increased returns and quality production.Through international collaboration of ICT policy, e-business can be properly managed and mainstreamed into a significant contributor to GDP.

I. INTRODUCTION

Available ICT infrastructures together with government's willingness to implement e-governance & building infrastructure have already brought success in IT initiatives across the industrialized world.[1] Some developing countries have taken steps in this regard. They often fall short of expectations in improving their governance structure and relevant outcomes. In this regard, a number of barriers exist that need to be understood and tackled by developing countries. These include, lack of ICT resources and infrastructure such as high-speed broadband network connections, unequal access to

* Assistant Professor, Institute of Business Administration, University of Dhaka.
** Professor,Institute of Information Technology, University of Dhaka.

[1] Robins, G., & J. Burn. Recreating government through effective knowledge management. In B. Schmid, K. Stanoevska-Slabeva, & V. Tschammer (Eds.), *Towards the E-society: E-Commerce, E-Business, and E-Government*. Kluwer Academic Publishers, 2001 London.

technology (named as 'digital divide'[2]), corruption and the lack of government policy initiatives. Oftenthe lack of resources and technology is compounded by a lack of access to expertise and information.[3] A strong political will and commitment, reflected in a country's politico-legal structure, are in the core of combating these barriers and achieving success. Together with other laws of the land, the presence of a well-orchestrated IT Act could provide the necessary foundation and benchmark in this regard and facilitate the smooth functioning of a country's ICT sector.

As a least developed but emerging economy, Bangladesh has always facing challenges to work on policy formulation. Tainted by political division and bureaucratic democracy, it has been a difficult task for the government of Bangladesh to put the country on the right development path.[4] However, the country has been endeavoring to implement useful ICT policies in recent years to improve its current administrative practices and to establish a better relationship and transparency between the government and its various stakeholders.[5] In order to achieve this objective, the government formulated its ICT policy in 2002 and passed ICT Act in 2006.[6]

This paper attempts to identify issues relevant to the use of ICT and e-government in Bangladesh. The next section highlights the discussion on the legal aspects of the use of ICT. The paper also focuses on the importance of ICT policy and what should ICT policy makers keep in mind while forming and reforming ICT Act. The paper ends with concluding remarks and recommendations.

II. PROSPECTS OF ICT IN BANGLADESH

It is a fact that ICT not only as a sector can contribute immensely to the national GDP of a nation but also it can act as an enabler for other sectors, which can contribute immensely in improving market competitiveness globally. Proper ICT policy can impact positively on governance and other sectors of the economy. At the same time, it can effectively assist international economic integration, narrow the digital divide, and even improve biodiversity.

[2] EszterHargittai. The Digital Divide and What to do about it. Book chapter from New Economy Handbook, published by San Diego, CA: Academic Press 2003. Retrieved on August 13, 2014 from http://www.eszter.com/research/pubs/hargittai-digitaldivide.pdf

[3] PCIP (Pacific Council on International Policy). Roadmap for e-government in the developing world: 10 questions e-government leaders should ask themselves. Pacific Council on International Policy, 2002, Los Angeles.

[4] Jamil, I. Administrative culture in Bangladesh: Tensions between tradition and modernity. *International Review of Sociology*, 12(1), 2002, pp. 93-125.

[5] MOSICT (Ministry of Science and ICT). E-governance activities 2006. Retrieved June10, 2006, from http://www.mosict.gov.bd/what_new.htm

[6] Parveen, K. Computer based crime: A new legal challenge in Bangladesh. The Daily Star. 2006, April 22. Retrieved September 10, 2006, from http://www.thedailystar.net/law/2006/04/03/indepth.htm

The digital divide, which is characterized by uneven access to and use of ICT, both at national and international levels needs to be tackled. Through effective utilization of ICTs in education, industry and agriculture, digital divide can be narrowed and eventually it can reduce poverty nationwide.[7] Success of ICT demands a business environment that can ensures fair competition, trust, interoperability, security, and enough infrastructural resources. In order to achieve full benefit of ICT, sustainable measures need to be taken to improve access to the Internet nationwide, expand telecommunications infrastructure and develop local Internet-based content to increase e-literacy. Like most developing and underdeveloped countries, Bangladesh still depends on content developed and managed by the developed world. It results in substantial costs as citizens of Bangladesh try to access e-contents.

There is no doubt that one of the leading causes that deter access to e-information is culture and language hurdle. Encouragement and enthusiasm should be poured to make ICTs available in Bengali. Local content development and encouraging national ICT policy can play a vital role in this regard.[8]

ICT policy goals in Bangladesh can be such that it ensures an encouraging environment of international collaboration of services. Ease of e-commerce and trade programs for goods and services needs to be promoted. At the same time, Bangladesh should ensure mass Internet access to digital contents, if necessary through providing subsidies. Promotion of e-government,[9] e-education, strong network security, and overall developing an e-society should get prime focus.

III. METHODOLOGY

The paper depicts an exploratory study to find out the initial environment of ICT in Bangladesh. There was no extensive work in this sector and the field is growing fast internationally; the authors explored and used published articles in this field to formulate the recipe in Bangladeshi context.

This qualitative study also includes few interviews with government officials and industry experts to dig deep about ICT policy issue requirement.

[7] Kundishora, S. M. The Role of Information and Communication Technology (ICT) in Enhancing Local Economic Development and Poverty Reduction. Retrieved from http://siteresources.worldbank.org/CMUDLP/Resources/Role_ICT_paper.pdf on July 18, 2014.

[8] As Saber, Srivastava&Hossain, Information technology law and e-government: A developing country perspective, *JOAAG*, 2006, Vol. 1. No.1.

[9] Young Suh, S. Promoting Citizen Participation in e-Government <From the Korean Experience in e-Participation>. Retrieved from http://unpan1.un.org/intradoc/groups/public/documents/un/unpan020076.pdf on July 28, 2014.

IV. ICT POLICY OBJECTIVES

Policy is very crucial and important as it acts as guideline for business home and abroad for local companies. The policy needs to address economic development and business issues. The objective is to provide strategic direction for sustainable national development and international collaboration through the systematic application of ICT policies. Following objectives may guide crafting successful policy:

- To ensure provision to maintain the infrastructural facilities required for ICT development. Reliable and continuous supply of electricity and telecommunications is included.
- To support systematic and sustainable development of ICT across the nation.
- To encourage extensive training programs to create adequate supply of qualified ICT personnel in all sectors.
- To establish useful structures/ boards for effective implementation of ICT policies.
- To promote standard institutional mechanisms and processes for business and international collaboration.
- To encourage the development and use of ICT access across gender, different age groups, different level of education and different occupation.

V. ICT LEGAL AND POLICY ISSUES

ICT enables individuals and businesses to communicate and transact with each other irrespective of time and place. But, this opportunity also gives rise to a variety of legal and regulatory issues. Security and privacy issues are among few of them. There are concerns about cybercrime and intellectual property rights. This paper examines ICT legal issues into few distinct areas. The main areas are given below:

- Legal infrastructure : It focuses on some of the key legal and regulatory enablers for e-commerce. It addresses issues related to 'technology neutrality' to regulatory structures and market liberalization.
- Legal environment : It inspects the legal situation of electronic communications and forms of contracting. It specifically focuses on the need to explicitly recognition of the validity and enforceability of electronic means of executing legal acts.
- Legal security : It examines the security risks intrinsic in any electronic

environment, especially the use of digital signatures and online certificates.

- Legal safeguard : It reviews intellectual property rights and its protection in an online environment. At the same time, it includes consumer protection issues as well.
- Legal restriction : It scrutinizes the growth of cybercrime and the regulatory approaches to stop such harmful conducts. It also ensures that law enforcements are capable of investigating and prosecuting offenders.

A. Legal Infrastructure for ICT

Economic development of Bangladesh is dependent heavily on having appropriate infrastructure to facilitate ICT development. The legal and regulatory framework of Bangladesh ICT policy should review the following three areas for advancement of international collaboration and progress.

1. Legal Principles

Technology neutrality[10] is the leading regulatory principle now a day. Policymakers in different countries have made reference to this concept. The business environment is moving too rapidly. The principle has been used in two key ideas. One of the key idea is that which is regulated offline should be regulated online as well. Another idea is about its treatment. There is a need to treat different technologies similarly to the extent that they have the same effect.[11]

2. Regulatory structures for ICT actors

Effective regulatory institutions require adequate expertise and useful resources, which Bangladesh may find difficult to support. To address such barriers, capacity building in the regulatory field is must. It includes training and exchange programs with developed nation regulatory institutions time to time. However, such formal institutions can also be supported by non-public sector entities both business and society.

3. Harmonizing ICT Policies

In our global information economy, law reforms with the frameworks of other countries are very necessary. Without harmony in ICT policy, Bangladesh may find it a significant barrier to economic development. Bangladesh might be concerned to reflect regional or international best practices when reforming national laws. Bangladesh should

[10] Craig, C. J. Technological Neutrality: (Pre)Serving the Purposes of Copyright Law. *Osgoode Hall Law School Legal Studies Research Paper* (2014), No. 28.

[11] Koops, B-J., "Should ICT regulation be technology-neutral?", in Koops, B-J., *Starting Points for ICT Regulation*, Cambridge, 2006.

always keep in mind that their ICT policies are harmonized[12] with neighboring countries that have maximum trade relationship with Bangladesh.

B. Legal Environment

This section discusses about legal validity and enforceability of electronic communications. In Bangladesh, there are potential restrictions on the use of electronic means of communication because of the incorporation of terms into the regulatory provisions. These form requirements within national regulations have given rise to a degree of uncertainty about the legal validity of electronic communications. Few of the aspects are discussed below:

1. Legal recognition of electronic communication

Exchange of electronic messages is the heart of e-commerce. Electronic messages should not be considered invalid solely on the grounds of their electronic form. That is very important. Measures may therefore need to be taken to ensure that national legislation does not discriminate against generation, storage or communication in electronic form.

2. Requirements of e-form

Many regulations stipulate requirements for documents to be produced in writing, or for a contract to be signed by both the parties in stamp. There is no such certainty for the validity and enforceability of e-communications or signatures. It may therefore be necessary to amend regulatory provisions to enforce electronic communications so that it can equally be used as regular way of communications or contracts.

3. Retention of electronic messages

Storage of information and record keeping are vitally important in business. Retention of documents electronically can provide an efficient and cost effective way of storing large volume of data. If this form of record keeping is enforced by ICT policy, it can even play a vital role in green environment by saving trees. Many regulations require the maintenance of written records for a period of time. Usually the purpose of this record keeping is for the purpose of accounting, tax, or auditing. By making it optional to keep paper documents, government can play a big role in promoting electronic documents.

4. Recognition of foreign electronic documents and signatures

It is mandatory for International commerce that not only of domestically produced electronic documents and signatures but equally of foreign records. An issue to be

[12] ITU-EC Project-Harmonized ICT Policies in ACP countries. Retrieved from http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/HIPSSA_implementation_strategy_EN_090608.pdf on August 16, 2014.

considered when implementing such changes is whether recognition should be provided on exactly the same terms as national documents.

5. Recognition by parties of data messages

Ensuring recognition of data messages which do not form part of a contract but which do relate to the specific performance of contractual obligations, such as an offer to pay or recognition of a debt, is also important. Although this is provided for through the adopting of a provision that provides for non-discrimination on the basis that a communication is electronic, many of the models have considered that it is important that there should also be a provision specifically providing for recognition by parties of data messages.

C. Legal ICT Security

This section deals with the security of electronic commerce through policy. For thrift of any commercial environment cannot thrive without assurances of security of electronic data. This section will try to highlight few issues with integrity, authentication and confidentiality. At the same time, it will inspect the approaches to managing security risks online.

1. Integrity and authentication

Documents in pen and paper are difficult to alter without leaving a mark. The ease of alteration of any e-document makes it difficult to determine any alteration. Even an electronic contract could be altered by either of the parties after the agreement was reached. Therefore, the validity of electronic signatures should be have been adopted in the policy. At the same time, an adequate level of legal certainty should be ensured and enforced for e- communication and contract.

2. Managing ICT security risks

Increased use of firewalls to protect data has become a common phenomenon to businesses. This shows the importance of online security. Public authorities need to consider the impact of electronic commerce.[13] Specially, it needs to be ensured that the availability of information systems at all time is very important for financial sector. There is zero tolerance for data loss and data going to wrong hand. ICT policy should clearly indicate the punishment for this type of behavior for both the organization, for not taking proper measure, and the intruder or data thief.

