발 간 등 록 번 호
11-1620000-000543-01

ICTs and Human Rights

National Human Rights Commission of Korea

발 간 등 록 번 호
11-1620000-000543-01

ICTs and Human Rights

National Human Rights Commission of Korea

Remarks on the Occasion of Publication

Developments of the Information and Communication Technology (ICT) have brought about unimaginable political, social, religious and cultural benefits to humanity. However, behind all these benefits exists numerous challenges including misuse/abuse of private information, monitoring/control by ICT, and social gap due to the digital divide.

Under these circumstances, it is ever more important to emphasize ICTs and human rights in order to secure human dignity in an increasingly developing information society.

The National Human Rights Commission of Korea strived to set human rights standards in an information society through numerous rounds of expert meetings, debates, domestic/international symposium. In addition, in 2012, the NHRCK hosted the ASEM Seminar on Human Rights which laid a foundation for establishing standards of the international community by sharing exemplary cases of 48 member states.

The Report on Information and Communication Technology and Human Rights is first of its kind and an effort to compile diverse discussions on information rights both domestically and internationally, moving beyond simple discussion focusing on individual basic rights and fragmentary cases. The report reflects results of deliberations with experts, civil groups and the academia on ICTs and human rights, introduces international trends and standards on information rights, and presents current status and national policy direction.

We truly wish that through the report, the international community pays more attention to the issue of ICTs and human rights which is being widely discussed in Korea, an advanced nation in ICT, and that the report can serve as an opportunity to expand comprehensive discussion on information rights both domestically and internationally.

Once again, we would like to express our words of appreciation to all the experts for their valuable advice and we will further strengthen our efforts for promotion and protection of ICTs and human rights.

January 2013

National Human Rights Commission of Korea

Chairperson **Hyun, Byung Chul**

Contents

Chapter 1. Introduction ····· 1

Section 1. The Importance of Report on Information and Communication Technology and Human Rights ····· 3

Section 2. General Information on Different Types of ICTs and Human Rights ····· 6

Chapter 2. Current Status and Issues of ICTs and Human Rights ···· 15

Section 1. Right of Information Privacy ····· 17

Section 2. Freedom of Expression on the Internet ····· 54

Section 3. Right of access to information ····· 86

Section 4. Right to Enjoy Information and Culture ····· 120

Chapter 3. National Human Rights Commission's Contributions related to ICTs and Human Rights ····· 143

Section 1. Current Data on Petition, Consultation, and Appeal ····· 145

Section 2. Petitions, Consultation, Appeal, and Guidance Cases ····· 150

Chapter 4. Suggestions for Promotion of ICTs and Human Rights ···· 163

Section 1. Reinforcement of Protection of Right of Information Privacy ····· 165

Section 2. Reinforcement of Freedom of Expression on the Internet ····· 171

Section 3. Reinforcement of Right of Access to Information ····· 174

Section 4. Reinforcement of Right to Enjoy Information and Culture ····· 176

List of Tables

〈Table 1〉 Major Contents of Eight Principles of OECD Privacy Guideline ····· 24

〈Table 2〉 Major Contents of EU Directive on the Protection of Personal Data (1995) ··· 25

〈Table 3〉 Major Contents of ILO Code of Practice on the Protection of Workers' Personal Data (1997) ····· 25

〈Table 4〉 Major Contents of APEC Privacy Framework (2004) ····· 26

〈Table 5〉 Comparison between OECD Privacy Guideline and Personal Information Protection Act ····· 29

〈Table 6〉 Prospect for the Increase in Number of CCTV Installation Nationwide ····· 32

〈Table 7〉 Provision of Tapping and Communication Data from Telecommunication Businesses to Investigation Agencies ····· 47

〈Table 8〉 Provision of Data by Investigation Agencies ····· 48

〈Table 9〉 7 Principles for Freedom of Communication on the Internet (Council of Europe) ····· 57

〈Table 10〉 Foreign Legislations on the Freedom of Expression ····· 58

〈Table 11〉 Principle of Due Process Applied on the Restrictions on Speech ····· 63

〈Table 12〉 Data on Criminal Copyright Infringement Cases ····· 139

〈Table 13〉 Data on Appeals According to Different ICTs and Human Rights ····· 145

〈Table 14〉 Types of Complaints ····· 146

〈Table 15〉 Number of Complaints on Rights of Information Privacy ····· 147

〈Table 16〉 Number of Complaints on Freedom of Expression on the Internet ····· 148
〈Table 17〉 Number of Complaints on Right to Enjoy Information and Culture ····· 149
〈Table 18〉 Recommendations related to ICTs and Human Rights ····· 156

Chapter 1

Introduction

▸ **Section 1.** The Importance of Report on Information and Communication Technology and Human Rights

▸ **Section 2.** General Information on Different Types of ICTs and Human Rights

Section 1. The Importance of Report on Information and Communication Technology and Human Rights

South Korean society has rapidly developed from agricultural to industrialized, and finally to information society. Government ICT strategy, first implemented in the early 1990s, enabled South Korea to become an advanced information society. However, the level of legal or institutional reforms fell behind. Widely spread internet services and cutting-edge information technology have made life easier and have led to the increase of communication. Nonetheless, the development in information technology has certainly caused some side effects-personal information is now easily collected and distributed; rapid progress is being made in mass surveillance technology; social inequality based on accessibility to information and communication technology intensifies.

The Constitutional Court, in its decision,[1] recognized that certain social changes led to the emergence of the need for approval of the right of controlling one's personal information as a newly emerging form of basic human rights.

Human societies have transformed from industrialized societies into information-based societies in the late 20th century due to the rapid development in computer and communications technology. Alongside this drastic change, constitutional issues regarding the management of personal information have emerged.

As the role of the government has expanded, the public holds high expectation on government provision. In order to meet their expectations and to promote public welfare in an efficient way, nations are required to collect and manage private information. Development in information communication technology enhances administrative institutions' ability to collect and manage information and thus improves efficiency and fairness in administration. Information technology is definitely necessary in order to provide the public more stable and fair treatment.

However, improvement in information technology casts a shadow. Personal

1) Constitutional Court 2005.5.26. Decision 99Hun-Ma513

information database, is not only ubiquitous but also managed and utilized with ease. Also, as institutions can interchange information through automated information processing systems, different institutions can simultaneously use personal information data. Eventually, the government as well as the information and communications enterprises can overlook and control individuals in systematic ways. In other words, individual's personal information can be collected, utilized and made public regardless of his or her intentions and governmental surveillance upon individual privacy is increasing.

Under these circumstances, recognizing the right of controlling one's personal information as one of basic human rights, and thus protecting personal information from dangers inherent in developed information and communications technology, is deemed as a minimal constitutional apparatus for protecting self-determination and the fundamentals of liberal democracy.

Moreover, as the number of petitions regarding ICTs and human rights issues increased, National Human Rights Commission of Korea faced demands for resetting the direction and scope of ways of approaching ICTs and human rights issues through examining current status according to the commission's previous recommendations and through organizing diverse stances on the issue.

As Alvin Toffler has asserted,[2] South Korean government has not yet published any official report that introduces the basic concept of ICTs and human rights. Also the values stated in the Universal Declaration of Human Rights are ignored on the Internet. We have decided to publish an official report that will help South Korean government establish a balanced policy that protects human rights values through reducing the information gap.

Utopian as well as dystopian views have coexisted since the birth of information society. The digital world, or the cyber space also bears pros and cons, but those

2) Alvin Toffler, argued, "Korea has successfully followed the industrial society models accumulated by the United Kingdoms and the United States. but no verified model is left for Korea to follow and the world is watching Korea." (Alvin Toffler, Beyond the crisis: Korea in the 21st Century, 2001, Korea Information Society Development Institute, p32.)

negative aspects are proliferated due to its characteristic features.[3)]

Governments can utilize electronic government system which, through collecting personal information, enables governments to achieve efficiency while facilitating governmental censorship. Especially, considering that governments have been trying to strengthen their power through "a control-mechanism," or a systematic way of monopolizing and utilizing information, we can easily assume that information technology can be employed to censor and control the public.

In terms of business, information technology can produce numerous business models and create profit while the danger of "personal data leakage" prevails. There is a possibility that a new identity of oneself may exist in cyber space. Also, individuals may now overlook others like the governments or enterprises do.

Therefore, ICTs and human rights is becoming a global issue. However, debates on ICTs and human rights issues have been dispersed among diverse academic fields such as law, politics, education, and engineering, and have failed to come up with a holistic approach to implement an institutional change.

This report aims to introduce international trend in handling ICTs and human rights and to highlight national issues regarding ICTs and human rights to show current problems in legislative approaches to the issue. It will also analyze the commission's activities regarding ICTs and human rights and report their progresses to the National Assembly and the President. We hope this would become a touchstone for implementing a new legislative strategy that meets 21st century global standards for protecting human rights. National Human Rights Commission of Korea aims to promote policy directions and standards. This report was written in accordance with National Human Rights Commission Act Article 19 subparagraph 1.[4)]

---

3) Korea Agency for Digital Opportunity and Promotion (2009), "Research on the Policy Plan for the Digital Risk Society"

4) Article 19 (Duties)
The Commission shall perform the duties of the following subparagraphs:
1. Investigation and research with respect to Acts and subordinate statutes (including bills submitted to the National Assembly), institutions, policies and practices related to human rights, and recommendation of their improvement or presentation of opinions thereon;

Section 2. General Information on Different Types of ICTs and Human Rights

1. Discussions on ICTs and Human Rights and its Basic Concepts

Since the 1990s, many scholars have participated in diverse discussions on the Information Society in which, unlike in Industrialized Society, information places center of the power.[5] However, regarding the fact that many now take Information Society, which is based on computer, internet and digital revolution, as granted, discussions on its difference with Industrialized Society are pointless.

Many initially approached the term “ITCs and Human Rights” as a new form of constitutional right which evolved in Information Society due to revolutionary development in internet and information technology. In 2001, human rights on information was re-named as “information basic rights” and since then, it was

---

2. Investigation and remedy with respect to human rights violations;
3. Investigation and remedy with respect to discriminatory acts;
4. Investigation on actual conditions of human rights;
5. Education and propaganda of human rights;
6. Presentation and recommendation of guidelines for categories of human rights violations, standards for their identification and preventive measures therefor;
7. Research and recommendation with respect to the conclusion of any international treaty on human rights and the implementation of said treaty, or presentation of opinions thereon;
8. Cooperation with organizations and individuals engaged in activities to protect and improve human rights;
9. Exchanges and cooperation with international or foreign organizations for human rights protection; and
10. Other matters deemed necessary to guarantee and improve human rights.

5) The concept of information society can be distinguished analytically by technical, professional, spatial, cultural criteria. Also, there are Daniel Bell’s conceptualization of post-industrial society that emphasizes the importance of information, Anthony Giddens’s work on the nation states and violence that shows the role of data accumulated through surveillance, Herbert Schiller’s view on advanced capitalism’s demand and manipulation of data, Jüergen Habermas’s discussion on the contraction of public domain and weakening of the integrity of data, argument that current society is moving into post-Fordism where management of data is the key to success. (see F. Webster, Theories of the Information Society, 1995).

conceptualized as “ICTs and Human Rights” in a more independent / holistic view.[6][7] Since then, scholars have been discussing on “ICTs and Human Rights,” often referring it as “human rights issue in information society” or “information basic rights.” Ministry of Information and Communication facilitated Korea Information Society Development Institute, a national policy research organization, to publish the “Reports on developing information-communication public policy” with scholars in the field. Civil society organizations also made efforts to familiarize Koreans with the term “ICTs and Human Rights” by raising several social issues including electronic identification card issues and privacy issues raised by the implementation of the NEIS system. The term was publically used around 2003 in diverse literature written by social activists.[8] In 2003, National Human Rights Commission of Korea hold an open forum on “Human Rights Issues in Information Society,” invited scholars, legal experts, activists, legislatures and administrative institutions as panels, and used the concept “ICTs and Human Rights” for the first time in its public release (published in August 13th, 2003). The concept was also used in a public release published in November 13th, 2003, which expressed its opinion on revising Act on the Protection of Personal Information Maintained by Public Institutions. The Commission has selected “Privacy infringement / information gap and other protection of information right” as one of its major task in 2008 while placing ICTs and Human Rights protection as one if its major 3-year-long-business plan (2009~2011). In 2012, the Commission has pushed ahead plans to enhance ICTs and Human Rights.

Thus, the term “ICTs and Human Rights” seems to have originated from the concept “information basic rights” that was used among the scholars. It was spread among the public in 2002, as social activists raised issues around NEIS (National Educational Information System) and used campaign slogans that included such terms.

---

6) Kim Bae-Won, “Public opinion for independent/holistic protection of information-related rights”, Korea Constitutional Law Association, *Constitutional Law Review* (2001.8)

7) Organized the search result of keywords “Information basic rights”(54 results) and “information rights” (224 results) in the Library of National Assembly.

8) Oh, Byung-Il, “Seeing ICTs and Human Rights with the Opening of World Moonhwa Gwahak Sa.

After that, the concept has been growing its scope to encompass these issues-issues on privacy, information-communication confidentiality issues, right of controlling one's personal information, information accessibility right, freedom of expression on the Internet, and right to enjoy information and culture.

The concept of ICTs and human rights is not clearly defined. Many scholars often provide different definitions;[9)]

9) See the following work of scholars 1. Lee In-Ho, "Citizen's control on the distribution of information 'Freedom of information (freedom of fair information)' and 'information privacy(protection of private information)' for the constitutional information order", 'Constitutional frame that discussion of ICTs and human rights suggest: Tension and harmony of the authority and freedom around information in the digital era', *Legal Studies* Vol. 3, Catholic University Center for Legal Studies(2008)

2. Lee, Chang-Bum, "ICTs and human rights is the right of having protection and free equal access to the digital information and media and is composed of the right to participate in information production, right to disclose and share information, right to access the information, right to enjoy information, and right to control one's own information."

3. Lee, Min-Young, "ICTs and Human Rights is the right that protects the dignity of man from the process of collection, distribution, and use of information and the value of produced information, and in result, leads to the improvement of life" 'Legal meaning and coordination of ICTs and human rights', National Human Rights Commission Joint Symposicum(2010)

4. Kwon Gun-Bo, "ICTs and human rights is a general concept of the right to easily access the information required for communication, and furthermore, right to control one's information.", 'Promotion of ICTs and Human Rights and the role of National Human Rights Commission", 「Results, Challenges, and Prospects of National Human Rights Commission」, National Human Rights Commission of Korea·Constitutional Law Association Joint SyKim, Bae-Won, "ICTs and human rights is the result of securing the independent status for the rights that are correlated around information in the name of information constitution.", Public opinion for independent/holistic protection of information-related rights", Korea Constitutional Law Association, *Constitutional Law Review* (2001)

6. Kim, Sang-Kyum, "ICTs and human rights emerged as the discussion of human rights related to information began as the society moved into the information society. And ICTs and human rights is the comprehensive term explaining the human rights related to the information.", 'Research on the protection of personal information in the information state', *International Study of Constitution* Vol. 14, Issue 3

7. Ha Woo-Young, "ICTs and human rights is the development of the conventional right in the era of information era and is indispensable for the freedom and equality in the information.", 'Dealing of labor information and protection of ICTs and human rights', Journal of Information Protection Association Korea, Vol. 13, issue 6 (2003)

However, it is generally regarded as a form of basic rights on information. Though it is a newly emerged independent basic right, it can also be understood as an element of preexisting rights. That is, while ICTs and human rights can also be protected through assuring preexisting basic human rights such as the freedom of speech, which is directly and indirectly related to information management, there are some subparts of ICTs and human rights-such as right to know, right to access, right to control one's personal information-cannot be incorporated in the scope of traditionally recognized forms of human rights. It is often acknowledged as a basic right that is not delineated in the Constitution[10] but is deducted from other preexisting basic rights or other constitutional principles.

As discussions on ICTs and human rights prevail, the Commission has hosted a forum[11] and has discussed on the concept and different categories of information right with experts of diverse fields. Some suggested that, though scholars often confuse the concept of human rights and the concept of basic rights, the Commission should use the concept of ICTs and human rights rather than that of information basic rights as the former is more in accordance to its policy direction. They also encouraged the commission to use the concept of ICTs and human rights in order to prove that Korea, as a nation of developed internet technology, achieves prominence in developing information right. Also, panels at the forum claimed that the concept of ICTs and human rights should be an expansive, not a restrictive concept and that it should be able to encompass potential human rights issues that are to be raised in the course of the development of information technology. This report defines "Information and Communication Technologies (ICTs) and Human Rights ("Information Rights")" as basic human rights that guarantees free and nondiscriminatory use of digital information earned by information communication technology.

---

10) Constitutional Court 2005.5.26. Decision 99Hun-Ma513

11) 1st Information Rights forum: Discussion on the Definition and Types of Information Rights (2012.10.5.).

2. Types and Contents of ICTs and Human Rights

There can be diverse types of ICTs and human rights derived from different concepts and distinctive usage of the term 'information.' The definition of 'information' may vary-it may be a digital information realized by technological terms, '0' and '1,' while it may be defined as socially significant data. In legal terms, the word "information" is widely used as a general terminology-it appears 694 times in laws and 2,052 times among the whole legislation.[12)]

The word "information" is derived from the concept of "informatio."[13)] Generally, in social terms, it is understood as "informed knowledge on circumstances and situations of objects." However, as the information society emerged, the concept of information went through a transformative stage. Due to the development of information technology, every pieces of information are now transferred in digits, unlike how they once had been transferred in analogue method. The integration of information, which enabled different types of information such as music and image be managed through the same formation, led this transformation of information.

Likewise, information began to rapidly transform into electronic information, and this spread of electronic information led to the advent of new exchangeable objects such as electronic items and database. Many anticipate that these will gain higher economic value in the future.[14)]

Thus the concept of one-dimensional information, mainly transferred through printed media, is now substituted by the concept of multi-dimensional information due to the rise of digital information technics. This poses a fundamental change in the traditional view of information and circulation system.

Article 3 of Framework Act on National Informatization specifies that "information

12) Lee Min-Young, "Meaning and coordination of information rights" Commission of human rights, 2010.
13) Christopher John Fox, Information and Misinformation: an investigation of information, misinformation, informing, and misinforming, Westport, Conn., Greenwood Press, 1983, pp.4～6.
14) Lee Min-Young, Theory on Personal Information Law, Jinhan M&B, 2007, pg 23

is any form of data or knowledge, with some purpose, processed through optic or electronic methods, and expressed through signals, letters, voice, or images." This limits the definition of the word information so that it only stands for digitalized information processed through optic or electronic methods.

We should focus not only on the benefits that are offered by the development of information-communication technology but also on problems that are newly emerging. Things that were not matters of concern in offline world are now viewed as problematic as it is becoming ever more difficult to provide legal interpretations. To focus more on the human rights issues that stem from these matters, it would be better for us to limit the bounds of information to digitalized information.

There is no well-formulated way to categorize ICTs and human rights and thus some scholars have come up with disparate ways to classify it.[15] Though they vary, the categorization systems generally classify information right under two big notions-the freedom of public information and the protection of personal information. Information right is then categorized into smaller groups-rights of privacy, rights to freely express one's opinions, and rights to access information. Some include rights to cultural enjoyment as one another subgroup.[16]

---

15) 1. Lee In-Ho "Constitutional frame that discussion of ICTs and human rights suggest: Tension and harmony of the authority and freedom around information in the digital era", *Legal Studies* Vol. 3, Catholic University Center for Legal Studies(2008)
2. Lee, Min-Young, "Legal meaning and coordination of ICTs and human rights", 「Legal protection and materialization of ICTs and human rights」, National Human Rights Commission · Catholic University Joint Symposium (2010)
3. Kwon, Gun-Bo, Promotion of ICTs and Human Rights and the role of National Human Rights Commission", 「Results, Challenges, and Prospects of National Human Rights Commission」, National Human Rights Commission of Korea · Constitutional Law Association Joint Symposium (2012)
4. Myung, Jae-Jin · Lee, Han-Tae, "Research trends on the ICTs and human rights in the field of modern legal studies", 「Information Policy」 Vol.18, Issue 1(2011)
5. Kang, Byung-Geun 「Constitution」(2004)
6. Kim, Bae-Won, "Consideration on the independence and proper range of ICTs and human rights-focus on the formation of structure relating to the constitutional amendment", 「Constitution Studies」 Vol.12 issue 4 2006

16) Lee In-Ho "Constitutional frame that discussion of ICTs and human rights suggest: Tension and harmony of the authority and freedom around information in the digital era",

However, this categorization system is not structured-it rather shows different aspects of rights. So it is more important to look into present conditions of human rights issues than trying to devise a consistent way of classification.