3. Digital Signatures

For any form of online transactions, they need to be able to make sure that the

[13] Bakari, J. K. A Holistic Approach for Managing ICT Security in Non-Commercial Organizations: A Case Study in a Developing Country. Stockholm University. (2007). Retrieved from http://www.diva-portal.org/smash/get/diva2:197030/FULLTEXT01.pdf on July 21, 2014.

messages sent and received reach their intended recipient without any change. Verification of each party is also very important. These contributed to the need for creating and using of digital signatures.[14] Reliability of digital signature will vary according to the method. It can be as simple as writing a name at the bottom of an emailer even some form of cryptographic elements. Proper policy should be made for what type of document what type of digital signatures can serve the purpose.

4. Data Protection

The wide use of the Internet, with the ability to process large quantities of data, may raise significant concerns over the use of data, user of data and purpose of use. Therefore, it has become very crucial to build the ability to store large volumes of records with full search support. It can also enable fast transfer data. At the same time, it increases the vulnerability of data. So, there should be central policy for all types of institution so that they take special measures for data protection. Otherwise, it has the potential to harm any organization in the worst manner.

D. Legal Safeguard

Intellectual property rights are becoming a burning issue in our modern business. Issues on copyrights, patents and trademarks are very crucial now a day. If we look at online transaction and business over Internet, it has increased exponentially as it has opened a window to numerous suppliers all over the world. Intellectual property rights are generally national in scope but the Internet has placed great emphasis on the ability to protect and enforce these rights internationally. Issues related to these are highlighted below:

1. Trademarks

Trademarks are generally protected through registration on a national basis. Therefore, it is possible and more likely that the same name can be registered with different goods and services. As we all know that registration of a trademark has only national boundary effect, it must be carried out in each country where an individual wishes to receive protection. Harmony and collaboration of policies among different countries can effectively reduce the risk of trademark dilution of any well-known brand.

2. Copyrights

Unlike trademark, copyright protects the expression of an idea. It cannot be used to protect the idea itself. Therefore a copyright owner has the exclusive right to carry out certain activities in relation to the work. Proper policy needs to be there if anybody wants to use any idea that are foreign. Policy should support the owner irrespective to his or her

[14] Pointcheval, D. and Stern, J. Security Arguments for Digital Signatures and Blind Signatures. *Journal of Cryptography*, Vol. 13, No. 3, (2000), pp. 361-396.

nationality. Licensing policies should be discussed properly in the policy so that no one feels deprived. Infringement of copyright should be strictly discouraged by policy.

3. Consumer protection

Sometime existing consumer protection[15] law can be used to cover Internet-based transactions. However, various measures need to be taken to increase consumer confidence regarding online transactions. Not only regarding the information of the supplier and the product to a great extent should be there but also actions against the fraudulent use of payment cards for online transactions should be enforced.

E. Legal Restrictions

Electronic commerce not only opened doors of new opportunity and business but also opened doors for cyber criminals. For an example, Internet allowed us to enter into commercial agreements or contracts with any companies from any corner of the world. Similarly, it enabled the cyber-criminal to get access to the computers of enterprises from any corner of the world.

There are criminal procedural laws already active in the system. These provide law enforcement agencies certain powers and authority to investigate criminal activities. The requirement is to make such an ICT policy so that with minimum amendment law enforcement agencies can act against cyber crime. At the same time, peoples voice should not be barred. Specially, in the case of blogging or social networking citizens should have freedom of speech. The advancement of ICT is creating new issues almost everyday. For example, now a day many of the cyber criminals are living or staying across the boarder. It is very difficult to trace them due to different jurisdiction. So, ICT policy is very crucial as the policy should be collaborative in nature with different countries to trace cyber crimes.

VI. INTERNATIONAL COOPERATION

As it was discussed in the previous section, in the field of cybercrime international coordination and cooperation is vital. Cybercrimes are not limited to national boundaries and the detecting and prosecuting of these activities will likewise necessarily cross these boundaries. Cybercriminals may choose to route their communications through several jurisdictions in order to try to avoid detection and likewise the evidence of their crimes may be located across a variety of jurisdictions.

Multinational agreement to provide for assistance in the investigation and prosecution of crimes is therefore necessary. In 2005 Interpol established the Virtual Global Taskforce to deal with child pornography. There have been several initiatives

[15] Bar-Gill, O. and Ben-Shaher, O. Regulatory Techniques in Consumer Protection: A Critique of European Consumer Contract Law. *Common Market Law Review*, (2013). Vol. 50, p. 109.

designed to promote international coordination in this area including the OECD Guidelines for the Security of Information Systems and Networks-Towards a Culture of Security.

VII. FREELANCING: AN EMERGING MARKET

Freelancing business[16] in Bangladesh has not started long time ago. It became popular for last five years years. But the idea of freelancing is not new at all. Due economic downturn in world economy, small businesses were forced to cut cost for survival. As a result they have looked for workers with lowest possible cost and almost no employee benefit to be profitable. As a result, freelance marketplaces grew. The first marketplace was launched in 1998 and after that few of them came and gone. Freelance workers are often represented by a company or an agency that sells their finished products in the market. Other than those most of the freelancers are completely independent. Even they can be called as independent contractor. 'GURU' was the first online freelancing marketplace. It was established in 1998 as SOFTmoonlighter.com. After GURU, there were Elance, Odesk, Freelancer.com, Limeexchange.com, etc. Some of them agencies organized seminar and workshop to market freelancing business. They tried to educate individuals about the potentiality of freelancing business. Before that freelancing work and business were in a limited format.

Now a day, media also is highlighting freelancing business a lot. Many enthusiastic young people, even living in remote areas, are earning their livelihood successfully through freelancing. Some of they are even running their entire family only by freelancing. The Daily Prothom Alo published several a report and success story on freelancing time to time. Currently about 10,000 freelance software developers in the country are earning roughly $40 million annually.[17] Growth rate of the industry has been around 40% for last few years. But the major issue with individual freelancers is money transferring. If Bangladesh Bank and ICT ministry jointly can take some steps to mitigate this issue; Bangladesh can be a part of huge industry world-wide.

VIII. CONCLUSION& RECOMMENDATION

ICT is a strong enabler for economic growth of Bangladesh. Its crosscutting nature affects all sectors of the economy. Adoption and proper utilization of ICTcan lead to increased output and quality production. Other than cybercrime, there are few ICT

[16] www.spotlightbd.com. Freelancing. Retrieved from http://www.spotlightbd.com/earn-money-online/freelancing/ on July 22, 2014.

[17] Nascenia (www. Nascenia.com). Bangladesh Outsourcing Conference 2011. 2011. Retrieved September10, 2006 from http://www.nascenia.com/bangladesh-outsourcing-conference-2011/

policy issues regarding international and domestic trade that Bangladesh should consider at the time of next amendment of ICT act 200.[18] A comprehensive and consistent approach needs to be considered of ICT development strategy. In addition, consideration needs to be given to any regulatory structure required to support and enforce any obligations placed upon public or private entities. The most important aspect is regional and international legal harmonization. Now it is an age dominated by the Internet and it is often a critical element in achieving the goals of each nation with others.

This paper highlights some important issues that Bangladesh may take into consideration in future policy reforms with respect to the ICT sector. The main among them are the followings:

- Political commitment would be a key precondition for successful law reforms in support of national ICT strategies within a specified timescale.
- Further efforts need to be made to familiarize Bangladesh with the legal and regulatory implications arising from the use of ICTs and e-Commerce.
- Efforts should be made to facilitate a transfer of experience in the area between neighboring countries, though regional training seminars and workshops.
- Bangladesh will be better off if it is aware of international best practices on the various topics and the existence of model laws and other international instruments.
- Coordinated and harmonized initiatives should be promoted among neighboring countries, enabling significant savings in terms of time, experience and resources required for such activities.
- Consumer protection is a vital issue for local and even international business expansion over Internet. Bangladesh needs to be very careful at the time of next amendment so that it can protect consumers who are trading online.
- Bangladesh should engage in some collaborative research with other countries that are leading ICT field. Though collaborative engagement Bangladesh can learn and improve its ICT policy in favor of safe online transaction.
- All the different stakeholders, from business, public administration and civil society, need to be represented in discussions at a country level aimed at facilitating the law reforms.

[18] ICT Policy Act 2006. Retrieved from http://www.btcl.gov.bd/act/act.htm on August 16, 2014.

As we already mentioned that Bangladesh has its ICT policy act 2006. There were few amendments as well time to time. But still there are gaps between real need and ICT act. It will take time to mature the act and cover most of ICT aspects into the policy. Next study of this series will be to show the gaps between ICT act 2006 and what are required most at this point of time to be competitive in e-commerce globally. At the same time, there are few things that are included in the act, which might not be friendly terms to formulate collaboration among nations for e-commerce. ICT policy should definitely support international trade and emphasize harmony among neighboring nations' ICT policy. The act should not be contradicting in case of treatment between domestic and international issues. These areas will be discussed and explored further in our upcoming study.

KEYWORDS

ICT Policy, ICT Development, Legal Issue, Bangladesh, International Collaboration.

Manuscript Submitted on Oct 20, 2014
Review Begun on Nov 10, 2014
Accepted for Publication on Dec 10, 2014

A Study on the Legal System of Personal Information Protection in the Financial Sector

Seokhan Hong*

I. INTRODUCTION

With the development of Information and Communication Technology (ICT), personal information protection is turning into an important condition for privacy and freedom. At the same time, as personal information itself has begun to have its own value as a property in the financial aspect, the issue of properly harmonizing the protection and use of personal information is now becoming an important challenge in the relevant legal system. The same is true of financial transactions. Financial transactions via online banking and use of credit cards and prepaid cards are generalized, and goods and services are traded electronically online. In this reality, personal information or credit information related to financial transactions is a type of personal information with conflicts between the necessity of protection and demand for use, just like any other types of personal information.

Today, many aspects of an individual's daily life, from private transactions with others to the government's supply of welfare services, are mediated by financial institutions. Moreover, an individual's financial transaction information and credit information also act as important evidentiary materials to confirm tax imposition and determine individual levels of welfare services. In particular, with the activation of online banking and e-commerce, an individual's financial transaction information or credit information is digitized and thus can be collected, processed and handled comprehensively and systematically. Considering the fact that the advancement of capitalism and progress of informatization will continue, issues regarding protection and use of such information will be raised more seriously in the future.

Meanwhile, there have recently been many repeated cases in which massive personal information was leaked by financial institutions, resulting in damaged trust in their personal information management and increased national anxiety. Of course, cases of personal information leakages in financial institutions are generally crimes that violate the law, and not necessarily the issue of the legal system on personal information protection. However, this phenomenon provides the opportunity to review the relevant legal system on personal information protection in the financial sector. It is necessary to look back on whether the protection and use of personal information are well harmonized, and

* Professor, School of Law, Mokpo National University.

whether there is a formality to properly implement the measures for and monitoring of personal information protection.

The legal system of personal information protection in Korea is divided into the public and private sector, with different legal grounds and promotion system. However, with the enforcement of the Personal Information Protection Act that integrates the public and private sector on September 30, 2011, the same Act has come to be applied as the general law in the financial sector of the private territory as well. In addition, the Act on Real Name Financial Transactions and Confidentiality, Act on Reporting and Using Specified Financial Transaction Information, and Use and Protection of Credit Information Act are being applied as special laws on protection of financial transaction information and credit information.

This paper will examine the issues of personal information protection that are raised with regard to financial transactions by analyzing the relevant legal system. In particular, it aims to review the main contents of the Act on Real Name Financial Transactions and Confidentiality and Act on Reporting and Using Specified Financial Transaction Information in the perspective of personal information protection. To this end, this study will first examine the meaning of personal information and its protection in the financial sector, organize the contents of the Act on Real Name Financial Transactions and Confidentiality and Act on Reporting and Using Specified Financial Transaction Information, and present issues and improvement plans of the relevant Acts in the perspective of personal information protection.

II. MEANING OF PERSONAL INFORMATION AND PERSONAL INFORMATION PROTECTION IN THE FINANCIAL SECTOR

A. Meaning of Personal Information in the Financial Sector

The Personal Information Protection Act stipulates in Article 6 that "Unless otherwise provided for in other Acts including the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc., and the Use and Protection of Credit Information Act, the protection of personal information shall be governed by this Act." Thus, the same Act is applied as a general law on personal information protection. Moreover, the same Act also has a regulation on the concept of personal information. That is, Article 2, subparagraph 1 stipulates that "The term 'personal information' means information that pertains to a living person, including the full name, resident registration number, images, etc., by which the individual in question can be identified (including information by which the individual in question cannot be identified but can be identified through simple combination with other information).