Also, as this report defines information right as "fundamental right to use digital information that is collected, processed, distributed and used without damaging human dignity, in free and nondiscriminatory ways," it may face some problems if it only focuses on discussing categorization methods. If it follows the general categorization method, some may argue that information right cannot be easily differentiated and that it will be seem congruous with constitutional basic rights.

In regards to the independence property of ICTs and human rights, we should not forget that though some aspects of ICTs and human rights can be protected by protecting related basic rights such as freedom of speech, freedom of expression, and rights to protect one's privacy, there are particular aspects that cannot be incorporated to preexisting constitutional rights nor can be derived by constitutional principles. One of those particular aspects are newly emerged rights such as rights to know, rights to access, and rights to control one's private information.[17)]

As mentioned earlier, though the mechanisms through which information right is protected is quite similar to that of pre-existing constitutional rights, the subject of debate here is information itself. It is pertinent to note that we should focus on specific phenomenon that rise within the mechanism of digital information transformation.[18)]

For example, the concept of modern right of privacy was initially used by Justice Thomas Cooley, who in 1880 presented right of privacy as "the right to be let alone" in his own book on tort law cases.[19)] Warren and Brandeis developed this term in

---

Legal Studies Vol. 3, Catholic University Center for Legal Studies(2008)

17) Kwon Gun-bo(2012), "Promotion of ICTs and Human Rights and the role of National Human Rights Commission", 「Results, Challenges, and Prospects of National Human Rights Commission」, National Human Rights Commission of Korea·Constitutional Law Association Joint Symposium

18) 1st Information Rights forum: Discussion on the Definition and Types of Information Rights (2012.10.5.).

19) Thomas C. Cooley, Laws of Torts (1st ed. 1880), Sec. 29.

their works[20]-they argued that "right of privacy if essential for individuals living in advanced civilized world." Right of privacy before the advent of computer and digital technology is often referred to as the first-generation-right of privacy while the right to control one's personal information is often called as the second-generation-right of information privacy.

The conventional type of right of privacy, the first generation right of privacy, is the right to be let alone, or the "right to refuse disclosure of private data." In other words, it is rather the right of protect one's secrecy in private lives in physical realm. Compared to this, the second generation right of privacy, or the right to control one's private information, as the Constitutional Court defines,[21] enables individuals to participate in the processing stage of his or her own personal information. It includes right to be informed of the purpose of the collection of personal data and the ways in which it would be controlled, right to claim inspection, right to claim for correction, and etc. This new type of right or privacy is required in current information environment in which the state and businesses can easily collect, process and provide digitalized personal information.

Moreover, some view that concept of right of privacy should be adjusted so that it can adapt to the new communication environment. They argue that privacy protection methods are based on pre-existing concepts and that they fall short to solve problems that are emerging in the internet.

In other words, it is unrealistic to rely on information privacy concepts in network environment considering the fact that the environment is already designed according to unequal distribution of power among individuals or the innate social nature of networks. Especially, considering the fact that the unequal distribution of power among individual users and information agencies is based upon one's ability to identify, some assert that we should put the right to refuse to be identified at the center of our debate.[22]

---

20) Samuel D. Warren & Louis D. Brandeis, "The Right of Privacy", 4 Harv. L. Rev. 193, 195 (1890)

21) Constitutional Court 2005.5.26. Decision 99Hun-Ma513

Furthermore, when approaching the issue of data disclosure, one should take into consideration that a lot of information is transparently transferred online. Also, one should consider copyrights enable strangers to request for the disclosure of information as well as allowing them to let others fully enjoy their works.

Therefore, what we should focus on the digitalized information when explaining ICTs and human rights. It is important to look into the incidents that happen along the life-cycle of information.

The aforementioned right of privacy as well as ICTs and human rights cannot be easily distinguished from constitutional rights if we define them as something that resembles existing basic human rights such as freedom of speech. This report will try to focus on ICTs and human rights as something that has peculiar aspects that cannot be explained by traditional constitutional approaches and will try to deliver specific social issues[23] that are to emerge in this digitalized information society.

This report will also refrain from developing a structured definition for information right as there is no consensus standards. Rather, it will try to enumerate different subparts of information right following some of the common categorization method that a number of scholars use.

---

22) WOO Jisuk, From information privacy to identity privacy - Reconsidering the concept of network privacy, the Press and the Society, Vol. 13. No. 4.

23) Right of information privacy not right of privacy, freedom of expression on the Internet not freedom of expression, right to access information not right to know, right to enjoy information and culture not right of culture and art.

Chapter 2

Current Status and Issues of ICTs and Human Rights

- **Section 1.** Right of Information Privacy
- **Section 2.** Freedom of Expression on the Internet
- **Section 3.** Right of access to information
- **Section 4.** Right to Enjoy Information and Culture

Section 1. Right of Information Privacy

1. The Need for Protecting Right of Information Privacy

Right of privacy is one of major basic human rights that should be cherished and be protected as it certainly is a touchstone of a democratic society. It is a foundation of the freedom of the individual-political freedom, freedom of expression, freedom of assembly-and other values that our society protects.

Due to the rapid development in Information Communication Technology (ICT), it is becoming easier to collect and store personal information. Demands for personal information in both the public and private sphere are increasing proportionally. Privacy is in great danger and protection of information privacy has become one of most hotly debated public policy issues worldwide.

As personal data are often leaked, misused or abused, many argue that unprecedented development in information communication technology has posed negative impact on independent autonomy, individuals' social relations and democracy itself. They claim that more and more are suffering of insults and economic damages as well as discriminatory treatments. Especially since the 9.11 terrorist attack, legislators of each nations have been trying to find ways to balance the value of individual freedom and that of national security. Privacy protection is still a big social and political issue.

Personal surveillance and data collection enable enterprises or governments to categorize people into groups and thus intensify social discrimination. Moreover, surveillance infringes on rights of privacy and other basic rights such as freedom of expression and freedom of assembly. Therefore in order to protect privacy in information society, we, the bearers of our own personal information, should be able to determine how and when our personal data can be provided to others.

Information privacy is the right of individuals to self-regulate his or her own private data. As many privacy infringements are done through collecting, manufacturing, utilizing and distributing personal information, information privacy issue is equivalent

to an issue on how one can control the collection and usage of his or her personal data. In that sense, information privacy is different from traditional form of privacy which generally means an exclusion of intrusion in private life.

Right to control one's personal information is the core of information privacy. It is consisted of mainly three different subparts-right to consent to collect and use personal data, right to withdraw one's consent, right to request for correction and deletion, right to request for checks on processing history. A number of states emphasize on anonymity in processing personal information. Yet, anonymity is generally just a subject of advice, so it may not develop to become a form of information right.

As mentioned earlier, information privacy problems include problems in using information communication technology, issues in collecting, using and transferring personal information and other legal/political issues.

2. International Standards

(1) Current Trend

We can observe two disparate trends in collecting and utilizing personal information. Internationally, there is a tension between governments (especially the investigative or the law enforcement agencies) or corporates that wish to widely collect and use personal information and citizens (or consumers) who wish to protect their own privacy. Privacy protectionists assert that the improvement in ICT poses a threat to democracy as it enables entities to easily collect, store and use personal information. Though they claim that we should protect individual autonomy in order to defend democracy, investigative and law enforcement agencies claim that it is inevitable to collect and use personal data for efficient investigation and law enforcement. Corporates also claim that they should be guaranteed to do business in a creative and liberal way through utilizing personal data.

1) The Creation of Anti-terrorism Law and Data Storage Law

Since the 9.11 terrorist attack, nations have been working to enact anti-terrorist laws. Anti-terrorist laws not only have wide ranges of application but also lack strict standards on governmental intrusion. Although many criticize that these laws lack procedures to prevent them being abused, there has been an increase in the number of these laws being legislated in various countries. Increase in the number of monitoring cases by using CCTV aggravate the crisis. A number of western countries including U.K. have increased their use of CCTV with the purpose of crime prevention and investigation.

There has also been a rise in legislating laws that enable preserving usage records of internet, mobile phones and other communication services. In March 15, 2006, EU, pressured by law enforcement agencies, adopted Directive 2006/24/EC[24] which regulates enterprises to store any information in the supply and usage of electronic communication service or public communication network service. Under the directive, enterprises should store data that help one to track location and to check date, time, period and form of communication. Also it requires them to keep data used to check the exact communication device used, and to locate the device. These data should be kept at least for 6 months and some are kept for 2 years max. U.S. federal government has also been trying to require enterprises to store communication data. A bill that makes it an obligation for electronic communication service providers or remote-computing service providers to store identity information for at least 2 years was passed at both the House and the Senate in 2009.[25] In July 2011, a bill[26] that requires internet service providers to keep the log record of every users for 12 months in order to expedite investigations on child pornography was passed in Senate Judiciary Committee.

---

24) "Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC"

25) The Internet Stopping Adults Facilitating the Exploitation of Today's Youth (SAFETY) Act of 2009 (H.R.1076 and S.436).

26) Protecting Children From Internet Pornographers Act of 2011.

Corporates are also implementing aggressive marketing techniques based on big-data such as customer relationship management (CRM), tailored online advertisements, 1-on-1 direct marketing and analysis method on consumer trends. There has been an increase in the number of enterprises that specialize in online advertisement. These enterprises continuously trace and analyze potential consumers and produce advertisements that would work for them. Recently in U.K., there was a controversy over Phorm, a corporate that analyze internet users' web surfing records using technology called "Deep Packet Inspection." It was mainly on Phorm's monitoring techniques that in 2008 had raise unlawful monitoring issues. Despite this, BT, one of the largest communication enterprise in U.K., was known to have applied this techniques and been investigated by U.K. Fair Trade Commission and Crown Prosecution Service.[27] There was similar issue in U.S. in 2008-NebuAd's packet monitoring technique, which resemble Phorm's monitoring techniques, was adopted by Charter Communications, Inc. Congressional hearings were held and eventually Charter Communications withdrew their plan to adopt the packet monitoring technique.

Moreover, new information communications services based on IT, such as SNS, mobile service based on GPS, and internet map services, are causing serious privacy issues.

2) Reinforcing Rights of Information Subjects and the Right to be Forgotten

Meanwhile, on the contrary, as cloud-computing, social network services, and big-data services are becoming more common, we can observe efforts to legislate or design policies that reinforce the protection of privacy. In May 29, 2009, delegates from twenty-seven member states of Council of Europe, a pan-European supportive organization, adopted "Resolutions on the new notion of media, critical internet resources, and the protection of freedom of expression and information with regard to anti-terrorist laws" to protect freedom and expression and personal information

27) Phorm and BT (British Telecom) Group conducted several trials since 2006, but finally abandoned launching the online behavioral targeting advertising service on July 2009.

from anti-terrorist laws. Prior to that, in March 26, 2009, European Parliament adopted "'Proposal for a European Parliament Recommendation to the Council on Strengthening Security and Fundamental Freedoms on the Internet " in order to protect right of privacy of internet users. European Commission in January 25, 2012 has also suggested General Data Protection Regulation,[28] which mainly deals with ways to strengthen the right to peruse, to regulate profiling, and to introduce right to be forgotten in cloud-computing and social network system. These efforts show that legal and institutional investigation and supplementation processes on personal surveillance and personal information collection indiscriminately practiced by law execution institutions and enterprises are becoming more serious.

There are many advocates of personal information protection act in U.S. Though there already are several different state statutes that aim to protect personal information, they claim that there should be a general federal law that can be applied to all private sectors in order to eradicate blind-spots of personal information protection. Reflecting this, White House announced "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy" in February 2012, and a month later, FTC adopted "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers." The recommendation mainly covers these areas-online do-not-track function, "Privacy by Design," mobile privacy, platform privacy and data broker regulation. Both the framework announced by White House and the recommendation adopted by FTC urge for enacting a federal personal information protection act. At the state-level, several states including Illinois, Alaska, Arkansas, California, Vermont, Wyoming and Kansas enacted personal information protection laws.

Twenty-seven EU members, U.S. and Canada have announced 28th of January as National Data Privacy Day. Governments, local governments, corporates and schools participate in various programs to protect privacy. One of major purposes of designating

28) European Commission (2012.1.25), 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.

this day as National Data Privacy Day is to raise the level of consciousness of data privacy especially among teenagers and to promote data privacy education. It aims to allow teenagers to speak up about privacy and to raise them as self-protectors of their own privacy. Thus on this day, privacy specialists, corporations, governmental agencies and legislatures join schools, teachers and students to participate in heated debates on right of privacy.

(2) International Standard

Governments and international organizations' interests on right of privacy and efforts to protect it are expressed in diverse ways. The Universal Declaration of Human Rights, proclaimed in 1948, is the first international rule that recognizes individual's right of privacy.[29] The European Commission has adopted "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" in 1981, which includes principles on collection, storage, usage and international transference of personal data. The European Union, under "Directive on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data (1995)," has made it an obligation for all member states to legislate personal information protection laws and independent institutions that work for personal information protection. Also EU bans transferring personal data to nations that fail to reach certain level of personal information protection.

OECD has also adopted and recommended "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ("OECD Privacy Guideline")" in 1980.

---

29) Article 12 No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.; ARTICLE 8 (Right to respect for private and family life) 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

OECD Privacy Guideline regulates that personal data should be collected directly from its owners and should be used only for specified purposes. Also the information owners have rights to be informed how their personal data are collected and used. They should also be able to access and correct their personal data if needed. Moreover, the guideline suggests that independent personal information manager should be appointed to overlook the process.

Most recent international rule on data privacy protection is "APEC Privacy Framework (2004)." APEC Privacy Framework is adopted in order to protect privacy in collecting and utilizing personal information and to promote safe electronic commerce. It is based on OECD Privacy Guideline but includes new principles for preventing harm, notice, and choice. Korea has also contributed much in adopting this framework.

In 1997, ILO has also adopted a Code of Practice named "Protection of Workers' Personal Data"[30] to protect laborers' privacy while signing employment contract or during the employment period. It overlooks collection and usage of workers' personal data and surveillance on workers or workspaces. It does not have a legal force to restrict member states but works as a guideline. It adopts 13 major principles including principles on fair collection of personal data, principles on usage on its sole purpose, and principles on limiting electronic monitoring.

The 12th ASEM Seminar on Human Rights held in Seoul in June 2012 presented following guidelines. Firstly, stressing the need for regulation based on governmental human rights protection, it suggested that public agencies as well as private sectors should be held responsible for personal data protection, that they should prevent human rights abuse through applying governmental human rights protection framework, and that they should adopt multilateral approaches for regulating data protection and privacy protection issues. Secondly, it suggested that there needs to be an effective solution to guarantee data privacy rights and that establishing independent institutions and introducing information managers for each corporates

30) "Protection of Workers' Personal Data" (1997)

should been expedited. Also it suggested that corporates should fulfill their social responsibility, that fundamentals on privacy and private information protection (right to know, right for consent, right to access personal data, right for truth and security) should be applied, and that privacy protection technologies should be implemented. Thirdly, it delivered that it is important for the young generation to acknowledge the importance of personal data protection and that there should be international collaboration in legislating related laws and in enhancing rights of privacy especially of minors and the disadvantages.

〈Table 1〉 Major Contents of Eight Principles of OECD Privacy Guideline

Principle		Contents
Principle 1	Collection Limitation Principle	• Data collection through lawful and fair means • Collection with the knowledge or the consent of data subject
Principle 2	Data Quality Principle	• Need for relevance to the purposes for which they are to be used • Personal data should be accurate, complete and kept up-to-date, to the extent necessary for those purposes
Principle 3	Purpose Specification Principle	• Need for specification of the purposes for which personal data are collected no later than at the time of data collection • Subsequent use limited to the fulfilment of those purposes
Principle 4	Use Limitation Principle	• Personal data should not be disclosed, made available or otherwise used for other purposes except with the consent of the data subject or by the authority of law
Principle 5	Security Safeguards Principle	• Protection of Personal data by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data
Principle 6	Openness Principle	• Need for general policy of openness about developments, practices and policies with respect to personal data • Readily accessible means of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller
Principle 7	Individual Participation Principle	• Need for protecting individual right to have the data erased, rectified, completed or amended • Need for guaranteeing readiness in accessibility
Principle 8	Accountability Principle	• Data controller being accountable for complying with measures

〈Table 2〉 Major Contents of EU Directive on the Protection of Personal Data (1995)

Sections	Contents
Duties of Data Controller	• Process fair and lawful personal data • Publicize the purpose of data processing • Maintain propriety, relevance, and proportionality with the purpose • Secure correctness of data and keep them up-to-date • Secure technological and organizational security measures • Notify the national supervisory authority of any processing operation
Data Subjects' Rights	• The right to be informed of general facts on data processing • The right to discuss general facts on data processing • The right to request change on one's personal data • The right to object, on legitimate grounds, to the processing of data relating to him/her.
Ban on Transferring Data to a Third Country	• Transfers may not be made to a third country which does not ensure this level of protection
Establishment of Independent Public Authority	• Establishment of independent public authorities responsible for monitoring the application

〈Table 3〉 Major Contents of ILO Code of Practice on the Protection of Workers' Personal Data (1997)

Principle		Contents
Principle 1	Restriction on Personal Data Process	• Personal data should be processed lawfully and fairly, and only for reasons directly relevant to the employment of the worker
Principle 2	Prohibition of Use for Other Purposes	• Personal data should, in principle, be used only for the purposes for which they were originally collected
Principle 3	Compatibility with the Original Purpose	• If personal data are to be processed for purposes other than those for which they were collected, they should not be used in a manner incompatible with the original purpose
Principle 4	Prohibition of Use to Control Behaviour	• Personal data collected in connection with technical or organizational measures to ensure the security and proper operation of automated information systems should not be used to control the behaviour of workers
Principle 5	Prohibition of Overdependence on Automated Processing	• Decisions concerning a worker should not be based solely on the automated processing of that worker's personal data

Principle		Contents
Principle 6	Limitation on Performance Evaluation	• Personal data collected by electronic monitoring should not be the only factors in evaluating worker performance
Principle 7	Regular Assessment of Data Processing Practices	• Employers should regularly assess their data processing practices to reduce the kind and amount of personal data collected and to improve ways of protecting the privacy of workers
Principle 8	Informing of Rights	• Workers and their representatives should be kept informed of any data collection process, the rules that govern that process, and their rights
Principle 9	Training and Understanding of Role	• Persons who process personal data should be regularly trained to ensure an understanding of the data collection process and their role in the application of the principles in this code
Principle 10	Prohibition of Discrimination	• The processing of personal data should not have the effect of unlawfully discriminating in employment or occupation
Principle 11	Cooperation for Privacy Protection	• Employers, workers and their representatives should cooperate in protecting personal data and in developing policies on workers' privacy consistent with the principles in this code
Principle 12	Confidentiality	• All persons, including employers, workers' representatives, employment agencies and workers, who have access to personal data, should be bound to a rule of confidentiality consistent with the performance of their duties and the principles in this code
Principle 13	No Waiver	• Workers may not waive their privacy rights

〈Table 4〉 Major Contents of APEC Privacy Framework (2004)

Principle		Contents
Principle 1	Preventing Harm	• Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information • Acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information

Principle		Contents
Principle 2	Notice	• Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information • Such notice should be provided either before or at the time of collection of personal information. Otherwise, such notice should be provided as soon after as is practicable
Principle 3	Collection Limitations	• The collection of personal information should be limited to information that is relevant to the purposes of collection • Such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned
Principle 4	Uses of Personal Information	• Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes except a) with the consent of the individual; b) when necessary to provide a service or product requested by the individual; or, c) by the authority of law and other legal instruments, proclamations and pronouncements of legal effect
Principle 5	Choice	• Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information
Principle 6	Integrity of Personal Information	• Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use
Principle 7	Security Safeguards	• Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses
Principle 8	Access and Correction	• Individuals should be able to obtain from the personal information controller confirmation of whether or not he/she holds personal information about them; have communicated to them, after having provided sufficient proof of their identity, personal information about them; and, challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted

Principle		Contents
Principle 9	Accountability	• A personal information controller should be accountable for complying with measures that give effect to the Principles stated above • When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles

3. Data Privacy Law

(1) Enactment and Implementation of Personal Information Protection Act

The Personal Information Protection Act, which had been first debated by the members of the 17th National Assembly, passed through congress in March 29, 2011, and has been in practice since September 30, 2011. Article 1 of the Personal Information Protection Act makes clear that the law aims to “protect privacy from collection, leak, abuse, or misuse of personal information to promote citizen’s rights and interest and implement value of personal dignity.” Article 3 announces general principles for personal information protection and seeks to harmonize them with other internationally recognized principles. The following table compares personal information protection principles of international rules with those of the Personal Information Protection Act. These principles are just declaratory norms-yet they propose standards in implementing personal information protection policy for policy makers, work as personal data processing guidelines, and provide theoretical criteria necessary in interpreting the law for the judiciary.

〈Table 5〉 Comparison between OECD Privacy Guideline and Personal Information Protection Act

OECD Eight Principle	Personal Information Protection Act
Collection Limitation Principle (Principle 1)	• Limitation on collection to the minimum extent necessary (paragraph 1) • Management of personal information in such a manner that the privacy infringement of a subject of information is minimized (paragraph 6) • Principle of anonymous management (paragraph 7)
Data Quality Principle (Principle 2)	• Keeping personal information accurate, complete and up-to-date to the extent necessary within the purpose (paragraph 3)
Purpose Specification Principle (Principle 3)	• Clear management purpose (paragraph 1)
Use Limitation Principle (Principle 4)	• Appropriate management of personal information within the purpose and prohibition on use for other purposes (paragraph 2)
Security Safeguards Principle (Principle 5)	• Safe management of personal information considering the risk of infringement on the rights (paragraph 4)
Openness Principle (Principle 6)	• Public disclosure of personal information management policies (paragraph 5)
Individual Participation Principle (Principle 7)	• Guarantee of information subjects' rights (paragraph 5)
Accountability Principle (Principle 8)	• Compliance requirement of personal information managers (paragraph 8)

The Personal Information Protection Act is applied to personal information processed in online, offline and in public and private field. The enactment of the law certainly reduced the blind area in personal information protection. Also the government-affiliated independent agency that overlooks personal information protection prevents personal information being abused for political or economic reasons.

(2) Problems of Current Law and Improvement Plans

Though blind spots of personal information protection have been reduced and an independent agency has been established, problems of multiple regulation and double

supervision are raised. Western governments have adopted single legal systems to prevent those problems and have unified Data Protection Agencies (DPA). However, though we have enacted a general law on personal information protection, other individual laws such as the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. and the Use and Protection of Credit Information Act are still in practice, creating conflicts with the Personal Information Protect Act. Also, one should face redundant regulations by the Private Information Protection Committee, the Ministry of Security and Public Administration, and other related offices.

To prevent confusion due to redundant regulations and to reduce waste of budget due to competitive interference among regulatory agencies we should abolish other individual laws regarding personal information protection and unify many different administrative bodies to one Personal Information Protection Committee. Applying different standards and principles created by different agents to similar cases without any special reason is only a discrimination. Looking back the experiences of European nations of the last 40 years, we can easily find out that personal information protection principles do not need to be differentiated when being applied to online or offline corporations, manufacturing or service businesses, medical, banking, or communications industries. Therefore, we should eradicate redundant or similar rules, and under strict standards leave only those cannot be substituted by the general principles of the Personal Information Protection Act.[31)]

Initially the government opposed to the idea of abolishing various committees and unifying different governmental agencies. The government opposed while political parties as well as other organizations consented establishing an independent personal information protection committee.[32)] Yet the government's claim seemed to have lost its basis as the independent committee had already been established through

31) YI Changbeom, Direction for Reform on the PIPA from the Perspective of Comparative Law, Internet and Information Security Vol 3. No. 2, Korea Internet Security Agency.

32) Future Society Research Forum of the National Assembly, Roadmap and Main contents of the Personal Information Protection Bill (public hearing material, 2006. 11. 21.), pp48-50.

congressional discussions. UN Guidelines Concerning Computerized Personal Data Files (1990) suggests its member states to establish independent institutions that specialize in personal information protection and the EU Directive (1995) also states it as an obligation of its member states. Personal information protection agencies of EU member states are fully in charge of personal information protection policies and administrations.

To be more specific, personal information protection businesses are not spread among different offices but are concentrated in the personal information protection institutions. Also, the institution takes in charge of exceptional cases that are included in individual laws according to the execution principles of unified laws.[33] Thus, the member states merge personal protection policies, administrations and law enforcement structures and create unified institution that takes in charge of every related issues. Corporates and citizens are the ones who should suffer due to the dispersion of authority and it is a serious waste of budget and administrative ability. About 30% of officers of Personal Information Protection Committee are dispatched officials of central administrative agencies. They have only limited authority to review and vote on issues and no rights to investigate-it is actually hard to regard it as an independent institution. It is better to follow the EU model considering various aspects.[34]

4. Major Information Privacy Issues

1) Installation and Abuse of Image Information Processing Devices

Image information processing devices including CCTVs are widely installed and used for diverse purposes such as crime prevention, traffic regulations enforcement, disaster management, industrial accident prevention and store management. More than

33) YI Changbeom, supra.

34) See also, Marie Georges, History, structure, and Function of European Independent Data Protection Supervisory Authorities, International Symposium on the Role and Position of an Institution Protecting Individual Privacy (2009.10.30), National Human rights commission of Korea, for reasons for a centralized personal information protection system

4290,000 CCTVs are operated now in 2012. Especially it is estimated that CCTVs are installed in more than 100,000 out of 250,000 taxis. CCTV penetrate deeply in our private lives and the number of CCTV is increasing every year.

If one overlook others-their appearances, itineraries, and deeds-through image information processing devices such as CCTVs, private activities are easily recorded without their consent, letting one to monitor private lives of others and limit their freedom. It can actually cause serious problems. Moreover, network cameras, which not only can collect image information via internet but also are remotely controlled,[35] are posing more threat to privacy issues. In future ubiquitous society, personal image information can automatically be collected and manufactured without letting the information subject aware of the fact. Thus we should provide privacy protection standards for precaution.

〈Table 6〉 Prospect for the Increase in Number of CCTV Installation Nationwide

(thousands)

	2007	2008	2009	2010	2011	2012	Average Increase/year
Analogue CCTV Camera	2,516	3,145	3,187	3,396	3,522	3,711	8.1%
Network Camera	68	118	193	282	362	583	53.45%
Total	2,584	3,263	3,380	3,679	3,885	4,294	11.0%

Source: IDC Korea CCTV Market Study (2008)

The Private Information Protection Act restricts purposes for installing image information processing devices in public areas as following-1) cases in which the law specifically permits the use, 2) cases in which they are necessary for crime prevention and investigation, 3) cases in which they are necessary for security issues or fire prevention, 4) cases in which they are necessary for enforcing traffic regulations and providing traffic information. Also, in order to install and operate image information

35) Network cameras are those imaging devices transmitting images and sounds via an internet network, which is an open circuit network and not a closed circuit network. It is also called “web cameras.”

processing devices in public area, it needs to go through certain procedures that inform neighbors of the issue and collect their opinions. Direction boards informing that an image information processing device is operated should be installed and guidelines for its operation should be established.

Especially the Private Information Protection Act bans the installation and operation of image information processing devices in areas such as public baths, public restrooms or fitting rooms as they might noticeably infringe upon individual privacy. Yet it makes it an exception for prisons and detention centers that by law incarcerate or protect individuals. For example, in order to prevent suicide, arson, violence or breakout and especially for security reasons, exceptions are allowed.

However abusing CCTVs for crime protection, safety issues, or fire prevention without any clear analysis on the effects of surveillance cameras in crime protection is a big problem. The Ministry of Public Administration and Security, which is in charge of personal information protection policies, encouraging and facilitating the establishment of regional CCTV Control Centers is also a more serious problem. According to governmental comprehensive plans for CCTVs (2011.5), the Ministry of Public Administration and security will facilitate the establishment of CCTV Control Centers in 230 local governments by 2015. The ministry aims to integrate 100,000 public CCTVs used for crime protection, child protection and disaster protection and plans to make MOU contracts with military camps to let them use personal image information for military purposes. If CCTVs are integrated, investigation institutions or military camps can demand for personal image information anytime and thus it may pose serious threat to privacy protection.

In order to prevent the use of CCTVs only to expedite investigations, we should 1) order regional governments to come up with a more concrete purposes in establishing CCTV Control Centers, 2) provide requirements and procedures for minimum sharing of personal image information, 3) make CCTV operations procedures public, 4) guarantee residents, human rights organizations, or other specialists to participate in setting purposes and guidelines for CCTV usage.

Moreover, the Ministry of Public Administration and Security should try to minimize any threats to human rights issues by organizing consultation groups for operating CCTV Control Centers with the help of human rights organizations, personal information specialists, and other related administrative bodies.

2) Increase in the Collection and Use of Fingerprints, DNA and other Biometric Data

Biometric data such as fingerprints, facial information, iris code, voiceprint and DNA are information that are inherent to individuals and can neither be revised nor altered. These types of information can be used to identify individuals easily but at the same time have high possibility of posing threats on privacy protection. Once those types of information are leaked or counterfeited, one should suffer under unresolvable pain and should face uncomfortable incidents as individuals cannot give up the data. Also as biometric data consists of a person's biological information such as ethnic characteristics, medical condition, or genetic disorder, leakage or misuse can cause enormous harm.

Recently, biometric data such as fingerprints, iris code, and DNA are collected and used for various purposes such as criminal investigation, searching for the missing person, identification for access control, identification for credit card use, parental testing, biotechnology research, and medical research. And human genetic information database is being planned or under construction. The Act on the Protection and Support of Missing Children allows the institutions to collect genetic test samples from children whose custodians are yet to be ascertained or family members seeking the missing children. According to the Act on use and protection of DNA Identification Information, the police and prosecutors can collect the DNA information from the persons found guilty of 11 types of crimes such as murder, arson, rape, robbery, habitual violence, or organized violence for future crime investigations. Those who committed one of these crimes only once are also subject of genetic information collecting.

These legislations, however, are too focused on the use of genetic information and do not have enough regulations on collection and handling of DNA samples, protection of DNA information, and destruction of the samples and information. Likewise, the Personal Information Protection Act only regulates to obtain consent prior to the collection or use of genetic information and does not have any regulation on protection of the acquired genetic information such as encrypting them. Considering the danger of hacking and theft, special legislation to regulate genetic information database or guidelines based on the Article 12 of the Personal Information Protection Act for preventing the misuse of genetic information is needed.

Meanwhile, the DNA Identification Information Act allows the law enforcement agencies to collect the DNA samples from the crimes occurred in labor disputes or demonstrations that are otherwise lawful. The proposal for revision of DNA Identification Information Act was submitted to the National Assembly on May 11, 2011 to stop the application of the Act on labor disputes or demonstrations, but was abrogated due to the termination of session. Measures to protect the citizens' freedom of expression from the DNA information collecting need to be provided.

The disparity in criminal punishment between the abuser of DNA information and the abusers of general personal information is also problematic. According to the Missing Children Act, a person who uses information, such as fingerprint for any purpose other than the recovery of a missing child, a person who takes a test sample, conducts genetic testing or uses genetic information for any purpose other than original purposes, or a person who leaks any test sample or genetic information is punished by imprisonment for not more than two years or by a fine not exceeding ten million won (Article 18). According to the DNA Identification Information Act, a person who falls under any of the following subparagraphs is punished by imprisonment with prison labor for not more than two years, or by a fine not exceeding five million won (Article 17 (4)) and a person who uses DNA samples or DNA identification information for any purpose, other than performance of his/her duties is punished by imprisonment with prison labor for not more than three years,

or by suspension of qualification for not more than five years (Article 17 (3)). This is a lot lower of a punishment compared to the punishment for misuse of general personal information (punishment by imprisonment with for not more than five years or by a fine not exceeding fifty million won), which can cause negligence among the public officials, medical personnel, or other regular citizens.

3) Sex Offenders

Inspired by Megan's Law that makes information available to the public and notify the local community regarding registered sex offenders, Korea's revised the Act on the Protection of Children and Juveniles from Sexual Abuse enables the Ministry for Health, Welfare and Family Affairs to provide information (name, age, date of birth, occupation, address, and nature of crime) to the public regarding those convicted of sex crimes such as rape, indecent sexual act by force, sexual traffic, and arranging sexual traffic. On July 19, 2002, the Seoul Administration Court requested the constitutional review of the statute questioning the possible violation of principle of double jeopardy and right to receive a trail by justice, but the Constitutional Court decided the statute constitutional on June 26, 2003. Although the Court did not reach the quorum to declare the statute unconstitutional, the majority opinion was that the statute is unconstitutional.

Identity disclosure system prevents recidivism by disclosing offenders' personal information and thus causing humiliation. It is similar to the punishment by public humiliation in the way it functions. Identity disclosure system is criticized as the modern system of guilt-by-association because the friends and family members must share the pain of public discrimination and contempt. Offender's friends and family members suffer greatly from identity disclosure. In fact, over 170 complaints and counseling requests about friends and family members of sex offenders unable to keep the job or settle in a community after the identity disclosure were filed with the National Human Rights Commission.

Publication of facts of suspected crime during the investigation process involves

even severer privacy invasion. The National Human Rights Commission recommended the National Police Agency to improve suspect transportation to be less invasive of privacy and the National Police Agency responded with a directive, the Police Officer Duty Regulation for Human Rights, stating "Scenes that might expose the identity of the suspect or the victim should not be photographed or filmed in police station." However, recent increase in heinous crimes such as child kidnap murder and serial rape murder led to the press and investigation agencies exposing the face, name, and facts of suspected crimes of the suspects' for citizens' right to know, prevention of repeated crime, prevention of copycat crime, and psychological compensation of the victims. The government responded by submitting the proposal for revision of the Act on Special Cases Concerning the Punishment of Specific Violent Crimes to the National Assembly on July 21, 2009, which made it possible to reveal the basic information such as name, face, and age of specific violent crime suspects. The bill passed the National Assembly on March 31, 2010, and is currently in effect.

The revision, which empowers the investigation agencies to release the information of violent crime suspects before the court decision, is criticized for violating the constitutional principle of presumption of innocence, principle against excessive restriction, principle of due process, and the rule of clarity. Although the publication of personal information is only limited to circumstances where there is sufficient evidence to believe a suspect to be the criminal or the suspect has already confessed, the means of crime is cruel, and the crime is of serious harm (murder, robbery rape, or kidnapping of minor), confession of a suspect can be due to flawed interrogation, coercion, or desperation.

Supporters of identity disclosure system emphasize that the other countries such as the U.S., France, and Japan have already adopted such system, but the way that society sees crime is different in Korea. Korean society has tradition of treating criminal activity as the result of family history or bad parenting, expanding the target of criticism to the family.[36] Because of this reason, prejudice against the family

36) Shocking personal history of 159 Violent crime offenders (Tracking the personal history

members of an offender is very strong and still de-facto guilt-by-association system is a tradition. The press has tendency of focusing on the private life and related persons of the suspect rather than the crime itself,[37] burdening the friends and family with pain and privacy invasion. Thus, the National Human Rights Commission created the 'media report guideline for sex crime' with Journalists Association of Korea in September 2012.[38]

Identity disclosure or publication of facts of suspected crime should be considered in the aspect of protecting the rights and privacy of friends and family of the suspects, not the evil deed of the offender, psychological satisfaction of the victims, or our right-to-know. It is controversial whether the portrait right and privacy of the suspect with sufficient evidence of guilt is necessary, but it is indisputable that related persons of the suspect should be protected. Identity disclosure system can be unfit for Korean tradition with strong emphasis on the community. Identity disclosure of violent crime suspect or sex offenders must be limited to never affect the friends, family members, and neighbors. Related legislation must clearly state that associated persons are to be protected and the report guideline of the press must also protect them. Most importantly, the government should eliminate the cause of social discontent and expand social security system to prevent violent crimes and protect the lives of citizens.

---

of 159 violent criminal offenders in Suwon district court) (Joongang Daily, 2012.5.28.)

37) "Elementary student in Anyang murdered - Who becomes the 'devil'?" (Ilyo Newspaper, 2008.3.28.)

38) Following are the 10 guidelines - △ Disclosing the victims' and their family members' personal information should be prohibited. △ Media coverages that stresses the blame on the victims should be prohibited. △ The usage of assailant-oriented vocabularies should be abstained △ Media coverage on specific crime method and investigation process should be prohibited. △ Disclosing assailant's personal information should be prohibited. △ Information provided by the investigation agencies should be closely examined. △ Careful concern is needed in dealing with juvenile-involved crimes. △ Secondary damages that can be caused by using images should be prevented. △ Awareness-rasing media coverages should be widely used.

4) Construction and Management of Integrated Criminal System

The Ministry of Justice finished the construction of KICS (Korea Integrated Criminal System) in August 2009 and the system is in use starting from January 1, 2010. Integrated criminal system is an electric management system with integrated hardware, software, database, network, and security for the criminal justice institutions such as the Court, the Ministry of Justice, the Prosecutor's office, and the National Police Agency to create, acquire, save, and transmit criminal justice information. All criminal justice institutions must use this system when creating documents related to criminal justice such as interrogatory, warrant, indictment, and written judgment. Accordingly, all kinds of criminal justice data such as police's reports of investigation, prosecutor's prosecution/non-institution prosecution records, court decisions, and sentence execution records from correctional institutions is recorded and stored electronically. The criminal justice related data collected and handled by not only the primary criminal justice institutions such as the National Police Agency, Prosecutor's office, and the Court, but also correctional agencies such as prison/juvenile prison, intelligence agencies such as the National Intelligence Service and Defense Security Command, the administrative agencies and local governments such as the Fair Trade Commission, the Communications Commission, the Ministry of Health, the Welfare and Family Affairs, the Ministry for Food, Agriculture, Forestry, and Fisheries, the Ministry of Land, Transport and Maritime Affairs, and the Customs Service will be stored and managed by this system.

The Ministry of Justice launched the 'Criminal justice integrated information system project' planning to create the integrated criminal justice network system that manages all criminal justice information from the police, Prosecutor's office, court, and the Ministry. But this project faced severe opposition from the human rights groups fearing the emergence of the 'Big Brother' and information human rights violation. The opposition is later joined by the court and police fearing the violation of independence of the judiciary and Ministry's monopolization of information and the Ministry backed up by changing the project from 'system integration' to 'system link.'

Integrated system will always lead to human rights violation and increase of information abuse cases. Because citizens' every criminal case records is controlled by a single database, authorities gain access to the records that are not directly related to each cases, ultimately influencing not only the investigation but also prosecutors' indictment decisions, demanding and sentencing of penalty, and probation. Also, a single hacking incident can cause enormous damage. Even if the access authority is technically and administratively limited, information abuse in practice is practically difficult. The court expressed its concern over investigation and intelligence agencies infringing judicial independence by stating that the system "can be the threat to the judicial independence because it takes the form of the Ministry of Justice unilaterally taking the trial information."[39] Thus, the Ministry of Justice's decision to not take the criminal justice information system to the level of 'integration' is a positive change.

Crime justice information system connects the independent information system managed by the Prosecutor's office, court, and the Ministry of Justice and also includes the CIMS (Crime Information Management System) of the police. Criminal justice institutions must follow the system circulation guideline for the digitalization of criminal justice procedures and also follow the guideline of system when creating and using documents such as interrogatory report, warrant, indictment form, or correctional record. Also, the criminal justice institutions must cooperate for the criminal justice information to utilized and quickly distributed through the system and provide other institutions with the information via the system if needed for quick and accurate criminal justice affairs.