Meanwhile, the meaning of information on financial transactions or on credit is presented in the regulations of the Act on Real Name Financial Transactions and

Confidentiality and Use and Protection of Credit Information Act. To begin with, Article 2, subparagraph 3 of the Act on Real Name Financial Transactions and Confidentiality defines financial transactions as "transactions in which financial companies, etc. receive, sell and purchase, repurchase, mediate, discount, issue, redeem, return, are entrusted with, register, or exchange financial assets, or in which financial companies, etc. pay interest, money discounted, or dividends of those financial assets or carry out such payment as an agent, or other transactions involving financial assets as determined by Ordinance of the Prime Minister." Also, Article 4, paragraph 1 states that no person working for a financial company, etc. shall provide or reveal information or data concerning the details of financial transactions, and no person may request a person working for a financial company, etc. to provide transaction information, etc., with only exceptional allowances in some cases. Here, information or data on contents of financial transactions means "the conduct of financial transactions by a specific person, any original or copy of records on financial transactions which any financial institution possesses, and any information learned from the records (hereinafter referred to as 'transaction information'). Provided, this shall not include transaction information from which it is impossible to determine who is conducting the financial transaction or for whom it is made (except where the identity of the trader can be easily determined in combination with other transaction information, even if his identity cannot be determined solely on the basis of the transaction information in question)" (Article 6 of the Enforcement Decree of the Act).[1]

Moreover, the Use and Protection of Credit Information Act stipulates the concepts of credit information and personal credit information. According to Article 2, subparagraph 1 of the Use and Protection of Credit Information Act, credit information means information, as prescribed by Presidential Decree, that is necessary to determine the credit worthiness of the other party to financial transactions and other commercial transactions, such as information by which a particular subject of credit information can be identified, information by which the transaction details of a credit information subject can be determined, information by which the credit worthiness of a credit information subject can be determined, information by which the credit transaction capacity of a credit information subject can be determined, and other information similar to that referred to above. Furthermore, personal credit information refers to information necessary to determine the credit rating, credit transaction capacity, etc. of an individual, excluding the information on a company and a juristic person (Article 2, subparagraph 2

[1] For details about the view criticizing the definition of Article 6 of the Enforcement Decree of the Act regarding 'the information or data concerning the details of financial transactions' that this comprehensively expands the scope of financial transaction information than that stipulated by its mother law, refer to Sung Nak-in, Legislative Policy Tasks for Privacy and Personal Information Protection, Yeungnam Law Journal Vol.5, No.1, 2, Institute of Legal Studies of Yeungnam University, 1999, p. 47.

of the Act and Article 2, paragraph 2 of the Enforcement Decree of the Act).

As such, this study examined the concept of personal information in the Personal Information Protection Act, contents of financial transactions in the Act on Real Name Financial Transactions and Confidentiality, and the concept of personal credit information in the Use and Protection of Credit Information Act. Considering the examination, if the subject of the relevant information is a living person, his or her information on financial transactions or data as well as personal credit information must be protected by the right of informational self-determination by the Constitution which is acknowledged as a fundamental right. In particular, an individual's financial transaction information and credit information have a critical influence on an individual's economic life in general including financial transactions, employment or housing lease, and thus they are personal information that must be handled with more importance than other types of personal information.

B. Meaning of Personal Information Protection in the Financial Sector

With the development of ICT, entrance into the information society and advancement of capitalism, the need for protection of financial transaction information and credit information is emphasized more than that of any other types of personal information. An analysis of the records of an individual's financial transactions reveals a certain person's occupation, consumer behavior, economic activities as well as personal interests. If the records of donations or contributions are also determined, even the person's ideological tendencies such as the political party he or she supports will also be revealed.

However, in the public sector, it is necessary to use an individual's financial information particularly to conduct governmental tasks such as criminal investigation or tax imposition. It is true that the private sector also intends to use an individual's credit information since finding out about the accurate credit information of the other party is a key element that determines success of the transaction and safety of assets in creating new trade connections such as financial accommodation, especially for financial institutions or individuals dealing with other individuals whose credit standing is unknown. This is also a reason why Article 2, paragraph 1 of the Enforcement Decree of Use and Protection of Credit Information Act excludes "the information publicly notified or disclosed in accordance with other Acts and subordinate statutes, or publicly notified or disclosed through publications, broadcast media, or the Internet home page, etc. of the State, local governments or public institutions" from the category of credit information.

Ultimately, how to harmonize protection and use of personal information is crucial in the financial sector as well. In the modern economic reality, financial transaction information and credit information are types of personal information that strongly require protection as much as they require use.

III. STATUS OF THE LEGAL SYSTEM ON PROTECTION AND USE OF PERSONAL INFORMATION IN THE FINANCIAL SECTOR

A. Overview

Protection of financial transaction information and credit information is basically regulated by the Personal Information Protection Act as well as the Act on Real Name Financial Transactions and Confidentiality and Use and Protection of Credit Information Act. They each regulate the protection and use of personal information, financial transaction information and credit information. Only, the Act on Reporting and Using Specified Financial Transaction Information regulates the use of certain financial transaction information in order to control money laundering and financing of terrorism using financial transactions.

Article 6 of the Personal Information Protection Act clearly states that unless otherwise provided for in other Acts, the protection of personal information shall be governed by this Act as a general law. Thus, financial transaction information or credit information that is included in personal information are governed preferentially by the Act on Real Name Financial Transactions and Confidentiality, Act on Reporting and Using Specified Financial Transaction Information, and Use and Protection of Credit Information Act.[2]

The Act on Real Name Financial Transactions and Confidentiality plays a significant role in confidentiality of financial information while also enforcing real name transactions in financial activities to fulfill economic justice. The Act on Reporting and Using Specified Financial Transaction Information imposes restrictions on protection of financial information by establishing the legal grounds for the government to directly have access to financial transaction information between financial institutions and individuals in certain cases. With regard to credit information, there had not been a properly organized legal system on collection, management and use of credit information in the past, with only fragmentary regulations by the Credit Investigation Business Act, Credit Card Business Act, Consumer Protection Act, Regulation of Standardized Contracts Act, and Installment Transactions Act. However, with the enactment of the Use and Protection of Credit Information Act in 1995, integrated regulation on personal credit information became possible. As examined above, financial transaction information and credit information may be overlapped in certain areas. The following section will analyze the contents of the Act on Real Name Financial Transactions and Confidentiality and Act on Reporting and Using Specified Financial Transaction Information, and consider the problems and improvement plans for each Act in the perspective of personal information protection.

[2] In particular, the Act on Real Name Financial Transactions and Confidentiality clarifies the position of this Act as a special law by stipulating in Article 9, paragraph 1 that "Where this Act conflicts with other Acts, this Act shall apply."

B. Main Contents of the Act on Real Name Financial Transactions and Confidentiality

1. Prohibition of Providing and Revealing Financial Transaction Information

Article 4, paragraph 1 of the Act on Real Name Financial Transactions and Confidentiality stipulates that no person working for a financial company, etc. shall provide or reveal information or data concerning the contents of financial transactions (hereinafter referred to as 'transaction information, etc.') to other persons unless he/she receives a request or consent in writing from the holder of a title deed (in case of trust, meaning a truster or beneficiary), and no person may request a person working for a financial company, etc. to provide transaction information, etc. Provided, the same shall not apply in any of the cases from subparagraphs 1 to 8 in which the said transaction information, etc. is requested or provided to the minimum extent as necessary for the purpose of the use thereof.

No person who becomes aware of transaction information, etc. pursuant to each subparagraph of paragraph 1 shall provide or disclose such information, etc. to other persons, or use such information, etc. for other purposes than the original purpose (paragraph 4 of the same Article). Persons who have any transaction information, etc. provided or disclosed in violation of paragraph 1 or 4, including those who have obtained such transaction information, etc. again from them, shall not provide or disclose such information, etc. to others where they become aware of such violation (paragraph 5 of the same Article).

2. Keeping Records of and Management of Details concerning Provision of Transaction Information, etc.

Where a financial company, etc. has provided transaction information, etc. with the written consent of the holder of a title deed, or has provided it pursuant to Article 4 (1) 1, 2 (excluding taxable data, etc. that shall be submitted under the tax-related Acts), 3 and 8, the financial company, etc. shall notify in writing the holder of the title deed of the major contents, purpose of use, person provided, date of provision, etc., within 10 days from the date of such provision (where such notice is deferred under paragraph (2) or (3), the date on which the deferred period of notice expires (Article 4-2, paragraph 1).

However, where a financial company, etc. receives a written request for a deferment of notice from a requester for transaction information, etc. subject to notice on the grounds falling under any of the following subparagraphs, the financial company, etc. shall defer such notice for the requested deferment period (6 months where the deferment of notice has been requested for 6 months or longer on the grounds of subparagraph 2 or 3): ① where the relevant notice carries a matter of concern about threatening the safety of human life or body (subparagraph 1), ② where the relevant notice carries a matter of obvious concern about obstructing the progress of a fair judicial

process such as destruction of evidence or threat to witness (subparagraph 2), or ③ where the relevant notice carries a matter of obvious concern about obstructing the progress of a fair judicial process such as destruction of evidence or threat to witness (subparagraph 3) (Article 4-2, paragraph 2).

Moreover, where a requester for transaction information, etc. presents that the reason falling under subparagraphs 1 to 3 is continued and repeatedly requests in writing a deferment of notice, a financial company, etc. shall defer such notice for the requested deferment period according to certain requirements (Article 4-2, paragraph 3).

A financial company, etc. shall keep records of and manage, pursuant to the standard form as stipulated by the Financial Services Commission, information containing certain information,[3] in cases where it has provided transaction information, etc. to other persons than the holder of a title deed with his/her written consent, has received a request for provision of transaction information, etc. from other persons than the holder of a title deed pursuant to Article 4 (1) 1, 2, 3, 4, 6, 7 or 8, or has provided transaction information, etc. to other persons than the holder of a title deed (Article 4-3, paragraph 1). These records shall be preserved for five years from the date of the provision of transaction information, etc. (where the provision of information has been refused, the date of receiving a request for such provision) (paragraph 2 of the Article).

C. Main Contents of the Act on Reporting and Using Specified Financial Transaction Information

1. Reporting on Transactions of Suspected Illegal Assets by Financial Companies, etc.

Each financial company, etc. shall immediately report any of the following cases to the Commissioner of the Korea Financial Intelligence Unit, as prescribed by Presidential Decree: 1. Where reasonable grounds exist to suspect that an asset given or received in relation to any financial transaction is illegal or the other party to a financial transaction engages in money laundering or financing of terrorism, and the amount involved in the relevant financial transaction is not less than that prescribed by Presidential Decree; 2. Where reasonable grounds exist to suspect that the other party to a financial transaction engages in making installment transactions in order to circumvent subparagraph 1, and the total value of the installments is not less than the amount prescribed by Presidential Decree under the same subparagraph; 3. Where any person who works for a financial

[3] ① Personal information on a requester (person in charge and responsible person), details and date of such request (subparagraph 1) ② Personal information on a provider (person in charge and responsible person) and the date of provision (subparagraph 2) ③ Details of transaction information, etc. provided(subparagraph 3) ④ Legal ground for provision (subparagraph 4) ⑤ Date on which the financial company, etc. has notified the holder of the title deed (subparagraph 5) ⑥ In case where notification is deferred, date on which the deferment of notification is made, ground, period and frequency (subparagraph 6)

company, etc. reports to the competent investigation authority under Article 5 (1) of the Act on Regulation and Punishment of Criminal Proceeds Concealment, or Article 5 (2) of the Act on Prohibition against the Financing of Terrorism (Article 4, paragraph 1). Where a financial company, etc. files a report, it shall clearly state the reasonable ground for such suspicion (paragraph 3 of the same Article). Where a financial company, etc. has filed a report, it shall retain each of the following materials related to the relevant report for five years from the date of reporting, as prescribed by Presidential Decree: data to verify the real name of the other party to a financial transaction, data on financial transactions subject to reporting, and data where a financial company, etc. has recorded reasonable grounds for suspicion (paragraph 4 of the same Article).