Creating the electronic criminal justice information database itself will lead to the personal information security hazard and information abuses without its distribution between institutions. In other words, digitalizing the non-electric data will increase the frequency of their usage, but will also increase the danger of hacking attacks and abuses. CIMS, created and used by the police is a good example to easily assess the

39) http://www.itdaily.kr/news/articleView.html?idxno=16300#

risk of the criminal justice information system. CIMS contain 301 sorts of documents including interrogatory reports collected by the police from the suspects, investigation reports, search and confiscation warrant application, arrest warrant application, and written opinions collected from the victims and witnesses.[40] All documents are storage no matter what the outcome of the case is. It does not matter whether the suspect is found not guilty during the investigation level, send to the prosecutor but found not guilty during pre-indictment stage, or after trial. Thus, the personal information of the sex crime victims is also in danger of exposure. Not only the investigation information, but also the resident information and criminal records can be acquired using CIMS and CIMS is actively utilizing by the police for investigation purposes.

Nevertheless, the type, range, and retention period of the information recorded and stored by the criminal justice information system are still left unannounced and guideline for access authority and access boundaries for the criminal justice institutions are still unprepared. The Ministry of Justice submitted “Bill on Use of Electronic Documents in Summary Proceedings” and “Bill on Promotion of the Digitalization of the Criminal Justice Process” to the National Assembly in May, 2009 to create the legal basis and these bills passed the National Assembly on December 29th, 2009. However, these legislations still do not include the safeguard measures for privacy protection such as the type, range, or retention period of the information, type of information not to be collected and stored, or access limitation on certain sensitive information. Creation and management of criminal database, which can profoundly affect citizens’ rights is operated without any measures to guarantee its transparency and safety. “More the better” does not apply to the issue of information safety. Information system should be redesigned in the perspective of human rights protection. The type of information managed by the system needs to be minimized, type of collected and stored information must be disclosed, and information should be treated differently on the retention period and granting the access authority according to the sensitivity.

---

40) Report from Congressman Kyu-Sik Choi (2009.9)

5) Resident Identification Number leakage due to frequent hacking incidents

Recently, mass exposure accidents of over 10 million people's personal data occur every year. In 2008, personal information of 11 million customers leaked from GS Caltex, an oil company. Same year, 18 million customers' personal information leaked from Auction, the largest online open-market. In 2010, 20 million customers' information from Sinsaegae and 35 million users' information from SK.com was leaked. These repeated incidents clearly show the current state of Korean businesses regarding privacy protection.

The private sector collecting and using customers' personal information is a global phenomenon in the era of information technology, but Korea's case is serious considering the use of resident registration number system. The value and risk of personal information Korean businesses collect and use are much larger than that of information foreign companies have access to. Leaked resident registration numbers are used for crimes such as bank frauds, cloning phones, phishing, or identity theft. Furthermore, this leaked information is sold abroad and the risk is expanded into global scale.

Regardless of the enormous damage caused by repeated personal information exposure accidents, Korean resident registration law allow changing one's resident identification number only on extremely limited circumstances such as the case of North Korean refugees or transsexuals. Contrast to the Korean resident registration system that mandatorily give all citizens an identification number, United States' SSN(Social Security Number) is given to a person upon request for the definite purpose of social security. And a person with a SSN can replace his or her SSN when fraudulent use of SSN and the damage caused by someone's fraudulent use of his or her SSN is confirmed. Change of SSN can be done without a court decision 3 times a year, 10 times lifetime maximum.

On the contrary, the Ministry of Public Administration and Security does not allow the victims of personal data leakages to change their RRNs. And the court decided

the leakages to be not the reason for RRN changes due to legal vacuum.[41] Thus, a change in the RRN issuing system along with statue to allow changing the RRNs with court permission needs to be legislated. With use of computer technologies, changing the RRNs no longer involves administrative difficulties. Also by recording the RRN changes, dangers of identification clean-ups can be prevented.

Furthermore, laws that require private businesses to collect identification data from the customers need to be revised. The Constitutional Court ruled real-name Internet system to be unconstitutional unanimously[42] and recent changes in the Information and Communications Network Act (Act on Promotion of Information and Communications Network Utilization) made it illegal for businesses to arbitrarily collect and use customers' RRNs online. Nevertheless, businesses are allowed to collect and use customers' RRNs online if the related legislation allows and there is no restriction on collecting and using the RRNs offline. To enhance privacy protection, current legislations laxly allowing the private sector to collect and use personal data need to be revised. Also, the private sector should change its current practice based on real-name system to anonymity based system so the customers are provide with more options. The Personal Information Protection Act emphasizes the principle of anonymity by stating "A personal information manager shall ensure that personal information is managed anonymously whenever such management is possible." (Article 3 (7))

Lastly, the Ministry of Public Administration and Security's idea of eliminating all problems of RRN system by simply introducing 'electronic resident card' is very dangerous. Problems of RRN system is fundamentally caused by its unchangeable and personally attached nature not by resident registration cards' vulnerability to counterfeiting and falsification. Thus, the Ministry should decrease the use of RRN not digitize them to handle RRN abuses. In other words, personal identification data should be deleted or reduced not electronically recorded.

41) Seoul Administrative Court 2012.5.4. Judgment 2011Guhap37633
42) Constitutional Court 2012.8.23. Decision 2010Hun-Ma47, 252

6) Social Network Service and 'cyber-tailing'

Social Network Service (SNS) is a kind of personal network management service that allows the users to strengthen personal relationship with their friend or colleagues and even create new relationships with the strangers. Also, SNS enables the users to share their information and perform as a private media or a community. With use of mobile smartphones and tablet PCs enabling the real time use of the service everywhere, number of people using the service is showing an explosive growth. Korea's most popular SNS includes Cyworld, Metoday, and Kakao Talk. SNS such as Facebook, Twitter, and Myspace has large number of service users globally. In broad terms, any service that provides online communications, such as blogs or 'internet cafes,' can be defined as SNS.

Recently, however, the use of SNS seems to be digressed from the initial purpose of personal network building and communications to commercial marketing. SNS turned into the space for talking about the others. SNS became a manufacturing plant of personal information for various kinds of violence and crimes such as reckless-enough to drive people to commit suicide-spreading of malicious rumors, 'cyber-tailing,' and sexual violence. Number of SNS users intended to build social connections but eventually becoming the victims of private information exposure and cybercrimes is increasing. SNS is problematic in privacy protection because the service is based on exposure of personal information. For the users to use the service they must join the service and expose their personal information to a certain level. To use Facebook, for example, the users must first join by filling in their name, password, sex, date of birth, and email address.

Personal information the users provide is basically set for not only the users of certain SNS, but every internet or smart phone users to find using search engines. Of course the level of information exposure can be changed by the users. But without the users changing their privacy setting, their personal information is exposed following the basic setting created by the service providers. And exposing some information such as names and 'profile pictures' is mandatory. Private policy that initially makes information public

and provides the user the option to change the setting is the 'opt-out' method. Such policy can be a problem in Korean legal system adopting the opt-in method,[43] while the U.S. and Japan is adopting the opt-out method.

According to the existing law, when a personal information manager obtains the consent of a subject of information about the management of personal information, he or she shall classify respective matters requiring consent and notify the subject of information of such matters to clearly understand them, and obtain consent respectively to such matters.[44] Having the service users to personally choose the

---

43) Personal Information Protection Act Article 17 (Provision of Personal Information) (1) A personal information manager may provide (including sharing; hereinafter the same shall apply) a third person with the personal information of a subject of information in any of the following cases:
1. Where he/she has obtained the consent of a subject of information;
2. Where he/she provides personal information under a purpose for which the personal information was collected pursuant to Article 15 (1) 2, 3 and 5.
(2) and (3) are omitted.
Information and Communications Network Act Article 24-2 (Consent to Provision of Personal Information) (1) Every provider of information and communications services shall, whenever it intends to furnish a third party with personal information of a user, notify the user of all the following matters and obtain consent from the user, except as provided for in Article 22 (2) 2 and 3. The same shall apply in cases where there is a change in any of the following matters:
1. The person to whom the personal information is furnished;
2. Purposes of use of the personal information of the person to whom the personal information is furnished;
3. Items of the personal information furnished; and
4. Period of time during which the person to whom the personal information is furnished will possess and use the personal information.
(2) and (3) are omitted.

44) Personal Information Protection Act Article 22 (Methods of Obtaining Consent) (1) When a personal information manager obtains the consent of a subject of information (including his/her legal representative under paragraph (5): hereinafter the same shall apply in this Article) about the management of personal information, he/she shall classify respective matters requiring consent and notify the subject of information of such matters to clearly understand them, and obtain consent respectively to such matters.
(2) When a personal information manager obtains the consent of a subject of information about the management of personal information pursuant to Articles 15 (1) 1, Article 17 (1) 1, subparagraph 1 of Article 23 and Article 24 (1) 1, he/she shall classify the personal information that can be managed without obtaining the consent of the subject of information and the personal information requiring the consent of the subject of

information to be made public or control the range of disclosed personal information would be the method that achieves both privacy protection and service development. The Personal Information Protection Act should be amended to include the principle for disclosure and sharing of personal information to unspecified or specified individuals along with the existing principle for providing or sharing personal information with the third person.

7) Increase of Communication Monitoring such as Deep Packet Inspection (DPI)

According to the Communications Commission report on tapping telecommunication businesses' tapping cooperation and provision of communication data or communication confirmation data, investigation agencies' (prosecutors, judicial police, the National Intelligence Service, military investigation agency) tapping or communication data (including the communication confirmation data) provision sum up to over 830,000 provisions in the year of 2010 alone. If we look closer to the data, there were 1,081 tapping s,[45] 238,869 communication confirmation data provisions,[46] 591,049 communication data

---

information for the purpose of entering into a contract with the subject of information. In such cases, a personal information manager is responsible for proving that the subject personal information is the one that can be managed without obtaining consent.

(3) When a personal information manager intends to obtain the consent of a subject of information on the management of his/her personal information in order to publicize or solicit the sale of goods or services to him/her, the personal information manager shall notify the subject of information thereof to clearly understand this and obtain his/her consent thereto.

(4) No personal information manager shall refuse to provide a subject of information with goods or services on the ground that the subject of information fails to give his/her consent to matters he/she is entitled to give selective consent pursuant to paragraph (2) or fails to give his/her consent required under paragraph (3) and Article 18 (2)1.

(5) and (6) are omitted.

45) Tapping is the system of investigation agencies checking the content of communication of investigation targets with cooperation of the communications service providers. General communication-restricting measure is processed by investigation agencies such as prosecutor, police, National Intelligence Service request cooperation with court's permission. For the emergency communication - restricting measures, investigation agencies can take the communication-restricting measures with head prosecutor's order or

provisions.[47] This is an increase of 170% from 2006. Especially for the tapping, 5,099 tapping by the National Intelligence Service, which is the 86% of the total sum, took place during the five year (2006~2010) period. Considering that the National Intelligence Service only investigate special cases related to national security or military secrets and not the common criminal cases, the data suggests that there are frequent wiretappings by investigation agencies.

〈Table 7〉 Provision of Tapping and Communication Data from Telecommunication Businesses to Investigation Agencies

Year	Tapping	Communication Confirmation data	Communication Data	Total
2006	1,033	150,743	323,566	475,342
2007	1,149	183,659	426,408	611,216
2008	1,152	212,745	474,568	688,465
2009	1,516	248,552	561,467	811,535
2010	1,081	238,869	591,049	830,999
Total	5,931	1,034,568	2,377,058	3,417,557

Source: Korea Communications Commission, 2007~2011 press release

permission of NIS chief and obtain the permission from the court within 36 hours.

46) Provision of communications data is the system of investigation agencies obtaining the personal information (name, resident registration number, address, dates on which users subscribe or terminate their subscription, user identification word) of the investigation subject from the telecommunications business. Investigation agencies can confirm the identification data of the user with the written request for provision of data signed by a prosecutor, a senior superintendent of the police, or a public official of grade 4 or higher and court warrant is not necessary.

47) Communication confirmation data is the system of investigation agencies receiving the communication confirmation data of the investigation subject from the telecommunication business upon request with the court's permission. Communication confirmation data is not the 'content' of the communication, but formal facts of communication such as the date, duration, frequency, and location of communication. For the Internet communication confirmation data includes Internet log records and IP address. Investigation agencies such as the Prosecutor's Office, judicial police, the National Intelligence Service requests the telecommunications business for the data with the court permission and telecommunications business cooperates. For emergency circumstances, investigation agencies may obtain the court permission after they are provided with the data.

〈Table 8〉 Provision of Data by Investigation Agencies

Year	Prosecution	Police	National Intelligence Service	Military Investigation Agency	Total
2006	35	99	870	29	1,033
2007	24	81	1,010	34	1,149
2008	18	75	1,043	16	1,152
2009	9	145	1,320	42	1,516
2010	2	186	856	37	1,081
Total	88	586	5,099	158	5,931
Percentage	1.5	9.9	86.0	2.7	100.0

Source: Korea Communications Commission, 2007~2011 press release

With the increased usage of internet and email, the form of communication tapping is changing from the wiretapping to the inspection of internet usage or emails and communication data provision requests. The National Intelligence Service's use of DPI (Deep Packet Inspection), disclosed by the press in September 2009 is a method of restoring the tapping subject's internet usage by filtering the internet packet with the tapping equipment installed on the lines.[48] Among the 57 tapping equipment sales approved between 2008 and August of 2011, 46 were the packet inspection equipment.[49] As of 2009, the National Intelligence Service owns 31 pieces of packet inspection equipment.[50]

By using the DPI, the investigation agencies can look into one's internet usage and the content of the usage including electronic mail, instant messenger, web surfing, message board, or peer-to-peer file sharing. Such inspection is possible regardless of the location of the website one connects and even if one seeks 'cyber asylum'

48) "National Intelligence Agency has 31 Deep Packet Inspection equipment", Hankyeoreh (2009.11.17), "Civil Society files constitutional complaint on NIA's Packet Inspection", Tongil News(2011.3.29)
49) Report from Congressman Jae-Yoon Kim (2009년)
50) "National Intelligence Agency has 31 Internet inspection equipment" (mbn, 2009.11.17)

to the foreign server electronic mail is still inspected because the packet inspection can be done on the pathway all information going in and out of the country pass. Packet inspection is very comprehensive and thus all sorts of internet activity can be the target of inspection. DPI arouses the controversy about the invasion of privacy because every communication including those unrelated to criminal activity becomes the subject of inspection. Also, family members or colleagues sharing a computer or those sharing the internet connection through a router can be inspected along with the subject, which can be a serious human rights violation. The report[51] ordered by the Secretariat of the National Assembly points out that packet inspection can lead to the surveillance on citizens' entire private lives, is violating the principle of the least restrictive means described in Protection of Communications Secrets Act, Article 3(2), and is violating the prohibition of comprehensive warrants.

On March 29, 2011, 'Public security agency watch network' composed of civic organizations including Lawyers for a Democratic Society, Progressive Network Center, People's Solidarity for Participatory Democracy, and Korea Alliance for Progressive Movement filed a constitutional complaint arguing that communication-restricting measures permission, which is about allowing the internet line tapping, violates the principle of arrest by warrant, the principle of due process, the right of privacy, human dignity and worth, and the right of pursuit of happiness. Also, the complaint argues that Article 2 Subparagraph 7[52], Article 5 Paragraph 2,[53] and Article 6[54] of the Protection of Communications Act are unconstitutional.[55] There have been numerous arguments regarding the problems of the Protection of Communications Secrets Act

51) The Secretariat of the National Assembly, 'Constitutional Review on the Packet Inspection and Opinions on Legislatio' (2009.12.31.)

52) The term "wiretapping" means acquiring or recording the contents of telecommunications by listening to or communally reading the sounds, words, symbols or images of the communications through electronic and mechanical devices without the consent of the party concerned or interfering with their transmission and reception.

53) Article 5 (Requirements for Permission of Communication-Restricting Measures for Criminal Investigation)

54) Article 6 (Procedures for Authorization of Communication-Restricting Measures for Criminal Investigation)

55) Constitutional Court 2011 Hun-Ma165

in terms of information human rights. Legislative for protection of communication secrets, the Protection of Communications Secrets Act is applied to legalize wiretapping in reality. Also the act is problematic because act's definition of crimes subject for tapping is too broad and "emergency wiretapping" system allows the investigation agencies to wiretap and request communication confirmation data provision without the court warrant. Tapping by the government, which should be the last measure after prior remedies have exhausted, add up to 6,000 tapped wires in last five years.[56] There are criticisms that the court is granting permission to wiretap citizens without proper examination of the need and range of the tapping and thus failing to check the information or investigation agencies from reckless monitoring activities. There is even a case that the court renewed the warrant 13 times to allow 28 months of wiretapping. Means to restrict indiscriminate permission of communication tapping, especially the internet packet inspection, and control the range and method of communication monitoring need to be created.

8) Comprehensive search and confiscation for digital evidence gathering

In conjunction with technological advancements, gathering of evidence is important not only in solving cybercrimes but also solving conventional crimes and investigative body's reliance on digital evidence is evermore increasing. In contrast investigative body's effort to respect one's information privacy in the process of investigation is still lacking and the level harm from infringement of the rights through confiscation and searching has reached is serious. Although one is only entitled to information that is directed related to the crime under criminal laws, one has been abusing unreadable and unforeseeable characteristics of digital evidence to gather the entire set of datum.

For example, in April 2009 prosecutors investigating violation of election law committed by a candidate running for the office of the superintendent of education in Seoul collected one hundred persons in Korean Teachers Union and some of them

56) Constitutional Court 2010.12.28. Decision, 20109Hun-Ga30

were searched for email dating back to seven years. Also in June 2009, investigative body probing a case involving "PD Note" publically released a private email conversations sparking controversy over the scope of confiscation and searching of digital evidences. In regards to this the prosecutor's office claim the search was conducted under the court's order and therefor was within a legal boundary.

Evidences in real life specified just like a witnesses testimony or objects; however, evidences in transition through telecommunications network and digital evidences stored in a server is not only stored in a network of countless servers along with other data but also is difficult to pin point its parameter. Hence, there has been a call to clarify legal evidence and limitations in investigation agency's search and confiscation of digital evidences to have it fall in line with principle of compulsory disposition by statute and principle of search and confiscation by warrant.[57)]

On the other hand, computer search investigation, or online searching,[58)] is an investigation that precedes searching and confiscation but it is different from compulsory disposition in that it requires special attention to secrecy. Its level of intrusion is lower than that of other searches and confiscations and thus lead some to believe it does not require legal standard[59)]. Yet, whether a citizen is aware of the fact that one is subjected to a secret or an open investigation is not important at the level of fundamental civil rights and searching without a consent itself can be regarded as violation of fundamental rights. Moreover, permitting investigation agency to forego with computer searching investigation for a person's simple charge of crime when a special legal basis can be subjected to controversy over human rights.

Harm imposed through a broad use of confiscation of digital evidences does not end here. Without a specified and codified procedure for the destruction of confiscated data, it has a risk of creating the "Big Brother". Although the codes require materials

57) Kang Dongwook(201.12)., Articles for General Subject : A Study on the Revisionist Bills of Criminal Procedure Act about the Collecting of Digital Evidence, Legal Search 18. 3.
58) It refers to government agency's searching or copying of data stored in a user's IT system without them through internet connection without notification.
59) LEE Won-sang, Thoughts on Online-Durchsuchung: With Focus on New Dialogues in Germany, The Korean Criminal Law Association, 20(4), Fall 2008.

irrelevant to the allegation to be returned, materials are not only returned with extreme delay but also are often used against investigated subjected as threats. Policy for return is not only important in allowing the subjects resumption of business but also is critically important for protection of information privacy. Therefore, returning of copied material should be codified and a duty to destroy irrelevant information should be institutionalized to guarantee the subjects information privacy.

Following this the national assembly introduced two amendments[60] to the related legislations to address the issues surrounding received and sent emails. National Human Rights Commission also submitted an opinion to the national assembly calling to institutionalize a legal foundation for searching and confiscation of emails stored in a server, notify the defendant of email account holder and subject of investigation about a search, specify the time frame of emails regarding a case, allow public involvement in execution of orders, and deleting and returning of irrelevant information. Revised criminal law which came into effect since January 2012 mandates submission of materials that show material relevant to the case along with a request for a search warrant. Also if the object of confiscation is an online communication log, it must specify the time frame of the materials which will be retrieved. If the object is a storage device such as a hard-drive, materials within a designated boundary may be printed out or copied to alleviate a significant portion of concerns regarding violation of information privacy. It also mandates immediate notification of collection to a subject to both the subject of investigation and people involved in that communication. But in some cases where information extraction is impossible or insufficient, it can be confiscated.

The Supreme Court also made a meaning decision.[61] The court ruled that execution of search or confiscation can happen only if a warrant recognizes the relevance and the material can only be retrieved in a printed or digitally copied form. Even if such methods are impossible or extremely difficult, the warrant must specifically allow

60) Criminal Procedural Act, Protection of Communication Secrets Act. (Proposal 5246, 2009.6.23)

61) Supreme Court 2011.5.26 Decision 2009Mo1190

extraction of an original storage device to the investigation agency. Even when the storage device is extracted to the investigation agency office, it can only be searched for printing or copying within the scope specified in the warrant.

9) Use of Big Data and right to be forgotten

With advancement of communication technology everyone can simultaneously be a consumer and a producer of information. With addition of devices suited for mass production of information such as smartphones and digital cameras and digitalization of televisions, information or data is projected to increase exponentially.[62] Increase of data is also influencing the computer devices that process these information to change from individually stored data to collectively stored cloud computing.[63] In a flood of information, use of big data[64] recent became an issue worthy of attention. Recently, National Information Strategy Commission released a plan for "Smart Government" using the big data with a system for a pan-government data synchronization and analysis.

The value of big data lies in that a corporation and governments can identify and provide services for customer needs at an optimal moment and that it contributes to national competitiveness by improving government efficiency. However, use of big data comes with a huge price of privacy and freedom. In order for a big data to be used, management and compilation of information necessary and synchronization and unification of databases is unavoidable which forces consumers and citizens to give up on the principle of minimal treatment of information. Therefore, in a policy facilitating a use of big data, it is important to find a balance between economic and social benefits from the use and protection of information privacy.

---

62) Lee Man-Jae, Use of Big Data and Public Data, Internet and Information Security, Vol. 2 (2).
63) Cloud Computing refers to the idea that all information is absorbed in an internet which is like a cloud without to allow access to server managements, emails, and documents in works without physical hardware devices.
64) Big Data is not a database categorized by for its size but for its requirement for different way of processing and analyzing than a conventional database. (Manyika, 2011, 'Big data: The next frontier for innovation, competition, and productivity')

Using the big data for data analysis, research and development, and production of new services through predicting economic trends, disease outbreaks, and consumer or customer trends, or creating crime prevention system has minimal risk of intrusion of privacy and has great social and economic benefits. However, collection and analysis of customers' behavioral patterns, consumption trends, hobbies, interests, financial information, and ideologies simply for personalized advertisements or services without consent of the citizens should not be permitted. Therefore, the government should, prior to facilitating the use of big data, actively come up with standards, procedures, and preconditions for compilation or synchronization of databases, mandate provision of Do-Not-Track option,[65] and implementation of Privacy by Design and Privacy by Default,[66] or right to be forgotten.[67]

Section 2. Freedom of Expression on the Internet

1. Meaning of the Freedom of Expression

Freedom of expression is the right to express and communicate one's opinions and ideas to anyone. Social value achieved by the freedom of expression is the value of self-realization of one's speech activity building one's character. On the other hand, it is a democratic value of citizens participating in formation of political opinion through speech. Thus, freedom of expression is a core of freedom of opinion and fundamental of political freedom and democracy.

Media plays an important role in guaranteeing the freedom of expression. However, historically, government in power has reacted negatively towards the emergence of

65) A user is given an option to turn of service provider's tracking of a user's online activity used for personalized advertisements.
66) In developing a service or a product, it must be designed to collect minimal information from the user and such data shall be open to public access.
67) Right to be Forgotten based on EU laws is comprised of user's right to demand deletion stop processing of private information and duty to notify on collection and use of user information.

a new medium and controlled the formation of public opinion through regulations. However, in modern government by the rule of law, freedom of expression is guaranteed by the constitution and since freedom of expression is guaranteed by the constitution in the modern government by the rule of law, government regulation on the media is only possible within the legal boundaries. This is still the same in the Internet era.

Freedom of expression was not properly protected during the era of authoritarian regimes in Korea. Protection of freedom of expression expanded as the constitution gained it normative power after 1987 when democratization started to progress. Moreover, as the Internet usage increases, freedom of expression is expanding its domain. Internet has become a powerful medium to influence public opinion and politics even surpassing the television broadcasting or paper press. Political influence of the Internet was demonstrated by elections. Online debate section that triggered the 2008 candlelight demonstration against U.S. beef import showed the power of the Internet.

However, while Internet expanded the freedom of expression through the 'reply culture,[68]' it also had negative impact by producing cases of violating personality interest (libel, defamation, privacy invasion). As Internet continues to show its negative aspect, government is building legislations and system to regulate online information distribution. Nevertheless, such government intervention can lead to the stifling of freedom of expression. This demonstrates that the Korean society is still unable to create a consensus on the democratic value of freedom of expression shows the sign of lingering paternalistic interventionism.

68) 'Reply' is short comment internet users can leave on the online articles or postings. Postings of popular or controversial issues attract many users leaving the replies, which lead to the creation of public opinion.

2. International Trend and Standard

Freedom of expression has always been the core of declarations and charters of human rights historically. The French declaration of human rights in 1791 and U.S. Bill of Rights in 1791 stipulated freedom of expression as the most important right.[69] The right to freedom of expression is recognized as a human right under Article 19 of the Universal Declaration of Human Rights[70] in 1948 and Article 19 of International Covenant on Civil and Political Rights in 1966 also stipulated freedom of expression as a human right.[71] European Convention on Human Rights[72], ratified by the Council of Europe in 1950, also provides freedom in expression in detail on Article 10.[73]

---

69) France 「Declaration of the Rights of Man and of the Citizen」 Article 11 stated "The free communication of ideas and of opinions is one of the most precious rights of man. Any citizen may therefore speak, write and publish freely, except what is tantamount to the abuse of this liberty in the cases determined by Law..". And U.S. First Amendment defined freedom of expression.

70) "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

71) "1. Everyone shall have the right to freedom of thought, conscience and religion. This right shall include freedom to have or to adopt a religion or belief of his choice, and freedom, either individually or in community with others and in public or private, to manifest his religion or belief in worship, observance, practice and teaching. 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice. 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals.

72) Formally the "Convention for the Protection of Human Rights and Fundamental Freedom"

73) "① Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. ② The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity

Freedom of expression is equally protected on Internet. In May 28th, 2003, Committee of Minister of Council of Europe drafted the Declaration on Freedom of Communication on the Internet[74] based on the Article 10 of the European Convention on Human Rights, declaring the seven principles for the member states to follow.

〈Table 9〉 7 Principles for Freedom of Communication on the Internet (Council of Europe)

Principle 1	(Content rules for the Internet): Member states should not subject content on the Internet to restrictions which go further than those applied to other means of content delivery.
Principle 2	(Self-regulation or co-regulation): Member states should encourage self-regulation or co-regulation regarding content disseminated on the Internet.
Principle 3	(Absence of prior state control): Public authorities should not, through general blocking or filtering measures, deny access by the public to information and other communication on the Internet, regardless of frontiers. This does not prevent the installation of filters for the protection of minors, in particular in places accessible to them, such as schools or libraries. Provided that the safeguards of Article 10, paragraph 2, of the Convention for the Protection of Human Rights and Fundamental Freedoms are respected, measures may be taken to enforce the removal of clearly identifiable Internet content or, alternatively, the blockage of access to it, if the competent national authorities have taken a provisional or final decision on its illegality.
Principle 4	(Removal of barriers to the participation of individuals in the information society): Member states should foster and encourage access for all to Internet communication and information services on a non-discriminatory basis at an affordable price. Furthermore, the active participation of the public, for example by setting up and running individual websites, should not be subject to any licensing or other requirements having a similar effect.
Principle 5	(Freedom to provide services via the Internet): The provision of services via the Internet should not be made subject to specific authorization schemes on the sole grounds of the means of transmission used. Member states should seek measures to promote a pluralistic offer of services via the Internet which caters to the different needs of users and social groups. Service providers should be allowed to operate in a regulatory framework which guarantees them

or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

74) https://wcd.coe.int/ViewDoc.jsp?id=37031

non-discriminatory access to national and international telecommunication networks.

Principle 6 (Limited liability of service providers for Internet content): Member states should not impose on service providers a general obligation to monitor content on the Internet to which they give access, that they transmit or store, nor that of actively seeking facts or circumstances indicating illegal activity.

Member states should ensure that service providers are not held liable for content on the Internet when their function is limited, as defined by national law, to transmitting information or providing access to the Internet.

In cases where the functions of service providers are wider and they store content emanating from other parties, member states may hold them co-responsible if they do not act expeditiously to remove or disable access to information or services as soon as they become aware, as defined by national law, of their illegal nature or, in the event of a claim for damages, of facts or circumstances revealing the illegality of the activity or information.

When defining under national law the obligations of service providers as set out in the previous paragraph, due care must be taken to respect the freedom of expression of those who made the information available in the first place, as well as the corresponding right of users to the information.

In all cases, the above-mentioned limitations of liability should not affect the possibility of issuing injunctions where service providers are required to terminate or prevent, to the extent possible, an infringement of the law.

Principle 7 (Anonymity): In order to ensure protection against online surveillance and to enhance the free expression of information and ideas, member states should respect the will of users of the Internet not to disclose their identity. This does not prevent member states from taking measures and co-operating in order to trace those responsible for criminal acts, in accordance with national law, the Convention for the Protection of Human Rights and Fundamental Freedoms and other international agreements in the fields of justice and the police.

〈Table 10〉 Foreign Legislations on the Freedom of Expression

U.S. First Constitution Amendment	Congress shall make no law… abridging the freedom of speech, or of the press
Constitution of Japan Chapter 3 Article 21	Freedom of assembly and association as well as speech, press and all other forms of expression are guaranteed. 2) No censorship shall be maintained, nor shall the secrecy of any means of communication be violated.
French Declaration of Human Rights	Article 10: No one may be disturbed on account of his opinions, even religious ones, as long as the manifestation of such opinions does not interfere with the established Law and Order

	Article 11: The free communication of ideas and of opinions is one of the most precious rights of man. Any citizen may therefore speak, write and publish freely, except what is tantamount to the abuse of this liberty in the cases determined by Law.
Basic Law for the Federal Republic of Germany Article 5	(1) Every person shall have the right freely to express and disseminate his opinions in speech, writing and pictures, and to inform himself without hindrance from generally accessible sources. Freedom of the press and freedom of reporting by means of broadcasts and films shall be guaranteed. There shall be no censorship. (2) These rights shall find their limits in the provisions of general laws, in provisions for the protection of young persons, and in the right to personal honour.
EU directive following the guideline for privacy protection in the Internet	Technology that can guarantee the anonymity of information object while respecting the rights and freedom of others and value of democratic society needs to be developed.

As the demonstrated by the international norms, freedom of expression on the Internet is equally guaranteed as an important human right. Freedom of expression is not an absolute right and can be limited when necessary for national security, the maintenance of law and order, or public welfare as the Article 37 Paragraph 2 of the constitution states. However, restriction of freedom of expression has to be done in a least amount and should not invade the essential content. Of course this equally applies to the speech on the Internet. Freedom of expression must be guaranteed based on the principle of free market of opinion and it needs to be restricted by the society not by government intervention. This is demonstrated by Council of Europe emphasizing the importance of self-control and anonymity in its declaration in 2003.

3. Current Domestic System and Controversial Cases

(1) System Controversy

1) Illegal Information Deliberation System on Internet

Korea has long history of using regulatory means inspecting the content of information circulated in the Internet and later censoring it. The Telecommunications

Business Act of 1991 that replaced the Public Telecommunication Service Act of 1983 included the "seditious communication deliberation system." According to the statue, communication that harms the public safety and social morals and good customs is prohibited seditious communication.[75] The competent Minister could order the communication business operator to reject, suspend, or restrict handling of seditious communication and communication business operator not following the order was criminally punished. It was a shoddy ex post facto regulation subjecting the communication business operators not the users.

This seditious communication deliberation system was enhanced by comprehensive enforcement system called the content deliberation of Information Communication Ethics Committee. The statue maintains the seditious communication deliberation system with competent Minister's ordering system and content deliberation system of Information Communication Ethics Committee is supplemented. This system was launched in name of creating a clean online culture by filtering unhealthy information from the "PC Communication" of the past. This system is applied to the Internet that came after the PC Communication. However, this system was criticized for suppressing the freedom of expression broadly and excessively.

This seditious communication deliberation system was declared unconstitutional by the Constitutional Court in June, 2002.[76] In this case the Constitutional Court defined

---

75) Subject of seditious communication was specified by Presidential decree (Paragraph 2). Presidential defined seditious communication by "1. Communication with a content that attempts, aids, or abets to commit crime. 2. Communication with content to attempt anti-government activity 3. Communication with content to harm social morals and good customs."

76) Constitutional Court 2002. 6. 27. Decision 99Hun-Ma480 (Seditious Communication Case). The complainant is a student at Hankook Aviation University, and has signed up to Nownuri, a comprehensive computer network service provided by Nowcom, Inc., under the user ID of "I-ui-je-ki (request for correction-Trans.)".
On June 15, 1999, the complainant posted a message entitled "Exchange of Gunfire in the West Sea, Sloppy Kim Dae-Jung!" on the "urgent message board" of the internet community "Chanwoomul." On June 21, a system manager for Nownuri deleted this message from the board, and suspended the complainant's use of Nownuri service for one month according to an order of the Minister of Information and Communication.
On August 11, 1999, the complainant filed a constitutional com- plaint against Article 53

the Internet as "most participatory market," "expression promoting medium." The Court decided the concept of seditious communication, in other words, "communication with content that harms the public safety or social morals and good customs" in the Article 53 Paragraph 1 is vague and unclear and thus the statue violates the rule of clarity. The Court continued by stating that completely banning the circulation of such seditious communication "will lead to the censoring of communications not to be censored due to the vagueness, abstractness, and comprehensiveness of the concept and thus the statue violates the rule against excessive restriction." Prohibiting the expression that harms the existing norm or customs can block the oppositions or minority opinions. Especially, artistic expression that do not correspond to the existing norm and fundamentally creative, innovative, and highly subjective can be seriously repressed.

After the Constitutional Court decision, the statute was revised on December 26, 2002. "Seditious communication" was changed to "illegal communication." Minister of Information and Communication's restriction order system and deliberation system of the Communication Ethics Committee was left untouched. The opportunity to state an opinion, which the Court instructed to recognized, was only partially introduced. Seditious communication deliberation system was maintained only with the subject information for regulation being changed to illegal information.

Currently, this system changed its name to "illegal communication deliberation system" as it was moved from the Telecommunications Business Act to the Article 44-7 (Prohibition on Circulation of Unlawful Information) to the Act on Promotion of Information and Communications Network Utilization and Information Protection in January 2007. And Korea Communications Commission and Korea Communications Standards Commission was created in February, 2008. The authority

---

and parts of Article 71(vii) concerning Article 53(3) of the Telecommunications Business Act as well as Article 16 of the Enforcement Decree of Telecommunications Business Act, al-leging that the provisions infringe on his freedom of expression as well as freedom of science and arts, is against due process, and violates the principle against excessive restriction.

to orders to reject, suspend, and restrict was transferred to the Korea Communications Commission and Korea Communications Standards Commission took the task of deliberation.

According to the current statute, unlawful information includes obscene materials, information of defamation of others, unwholesome medium for juvenile, speculative activities, and State secrets. Unlawful information is rejected, suspended, and restricted of handling by the order of Communications Commission after Communication Standards Commission's deliberation. This regulatory system has two main problems. First, the range of regulated expression is too broad. Secondly, the 'unlawfulness' of the information is decided by the Communications Standards Commission, which is an administrative agency, and then is deleted, suspended, or restricted by the correction order before any court decision.

There is no doubt certain level of regulation is necessary for clean online culture and protection of the minors. Information Communication Ethics Committee's projects in the past such as information communications ethics education, 'e-Clean Korea' campaign, development and distribution of obscene spam interceptive software, management of 'Internet 911' (report center for unwholesome medium for juvenile), designation of juvenile recommended websites, and management of cyber-crime mediation center are adequate and necessary policies. However if the Communications Commission and Communications Standards Commission act as regulatory agencies or censors, freedom of expression in the Internet will be seriously intimidated and self-regulation within the Internet would diminish. Thus, the Constitutional Court decision in 2002 stating, "Broadly regulating the content of expression on the vague suspicion or possibility of harm cannot concord with the freedom of expression," need to be reminded.

Especially, unlawful information deliberation system of administrative agency's compulsory deletion, suspension, and restriction of information after 'unilateral' decision on the information's does not comply with the principle of due process. Exception on the principle of due process can be accepted only when urgent reason

to shut off illegal information is clearly recognized. Also in such circumstances, the Internet user needs to be informed of the reason for censorship and be given the chance to challenge the decision.

〈Table 11〉 Principle of Due Process Applied on the Restrictions on Speech

U.S. Supreme Court decided censoring of films is constitutional only when the effect of censorship on the freedom of expression is to be minimized by procedure. First, the burden of proving that the film is unprotected expression must rest on the censor. Second, while the State may require advance submission of all films, in order to proceed effectively to bar all showings of unprotected films, the requirement cannot be administered in a manner which would lend an effect of finality to the censor's determination whether a film constitutes protected expression. Third, the exhibitor must be assured, by statute or authoritative judicial construction that the censor will, within a specified brief period, either issue a license or go to court to restrain showing the film. Any restraint imposed in advance of a final judicial determination on the merits must similarly be limited to preservation of the status quo. Fourth, the procedure must also assure a prompt final judicial decision, to minimize the deterrent effect of an interim and possibly erroneous denial of a license. (Freedman v. Maryland, 380 U.S. 51 (1965)). After this decision, Maryland revised the statute to have the censorship committee to decide in five days, and if deciding to restrict the showing, the committee must submit the injunction to prohibit its showing. And the judiciary makes the decision in seven days and the committee bears the burden of proof for prohibition. On this revised statute the Supreme Court declared its constitutionality with 4:4 (without Justice Douglas) difference in opinion. (Grove Press, Inc. v. Maryland State Board of Censors, 401 U.S. 480 (1971)).

Current unlawful information deliberation system has few problems in terms of the principle of due process. Principle of due process is a constitutional demand that procedures for limiting a right must be impartial. Meaning of impartial procedure is that grounds for limitation needs to be impartially judged and the person limited of his/her rights be provided with the chance to challenge the decision. Although absolute impartiality is required at all circumstances, when freedom of expression, the most important right, is violated, the level of demanded fairness is very high. Whether the current deliberation system has such level of impartiality must be strictly scrutinized.

First problem is that the 9 types of illegal information are decided by Korea

Communications Commission and Korea Communications Standards Commission. For example, it is not that simple to decide whether an expression is obscene or a speech is a praise and incitement expression punished by the National Securities Act. There is no clear guideline set up by court cases to decide whether an expression is a praise and incitement speech. Granting a mere administrative agency to make such decision does not demonstrate demanded high level of impartiality. Especially, "other information with a content that attempts, aids, or abets to commit a crime" of Paragraph1 Subparagraph 9 is too broadly worded and can bring chilling effect on the protected expressions.

Second, it is doubtful whether the Communications Standards Commission is an impartial decision institution. Although deliberation duty of the Commission is independently performed, Commission established for "creating a sound culture in the areas of information and communications" (Article 18 Paragraph 1 Act on the Establishment and Operation of Korea Communications Commission) is difficult to not be a censoring agency. Also, investigation authority and decision authority is not separated.