2. Reporting on Large Cash Transactions by Financial Companies, etc.

Where a financial company, etc. has paid to, or received from the other party to a financial transaction, cash (excluding foreign currencies) or other cash-equivalent means of payment prescribed by Presidential Decree (hereinafter referred to as 'cash, etc.'), at least the amount prescribed by Presidential Decree within the extent of 50 million won, it shall report such fact to the Commissioner of the Korea Financial Intelligence Unit within 30 days.

Provided, this shall not apply to any of the following cases: 1. Paying to, or receiving cash, etc., from another financial company, etc. (excluding entities prescribed by Presidential Decree); 2. Paying to, or receiving cash, etc., from the State, a local government or other public organization prescribed by Presidential Decree; 3. Paying to, or receiving cash, etc., ordinary in nature, which poses no risk of money laundering, as prescribed by Presidential Decree (Article 4-2, paragraph 1).

Moreover, where reasonable grounds exist to suspect that the other party to a financial transaction is making installment transactions with intent to circumvent paragraph (1), a financial company, etc. shall report such fact to the Commissioner of the Korea Financial Intelligence Unit (Article 4-2, paragraph 2).

3. Provision of Information to Investigation Authorities, etc.

When deemed necessary for investigations into criminal cases concerning alleged illegal assets, money laundering or financing of terrorism, investigations into alleged violations of tax laws, tax investigations to verify alleged violations under Article 3 of the Punishment of Tax Evaders Act, investigations into alleged customs violations, customs duty investigations to verify alleged violations under Article 270 of the Customs Act, investigations into alleged violations of the Political Funds Act, or financial supervision (hereinafter referred to as 'investigations into specific criminal cases, etc.'), the Commissioner of the Korea Financial Intelligence Unit shall provide the "certain information on financial transactions" to the Public Prosecutor General, the Commissioner of the National Tax Service, the Commissioner of the Korea Customs

Service, the National Election Commission or the Financial Services Commission.

Here, "certain information on financial transactions" refers to 1. Information reported by financial companies, etc. under Article 4 (1) or (2); 2. Information received from foreign financial intelligence services under Article 8 (1); 3. Information compiling or analyzing the information set forth in subparagraphs 1 and 2 or the information reported or notified under Articles 4-2 and 6 (Article 7, paragraph 1).

Furthermore, when deemed necessary for investigations into criminal cases concerning alleged illegal assets, money laundering or financing of terrorism, the Commissioner of the Korea Financial Intelligence Unit shall provide certain information on financial transactions prescribed by Presidential Decree to the Commissioner General of the Korean National Police Agency and the Commissioner General of the Korea Coast Guard (paragraph 2 of the same Article).

Moreover, when deemed necessary for investigations into specific criminal cases, etc., the Public Prosecutor General, the Commissioner General of the Korean National Police Agency, the Commissioner General of the Korea Coast Guard, the Commissioner of the National Tax Service, the Commissioner of the Korea Customs Service, the National Election Commission or the Financial Services Commission (hereinafter referred to as the 'Public Prosecutor General, etc.') may request the Commissioner of the Korea Financial Intelligence Unit to provide the information set forth in paragraph (1) 3 as prescribed by Presidential Decree. (paragraph 4 of the same Article).[4]

4. Requests, etc. for Provision of Information

The Commissioner of the Korea Financial Intelligence Unit may request the head of a relevant administrative agency to provide data prescribed by Presidential Decree (excluding information on a financial transaction),[5] if deemed necessary for analyzing certain information on financial transactions (excluding information referred to in Article 7 (1) 3; hereafter the same shall apply in this Article) or information reported or notified under Article 4-2 or 6 (Article 10, paragraph 1).

Also, if deemed necessary for analyzing certain information on financial

[4] The Korea Financial Intelligence Unit merely performs the role of collecting and analyzing information on crimes and has no authority to investigate money laundering crimes, and thus shall provide relevant information to investigation authorities. Jang Il-seok, Understanding the Anti-money Laundering System, Parkyoungsa, 2011, p. 62.

[5] 1. Computerized information data on registration matters in Article 11 (6) of the Act on the Registration, etc. of Family Relationships; 2. Electronic data of resident registration in Article 30 (1) of the Resident Registration Act; 3. Criminal record materials and investigation record materials in Article 5-2 (2) of the Act on the Lapse of Criminal Sentences; 4. Data prescribed by Presidential Decree among basic details on business operators such as type of business and location of workplace; 5. Other data prescribed by Presidential Decree among those required for evaluation and analysis

transactions, the Commissioner of the Korea Financial Intelligence Unit may require the head of a credit information concentration agency under Article 25 of the Use and Protection of Credit Information Act, stating the purposes of use in writing, to provide credit information (excluding information on financial transactions), as prescribed by Presidential Decree (paragraph 2 of the same Article).

Moreover, the Commissioner of the Korea Financial Intelligence Unit may require the head of a financial company, etc. to provide information on financial transactions or data through transactions arising from foreign exchanges provided for in the Foreign Exchange Transactions Act in a document stating the following matters, only if reported or received matters are deemed to fall under the requirements referred to in Article 4 (1), in analyzing certain information on financial transactions: personal information of parties to a transaction, the purposes of use, and details of required information or data related to financial transactions (paragraph 3 of the same Article). Requests or requisition of provisions for information under these regulations shall be limited to only the minimum extent necessary (paragraph 4 of the same Article).

IV. REDESIGN OF THE RELEVANT LEGAL SYSTEMS FOR PERSONAL INFORMATION PROTECTION

A. Problems and Improvement Plans of the Act on Real Name Financial Transactions and Confidentiality

1. Reducing the Scope of Information Provision and Reinforcing Clarity

The key to personal informational self-determination is allowing the information subject to exercise the right to consent to the collection of personal information based on his or her free decision. To collect personal information without the consent of the information subject, applicable provisions must exist in the relevant Act according to the general principles of limitation of fundamental rights. Moreover, according to the purpose limitation principle, personal information that is already collected cannot be provided or used for purposes other than the original intent.

Of course, the Act on Real Name Financial Transactions and Confidentiality states that no person shall provide financial transaction information to other persons unless he/she receives a request or consent in writing from the holder of a title deed. It takes the form of protection in principle and exceptional use by allowing such provision only in exceptional causes.[6] However, the exceptional cases in which transaction information can be provided or requested without the holder's request or consent in writing have a broad

[6] Lee Joong-ki, Legal Structure of Financial Information Protection, Journal of Hallym Law Forum Vol.7, Hallym University Institute of Law, 1998, p. 145.

scope, and has the issue of the indefinite other party that can exceptionally provide such information or the subject that can request such provision of information.

As provision of information or data concerning the details of financial transactions without the consent of the information subject is restriction on the fundamental rights, it is necessary to deal with these cases based on a law with clarity required by the principle of constitutionalism when necessary.[7]

2. Concretizing the Notice of Fact of Providing Transaction Information and Reducing Deferment of Notice

Article 4-2 of the Act on Real Name Financial Transactions and Confidentiality states that where a financial company has provided transaction information, etc., it shall notify the holder of the title deed of the major contents and purpose so that the information subject can be aware of the management of his or her personal information (paragraph 1), and that such notice can be deferred for certain public interests (paragraph 2), and such deferment can be repeatedly requested (paragraph 3).

However, among the eight exceptional cases of Article 4, paragraph 1 in which information can be provided to other organizations without a request or consent in writing from the holder of a title deed, subparagraphs 4 to 7 are excluded from the target of notice for the holder.

To guarantee the right of informational self-determination, the information subject shall be able to understand by whom and how his or her information is managed, and the management status of such information shall be disclosed to the subject. Of course, this may be restricted by law, and the applicable law for the restriction is shown in paragraph 1 that limits the target of notice and paragraph 2 that regulates the deferment of notice. However, principles of limitation including that of proportionality must be obeyed even when it is restricted by law.

Examining Article 4-2, paragraph 1 in this perspective, if a financial company is obliged to notify the holder of a title deed as in Article 4 (1) 1 to 3 and 8, the provision is to exercise judicial power, perform taxation duties properly and investigate state administration, or is a matter that must be disclosed to unspecified individuals by other laws. In this case, securing legitimacy is clear in terms of content or procedure more than the case in which the duty of notice for the holder is exempted including provision of transaction information within or between financial institutions. Nonetheless, excluding the cases of subparagraphs 4 to 7 from the duty of notice for the holder does not comply with the principle of proportionality.

[7] For details regarding criticism that the scope of exception is too broad and that the lack of control system as a constitutional state makes the principle of confidentiality in financial transaction information merely nominal, refer to Yoon Dong-ho, Request of Financial Transaction Information and Rule of Warrant, Korean Criminological Review, Vol.20 No.2, 2009, p. 151.

Moreover, regarding the deferment of notice from a requester for transaction information of the holder, Article 4-2, paragraph 2 stipulates the time and period thereof. However, it stipulates that repeated request of deferment may defer notice for 6 months, and furthermore notice to the holder may be deferred without limitations according to the exceptional cases or clauses in the text. Excessively extending the deferment period by making a financial company defer notice without judgment on its validity if there is a request for a deferment of notice from the requester also violates the principle of proportionality, making it more likely to violate the right to informational self-determination.

In sum, even though the essence of informational self-determination is to grant the right of the information subject to agree to the collection of his or her information, the greater need is in notifying the information subject of the fact that such information is provided ex post facto beyond the issue of consent of information provision beforehand. Therefore, it is necessary to expand the scope of notification duty for the holder of a title deed of providing transaction information, and reduce the deferment period as much as possible in case notice is deferred by unavoidable reasons.

3. Improving the Management of Details concerning Provision of Information

Article 4-3, paragraph 1 of the Act on Real Name Financial Transactions and Confidentiality states that a financial company, etc. shall keep records of and manage, pursuant to the standard form as stipulated by the Financial Services Commission, information containing certain details, in cases where it has provided transaction information, etc. to other persons than the holder of a title deed with his/her written consent, has received a request for provision of transaction information, etc. from other persons than the holder of a title deed pursuant to Article 4 (1) 1, 2 (excluding taxable data, etc. that shall be submitted under the tax-related Acts), 3, 4, 6, 7 or 8, or has provided transaction information, etc. to other persons than the holder of a title deed. Paragraph 2 stipulates that records under paragraph 1 shall be preserved for five years from the date of the provision of transaction information, etc. (where the provision of information has been refused, the date of receiving a request for such provision).

The regulation for five years of preservation merely considers the purpose of the institution that receives or requests such information, without any regulation on the preservation period of the provided information or the point of disuse, thereby excluding consideration of the information subject. Since the regulation of the law enabled provision of information for other purposes, it is necessary to clearly state the restricted preservation period of information provided in order to be faithful to the principle of proportionality.

On the other hand, this Article stipulated that the records shall be preserved for five

years even where the provision of information has been refused just because there was a request for such provision, which shall be modified as it values merely the authority and convenience of the administration.[8]

B. Problems and Improvement Plans of the Act on Reporting and Using Specified Financial Transaction Information

1. Improving the Reporting System on Transactions of Suspected Illegal Assets

Article 4 of the Act on Reporting and Using Specified Financial Transaction Information does not clarify the purpose of acquisition of personal information when the Commissioner of the Korea Financial Intelligence Unit acquires such information through the report on transactions of suspected illegal assets from a financial company, etc. Only, reporting on transactions of suspected illegal assets is limited to cases where reasonable grounds exist to suspect illegal assets. Thus, the purpose of personal information acquisition can be regarded as prevention and investigation of crimes stipulated in Article 2, subparagraphs 3 and 4 in this Act, such as transaction of illegal assets, money laundering and financing of terrorism.

However, the Commissioner of the Korea Financial Intelligence Unit shall provide information to investigation authorities by Article 7, paragraph 1 of this Act, or the Public Prosecutor-General, etc. may request the Commissioner of the Korea Financial Intelligence Unit to provide information by paragraph 4. The purpose of information provision stated by Article 7 exceeds the scope of purpose by financial companies in reporting on transactions of suspected illegal assets, or that of the process in which the Commissioner of the Korea Financial Intelligence Unit collects personal information by reporting on transactions of suspected illegal assets. Considering the purpose limitation principle stating that, in processing personal information, the purpose must be clearly specified in the collection process and used according to the original purpose in processing such information later, there is a problem in this regulation.

Of course, personal information may be used for purposes other than those in collection by legislation, but the principle of proportionality shall be followed in this case as well. However, the Korea Financial Intelligence Unit is an organization that collects, organizes and analyzes financial information and provides this to investigation authorities; and the fact that other purposes are included in providing information to investigation authorizes while limiting the Commissioner of the Korea Financial

[8] There are other criticisms regarding the Act on Real Name Financial Transactions and Confidentiality: this Act rather focuses on confidentiality under the intent to minimize side effects caused by enforcement of the Act on Real Name Financial Transactions and Confidentiality, and as a result, comprehensively regulating the two conflicting requests of real name transactions and confidentiality in a single law has limitations. Sung Nak-in, op. cit., p. 47.

Intelligence Unit to acquire information within specific purposes when acquiring it through reports on transactions of suspected illegal assets violates the purpose limitation principle. In the end, it is necessary to clarify the purpose of reporting on transactions of suspected illegal assets, and make it so that such purpose is within the same scope as the purpose of providing acquired personal information for investigation authorities.

Article 4, paragraph 6 of the Act on Reporting and Using Specified Financial Transaction Information stipulates that where any person who works for a financial company, etc. intends to file or has filed a report on transactions of suspected illegal assets, he/she shall not disclose such fact to any third person, including the other party to the relevant financial transaction.

However, this is problematic in the perspective of the publication principle in collecting personal information. Information self-determination includes the information subject's right to consent to collection of personal information, as well as the right to know for whom and what purpose his/her information is provided. That is, the information subject shall be informed of the legal grounds of information collection and purpose of use of such information. Therefore, a financial company shall notify the information subject in advance that there may be a report on transactions of suspected illegal assets at the starting point of financial transactions, or at least inform that transactions of suspected illegal assets is reported ex post facto.

2. Improving the Reporting System on Large Cash Transactions

The Act on Reporting and Using Specified Financial Transaction Information states that where a financial company has paid or received cash at least a certain amount prescribed by law, it shall report to the Commissioner of the Korea Financial Intelligence Unit unless it applies to exceptional cases regardless of whether it is a transaction of suspected illegal assets. This is collecting personal information for preventive purposes only without suspicion, and it violates the purpose clarity principle in that the purpose of using personal information through the reporting system on large cash transactions is determined ex post facto.

Moreover, the reporting system on large cash transactions in the Act on Reporting and Using Specified Financial Transaction Information is collection of personal information on cash transactions at least a certain amount; in that sense, the amount of cash transaction that is subject to the obligation of report by a financial company shall be established according to the principle of proportionality. However, Article 4-2 stipulates that this amount shall be "at least the amount prescribed by Presidential Decree within the extent of 50 million won," while Article 8-2, paragraph 1 of the Enforcement Decree of this Act stipulates that this amount shall be 20 million won. Even though the determination of the amount suitable to the principle of proportionality shall be continuously reviewed in the process of law enforcement, the reporting system on large

cash transactions regulates the report of cash transaction information without a specific suspicion by limiting the fundamental right of informational self-determination; thus, it is appropriate to clarify the "lowest limit" of the amount subject to report by law.[9]

V. CONCLUSION

This study examined the details of the Act on Real Name Financial Transactions and Confidentiality and the Act on Reporting and Using Specified Financial Transaction Information, and explored the points of improvement in the perspective of personal information protection. Like other types of personal information, that of financial transactions does not apply only the request of absolute protection, but rather needs to be used for specific purposes. In particular, an individual's financial transaction information relatively has high necessity to be used for certain public interests such as crime investigation, tax imposition, inspection or supervision on manipulation of law in financial transactions. The Act on Real Name Financial Transactions and Confidentiality and Act on Reporting and Using Specified Financial Transaction Information thus stipulate the protection and use of financial transaction information while taking these aspects into account.

However, these Acts reveal certain issues concerning the exceptions to the principle and use of personal information protection or the information subject's right to consent to using personal information as well as the purpose limitation principle. This can be summarized as follows.

First, the Act on Real Name Financial Transactions and Confidentiality has a broad scope of exceptional cases in which transaction information can be provided or requested without a request or consent in writing from the holder of a title deed, while not clarifying the recipient of the information or subject that can request such information provision. As provision of information or data concerning the details of financial transactions without the consent of the information subject is restriction on the fundamental rights, it is necessary to deal with these cases based on a law with clarity required by the principle of constitutionalism when necessary. Moreover, to the right of informational self-determination, the management status and purpose of personal information must be disclosed to the information subject. Thus, it is necessary to expand the scope of duty to notify the holder of a title deed of the provision of transaction information, while reducing the deferment period of notice as much as possible. In addition, the Act on Real Name Financial Transactions and Confidentiality shall limit and

[9] Kim Seong-tae, Anti-Money Laundering System and Personal Information Protection: Review of Reporting on Transactions of Suspected Illegal Assets, Reporting on Large Cash Transactions, and Duty of Customer Care in the Perspective of Personal Information, Law Review, Vol.7, The Law Research Institute of Hongik University, 2005, pp. 15-26.

clarify the preservation period of provided information, where transaction information is provided for those other than the holder by the holder's consent in writing or by the regulation of this Act, which allows provision of information for other purposes.

Next, regarding the reporting system on transactions of suspected illegal assets in the Act on Reporting and Using Specified Financial Transaction Information, the fact that other purposes are included in providing information to investigation authorizes while limiting the Commissioner of the Korea Financial Intelligence Unit to acquire information within specific purposes when acquiring it through reports on transactions of suspected illegal assets violates the purpose limitation principle. Thus, it is necessary to clarify the purpose of reporting on transactions of suspected illegal assets, and make it so that such purpose is within the same scope as the purpose of providing acquired personal information for investigation authorities. Moreover, regarding the reporting system on large cash transactions, this is collecting personal information for preventive purposes only, and it violates the purpose clarity principle in that the purpose of using personal information is determined ex post facto. Thus, it is necessary to more clearly stipulate the purpose of reporting on cash transactions, and it is appropriate to clarify the lowest limit of the amount subject to report by law and establish an institutional strategy to notify the information subject of the details concerning the reporting system on large cash transactions.

KEYWORDS

Personal Information Protection, Financial Sector, Financial Transaction Information, Information Communication Technology, Legal System

Manuscript Submitted on Oct 30, 2014
Review Begun on Nov 10, 2014
Accepted for Publication on Dec 10, 2014

Legal Issues on Sustainable Development in the Arctic*

Seo, Won-Sang**

I. INTRODUCTION

Since the Industrial Revolution, mankind has been concentrated on the increase of wealth and benefits by industrialization and development, forgetting priceless environment. After that all the countries of the world have realized the side effect of environmental pollution caused by an act in one country's territory could occur damage not only to neighbouring countries but also to international common area, and polluted global environment could threaten the survival of human race, international society began to deal with environmental problem as a cross-border international concern.

Sustainable Development which is simultaneously considering the needs for environment and development has been accepted as a principle of international environmental norm at the Rio Summit in 1992. Although there is no clear definition of sustainable development in international community, it is an undeniable fact that the purpose is to survive for all mankind and the concept is based on equity between present and future generations.

Next year of the Rio Summit in 1992, the Arctic 8 States declared sustainable development in the Arctic, acknowledging Rio Declaration through Nukk Declaration in 1993. It means that principle of sustainable development concluded from multilateral environmental negotiation is integrated into the Arctic governance. After that, the Arctic Council established by Ottawa Declaration in 1996 has paid attention to the importance of sustainable development in the Arctic, as part of it Sustainable Development Working Group(SDWG) was established and is being operated. Sustainable development has repeatedly been declared through all of agreed documents of the Arctic Council.

There is, however, some difference between the meanings of sustainable development discovered at Multilateral Environmental Agreements(MEAs) and at the Arctic governance. Especially considering what the sustainable development is for and the importance of Arctic environment, the question arises as to whether or not the decision-making rights over sustainable development only belong to the Arctic States. The purpose of this paper is to ultimately seek achievement of sustainable development in the Arctic in the true meaning of the word.

* This Article was written by revised part of "Problems of the international law on sustainable development in the Arctic," which is a policy research project of the Korea Polar Research Institute in 2013.
** Senior research scientist at the Korea Polar Research Institute(KOPRI), Ph.D. in Law.

II. SUSTAINABLE DEVELOPMENT IN MULTILATERAL ENVIRONMENTAL AGREEMENTS

A. Emergence of sustainable development: sympathy with environmental protection and difference in priorities among countries

A trigger of multilateral international conferences and international treaties to protect the global environment may be said to be the 1972 Stockholm Conference (UN conference on Human Environment), in which the Stockholm Declaration on Human and Environment (hereinafter referred to as 'the Stockholm Declaration') and the Action Plan were adopted. Staring from this conference, the subject has expanded from the pollution crossing the border to the global level contamination, from the conservation of certain species to the conservation of entire ecosystem, from the control of direct emissions to a comprehensive system, from the protection of resources within a country's territory to the protection of common heritage of mankind.[1] The Stockholm Declaration noted in its introduction that "Human beings are the creature of nature," and emphasized that "The protection and improvement of human environment is an important topic for the welfare of human beings and human development." That is to say, the international interest until the Stockholm Conference was focused on the environmental protection or the control of environmental pollution for people or the existence of people.

From the Stockholm Declaration, despite of the recognition that mankind will cease to exist all together without new decision and the efforts in international law for regulation of environmental pollution, the situation in the global environment has deteriorated constantly. The most important cause is because preferential needs and interests of all countries for environment and development were so different one another so that it was difficult to conclude an agreement on universal and compulsory international environmental treaties. The United Nations Conference on Environment and Development (UNCED) held in Rio de Janeiro in Brazil in June 1992 adopted 「the Rio Declaration on Environment and Development (hereinafter referred to as 'the Rio Declaration')」with main contents that "Centering on human beings, 'environmentally sound and sustainable development' shall be discussed, and human beings have the rights to live healthy and productive lives in harmony with the nature," and its action plan, 'Agenda 21'. The Rio Declaration emphasized that the rights for development shall be implemented to be able to satisfy the needs of development and environment for the present and the future generations equitably, and at the same time declared common but differentiated responsibilities taking into account the principle of sustainable development and the historical responsibility for environmental damages as a principle of

[1] E. B. Weiss, D. B. Magraw, and P. C. Szasz, International Environmental Law - Basic Instruments and References (Transnational Publishers, 1992), p. 9.

equity. Although the Rio Summit failed to find fundamental legal solutions to overcome the confrontation among all countries with regard to the priorities of environment and development, it still has a great significance that it confirmed the consensus on the fact that the development and growth should be realized under the premise or common goals of environmental sustainability.

Despite of the Rio Declaration, due to the difference of opinions between the advanced countries and developing countries, a solution to the issue of global environment conservation and development has not been found out. Thus, the UN General Assembly held the World Summit on Sustainable Development (WSSD) in Johannesburg, the Republic of South Africa in 2002 to evaluate the performance until then and discuss methods for specific practice. This conference reaffirmed international support for the principle of sustainable development by adopting *The Johannesburg Declaration on Sustainable Development*,[2] and although *Johannesburg Declaration* has no legal binding force, it has significance that it accepts the principle of sustainable development as an obligation to form the framework of international law and international environment law.[3]

B. Concept of sustainable development: comprehensive harmony of various values

Despite of numerous discussions on sustainable development, agreed legal definition is still not established. Only the definition, "development that meets the needs of the present generation without reduce the ability to meet the needs of the future generation" presented by the Brundland Commission in 1987 through "Our Common Future" is generally cited.[4] The committee stated that the concept of sustainable development was not to set in any absolute limits, and that the limits were determined by contemporary scientific technology, social organizations, and the effect of human activity affecting the ecosystem.[5]

That is to say, this report connects the concept of sustainable development with the securement of economic, social and cultural rights to global environment, and states that a sustainable development is to ensure these rights to be realized in the future.[6]

[2] See The Johannesburg Declaration on Sustainable Development, 2002, *A/CONF.199/L.6/Rev.2*,

[3] Graham Mayeda, "Where Should Johannesburg Take Us? Ethical and Legal Approaches to Sustainable Development in the Context of International Environmental Law," 15 *Colorado Journal of International Environmental Law & Policy* (2004), p. 30.

[4] World Commission on Environment and Development(WCED), *Our Common Future* (Oxford Univ. Press, 1987), p. 43.

[5] *Ibid*., p. 8; Alexandre Kiss, "The Rights and Interests of Future Generations and the Precautionary Principle," in D. Freestone and E. Hey (ed.), *The Precautionary Principle and International Law*(Kluwer Law International, 1996), p. 23.

[6] A. F. Lowenfeld, *International Economic Law*(Oxford University Press, 2002), p. 304.