Third, the statue, in principle, provides the opportunity to submit the opinion, but is not "guaranteeing the practical opportunity to protest". It only provides a chance to submit an opinion not an actual hearing to perform a legal dispute over facts and legal issues.

2) Defamation on the Internet

Even with the guaranteed freedom of expression, one shall not defame others. However freedom to criticize with proven fact should not be repressed in the name of protection from defamation. A proper balance between freedom to express and protection from defamation need to be achieved.

According to Article 307 Paragraph 1 of Criminal Act, crime of defamation can be established by alleging the facts. Article 310 states such alleging of fact is lawful if it is "true and sole for public interest," leaving the room for the freedom of

expression. The Korean Supreme Court has interpreted the affirmative defense on Article 310 limitedly in perspective of harmonizing the freedom of expression and protection from defamation. The Court decided on the case on the act of civil and criminal defamation, one is not guilty if the expression is (1) of public interest, (2) solely for public interest, and (3) is true or there is substantial reason for the performer to believe that the fact is true.[77] The Court has continuously suggested "fact of public interest, purpose of public interest, proven truth or substantiality of demonstration of truth" for the affirmative defense both for civil and criminal cases. But the court imposes the burden of proof to the expresser.[78]

Legislative provision on affirmative defense and the Court's decision is criticized as neglecting the interest of the freedom to speak truth, leaning to the protection of external honor. Honor, the legal interest protected by criminal provision of defamation, is an "external honor as a social reputation" on a person's ethical or social activities and personal value, which can always be overestimated or underestimated. Nevertheless, the Criminal Act protects and confirms the 'honor' at the time of expression no matter how overestimated the social reputation is and consequently, the freedom of expression is limited. Rather, legal protection of a person's social reputation should be on the real value that person deserves. And by the spoken truth, social reputation is provided with the opportunity to readjust. If criminal or civil responsibility is established by speaking the truth, the freedom of expression will decrease and only the overestimated social reputation will be protected.

Thus, balancing of competing interest between the interest of freedom of expression and disadvantage created by the readjustment of social reputation needs to be done. If public interest achieved by speaking of the truth is adequately valued, it will

77) Supreme Court 1988. 10. 11. Judgment 85DaKa29.

78) "For a defaming activity to be justified according to the Crime Act Article 310, the act must be proven to be solely for public interest by the actor (Supreme Court 1988. 10. 11. 85DaKa29;1993. 6. 22. 92Do3160; 1996. 5. 28. 94다33828), but that proof is not required to be as compelling as the proof for the justices to find a person guilty of a crime. (Supreme Court 1996. 10. 25. 95Do1473)."

outweigh the private disadvantage of having a lowered social reputation. If this is the case than truthful speech is recognized as affirmative defense.[79] Freedom to speak truth can be easily intimidated in Korea because defamation is punishable criminally and civilly. Due to this, criminal complaints are overused.

This defamation provision is equally applied in the Internet. Act on Promotion of Information and Communications Network Utilization and Information Protection revise in January 16th 2001, with "Cyber defamation." According to the new provision, "A person who commits defamation of another person by disclosing a fact to the public through an information and communications network purposely to disparage his/her reputation shall be punished by imprisonment, with or without prison labor, for not more than three years, or by fine not exceeding 20 million won" and "A person who commits defamation of another person by disclosing a false fact to the public through an information and communications network purposely to disparage his/her reputation shall be punished by imprisonment with prison labor for not more than seven years, by suspension of qualification for not more than ten years, or by fine not exceeding 50 million won." The fact that although defamation in the Internet has strong propagation, the victim can also actively respond to engage in dispute needs to be reminded.

3) Controversy over Implementation of Cyber Defamation Law

Another controversy sparked in the society is on the issue of Cyber Defamation Law. It began after social controversy following suicides of several celebrities due to malicious comments online. Of course, current criminal law defines defamation law to punish a person who publically defamed another and is a crime prosecutable upon a complaint.

However, because information in the cyberspace is spread too quickly, once a

79) But we cannot conclude that the freedom to tell the truth is always more important than protection of personal right of others. The interest of privacy and the public interest of revealing of truth need to be weighed prior to the decision.

malicious comment is posted, it is spread immediately and causes exponentially increasing harm. Because of this, in 2008, executive branch and the national assembly created a proposal to create a new cyber defamation law on no punishment against will basis to quickly respond to malicious comments[80]. However, despite the support for its affect in protecting public characteristics of cyberspace and prevention of continuous cyber violence[81], its light criminality, risk of investigation agency's abuse, and possibility of only protecting the minority have been pointed out to strongly oppose the proposal.[82]

In the midst of this heated discussion, National Human Rights Commission in February 5th, 2009, expressed "if Cyber Defamation Law is to be implemented, it should require a victim's lawsuit"[83]. Anyhow, the issue of implementing the will require a close attention to possible side effects with basis in adequate social agreement.

4) System of Deletion Measure and Temporary Measure by Information and Communications Service Providers

As the number of cases regarding privacy intrusions and libel increased, the government and the legislature amended the Act on Promotion of Information and Communications Network Utilization and Information Protection and introduced deletion measures and temporary measures. The current the Act on Promotion of Information and Communications Network Utilization and Information Protection, which went through several more partial amending processes, enact provisions for information deletion requests and temporary measures in article 44.

---

80) Two proposals from Congressman Yoon Suk Jang and Congresswoman Kyung Won Na were submitted but became ineffective as the 18th National Assembly ended.

81) Jung, Wan, "A Study on Legal Institutional Response to Cyber Violence", Korea Internet Safety Commission, 2005. 8, p82

82) Yang, Dong-Chul, "Articles : A Study on the Direction of Legislation about Cyberviolence", Bubjo Vol. 55 (9) (2006. 9) p.158

83) National Human Rights Comission, Opinion on Proposed Revision to Telecommunication Act (Proposed by Congresswoman Kyung-Won Na), 2009. 2. 5.

Under these provisions, one who claims to have been affected by privacy intrusion can either request information communication service provider for deletion of information or demand for publication of refuting information. Information communication service providers should proceed to these measures without delay and should immediately notify both the applicant and the publisher and should post that so that users will be able to know that certain measures have been taken. Also when information communication service provider took deletion measures, he or she can be exempted from liability of reparation.

Moreover, under article 44 section 4, information communications service provider can take temporary measures to block any access to pertinent information for maximum of 30 days even though deletion is requested if it is difficult to decide whether the information publication itself have actually harmed one's rights or if conflicts between parties are expected. Also under article 44, section 1, information communication service provider can take temporary measures without any request for deletion if he or she thinks that the information distributed throughout information network system under his or her control may intrude privacy or infringe upon other's rights. Under article 44 - 2 section 3, information communications service provider is obliged to take direct measures to protect juveniles from unwholesome medium for juvenile.

But according to the current statute, the communications service providers are granted with immunity or leniency on the damage compensation responsibility if the deletion measure was due to the request of the authority. This policy aims for the quick deletion of illegal speeches on the internet, but possesses the danger of shutting of just criticisms towards public figures such as politicians or the business conduct of the corporations by quickly deleting them on authority's requests.

Whether the right to personality is violated should be decided with strict scrutiny through balancing of the interests. Nevertheless, an authority can quickly shut off the unwanted public criticisms. And communications service providers, who are mere intermediaries of information circulation, will follow the request of the authority for

the immunity. Thus, this system has the reasonable purpose of deletion of malicious comments, but also has the danger of shutting down the rightful criticism on the will of those that are criticized.

5) Freedom of Anonymous Communication and Identity Verification on Online Bulletin Board

In early 2003 when the "Participatory Administration" commenced, the Ministry of Information and Communication decided that anonymity on the Internet undermines sound discursive culture and allows frequent criminal activities such as defamation and threat, and adopted the real-name rule on the MIC's home page as a test case for beautifying the Internet and nurturing sound discursive culture. People had to identify themselves by inputting a resident registration number and a name to use the bulletin. At that time, real name verification was done by comparing to personal credit information held by Korean Association for Information and Communication and Korea Investors' Service. In April 2003, the Blue House adopted on its home page bulletin a three strikes policy of banning the users who have posted epithets and slanders more than three (3) times, and also limited the use of the anonymous bulletin to 10 posts per day per user.

In response to these bulletin policies, many civil society organizations pointed out that mandatory identity verification will cause harms including infringement of privacy when people are participating in self-corrective initiatives to establish sound Internet culture. The opponents of identity verification feared that it will require self-censorship from the netizens thereby not sanitizing but destroying discursive culture. The proponents sought for it citing the need to prevent abuse of free speech. The debate on online bulletin identity verification sharpened as it was made into law.

In May 2004, the amended Public Officials Election and Election Corruption Prevention Act (currently the Public Officials Election Act) adopted 'election bulletin board identity verification.' Thereafter, in January 2007, the Information Communication Network Act was amended to adopt 'ordinary bulletin identity

verification' and in September 2009, the Internet Address Resources Act was amended to adopt 'domain name real-name system'.

The election bulletin board identity verification rule went through several revisions after 2004 and now under Article 82-6 of the Public Officials Election Act allows the users to post any comment supporting or opposing a party or a candidate on the Internet press companies'[84] websites during the election period only after verifying their identities through the method offered by the Ministry of Government Administration and Safety or credit information providers. To that effect, the Internet press companies are required to install technological measures for identity verification and delete any posting not identity-verified. They are also required to comply with any deletion request by a party, a candidate, or the Election Commission. The users are allowed to us nicknames or fictitious id's once their identities are verified.

The rule indirectly requires the users to engage in an expressive act after revealing their identities when they post an opinion or a fact in support or opposition of a party or a candidate on the bulletin boards or the chatting rooms operated by the Internet press companies during the election periods It does not directly suppress such speech but requires the operators to delete any non-id-verified post. The current rule allows the government to manage the identities revealed thus and disclose or use them at its discretion. The Internet press companies, in rushing to delete all election related non-verified postings, are likely to delete all non-verified postings indiscriminately, in which case the users are prohibited from posting not just pro- or con- postings but any posting. It is likely that the current law greatly suppresses freedom of expression.

---

84) "Internet press agencies" shall refer to "Internet newspaper business operators under subparagraph 4 of Article 2 of the Act on the Promotion of Newspapers, etc., persons who run and manage Internet homepages, which are used to report, furnish or transmit Articles that are covered, edited and written through the Internet with the aim of propagating reports, commentaries, public opinions and information, etc. pertaining to politics, economy, society, culture and current events and any other persons who run and manage the Internet homepages that perform the functions of the press similar to those of the former; hereinafter the same shall apply"). Article 8-5 Paragraph 1 of Public Officials Election Act

The National Human Rights Commission, during a legislative debate on the law in February 2004, opposed it stating that restricting the freedom of online expression and of forming opinions anonymously is not compatible with Article 19 of the Universal Declaration of Human Rights and Article 21 of the Korean Constitution.[85] The Constitutional Court, however, upheld the law[86] and yet clearly announced that the right to anonymous communication is protected by Article 21.

The ordinary bulletin board identity verification rule adopted in July 2007 by the Information Communication Network Act also became controversial. Under the law, all public agencies[87] and large-scale service providers[88] installing and operating an online bulletin board were imposed identity verification obligations pursuant to the relevant presidential decrees and the non-complying service providers were subjected to administrative penalties (fine). The rule results in excessive restriction on freedom of speech because anyone wishing to criticize the government's policy or its members must reveal his or her identity and will chill him- or herself in fear of possible retaliation.

Despite the criticism, the Administration in November 2008 even proposed to delegate to a presidential decree which may expand the then current coverage beyond large-scale providers (average daily users in excess of 100,000). NHRC issued an opinion that the proposed amendment is likely to infringe on freedom of speech.[89]

In August 2012, the Korean Constitutional Court ruled that the limited identity

---

85) NHRC (First Sub-Committee), Opinion on "Political Relations" Act, 2004.2.16

86) Constitutional Court 2010.2.25 Decision 2008Hun-ma324

87) "Public agencies" here refer to "A State organ, a local government, a public enterprise, a quasigovernment agency under Article 5 (3) of the Act on the Management of Public Institutions, or a local government-invested public corporation or a local government public corporation under the Local Public Enterprises Act " (Act Article 44-5 Paragraph 1 Item 1)

88) "Large-scale service providers" here refer to A provider of information and communications services who falls under the criteria prescribed by Presidential Decree, where the average number of users of each type of information and communications services rendered by it reaches or exceeds 100,000 person per day" (Act Article 44-5 Paragraph 1 Item 2)

89) NHRC (Standing Committee), 2009.11.19

verification system violates freedom of expression and right to informational self-determination.[90] Thereafter, the Communication Commission announced that it will respect the Constitutional Court's decision and strengthen defamation mediation procedure and industry self-regulation.[91] The Central Election Commission also submitted an opinion for abolishing the election bulletin board identity verification rule to the National Assembly.[92]

The freedom of anonymous expression is a freedom to express and disseminate one's thoughts and opinions anonymously or pseudonymously without revealing his or her identity. The issues of online bulletin board identity verification rules depend on how much our society will accept that freedom, which allows social minorities a chance to freely express their views without revealing their identities thereby contributing to minorities' protection and therefore to democracy.[93]

(2) Cases at Issue

1) Minerva Case

On January 7, 2009, Internet writer Dae-Sung Park (pseudonym Minerva) was imprisoned and prosecuted for the crime of false communication under Article 47 (1) of the Framework Act on Telecommunications for posting two false articles about the government's foreign exchange policies on the "Agora," an economy discussion board at the internet portal site "Daum."

The issue in this case concerned whether false expression on Internet can be protected and by how much. Article 47 (1) of the Framework Act on Telecommunications stipulated, "A person who has publicly made a false communication over the telecommunications facilities and equipment for the purpose of harming the public

90) Constitutional Court 2012.8.23 Decision 2010Hun-ma47
91) Press Release, "Communication Commission's Position on the Constitutional Court's Unconstitutionality Decision." 2012.8.23
92) Central Election Commission's Press Release, 2012.8.24
93) In 2003, Council of Europe's Declaration on Freedom of Communication on the Internet states seven (7) principles, the seventh of which is the right of anonymity.

interest shall be punished by imprisonment for not more than five years or by a fine not exceeding fifty million won."

The prosecutors argued that he allegedly denigrated public confidence in the government's foreign exchange policy and the foreign currency payment capability by posting on the economy discussion board false information which said that Korean foreign exchange reserve was drained up and the money exchange service of the foreign exchange reserve was stopped, and letting thousands of people read it.

However, the National Human Rights Commission have submitted an opinion to the Seoul Central District Court and the Constitutional Court which stated that the case called for strict scrutiny on human rights infringement for the following reasons: (i) the international society has continuously pointed out the problems of the provision comprehensively punishing spreading of false expressions; (ii) most countries punish spreading of false expressions in very limited situations to protect the public interest; (iii) false communication is a very vague term which is unconstitutional; and (iv) prohibiting false expression does not serve the legislative purpose while gravely restraining freedom of expression.[94)]

The Seoul Central District Court found Minerva not guilty because it was hard to perceive that he posted the articles knowing that the contents are totally false, and as there was no intention to make a false communication, there was no evidence to prove that there was a purpose of harming the public interest.[95)]

The decision of the trial court didn't touch upon the unconstitutionality of Article 47 (1). On the contrary, the trial court was in a position that the provision itself was not unconstitutional. It can be inferred from the fact that the trial court denied the defendant's request for constitutional review by the Constitutional Court. Later on, the defendant filed a constitutional complaint to the Constitutional Court, and the Constitutional Court ruled the false communication provision of the Framework Act

94) National Human Rights Commission's opinion on Framework Act on Telecommunications submitted to the Contitutional Court and Seoul Central District Court (2009. 6. 8. decision)

95) Seoul Central District Court 2009.4.20. Judgment 2009Go-Dan304.

on Telecommunications unconstitutional on December 2010.[96]

The false communication provision is abolished by the decision of the Constitutional Court. However, the Constitutional Court only stated that the term "the purpose of harming public interest" was vague and thus in violation of the principle of clarity. The decision does not declare that all false expressions on Internet are protected by the Constitution and immune from punishment or regulation. Therefore, intentional false expressions harming reputation or credibility of others or malicious false expressions causing substantive social harm such as obstruction on fair election are not protected by the Constitution. The significance of this decision can be summarized as follows: false communications and false expressions are protected by freedom of expression and the press under Article 21 of the Constitution in principle, and laws restricting free speech must narrowly and clearly define the expressions subject to the restriction to guarantee freedom of expression to the maximum level.

2) Internet Portal Site Defamation Case

In this case, the Supreme Court held the Internet Portals limitedly liable for defamation caused by news articles the portals provided through their news sections and by their users' postings such as replies on their web pages.[97]

Facts of the case are as follows: On May 5, 2005, mother of a deceased female ("the deceased") posted an article on the deceased's "Minihompy" on Cyworld.com operated by SK Communications stating that the plaintiff had incessantly asked the deceased for sexual intercourse promising that he would marry her, verbally abused her and threatened to leave her after the deceased got pregnant for the second time after a miscarriage, filed an accusation for battery against the mother to the police, and, by ruthlessly refusing to settle, made the deceased to commit a suicide. The article also called for the readers to widely spread the story. Subsequently, visitors flooded into the deceased's Minihompy and many of them spread the article by

96) Constitutional Court 2010.12.28. Decision 2008hun-Ba157, etc.
97) Supreme Court en banc Decision 2009.4.16. 2008Da53812.

sharing it on their blogs and online cafes. An online café was opened to mourn for the deceased and to seek retribution against the plaintiff, and campaigns were initiated to collect signatures. Since May 8, 2005, the defendants (NHN and Daum Communication) published news articles about the incidents on news sections of their internet portals (NAVER and Daum). Among them were articles disclosing the name of the deceased or captured image of the Minihompy. Some of the articles criticized the plaintiff. Moreover, replies posted under the articles revealed the name and personal information of the plaintiff.

The plaintiff argued that the defendants were liable as the publishers of news articles harming his reputation, and also liable for breaching duty of care as operators of the portals for neglecting contents harming his reputation posted on online cafes, blogs, etc. of the defendants' portals and facilitating access to such contents through their search engines.

The Supreme Court in its en banc decision stated that internet portals are liable for damages for defamation if they save news articles from other news media in their news sections and selectively publish some of the articles that harm someone's reputation. Twelve Justices also found that the portals have duty to delete or block defamatory articles that are posted on the places they have provided (e.g. reply boards, blogs, online cafes, etc.).

However, the Justices were divided on the conditions that give rise to the duty to delete and block. The majority suggested three conditions: (i) illegality of the defamatory article must be clear; (ii) the defamed has requested deletion and blocking, or in case of no request, it is evident that the portal provider was aware of how the article was published or whether it was published; and, (iii) it is technically and economically possible to manage and control the article. The minority suggested four conditions: (i) illegality of the defamatory article must be clear; (ii) the defamed has requested deletion; (iii) the request must be specific and individual; and, (iv) it is technically and economically possible to take necessary measures.

3) Bad Review on Plastic Surgery Case

The defendant posted a reply on Naver's knowledge-search Q&A board about her subjective assessment that the result of her plastic surgery was disappointing, and was accused of defamation under the Information and Communications Network Act. Supreme Court reversed the decision of the court below and acquitted the defendant for the reason that she didn't have a "purpose to disparage."[98)]

The defendant received a radio frequency treatment on her chin at the plastic surgery clinic run by o o o, and unsatisfied with the result, posted a reply on Naver's knowledge-search Q&A board which states, "o o o is a breast specialist… that's why he ruined my eyes and chin… Had no idea…," and "My eye job went wrong… I'm screwed…"

The Supreme Court found that the reply is "disclosure of a fact" under the defamation provision of the Information and Communications Network Act. However, the Supreme Court found that there was no "purpose to disparage" based on the legal principle which states "there is no purpose to disparage if disclosed fact concerns the public interest, except in special cases."