The principle is a complex of various legal elements and principles, and contains various concepts. First, there are the concepts of right and obligation, i.e. necessity and limitation. In particular, the concept of 'necessity' is to be most preferentially consistent with the indispensable necessity of the poor in the world, and the other is the concept of limitation imposed on a state as a technical, social organization in order to conserve the environmental ability to meet the needs of the present and the future generations.[7] In other words, the concept of necessity for development and the concept of limitation on development conflict with each other within the extent to be consistent with the purpose of environment conservation. Along with these, two kinds of temporal concepts are dissolved, and the one is an issue of responsibility distribution among the present generations called intra-generation responsibility, and the other is an issue of responsibility of the present generation toward the future generation called inter-generation responsibility.[8]

The most common method for experts to understand the concept of sustainable development may be so-called 'umbrella approach'.[9] For example, 'the Centre for International Sustainable Development Law (CISDL)' explains that because the International Sustainable Development Law still has an ambiguity, various definitions are being made in process, but the contents summarized in each provision of treaties and legal documents will serve to embrace international environmental, social and economic issues.[10] For the same purpose, *Johannesburg Declaration* also comprehends the sustainable development as the concept composed of various pillars like economic development, social development and environmental protection at the domestic, national, regional and global level.

C. Contents of sustainable development: equity and an integrated consideration

As previously stated, the sustainable development is comprehensive concept so that it is difficult to make a clear definition of it in just a single sentence. The contents

[7] WCED, *op. cit*., p. 8.

[8] G. F. Maggio, "Inter/intra-generational Equity: Current Applications under International Law for Promoting the Sustainable Development of Natural Resources," 4 *Buffalo Environmental Law Journal* (1996-1997), p. 163.

[9] Some scholars also comprehend that the sustainable development is not one principle, but a collective concept of various principles comprising all principles in the international environmental law. V. Lowe, "Sustainable Development and Unsustainable Arguments," in A. Boyle and D. Freestone (eds.), *International Law and Sustainable Development* (Oxford University Press, 1999), pp. 25-26; In a case of Gabcikovo-Nagymaros dam between Hungary and Slovakia, Weeramantry judge presented an opinion, "Sustainable development is a principle of resources distribution regarding the cooperation for intergenerational rights, development and environmental protection, and it is related to international human rights law, national responsibility, international environmental law, international economic law and industrial law, equality, national sovereignty, prohibition of right abuse and the principle of good faith and sincerity." Gabcikovo-Nagymaros Dam(Hung. v. Slovk.), 37 *I.L.M*. (Judgment of Sept. 25, 1997), p. 162.

[10] See CISDL, "International Sustainable Development Law Principles, Practice and Prospects," A CISDL Legal Brief(Second Preparatory Committee Meeting for the World Summit on Sustainable Development 2002).

contained in a principle, however, can be summarized in several kinds. As a general consideration for a sustainable development, there are 'the principle of intergenerational equity', i.e. the conservation of natural resources for the benefit of the future generations, 'the principle of sustainable use of nature and environment' to use natural resources in a rational way, 'the principle of integration of environment and development' to ensure that the environmental consideration must be taken in economic development and other development plans, and 'the equitable use of natural resources' to use natural resources on the basis of equity taking into account the needs of other countries, and the above four principles are understood as concepts used in the mutual overlapping or combination.[11]

1. Intergenerational equity

The international community has confirmed that the development of scientific civilization could bring about the destruction of environment beyond recovery with the ability of mankind, and realized acutely the necessity to surely regulate the use of resources or environmental damages of the present generation so performed as to make the future generations are in adverse environmental conditions than the present. It was an inevitable choice for the present generation to impose the obligation of environmental conservation on itself for the future generations based on consensus for its continued existence. Therefore, based on the fact that the global natural environment is shared together regardless of the past, the present and the future generations, an intergenerational equity has been derived to the effect that the present generation should take environmental necessity of the future generations into consideration.[12]

Although there are some experts understanding the intergenerational equity as just a political goal, not a legal principle for a reason why the term of equity could be interpreted equivocally,[13] the international community has repeatedly confirmed the importance of intergenerational equity. *The 1972 Stockholm Declaration* declared, "Human beings have a solemn responsibility to preserve and improve the environment for the present and the future generations" by stating the consent of participant countries, "it is necessary to preserve the global natural heritage for the future generations." and also pointed out, "We should conserve the global natural resources including air, water, land, animal and vegetable systems through careful planning and management for the benefit of the present and the future generations."[14] The 1980 UN General Assembly emphasized

[11] Philippe Sands, "International Law in the Field of Sustainable Development: Emerging Legal Principle," in W. Lang (ed.), *Sustainable Development and International Law*(Graham & Trotman, 1995), p. 62.

[12] Edith Brown Weiss, *In Fairness to Future Generations*(The United Nations University, 1989), p. 17.

[13] Rüdiger Wolfrum, "International Environmental Law: Purposes, Principles and Means of Ensuring Compliance," in Fred L. Morrison and Rudiger Wolfrum (eds.), *International, Regional and National Environmental Law*(Kluwer Law International, 2000), p. 22; Ulrich Beyerlin, "The Concept of Sustainable Development," in R. Wolfrum (ed.), *Enforcing Environmental Standards: Economic Mechanisms as Viable Means*(Springer, 1996), p. 24.

[14] The Stockholm Declaration Preface, Principle 1, Principle 2.

the environmental protection as a responsibility for the future generations by declaring that the preservation of nature is a historically significant responsibility for the present and the future generations.[15] *The 1992 Rio Declaration* reaffirmed the intergenerational equity as a general rule by emphasizing, "The right to development should be realized to equitably meet all requirements of the present and the future generations for development and environment."[16]

Could we talk about the rights of the future generations not even born and the obligations of the present generation for them? As the ICJ stated in an advisory opinion on '*the Legality of the Treat or Use of Nuclear Weapons*', "the environment is not the subject of an abstract conception but the place of actually existing life, and the concept of mankind that is the principle of health and quality of life should include the unborn generations."[17] Professor Brown Weiss emphasized about this, "As the members of the present generation, we hold the Earth in trust for the future generation."[18] Each generation received the natural and cultural heritages by trust from the previous generation, and should preserve them by trust and hand them down to the future generations, and the present generation is both the administrator and the user of natural and cultural heritages.[19] Thus, the present generation should preserve the option for environment and development of the future generations, hand over to the future generations the global environment of the same quality as the present and enable each generation to get equitable access to benefits and use of environment (conservation of access).[20]

2. Sustainable use of natural resources

A number of environmental treaties often use the term of sustainable use of natural resources, mentioning the sustainable development. The sustainable use of natural resources refers to a principle that the natural resources and the environment should be used to enable their proper quantitative and qualitative state to be maintained in consideration of regenerative ability of the natural resources and the environment. This focuses on the adoption of standards with regard to what extent a certain natural resources may be used and developed beyond the level appealing to the necessity of environmental preservation for the future generations.[21]

The core issue of this discussion is the standards of judgement for sustainable use,

[15] UN General Assembly Resolution 35/8 (1980).
[16] The Rio Declaration Principle 3.
[17] *ICJ Reports* (1996), p. 226.
[18] Edith Brown Weiss, "Our Rights and Obligations to Future Generations for the Environment," 84 (1990), p. 199.
[19] *Ibid*., p. 21.
[20] *Ibid*., p. 38.
[21] Sands, *op. cit*., p. 257.

namely the sustainability. Although various concepts are present such as the rational, wise, sound, appropriate, optimal, and proper through environmental treaties and international declarations, but it is difficult to find a treaty defining such standards legally. Since the UN declared in *World Charter for Nature* in 1982, "Ecosystems and living organism shall be managed just like ground, marine and air resources to achieve and maintain maximum sustainable productivity,"[22] experts in each discipline of studies have thought the concept of 'maximum sustainable yield' as the most ideal for a management indicator to make the natural resource-related business to continue to prosper. The maximum sustainable yield refers to the maintenance of stocks to maximize the quantity of yield and use of resources every year based on the biological characteristics of resources.

3. Equitable use of natural resources

The equitable use of natural resources refers to the principle that all countries should use their natural resources on the basis of equitability considering the circumstances of other countries. The concept of equity or equitable principle here performs the function to re-distribute the contribution (in the nature of obligation) of finance and resources for environmental conservation to each country and properly distribute the benefits (in the nature of right) of natural resource development.

With regard to the distribution of responsibility for environmental protection, each document of UNCED describes that the equitable principle within generation shall be applied to individual issues. The *Rio Declaration* appeals to exercise the right of development as an equitable method to meet the development and environmental needs of future generations.[23] In the *United Nations Framework Convention on Climate Change*, all state parties agreed to perform the activities for achievement of purpose of the Convention on basis of equity, and state parties of 'Annex I' agreed with the necessity of 'equitable and appropriate contribution' as an effort to achieve the purpose of the Convention.[24] The *Convention on Biological Diversity* also prescribes that the benefits accruing from the use of natural resources shall be distributed in a fair and equitable way.[25]

The International Court of Justice also applies the equitable principle to the distribution of natural resources with a shared nature. In *Gabcikovo-Nagymaros* case,[26] the ICJ gave a judgement that Czechoslovakia infringed the rights of Hungary to have natural

[22] The World Charter for Nature (1982) General Principle 4.
[23] The Rio Declaration (1992), Principle 3.
[24] See the United Nations Framework Convention on Climate Change (1992), Article 3 (1) and Article 4 (2) (a)
[25] See the Convention on Biological Diversity (1992), Article 1 and Article 15 (7).
[26] This case is a dispute over hydrological system of the Danube River between Hungary and Czechoslovakia. In 1977 Czechoslovakia and Hungary signed a treaty, and began a construction work for the development of water

resources of the Danube River in an equitable and rational way, pointing out that the progress of development carried out by Czechoslovakia at its own discretion was obviously in contravention of the international law with regard to the resources shared together between Czechoslovakia and Hungary.[27]

4. Integration of environment and development

The integration of environment and development requires that the police making for economic or other development should be achieved through the environmental considerations, and that the necessity of economic and other social development must also be taken into account in the process of legislation, application and interpretation of environmental obligations. To properly comply with this principle, it is required to collect and spread the environmental information and implement the environmental impact assessment prior to the establishment of a development policy.

From the UNCED, the international community has given equal weight to the environment and development, and focused on the relationship between the two. The Rio Declaration stated, "In order to achieve a sustainable development, the environmental protection shall constitute an integral part of the development process, and not be considered after its separation from the development process."[28] And the *Convention on Biological Diversity* also stipulated, "The conservation and sustainable use of biodiversity shall be integrated into the relevant sectoral plans and policies, if possible, and the consideration for conservation and sustainable use of biological resources shall be integrated into the national policy-making."[29] This effort to integrate environment and development has changed the perspective on the interests and priorities of the international community, and the environmental consideration was integrated at last into the WTO Agreement System dealing with the fair trade.[30]

resources of the Danube River. During the construction work in progress, there was raised a criticism that this construction work caused a pollution of the Danube River, and Hungary stopped the construction work. However, Czechoslovakia determined to force this construction work alone, so in 1977 Hungary gave a notice to Czechoslovakia regarding the denunciation of the Treaty. Under this situation, the problems over if Hungary's denunciation of the Treaty was appropriate, and Czechoslovakia's execution of the construction work at its own discretion was legal have developed into a dispute between the two countries.

[27] *ICJ Reports* (1997), p. 56.

[28] The Rio Declaration (1992), Principle 4.

[29] The Convention on Biological Diversity (1992), Article 6(b) and Article 10(a).

[30] Sands, *op. cit*., p. 264.

III. SUSTAINABLE DEVELOPMENT IN THE ARCTIC

A. The motive for establishment of the Arctic governance: sustainable development

The Arctic Council is an intergovernmental consultative organization representing the Arctic governance and aimed at the environmental protection of the Arctic Circle, the protection of indigenous people and sustainable development. Although the Arctic Council was established on the basis of the 1996 Ottawa Declaration, but it is also the fruit of international agreements made continuously among the Arctic states since the 1987 Murmansk Declaration. From the Murmansk Declaration to the Ottawa Declaration, the Arctic states discussed to build up a cooperative system for sustainable development in the Arctic, and the outcome is none other than the Arctic Council.

In the Cold War period, Russia prohibited other countries from passing the Northern Sea Route (NSR) in the Arctic water for the reason of military security. In 1987, however, Mikhail Gorbachev visualized the opening of the Arctic Circle through the Murmansk Declaration proposing to "open to the ships of other countries the Northern Sea Route (NSR), the shortest route to go to the Far East and the Pacific Ocean from Europe, and provide the protection service by icebreaker ships," and "cooperate with the Arctic countries for joint development of the Arctic resources and environmental protection."

The opening of the Arctic Route was accompanied by environmental pollution concerns of the Arctic Ocean at the same time, and the eight Arctic states(hereinafter referred to as "the Arctic 8")[31] began the earnest discussion at the level of collaborative cooperation for marine environment protection in the Arctic Ocean since 1989. Those states adopted 'the Declaration on the Protection of the Arctic Environment (Rovaniemi Declaration)' in Rovaniemi, Finland in 1991. This declaration first defined the concept of Arctic Environmental Protection Strategy, which mainly aims to cooperate in the scientific researches for sources of pollution such as the Arctic acidification, radiation, noise, heavy metals, oil, non-degradable organic pollutants, and their impact on the environment and indigenous people, and the future prospects, etc., and to share the data related to these. In addition, the Strategy contains four programs to execute the Arctic Environmental Protection Strategy; 'Arctic Monitoring and Assessment Programme (AMAP)', 'Conservation of Arctic Flora and Fauna (CAFF)', 'Emergency Prevention, Preparedness and Response (EPPR)', and 'Protection of Marine Environment in the Arctic (PAME)'.[32]

[31] In this study, the Arctic 8 refers to the countries surrounding the Arctic Ocean like Canada, Denmark, Finland, Iceland, Norway, Russia, Sweden, and the United States of America.

[32] According to each program, four working groups are currently constituted under the Arctic Council. In addition, six working groups including the Arctic Contaminants Action Program(ACAP) and the Sustainable Development Working Group (SDWG) are in operation. The Arctic Contaminants Action Program(ACAP) was

The Arctic 8 announced the Nuuk Declaration giving shape to 11 Codes of Conduct for the Arctic Environmental Protection in Nuuk, Greenland in September 1993. This Declaration contains support to execute of AEPS, recognition of regulations in the *Convention on Biological Diversity* and the *United Nations Framework Convention on Climate Change*, establishment of their own environmental legislation for the execution of the Arctic Environmental Protection of the environment for the execution of its own and a sustainable development in the Arctic, etc. In the Inuvik Declaration in March 1996, they announced that they would make efforts mutually to establish the Arctic Council, intergovernmental conference among the eight states together with the Work of the Task Force on Sustainable Development and Utilization (TFSDU), etc. In Ottawa, Canada on September 19, 1996, the eight states finally announced the Ottawa Declaration containing 9 provisions as to permanent participations, observers, working groups, methods to hold the conference, enactment of rules of procedure, etc.

From the Iqaluit Declaration adopted by the Ministers Meeting of the Arctic Council held in Iqaluit, Canada in September 1998, the Sustainable Development Working Group (SDWG), one of the Arctic Council Working Groups was launched.[33] This was established aiming to promote the sustainable development in the Arctic, improve the environmental, economic, social conditions of the Arctic communities, and promotes the Sustainable Development Program[34] including not only economic and social development in the Arctic, but also improvement of health for residents and indigenous people, realization of cultural welfare, and consideration for future generations, etc.

In the Sustainable Development Framework Document adopted by the Ministers Meeting of the Arctic Council held in Barrow, the U.S.A. in October 2000, 6 priority tasks of SDWG were selected,[35] and the contents of priority tasks have converged on the enhancement of welfare for inhabitants of the Arctic, such as i) health issues and the wellbeing of inhabitants of the Arctic, ii) sustainable economic activities and increasing community prosperity, iii) education and cultural heritage, iv) children and youth, v) management of natural, including living, resources, vi) infrastructure development, etc.

The Kiruna Ministers Meeting for which the Republic of Korea acquired the observer status (May 15, 2013) adopted the Vision for the Arctic so that "the voice of the Arctic may spread to the world and be considered under the circumstance that the Arctic

established to reduce the discharge of local and regional contaminants and promote international cooperation for this at the Ministers Meeting of the Artic Council in Salekhard, Russia in October 2006. Sustainable Development Working Groups will be discussed later.

[33] The Secretariat is located in Ottawa, Canada, and as of July 2013, Canada is also currently the chair country. See http://portal.sdwg.org/. (Last Visit: October 9, 2014)

[34] Arctic Council (2000).

[35] See http://www.sdwg.org/content.php?doc=12. (Last Visit: October 9, 2014)

under change receives the worldwide attention."[36] Since the Arctic Council declared what it considered as the most important and urgent agenda, this document has lots of implications for us and it generally contains the value of the realization of sustainable development for the enhancement of welfare for the Arctic indigenous. Also, Seven items presented in the Vision for the Arctic reaffirmed the importance of sustainable development, and after setting forth as a premise in 'the Arctic living conditions' that they are responsible for the protection of rights for the Arctic indigenous in social structures, cultural traditions, language preservation and guarantee of minimum standards of living, etc., the document declared that a sustainable development was an important key and economic cooperation was the best value of the agenda (the Vision) to create 'the prosperous Arctic'. Then in the environment of 'the Healthy Artic', the document declared that the Arctic vulnerable to climate change would continue to be affected due to circumstances outside the Arctic including climate change, and at the same time that in consideration of the affecting power of the Arctic, it was required to get ecological-based approach for the sustainable use of natural resources. In particular, it expressed that the stronger Arctic Council would be required to solve these issues.

B. For whom the sustainable development in the Arctic is? : the Arctic states, people, and the indigenous in the Arctic Circle

The purpose of the Arctic Council to operate a sustainable development program is as follows; first, to enable the Arctic states to present and adopt a plan to advance the sustainable development in the Arctic, second, to protect and strengthen the environment and economy, the health and culture of indigenous people, and the Arctic communities, and third, to achieve improvement in the environmental, economic and social conditions of the whole Article communities.[37] It can be seen that the overall contents have intention point toward improvement in the quality of inhabitant's life. In order to achieve the purpose of the Arctic Council, the Senior Arctic Officials (SAOs) imposed main tasks to the SDWG such as the health of the Arctic indigenous, socio-economic issues of the Arctic, adaptation to climate change, energy and the Arctic communities, management of natural resources, and culture and language of the Arctic, etc.. Looking at the details, it becomes more obvious that the welfare of 'the Arctic indigenous people and inhabitants' is centered in the concept of sustainable development in the Arctic. 'The Arctic Human Health' is to ensure the development of the Arctic Circle to be done toward the direction of promoting the health and welfare of the indigenous and the inhabitants in the Arctic, and 'the Arctic Socio-Economic Issues' is to promote the improvement in the socio-economic conditions for Arctic environment and the indigenous and the inhabitants in the Arctic, and 'the Adaptation to Climate Change' is to eliminate the vulnerability of the

[36] *Vision for the Arctic*, MM08-15 May 2013-Kiruna, Sweden.
[37] See http://www.arctic-council.org/index.php/en/economics? (Last Visit: October 9, 2014)

indigenous and the inhabitants to climate change in the Arctic, and at the same time make preparations for adaptation measures to climate change in the Arctic, and 'the Energy and Arctic Communities' is to ensure socio-economic development of the Arctic region to be done in a way of environmentally-friendly economic activities as energy consumers, and 'the Management of Natural Resources' is to take a macroscopic approach to activities like marine transport, fishing, subsea development, etc. along with sustainability of natural resources because a sustainable use of natural resources is very important for the health and welfare of the Arctic indigenous and the Arctic communities, and 'the Arctic Culture and Languages' is to require people to strive for the preservation of the Arctic indigenous languages, supporting the culture of the Arctic.[38]

Sustainable development of the international community was apparently a concept for universal mankind. In case of sustainable development discussed generally, it attempts to balance between management of environment and economic development, approaching in a big framework of global environment protection (Stockholm approach) for mankind, especially for the future generations. Because mankind and all countries in the past, the present and the future are considered the global environment as a shared together, it is possible to discuss the equity between the present and future generations by applying the generation concept of whole mankind, and it is also possible to argue to use a country's resources equitably taking other countries into account, and it is further possible to require an integrated and coordinated policy by considering the environment in the development activities of a country. At this, although the principle in need of sustainable environment and development is mankind in a large scale, an integrated idea and approach are required because the interests vary from country to country. On the other hand, in case of a sustainable development toward which the Arctic is oriented, the beneficiaries of the development and the environment, at least the primary beneficiaries are the indigenous and the inhabitants in the Arctic. This is related to the order of international law selected by the Arctic countries for the Arctic Ocean governance. the five Arctic ocean states[39] opposed to the new system of international law in the Arctic through the 2008 Ilulissat Declaration, and asserted the right to the exclusive economic zone and the continental shelf up to 200 sea miles in accordance with the United Nations Convention on the Law of the Sea (UNCLOS).[40] As a new waterway on the high seas of the Arctic region is open due to ice-thawing and many countries are interested in the usefulness of the Arctic, the Arctic states block the entry of outside countries with asserting their rights to jurisdiction over the Arctic Ocean, and require the development to ensure the benefit of the indigenous and the inhabitants in the Arctic as a prerequisite

[38] *Ibid*.

[39] Five countries along the Arctic Ocean like the USA, Canada, Russia, Norway, Denmark (Greenland) are called 'the Arctic 5'.

[40] Declaration from the Arctic Ocean conference, 28 May 2008, Ilulissat.

for other countries' entry into the Arctic Ocean and development, and they also demand that the interests of the indigenous and the inhabitants in the Arctic should not be infringed due to the development.

IV. IS THE SUSTAINABLE DEVELOPMENT IN THE ARCTIC AN ISSUE ONLY FOR THE ARCTIC STATES?

A. The Arctic environment is a common concern of mankind.

The international community has already paid attention to adverse effects of one country's environmental pollution acts on the entire Earth for a long time, and the international environmental law has evolved from the critical mind. Moreover, the entire international community pays attention to the Arctic environment since the ice-melting in the Antarctic and the Arctic, especially in the polar regions resulted from the global warming, making the cause of climate change at the same time. From the Industrial Revolution, the global warming has progressed due to environmental pollution by mankind, and the global warming reduced the Arctic ice by more than 50% for the past 35 years, and the rise of sea level resulting from this is gobbling up such countries as Tuvalu vulnerable to climate change. Because the Arctic ocean ice performs the function to collect a large amount of greenhouse gases by reflecting most of the radiant energy of the sun, the Arctic ice and environment must be preserved in order to protect the Earth from climate change.

The Arctic environment is closely related to the global climate like this, and the international community has already dealt with climate change as a common concern of mankind. In 1988, Arvid Pardo, representative of Malta, proposed to "recognize the climate as common heritage of mankind" at the UN General Assembly.[41] The common heritage of mankind means that the resources should be developed and preserved for the benefit of mankind as a whole, and that no country will be able to enjoy the sovereignty over resources, and that the resources are open to use by all countries without discrimination.[42] At this, the UN General Assembly adopted a resolution "to recognize the climate as a common concern of mankind" by taking a step backward.[43] This resolution was adopted by consensus at the General Assembly, making an opportunity to officially recognize the climate as an essential element to maintain the lives on the Earth and a common concern of mankind as well, if not the common heritage of mankind.

[41] UN Doc. A/43/241(1988).

[42] Alan E. Boyle, "International Law and the Protection of the Global Atmosphere : Concept, Strategies and Principles," in Robin Churchill & David freestone (eds.), *International Law and Global Climate Change*(1991, Graham and Trotman), p. 9.

[43] United Nations General Assembly Resolution on Protection of Global Climate for Present and Future Generations of mankind, UN Docs. A/Res/43/53(1988).

Just as the climate is a common concern of mankind, so the issue of environmental protection and sustainable development in the Arctic giving and taking interactive influence with the climate change is also a common concern of mankind. It is a well-known fact that most of the Arctic Ocean consists of continental shelf or the exclusive economic zone of coastal countries which the sovereign rights of coastal countries reach, and the UN Convention on the Law of the Sea stipulating this should be respected and observed. Unlike the economic value of the Arctic Ocean, however, the fact that the concern and interests of whole mankind are melted in the environmental values are also not to be forgotten.

B. In order to achieve a sustainable development in the Arctic, the cooperation of the international community is surely needed.

The fact that the Arctic environment is a common concern of mankind can be interpreted to mean that the protection of the Arctic environment is accompanied by the responsibilities and obligations of non-Arctic states, and the Arctic states should also bear the responsibilities and obligations with respect to climate changes of the Earth resulting from the Arctic environment. So all countries of the Earth should cooperate together to protect the Arctic environment, and with respect to the Arctic development with the possibility of environmental pollution, all countries should be able to consult. At this, the most apprehensive thing is the closure property of decision-making system of the Arctic Council.