4) MBC PD Diary Case

After the Korea-US beef negotiation was closed on April 17, 2008, television documentary "PD Diary" of Munwha Broadcasting Cooperation (MBC) aired the program "Is U.S. beef safe from mad cow disease?" on April 29. Doubts on the safety of U.S. beef spread across the country and many massive assemblies and demonstrations protesting against U.S. beef were held including so-called "candlelight protest." "U.S. Beef Protests" developed into a political movement opposing the MB government commenced on February 2008 and the government's reactions were a calibrator measuring the status of free speech in Korea. Two typical cases are MBC PD Diary case and Newspaper Advertising Boycott case.

---

98) Supreme Court 2009.5.28. Judgment 2008Do8812.

Right after the program was broadcasted, the Ministry of Agriculture, Forestry, and Fishery which was in charge of the beef negotiation submitted a mediation request for correction and counterargument to the Press Arbitration Commission Committee on May 6, alleging that the program was mostly false and damaged credibility and reputation of the Ministry. The Committee accepted the request in part on May 15 and MBC appealed against the decision to the Seoul Southern District Court on May 26. The court ruled for the Ministry accepting its request for correction and counterargument in part.[99] The Seoul High Court also ruled in favor of the Ministry on June 17, 2009.[100] However, the Supreme Court reversed the decisions on the ground that the program only expressed opinions on the government and it did not constitute report of factual argument.[101]

Meanwhile, the Minister for Agriculture accused producers, screen writers and the MC of PD Diary for defamation and interference with business on June 20. Subsequently, the prosecutors requested MBC to submit materials including original tape recording of the program on July 2. MBC refused and did not either respond to the prosecutors summons. The prosecutors tried to attempt search and seizure on the MBC headquarter twice, arrested the defendants and prosecuted them on June 18.

On January 20, 2010, the Seoul Central District Court found the defendants not guilty for the criminal charges.[102] The prosecutors argued that there were five major falsities in the contents of the program directly related to the risks of mad cow disease, but the court, after stating legal principles on defamation, found that each disputed content is not false, considering true meaning of the program as a whole viewed from the viewers' perspective.[103]

The trial court seems to be in a position that insignificant falsity in immaterial part of a statement does not make the statement false as long as the important part

99) Seoul Southern District Court 2008.7.31. Judgment 2008Gahap10694.
100) Seoul High Court 2009.6.17. Judgment 2008Na80595.
101) Supreme Court en banc decision 2011.92. Judgment 2009Da52649.
102) Seoul Central District Court 2010.1.20. Judgment 2009Godan3458.
103) The prosecutors appealed and the case is pending appeal.

agrees with facts when viewed as a whole. The appellate court also found the defendants not guilty. The appellate court reached the same not-guilty conclusion as the trial court on the grounds that, although some parts of the main contents of the program are false, the program was not a malicious attack and freedom of the press on matters of public domain must be guaranteed more extensively compared to matters of private domain.[104)]

The Supreme Court affirmed the lower court's decision and dismissed the prosecution's appeal.[105)] The Supreme Court stated that in media defamation cases, the standard of review varies depending on whether the report concerns matters of public interest or matters of purely private domain, and "as to the speeches belonging to private domain, protection of reputation may prevail over freedom of the press. As to the matters of public and social nature, restriction on freedom of the press must be eased." Furthermore, the Supreme Court stated, "matters concerning the government's or state agencies' policy making or performance of their duties must be subject to the people's constant monitoring and criticism, which can be properly conducted only if the freedom is sufficiently guaranteed to the press whose main duties are monitoring and criticizing. The government or state agencies cannot be the victims of criminal defamation, and therefore, even if a media report mainly concerning the government's or state agencies' policy-making or work performance reduces the social reputation of the official involved in such policy-making or work, such report cannot be held to defame the official unless such report is malicious or a very rash attack against the official as an individual."

5) Termination of a National Tax Services' employee for criticizing the Service on internal bulletin

On May 28, 2009, Chonam Naju Tax Office employee o o o posted on the internal bulletin of National Tax Service a writing blaming the former Chief of the Service

104) Seoul Central District Court 2010.12.2. Judgment 2010No380.
105) Supreme Court 2011.9.2. Judgment 2010Do17237.

HAHN Sang-ryul for President ROH Moo-Hyun's death and casting doubt on the Service's investigation on Taekwang Industry Co., Ltd. Under the title "I Know What NTS Did Last Summer", he alleged that the former Chief Hahn, upon instruction of the new government, initiated a politically charged investigation into the company, the sponsor of the former government.

NTS's Posting Management Committee made the posting private and deleted it on June 4. NTS Kwangju Branch investigated o o o and placed him under disciplinary review for a violation of decorum set forth in the State Public Officials' Act and Public Officials' Code of Conduct. On June 12, the disciplinary committee of the Kwangju branch terminated o o o with prejudice for violently deprecating the former Chief, defaming the tax activities, defaming the NTS agents with false information, violating Article 63 of the State Public Officials' Act and Article 23 of the Public Officials' Code of Conduct. The Kwangju branch also on September 16 filed a criminal complaint with Kwangju District Prosecutors' Office for defamation of the NTS agents. The Police issued a no-suspicion opinion but the Prosecutors indicted o o o for defamation of the former Chief Hahn while dropping the case for defamation of NTS agents.

In an administrative appeal on the termination, the Ministry of Government Administration and Safety's Review Committee on January 15, 2010, reduced the termination with prejudice to termination without prejudice. o o o immediately filed a lawsuit challenging the Committee's decision in Kwangju District Court. The issues were whether o o o's posting was false, and whether he was intentional with respect to the falsity. The courts of first instance, though finding it difficult to establish falsity of his posting and also o o o's intent in view of circumstances, cancelled the termination decision but found him guilty of defamation under the Information Communication Network Act and fined him to 700,000 won, finding a slanderous purpose where "the posting was mainly personal attacks and was therefore not for public interest."[106)]

106) Kwangju District Court 2010.5.12 Judgment 2009Go-dan4255.

The court of second instance reversed and acquitted him, for the reasons that: (1) the NTS Chief was not a private figure but a public figure; (2) the internal bulletin was a space where NTS agents freely offered opinions and engaged in discussions; (3) o o o's posting was not in purely private domain but contributed to formation of collective opinions or discourse on the matters of public interest; (4) the defamed person's conduct left himself vulnerable to such criticism; (5) the media have reported on the relevant scandal in so much detail that o o o's posting did not cause any defamatory effect anew or additionally; and (6) a finding of public interest negates a slanderous purpose.[107)]

The Supreme Court on December 24, 2011, affirmed the appeals court decision ordering cancellation of the termination decision with the following comments on defamation charge: "A slanderous purpose and a purpose for public interest are mutually conflict directions of the speaker's intention. If the facts alleged are for public interest, a slanderous purpose is deemed negated. Being for public interest is defined as a state where the facts alleged are objectively for the interest of not just the general public but also special social groups or their members' interest. . . As long as the speaker's main motive or purpose is for public interest, presence of any privately interested purpose or motive does not establish a slanderous purpose."[108)]

This case embodied several issues such as the limit on the public officials' freedom of criticizing the superiors and whether defamation of groups is recognized as a crime, and called for due balancing of public officials' integrity and freedom of expression.

In a similar case, the Supreme Court found that a posting on an internal bulletin of the National Health Insurance Service, although endangering another person's personality, credit, honor, etc., and factually false to an extent or exaggerated or distorted in expressions, cannot constitute a cause of discipline as long as it is overall truthful and does not purport to infringe on another's rights and interests but purport to enhance or maintain the working conditions thereby promoting the workers' welfare and socioeconomic status.[109)]

---

107) Kwangju District Court 2010.8.10 Judgment 2010No1068.
108) Supreme Court 2011.11.24 Judgment 2010Do10864.
109) Supreme Court 2012.1.27 Judgment 2010Da100919.

(3) Conflict with Right of Information Privacy and Restriction on Freedom of Expression

1) Conflict with Right of Information Privacy

Freedom of expression is a very important right in that a human being uses it as a means to materialize him/herself as a personal being. It is an external expression of freedom of mind which is essential to modern democracy. Without freedom of expression, democracy cannot exist. Therefore, it is given superior status than general individual rights and firm legal principles are structured to protect the freedom.[110)]

Nowadays free speech on cyberspace is becoming more and important. Cyberspace is a virtual space where people communicate with each other through communications networks connecting computers. It creates very different human relationships from offline relationships: interactions in cyberspace do not necessarily involve face-to-face actions-the relationships are formed in a digitalized way that is different from an analog way. Cyberspace is different from others forms of communication in that its nonlocal, atemporal nature combined with impersonal and amorphous features liberates whole new social behaviors unparallel to the existing social order, from the strictures of the real world.[111)]

Moreover, universalization of the Internet has contributed in vitalizing information utilization by facilitating access to and gathering of information online, which fulfils citizens' right to know and information freedom. Freedom of expression entered into a new era as the place of communication is expanding infinitely with the advent of new forms of media and SNS services such as facebook and twitter.

On the other hand, misuse, abuse, or ill-use of information lead to breach on personal information or confidential information of national significance. Freedom of expression should be restricted in privacy infringement cases where personal information of the parties is disclosed or used without consent.[112)]

---

110) Sung, Nak-In(1995) "Freedom of Expression", 「Concept and Range of Basic Rights」, *Constitutional Court Case Studies* Vol. 6, Constitutional Court.

111) Han, Sang-Hee(1998), "Cyber Democracy-The meanig and Constitutional prospect", 「Sungshin Law Review」

Liberal communication space on the Internet has been expanded rapidly as the users may use it anonymously without confronting each other and there is no time and space constraints. With the emergence of the Internet, freedom of expression has been expanding its scope and is contributing to promotion of human rights. However, social responsibility ensues expression as in Article 21 (4) of the Constitution, and side-effects such as information leakage, breach on personal information, and personal attack on others should be taken into account. Easily accessing other's personal information and disclosing them online infringes on personal rights in the private domain of an individual and harms reputation, and measures to prevent or block such activities restrict freedom of expression. It is difficult to give one right superiority over the other when they are in a conflict.

Therefore, when right of information privacy and freedom of expression collide, protected legal interests of both sides need to be measured and balanced against each other. The Constitutional Court also stated in a case where freedom of expression and personal rights were in a conflict that it is a matter of constitutional assessment balancing freedom of the press which is essential basic right in a democratic society and protection of reputation which is the foundation of human dignity right to pursue happiness.[113)]

2) Limits and Restriction on Freedom of expression

Article 21 (2) of the Constitution stipulates, "Licensing or censorship of speech and the press, and licensing of assembly and association shall not be recognized," which recognizes the doctrine of prior restraint. However, post-restriction on freedom of expression may be allowed according to Article 37 (2) of the Constitution and most U.S. judgments recognize possibility of restriction. Freedom of expression is not guaranteed absolutely, and it may be relatively restricted for the sake of the public

112) Kim, Sang-Kyeom(2012), "Privacy Protection and Clash with the Freedom of Expression", 「Human rights protection in information era」, National Human Rights Commission · Korea Internet Law Assiociation.

113) Constitutional Court 1999.6.24. Decision 97Hun-Ma265.

interest. Even in the U.S. where free speech is strongly protected, majority of the Supreme Court agrees that it can be restricted according to the principle of balancing of interests and recognized its relativity despite few dissent opinions call for complete protection.[114] This logically follows the notion that externally exercised freedom assumes corresponding responsibility. Nevertheless, it should be noted that balancing of interests and superior status of free speech do not contradict each other because the superior status is given as free speech contributes to the public interest by promoting the citizens' right to know, and it is different from holding it responsible when it harms the public or private interests.[115]

There are also laws of other countries and international conventions that place certain restriction on freedom of expression. French Declaration of the Rights of Man and of the Citizen states that a citizen "shall be responsible for such abuses of this freedom as shall be defined by law." Germany Constitution Article 5 (2) states that the rights are subject to limitations in the provisions of general statutes, in statutory provisions for the protection of the youth, and in the right to personal honor. The International Covenant on Civil and Political Rights Article 19 (3) states that the exercise of the rights carries with it special duties and responsibilities, and may therefore be subject to certain restrictions for respect of the rights or reputations of others and for the protection of national security or of public order, or of public health or morals.

General comment No. 34 (CCPR/C/GC/34) of the Human Rights Committee adopted in 102nd session on July 2011 and disseminated on September 12 concerns Freedoms of opinion and expression under Article 19 of the International Covenant on Civil and Political Rights. It provides for detailed guidelines on the scope of restriction. That is: restrictions must be provided by law; a law may not confer unfettered discretion for the restriction of freedom of expression on those charged

114) Konigsberg v. STATE Bar of California 366 u.s. 36, 56, 81 S.Ct. 997, 1010, 6 L.ED. 2d 106, 1961.

115) Korea Internet and Security Agency(2010.12). "Freedom of Expression on the Internet and Protection of Privacy"

with its execution; and laws must also be compatible with the provisions, aims and objectives of the Covenant.

It states that restrictions for respect for the rights or reputations of others[116] which is the first legitimate ground must be constructed with care. For example, “while it may be permissible to protect voters from forms of expression that constitute intimidation or coercion, such restrictions must not impede political debate, including, for example, calls for the boycotting of a non-compulsory vote.”

The second legitimate ground is that of protection of national security or of public order, or of public health or morals. It is not compatible with paragraph 3, when laws and provisions relating to national security are invoked to suppress or withhold from the public information of legitimate public interest that does not harm national security or to prosecute journalists, researchers, environmental activists, human rights defenders, or others, for having disseminated such information. A restriction on the issuing of a statement in support of a labour dispute, including for the convening of a national strike, was not permissible on the grounds of national security.

When a State party invokes a legitimate ground for restriction of freedom of expression, it must demonstrate in specific and individualized fashion the precise nature of the threat, and the necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat.

In paragraph 43 regarding freedom of expression on the Internet, it states that any restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3. It is also inconsistent

116) The term “others” relates to other persons individually or as members of a community. 61 Thus, it may, for instance, refer to individual members of a community defined by its religious faith or ethnicity (General comment (CCPR/C/GC/34) paragraph 28).

with paragraph 3 to prohibit a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government.

Defamation laws must be crafted with care to ensure that they comply with paragraph 3, and that they do not serve, in practice, to stifle freedom of expression. All such laws, in particular penal defamation laws, should include such defences as the defence of truth and they should not be applied with regard to those forms of expression that are not, of their nature, subject to verification. At least with regard to comments about public figures,[117] consideration should be given to avoiding penalizing or otherwise rendering unlawful untrue statements that have been published in error but without malice. States parties should consider the decriminalization of defamation and, in any case, the application of the criminal law should only be countenanced in the most serious of cases and imprisonment is never an appropriate penalty.

Freedom of expression is an indispensable condition for the full development of the person and constitutes the foundation stone for every free and democratic society. Therefore the Human Rights Committee emphasizes that the restrictions should be tailored specifically and cautiously.

---

117) General comment (CCPR/C/GC/34) paragraph 38
the Committee has observed that in circumstances of public debate concerning public figures in the political domain and public institutions, the value placed by the Covenant upon uninhibited expression is particularly high. Thus, the mere fact that forms of expression are considered to be insulting to a public figure is not sufficient to justify the imposition of penalties, albeit public figures may also benefit from the provisions of the Covenant. Moreover, all public figures, including those exercising the highest political authority such as heads of state and government, are legitimately subject to criticism and political opposition. Accordingly, the Committee expresses concern regarding laws on such matters as, lese majesty, desacato, disrespect for authority, disrespect for flags and symbols, defamation of the head of state 89 and the protection of the honour of public officials, and laws should not provide for more severe penalties solely on the basis of the identity of the person that may have been impugned. States parties should not prohibit criticism of institutions, such as the army or the administration.

Section 3. Right of access to information

1. Definition and Contents

(1) Definition

Now that ICT almost have full authority over our lives, it will be more difficult for anyone to imagine a life completely cut off from information. As dependency on information increases, a society will lose its energy and eventually crumble down just like a patient who is suffering from clotted blood vessels. Also, in areas where information is structurally allocated unevenly, a power based on monopoly over information will arise, and a few with that power will suppress the many without such power.

In order for an individual to live as a dignified entity and to enjoy one's right as right holder in a democratic society, one must be able to freely form an opinion and express it outside. To do this, one should be guaranteed a right to freely access basic information necessary for living and collect, transfer, and use it.[118] In this light, many states are officially or unofficially guaranteeing citizens' right of access to information as a basic right. Germany defines in its basic law Article 5 section 1, "all has a right to obtain information from general source of information (informationasquelle) without distractions" and guarantees right to information (Informationsfreiheit). A Right of information originates from a tragic experience of wide media censorship during the Nazi Era and is defined as "freedom to collect information from general and widely accessed source of information and use it selectively."[119] On the other hand, the United States refers to the right to free access and dissemination of information as the "right to know".

The Constitution does not specifically enumerate such rights, right to know is still

118) Huh, Young, Theories on the Constitution and Constitution, Pakyoung Books (2008), pg 739

119) W. Hoffmann-Riem, Art. 5(Recht der freien Meinungsäußerung), in: GG-AK, 2. Aufl. 1989, Rdnr. 82.

accepted as one of basic rights. Academics generally understand right to know as an equivalent to freedom of information and sees a passive right to accept information from a generally accessible source and selectively use it and an active right to proactively collect information necessary to form a person or a public opinion.[120] The Constitutional Court also acknowledges the right to know as "free formation of an opinion is possible when sufficient level of access to information is guaranteed and in this light access, collect, and use of information, hence the right to know is closely tied to freedom of expression."[121]

Freedom to collect and use of information basically requires free access of information. Right of access to information, which is a right to freely access information, can be seen as a part of basic rights which serves as the foundation for freedom of information or the right to know. Free access to and collection of information enables sovereign rulers, the citizens, to be served with accurate information, thus reinforces realization of basic principle of the constitution regarding national sovereignty, and aids realization of citizens right to live dignified lives and right of a consumer in an information era.[122] Furthermore, it serves as a legal foundation for resolving the problem of political, economic, social, and cultural isolation from unequal distribution of information. Therefore, this report attempts to investigate right of access to information as a something beyond the concept of freedom of information or right to know, and as a basic right that covers rights related to unequal distribution of information

(2) Components of Right of access to information

Firstly, Right of access to information in a passive sense refers to right to demand elimination of policies or actions that curtails one's access to information. Furthermore, it can be extended to include one's right to demand disclosure of

120) Sung, Nak-In, Constitution, Bubmoonsa (2008), pg 542.
121) Constitutional Court 1991.5.13. Decision 90Hun-Ma133.
122) Kye, Hee-Yeul, Constitution(2), Pakyoung Books (2000), pg 384.

information held by the state and implementation of an active action to resolve an issue of unequal distribution of information. Here, a right to demand elimination of disturbances can surely be recognized as a part of defensive right included in freedom of information as seen in general basic rights. In contrast, subsequent rights extends beyond traditional basic rights to more proactive stance, thus is open to varying interpretation regarding its legal foundation, extend, and others.

Among those, right to demand a disclosure of information, according to domestic academics[123] and cases,[124] is guaranteed in the realm of right to know. South Korean state defines citizen's right to demand information and public entities' duty to disclose information to guarantee citizens' right to know; moreover, the Official Information Disclosure Act was enacted in 1996 to secure citizen's participation and transparency in state operations. Based on the stated legislation, policy on information disclosure has been active since 1998 and has faced a new phase as a comprehensive information disclosure system (www.open.go.kr) launched in 2006.

Yet, as information technology advanced, access and use of information has been unequally provided based on education, income level, gender, geological location, and others which led to widening digital divide that creates economic and social imbalance. This digital divide firstly can be seen as information inequality. Moreover, in a highly advanced information society, blocked access to information can lead to a complex problems such as absence of tools necessarily for humane survival, and lack of opportunity in political, economic, social, and cultural arena. Therefore, it would is advisable to approach the digital divide as problem beyond immediate perception on nondiscrimination or welfare but as practical provision of right to access to information.