Because the Arctic Council is an intergovernmental organization of the Arctic states in which only the Arctic states have the rights of decision-making as the member states, the activities and participation of non-Arctic states are bound to be relatively limited. The way to participate in the Arctic Council for the non-Arctic states is to express their opinions at the Ministers Meeting or the Senior Arctic Officials (SAO) only if they obtain the permission of the chairman after acquiring the observer status, or to participate in the working group activities. Non-Arctic states may not participate directly in the decision-making on the sustainable development pursued by the Arctic Council. Moreover, the 2008 Ilulissat Declaration adopted by the five Arctic ocean states excluded even the other Arctic states such as Iceland, Finland and Sweden, from the decision-making process for the Arctic Ocean.

To emphasize again, the Ilulissat Declaration and the UN Convention on the Law of the Sea should be respected. Environmental protection and sustainable development in the Arctic, however, is not an issue of only the Arctic states, and they correspond to a common concern of mankind. Therefore, it is necessary to distinguish between the matters for which the rights to decision-making are monopolized in accordance with the order of the international law, such as the economic values of the Arctic Ocean and the matters to be discussed and determined together with the international community, such as the environmental values rather than the Arctic Council or the eight Arctic states

exercise the rights to decision-making for all issues of the Arctic. All countries of the Earth bear the responsibilities and obligations to protect the Arctic environment, and are also entitled to discuss the environmental protection of the Arctic.

V. CONCLUSION

When looking into the realities of Arctic indigenous, it can be founded that leaving foundation and means for survival of Arctic indigenous are being disappeared since Arctic ice has melted. The Arctic indigenous people are placed in urgent situations where they should maintain or recover existing environment, or should immediately secure economic means for survival to replace it. Because it may be a problem for whole mankind to encounter someday in the future, this is not the problem only for the Arctic and Arctic indigenous people or classes vulnerable to climate change. From this, we can learn a lesson that the principle of sustainable development should be focused on human existence rather than conflict of interests between environmental conservation and economic development.

The principle of international law, however, should not be changed in meaning or lose consistency depending on areas or subjects. Although the sustainable development has already been quoted in international environmental treaties as well as in international trials such as ICJ or WTO, due to the uncertainty and comprehensiveness in its concept, it is still a controversy whether it has been established as a international practice or not. It is a clear premise that whole mankind and future generation would be the beneficiaries of sustainable development.

Although it is a well-known fact that the existence of the Arctic indigenous people is threatened, the climate change and the ice-thawing are circulating each other and threatening existence of mankind. The development and environment of the Arctic should be discussed and decided together with the whole mankind. In September 2013, the Greenpeace, non-government environment organization even attempted to occupy the offshore oil platform to protest the work of Russia's Arctic subsea oil drilling. Regardless of whether the acts of the Greenpeace are lawful or not, it is an example showing that all mankind pays attention to environment of the Arctic and development by the Arctic States. The Arctic Council has claimed to strong Arctic Council through the Kiruna Declaration in 2013. To establish strong Arctic Council with regard to the issues of environmental protection and sustainable development, universal support from the international community and mankind is required to be a preliminary step.

KEYWORDS

Sustainable development, Arctic governance, Arctic environment, Arctic Ocean, Common concern of mankind.

Manuscript Submitted on Oct 30, 2014
Review Begun on Nov 10, 2014
Accepted for Publication on Dec 10, 2014

EDITORIAL POLICY AND SUBMISSION GUIDELINES

The Editorial Board of the Sungkyunkwan Journal of Science & Technology Law(herein referred to as SJSTL) discussed the ruled governing contributions to the Journal and the guidelines on how to write the manuscript. The following guidelines are hereby set for your compliance.

1. Eligibility Requirement

SJSTL is open to all authors whose expertise and knowledge correspond to the field of science and technology law and other related areas.

2. File Format & Length

The manuscript should be prepared in Microsoft Word and shall not exceed 25 printed pages, including Table and photos. Manuscripts exceeding the allowed length can be published only with the approval of the Editorial Board. The manuscript should include enough space at the top and in the bottom, right and left margins to allow convenient editing.

3. Language

The manuscript should be written in English.

4. Cover Page

The following information must be included on the cover page:

- Type of Manuscript (Aritcle, Technical Note, Discussion, etc.)
- Title
- Keywords
- Author's Full Name, Affiliations, Accreditations, Licensures (if any)
- Author's Contact Information (Mailing Address, Phone Number, E-mail Address)

5. Due Date for Manuscript Submission

Authors may submit manuscripts anytime of the year. Deadlines for manuscript submission are May 10th for Number 1 (issued on June 15) and November 15th for Number 2 (issued on December 15).

6. Abstract

Once the manuscript is finally accepted for publication, the final version of manuscript should include abstract with less than 200 word, briefly outlining major conclusions.

7. Publication Dates

SJSTL is issued twice each year on June 15 and December 15 respectively

8. Submission of Manuscript

Submission to SJSTL must be made online though ilhwan@skku.edu

REVIEW POLICY OF SUNGKYUNKWAN JOURNAL OF SCIENCE & TECHNOLOGY LAW

The science & Technology Law Institute of Sungkyunkwan University has published Sungkyunkwan Journal of Science & Technology Law (hereinafter referred to as SJSTL) in order to help legal research activities related to science and technology law. SJSTL intends to publish articles concerning various legal researches following the development of science and technology. In order to become the best journal in the field of studies related to science and technology, SJST promotes the fairness and transparency of review process as follows:

1. Submission of manuscript

(1) A submitted article can be accepted by the Executive Editor at any time. After Executive Editor receives an article, he should acknowledge the submission of such article.

(2) SJSTL provides an opportunity to submit manuscripts through online in order to shorten the review process and facilitate the convenience of submitting manuscripts. An author should attach of copy of manuscript, which covers author's personal information and two copies of manuscript without disclosing his/her personal information.

* E-mail address: ilhwan@skku.edu

2. Selection of Reviewers

(1) After an Author's manuscript is submitted, the Executive Editor should ask members of the Editorial board with corresponding expertise and specialized field to recommend two reviewers.

(2) After the members of the Editorial Board recommends reviewers, the Executive Editor should confirm the selection. If the recommended reviewer cannot participate in the review process, such vacancy must be filled by other reviewer as soon as possible.

3. Request for Review

(1) After Reviewers are selected and confirmed, they should immediately proceed the review. The manuscript without Author's personal information must be sent to the reviewers. The review period is 3 weeks.

(2) The final result of the review are divided into 4 categories: Publishable, Publishable after minor modification, Re-Review after major revision, Unpublishable.

(3) The result of the first review must be notified to the Author within 6 weeks from the day the Manuscript was submitted to the Editorial Board.

4. Review Procedure

(1) If, as the result of the first review, the final opinions of the two reviewers are all 'unpublishable', or the final opinionof one is unpublishable and the other reviewer's opinion is re-review after major revision, the Executive Editor must terminate the review procedure and notify the Author of the result as 'unpublishable.'

(2) If the final opinion of one reviewer is 'unpublishable' and that of the other is 'publishable after minor Modification', or 'publishable', the Executive Editor should proceed the third review process after asking the members of the Editorial Board to recommend the third reviewer.

(3) Unless two reviewers' decisions are simultaneously 'unpublishable', the following procedure must be undertaken. The Executive Editor must ask the Author to modify themanuscript according to the recommendations by the reviewers. When the Author modifies the manuscript, an request must be made for the Author to submit an abstract of modification. The subsequent procedure must be carried based on the third reviewer's decision.

(4) If two reviewers' final decisions are 'publishable', the Excutive Editor-in- Chief should terminate the reviewprocedure and notify an Author of the result.

(5) If the final decision of two reviewer' are 'publishable after minor modification'. The Executive Editor-in-Chiefshould notify the Author of the result as 'publishable', after he/she ensures that all the modification are properly made.

(6) The review period after the first review process is one week.

5. Termination of Review Process

(1) Review process should be terminated when the modified manuscript is not submitted within 6 weeks after the Executive Editor-in-Chief requests an Author to modify the manuscript.

(2) In case, an Author needs more time to modify the manuscript, he/she must make an formal request to the Executive Editor for the extension.

6. Publication of Manuscript

(1) If the result of review is finally confirmed, the Executive Editor-in-Chief should publish the final draft after asking the Author to submit the final draft of the manuscript. The final draft must be in compliance with the editing rules of SJSTL.

(2) Publication of the manuscript is decided on the basis of the publication-confirmed date. The same rule applies to the printing order of the manuscripts.

7. Duty of Author

(1) An Author must not simultaneously submit the same manuscript to other journals. If it is found that the manuscript has been submitted to other journals, the Executive-in-Chief should terminate the review process of such manuscript.

(2) An Author should submit the manuscript which has not been published in other journals. If it is found that the manuscript has been published in other journals, the Executive Editor should terminate the review process of such manuscript.

8. Duty of the Editorial Board

(1) The Editorial Board must not disclose the review result and the Author's personal information concerning the accepted manuscript.

(2) The Editorial Board must ensure the prompt and transparent review process.

9. Copyright of the Published Manuscript

The Science & Technology Law Institute of Sungkyunkwan University holds the copyright of the manuscripts published in Sungkyunkwan Journal of Science & Technology Law.

CODE OF RESEARCH ETHICS

Article 1 [Purpose]

The Purpose of this code of research ethics is to establish a set of principles for ethical publication standard of the Work (hereinafter referred to as the Manuscript) such as articles, notes, critical reviews, case studies and other features contributed to Sungkyunkwan Journal of science & Technology Law, published by the Science & Technology Law Institute (hereinafter referred to as the Institute).

Article 2 [Manuscript Submission]

1. Author submitting manuscripts to Sungkyunkwan Journal of Science & Technology (hereinafter referred to as the Author) must refer to the following rules.
   a. The Author must abide by general principles for the citation of scholarly sources.
   b. When The Author submits a manuscript must me an original work. The manuscript must not have been previously published or accepted for publication elsewhere, either in part or in whole.
2. The Author must inform the Editorial Board of any manuscripts that have been submitted for simultaneous consideration by two more journals. The Author bears full responsibility for any disadvantages consequences of a violation of this rule.

Article 3 [Plagiarism]

1. The Author is expected to explicitly cite other's works and ideas. All works in the manuscript should be free of any plagiarism and falsification.
2. Any act of presenting someone else's idea as his or her own constitutes plagiarism even if the Author has cited the sources.

Article 4 [Citation/Re-Citation]

1. The Author must accurately denote to scholarly materials with open access and must cite the sources which do not attribute to common knowledge. Information obtained through private channel must not be without permission from the original source.

2. The Author must give acknowledgement though references and citations to

published work and must properly point out the differences between his/her own original work and the thoughts of others.

3. The Author must reveal the re-citation of the work of others.

Article 5 [Publication Decisions]

Editorial Boardare exclusively responsible for making the final decision regarding acceptance or rejection of a manuscript.

Article 6 [Integrity and Respect for Authors]

1. Editorial Board members and reviewers should respect the intellectual independence of the author and ensure the objectivity in ending and a fair review process.
2. Reviewers must provide fair and informative critique for the submitted work on the evaluation sheet ans state the reason when requesting revision.

Article 7 [Complaint of Misconduct]

Allegations of ethical misconduct reported to the Editorial Board must be notified to the Author in writing. The Editorial Board must provide the accused the opportunity to respond to the allegations in the complaint. The accused Author must fully cooperate with investigating, if necessary.

Article 8 [Sanction]

If misconduct is found on the part of an Author whose manuscript is subsequently published, such individual may not be permitted to submit any further manuscripts for the terms not less than 3 years, but not more than 3 years, depending upon the decision made by the Editorial Board.

Article 9 [Notification of Investigation Result]

The Editor-in-Chief must promptly notify all parties in writing of the decision at the conclusion of investigation.

Sungkyunkwan Journal of Science & Technology Law

Publishing office	The Glocal Science & Technology Law Institute, Sungkyunkwan University
Publisher	Prof. Il Hwan Kim
Address	School of Law #204, Sungkyunkwan University, 53 Myeongnyun-dong 3-ga, Jongno-gu, Seoul, 110-745, Korea
Telephone	+82-2-760-0767 (BK21 Programs Office) +82-2-760-0846 (The Science & Technology Law Institute)
Printing office	Sungkyun Editing & Printing
Date of publication	2014. 12. 15

Vol.8 No.2

ISSN 1976-1422