The Constitution aims for a practical equality and guarantees one's right to human livelihood. When the digital divide raises an unfair discrimination intolerable by the constitution, the state has a duty to actively correct the problem. To enhance quality of life and encourage balanced economic advancement by guaranteeing free access

123) Sung, Nak-In, "Information Disclosure and Right to Know- Focusing on proposals on Information Disclosure Act", *Goshiyeongu*, 1995.2. pg 67.
124) Constitutional Court 1992.5.13. Decision 90Hun-Ma133.

to and use of information to those who face difficulty accessing information service due to economic, geological, physical, and social conditions, South Korea has implemented the Act on Resolving the Digital Divide on January 16, 2001. Anyhow, those who fall into the category of information poor has the right to demand the alleviation of the digital divide and this citizen's right can be read as an extension of a type of right of access to information.

In summary, right of access to information can be broadly divided in to right to demand disclosure of information and right to demand elimination of distractions and the legislations embodying these rights are the Official Information Disclosure Act and the Act on Resolving the Digital Divide. Then, the following will study international trend on legalization of right to access to information and the current state of the South Korea's policy on disclosure of information and the digital divide as well as issues surrounding them.

2. International trend and standards

(1) History of right of access to information

According to "charter of liberties" from the state of Massachusetts in the United States drafted in 1641, all men in the colonies had the liberties to review and have copies of all documents produced by the court and state agencies.[125] Also, in 1766, Sweden's law on freedom of press generally allowed copying and releasing state documentations to the public and freely access state documentations for them.[126]

The term "Right to Know" was first used by an American journalist Kent Cooper and was strongly argued for institutionalization through *The People's Right to Know, Legal Access to Public Records and Proceedings (1953) by* Harold L. Cross and *The Right to Know (1956)* by Kent Cooper.[127]

---

125) Altschull, Herbert. From Milton to McLuhan: The Ideas Behind American Journalism, Translated by Yang, Seung-Mok, Nanam (2001), pg 461.

126) Gun, Gyung. "Study on Policy of Right to Request Information Disclosure-in Relation to Theoretical Structure, PhD Dissertation from Seoul National University, 1998, pg 35.

127) Kim, Ok Jo, Media Law, Communication Books, 2006, pg 316.

(2) Trend on Institutionalization of Demand for Disclosure of Information

1) International Covenants

Universal Declaration of Human Rights adopted by the UN on December 10, 1948, states in its Article 19 that “Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers” and guarantees right of access to information.

Council of Europe in 1979 decided on Recommendation 854 on Access by the public to government records and freedom of information. This principle was visualized as European Council of Ministers urged all member states to implement domestic legislation on freedom of information on November 25, 1981, and February 21, 2002. Subsequently, right of access to information has been institutionalized by most of the European states now.

Right of access to information was formally recognized in the European Union based on Maastricht Treaty’s Appendix Declaration 17. This declaration confirms that making a process of making decisions transparent through guaranteeing right of access to information can enhance democratic characteristics and public trust for public administration of state agencies and thus demanded European Commission to submit a report on procedures for facilitation of disclosure of information held by the EU by 1993 to the board. Therefore European Commission conducted a research on policy for right of access to information and submitted a report on June of 1993 to the board and decided on codes of behavior (OJ 1944 L 46/58) which defines specific standards on information disclosure. If a request for disclosure of information was denied by the related agency, one may request for confirmation to the operations commission within one month period. Also, if the operations commission cannot respond to the request, the commission must explain reasons for its denial to the requested person within one month period. Those who object can bring the case to the European Court or file a case to the ombudsman.

Efforts for enhancing practicality of the policy has followed and resulted in codes

on information disclosure policies in Amsterdam Treaty (1997) and Regulation of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament (OJ L145, 31/5/2001).[128] The Regulation acknowledges access of document as one of basic rights. However, agencies other than three major agencies, Council of Europe, European Council of Ministers, and European Commission, is not subjected to the duty enumerated in the Regulation. This regulation corrects few problems in previous codes of behavior. For instance, it mandates replies to be given within 15 working days and allows the requesting person to request for confirmation in 15 days if the request has been fully or partially denied for fast proceedings. Also, the regulation allows documents obtained by the third party to be accessed by the public. In regarding documents held by the member states, unless there is a clear distinction on the public need to disclosure of requested information, decision is to be made after consultation with the agencies related to EU. Although it lists 9 types of information that are exception to this principle, it states that this cannot be the sole reason to deny release of information, mandates states to release information that can be released, and limits nondisclosure period to thirty years.[129]

2) International Trend on Institutionalization

Following the World War II, states have come up with legislations to legally secure right to know or access. Starting with Finland's 1951 legislation on public characteristics of state documents, 1996 U.S. Freedom of Information law, 1970 Denmark's legislation on access to administrative documents and Norway's legislation on public characteristics of administration, 1978 France's legislation on access to administrative documents and Netherland's legislation on access to administrative information, 1982 Australia's freedom of information act, Canada's legislation on access to information, and New Zealand's legislation on administrative information,

128) Regulation (EC) No1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission document.
129) Jang, Kyung-Won, "Information Disclosure Based on EU Administrative Law", Administrative Law Journal Vol.21, 2008, pg. 75-96.

1987 Austria's legislation on release of information on federal administrative agencies, 1994 Belgium's legislation on release of information on administration, 1999 Japan's legislation on release of information held by administrative agencies, 2000 UK's freedom of information act, and 2005 Germany's freedom of information act have been adopted. Following section will examine early cases of the U.S. and relatively recent cases of Japan, UK, and Germany.

A. The United States

In the U.S. right to access public record has been recognized by the common law. However, the record held by the public administration has been out of reach due to lack of proper legal measures. Therefore, in 1946, Administrative Procedure Act, APA, has been passed in which Article 3 defines the public access to administrative information. Still, public access to the information held by the state was severely curtailed due to various complications. To tackle this, in 1966, Freedom of Information Act, FOIA, was passed to establish a legal basis for the federal information disclosure. This law granted public wide access to request disclosure of information regardless of their interest and greatly shorten the list of 13 exceptions to the request. Also, courts were given the ability to review the denial of disclosure by the state to decide on practical and legal components of the state decision.

FOIA states the disclosure of the information held by the state and procedures necessary for request for disclosure. The law can be broadly seen as a collection of two parts, state's duty to disclose information and procedures for the quests. Information under the effect of the law include public information required to be registered in the Federal Register such as structure of an agency, function, procedure, practical codes, and general policy and those public agency must make available for public inspection and copying such as individual opinion on a policy, worker's manual, and others. Records outside of this parameters, a state has the duty to quickly release information upon request. However, (1) information specifically authorized under criteria established by an Executive order to be kept secret in the interest of

national defense or foreign policy, (2) related solely to the internal personnel rules and practices of an agency, (3) specifically exempted from disclosure by statute, (4) trade secrets and commercial or financial information obtained from a person and privileged or confidential, (5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency, (6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy, (7) records or information compiled for law enforcement purposes, (8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions, or (9) geological and geophysical information and data, including maps, concerning wells are to be exempted from the effects of this law.[130)]

This law was amended in 1974 following the Watergate Scandal in the early 1970s. Limitations and Inspection mechanism on the public agency was reinforced for swift and transparent disclosure of the information at the procedural level. Also, it was amended to especially limit the application and strengthen legal review of the aforementioned exceptions (1), (7), and (8) which were controversial in previous cases. It was further amended in 1976, 1978, and 1986 and is regarded as the most advanced law of its kind by other countries.[131)]

On the other hand, in 1976, government in the Sunshine Act was passed to require disclosure of state meetings and in 1996 Electronic Freedom of Information Act was passed to enable citizens to request and receive information through email. More recently in 2007, it was amended into Openness Promotes Effectiveness in our National Government Act of 2007.[132)]

130) http://www.nih.gov/icd/od/foia/efoia.htm. (visited on 2009. 10. 5)
131) Lee Kwan-Ki, Right to Know and Privacy, KOECC, 1993, pg. 98-100.
132) Jang, Kyung-Won "Information Disclosure Based on EU Administrative Law", *Administrative Law Journal* Vol.21, 2008, p.75-96

B. Japan

In Japan beginning between late 1950s and early 1960s, mass media went through an unprecedented advancement which led to discussions about privacy and citizen's right to know about public information held by the national and municipal government. While the institutionalization of the principle was under review, Lockheed incident inspired public discussion on citizen's right to know while the municipal governments argued for disclosure of information on the premise that it will serve to realize local self-government by the public. The first accomplishment occurred in Kanagawa Prefecture. In 1979, conversation about information disclosure led to public declaration of "Local Ordinance on Release of Public Documents Held by Public Agencies in Kanagawa Prefecture" in October 14th 1982 which came into effect on April 1st, 1983.[133] Beginning with this, a number of local governments adopting the principle into local ordinances increased dramatically. However the national government responded with lukewarm acceptance and dragged on for a long time.

The national legislation was created in May 14th, 1999 under the title "Legislation on Release of Documents Held by the Public Agencies" and came into effect in April 1st of 2001. This law lays out the procedures necessary for request of disclosure. Independent administrative legal bodies equal to administrative agency, courts and the parliament are subjected to separate legislations specifically designed for under the same principle.

The legislation designed for the public agencies declare the principles in the Article 5 which states, "the person in charge of the agency must release the information upon the request unless it falls under the following list of exceptions." The same article lists the exceptions: Personal information such as names and date of birth that can be used to identify a person, personal or business information which the release may harm one's interest, information that may hinder the national security or relationships

133) For detailed information on the introduction of information disclosure policy, see the following: Han, Young-Hak, "Special Characters and Meanigs of Information Disclosure Law in Japan" *Press Laws of the World* Vol. 23, Korea Press Foundation, 208, pg. 285-292.

with other countries, information recognized by the head of agency as the release has a risk of damaging public security or order, information that may harm the severely harm the neutrality in decision making process by national and local agencies, Information which the release may impede the operations of public workers. There has been some dispute about whether these exceptions mean prohibition of release of described information or exemption from this specific law. Yet current trend tends to understand it as an exemption from this law in its relation to the Article 21 of the constitution which guarantees freedom of expression.[134)]

C. United Kingdom

In 2000, UK implemented its version of information disclosure policy with Freedom of Information Act 2000. This law was created to guarantee citizen's right to know about the public agencies and was propelled by the Labour Party which promised in 1997 parliamentary election. It came into full effect on January 1st of 2005 and has been implemented on 100,000 public bodies including government agencies, schools, and committees. While the law appoints the Minister of Justice Department as the responsible for public disclosure of information, in realty, it has been executed by the Information Commissioner. Besides this act, another law exists such as Freedom of Information (Scotland) Act 2002. Based on these legal tools, about 120,000 citizens are requesting for information annually of which 60 percent are citizens, 20 percent are businesspersons, and 10 percent are journalists.[135)]

The British act in its first article states that all people has the right to demand disclosure of information and guarantees general access to the right. Yet, there are numerous exceptions to information such as those accessible by other means, those scheduled for public release, those related to national security, health information, court records, and others (Article 21 to 44).[136)] Some of them are under full exception

134) See 松井茂記, "情報公開法五條",「ジュ…リスト」No 1156(1999年6月1日號), 1999, pg. 45-46
135) "Every expense spared", The Economist, 23 December 2006, Number 8532, p. 46.
136) http://www.opsi.gov.uk/acts/acts2000/pdf/ukpga_20000036_en.pdf. (visited on 2009. 10. 5)

and are fully denied while others are subjected to relative disclosure following consideration for harms and goods of the release.

Those who cannot accept the denial of request can submit a case to the Information Commissioner who has the authority order disclosure. However, the agency ordered by the Commissioner can challenge the order by taking the case to the Informal Tribunal.

On the other hand, public agencies are mandated to in advance plan the release of important public information. This plan for publication must be approved by the Information Commissioner. Technically, the agency requested for disclosure must respond within twenty working days.[137)]

D. Germany

Until the mid-2000s, Germany did not recognize citizens' general right to request for public information. It was because request for disclosure of information was already under separate codes such as right to request viewing of public administrative procedures and right to participate in public procedures. Right to request viewing of public administrative procedures was defines in the German Federal Administrative Procedure Law (VwVfG); however, it was only limited to individuals and parties who are directly affected by or related to the procedure. Environmental Information Law (Umweltinformationsgesetz) recognized general right to request disclosure of information but it was limited to environmental information.

When Brandenburg state passed a law on freedom of information in 1998, Berlin in1999, Schleswig-Holstein in 2000, Nordrhein-Westfallen in 2002 and others followed the trend. Ultimately in 2005, Federal Information Access Law (Gesetz Zur Regelung des Zugangs zu Informationen des Bundes) came into effect to acknowledge general right to access information at the federal level.[138)]

The law, also known as Informationsfreiheitsgesetz or IFG, declared the principles

137) http://en.wikipedia.org/wiki/Freedom_of_Information_Act_2000.
138) http://www.informationsfreiheitsgesetz.net/blog/informationsfreiheitsgesetz

of the right in its Article 1.1 by stating “All citizens have the right to access public information at federal agencies based on regulations stated in this law”. Based on the Article 2.1, the law defines the limits of this law to all documentation used for public purpose. By this principle, all public information held by public agencies and offices are within the power of this law. Yet, inessential information such as drafts and memos are not recognized.

Because IFG has its base in division of power at the existential function, all federal agencies and offices are obliged to disclose information within the limits of their work defined by the law. Therefore, federal agencies are not allowed to disclose legislative or judicial information. Also, private parties, especially policy aid providers (Verwaltunshelfer), whose work is similar to that of a federal officer are levied the same duty as other federal agencies.

However, IFG recognizes the exceptions to this law. Article 3 limits disclosure of special public information for protection of public good. Article 4 acknowledges the limits on the information that could affect a development of a public policy. Despite these exceptions, Article 7.2.1 allows partial disclosure of information depending on the case.[139)]

Article 5 and 6 defines exceptions to the information to protect individual interest. While the Article 5 foremost considers information’s right to self-determination through protection of information related to individuals, the article 6 protects intellectual property rights and business secrets to realize freedom of occupation and protection of private property.[140)]

(3) Trends on Laws Relating to Resolve Digital Divide

Solidification of legal standards relating to resolving digital divide often occurs in a form of guideline to reconsider access to the web. Especially, Human Rights Charter

139) Matthias Rossi, “Free Access to Public Information and Administrative Process in Germany”, *Public Law Journal* Vol. 354 2007. Trans. Jang Kyung-Won, pg 249-260.

140) Jang, Young-Soo, “Information Disclosure Policy of Germany” *World Press Law Journal* Vol.23. Korea Press Foundation, 208, pg.190

for the Disabled which was created to guarantee disabled person's right access information states in its Article 4 that "a disabled person has the right to receive all service required for expression of an opinion and access information such as telecommunication, sign language, subtitles, and audiobooks". Also UN Convention on the Rights of Persons with Disability broadly takes on the issue of one's freedom of expression as the right to search, collect, and disseminate information through the means of one's choice. In this, sign language and other alternative communication methods are listed as means of communication.

In case of the U.S., Article 508 was added into Rehabilitation Act in 1998 and required all federal agencies to post information online. According to this article, federal government has an obligation to allow disabled public workers to access and use information at the equal level guaranteed to the non-disabled public workers. At the same time, disable citizens are guaranteed access to information at the level it is granted to non-disabled citizens. To abide by this law, a guideline of sixteen components for access to web was created based on World Wide Web Consortium's (W3C) guideline. In the UK, Discrimination Against Disabled Act (DDA) was created and 1995 and a new guideline was created by Committee on Rights of Persons with Disability in 2002. This guideline mainly concerns providing assistance service or a device to allow disabled persons to access online shopping malls and convenient services. Also, in 1999, a guideline to abide by the accessibility of UK government's website was created based on W3C's WCAG 1.0 and all website are now obligated to abide by the guideline by DDA from October, 2004.[141] In other counties, Japan created a web accessibility standard (JIS X 8341-3) in 2003. Australia has a similar guideline based on its own DDA.[142]

General Guideline[143] for countries in Asia-Europe Meeting states that Digital

141) Hyun, Geun-Shik et. al. Monitoring Disabled Person's Accessibility to Public Websites, National human Rights Commission, (November,2009). pg16

142) Ministry of Administration and Safety Department of Information and Culture, "Web Accessibility and Policy Direction", (April, 2009). pg.9-10.

143) The 12th ASEM Human Rights Seminar: Telecommunication Technology and Human Rights (2012.6.27.-29, Seoul).

Inclusion is important in guaranteeing human rights. Telecommunication technology worldwide is taking an important role in all aspects of human and social development. Access and ability to effectively use telecommunication technology is an essential condition for realization of human rights in broad areas. This telecommunication technology shows that the governments must work to achieve Digital Inclusion.

Therefore, a government must focus on investing in social foundation infrastructure, monitoring and regulating monopoly, providing telecommunication education to a targeted audience, protecting rights of users and guaranteeing equal access to contents, guaranteeing alternative methods for online services, and abiding by its own principles. All of these measures must begin with providing support for those who area in the risk of Digital Exclusion. Hence, the government must close the information gap, come up with plans to prevent new digital divide, and consider those problems with structural approach.

3. Debates and Issues in Korea

(1) Argument over policies

1) Request for information disclosure

A. Definition of right to request for disclosure of information

According to the constitution, the right to request for disclosure of information refers to the basic right to access and view information held by an administrative office. This recognizes citizen's free access to information carried by the authority and has a root in desire for democratization by guaranteeing citizen's right to kno w.[144] Also, it eliminates a habit of closed public administration, enhances the agency's transparency to further citizen's function as a monitoring body, and contributes to public nature of public information through distributing information.[145]

144) Kim, Dong-Hee, Administrative Law I, Pakyoung Books, 2001. pg. 374-375.
145) See Kyung, Gun, "Study on Policy of Information Disclosure Request Policy" pg. 24 for details

This right is related to monitoring public agencies and naturally concerns mainly about public information held by public agencies. Rather than a subjective tool to resolve violation of rights, it is generally regarded as principle for an objective polic y.[146] One the other hand, the information holder's right to access and modify information may be seen as a part of this right if the request was made to an administrative agency; hence, right to determine one's information and the right discussed above can overlap.[147]

B. Creation and amendment of the law on information disclosure

To practically guarantee this right, the academia has been arguing for a related legislation since the 1980s. The Constitution Court of Korea also recognized[148] right to know based on the article 21 of the constitution and High Courts especially stated a right to access state information is generally recognized in the freedom of expression based on the constitution and the contents of the right includes general right to request for disclosure of information.[149] In 1991 Chung-ju City created an ordinance on release of administrative information and a federal guideline on releasing administrative information was created in 1994.

Through these steps, in December 31st 1996, a Law on Information Disclosure of Public Agencies was declared and it came into effect a year later. Since, the law was amended on several occasions to add basis for release of electronic information and obligations to release a list of information held, to shorten the time it takes for a release, to eliminate abstract exceptions, to install a committee and a review board comprised of majority of civilians. Also, to avoid problems of subsequent agency's unjust interpretation and limitation of the released information, detailed clauses are added.

---

146) Kim, Young-Seob, "Clash and Harmony between Information Disclosure and Protection of Private Information", *Administrative Law Journal*, Vol.29(3), (May, 2001). pg. 172.
147) Kwon, Gun-bo Protection of Private Information and Right to Control Information, Kyunginmoonwhasa (2005), pg 171-172.
148) Constitutional Court 1989.9.4. Decision 88Hun-ma22; Constitutional Court 1991.5.31. Decision 90Hum-ma133.
149) Supreme Court 1999. 9. 21. Decision 97Nu5114.

C. Currents of policy on information disclosure

Through a modification of a law, in 2004, the government made a progress in establishing a basis for release of electronic information and creating a system that allows citizens to access information quickly and effectively. In April 2006, a comprehensive information disclosure system (www.open.go.kr) was launched to actively provide online services and since 2009 has been providing a one-stop service that combines search and request for an information, submitting of fees, and viewing. Systems like these made a huge contribution in facilitating information disclosure policies by enhancing accessibility and convenience for the citizens. Until March of 2008, three updates have been made and a web standard was implemented to guarantee accessibility to persons with disability in online settings. Inverted images and audio services are given to each of 220 pages and menus while magnification of letters and changing font color are now allowed to maximize accessibility of the visually impaired. Also, a page control without the need for a mouse was implemented for the physically disabled. Moreover, the pages that were previously reachable through Internet Explorer in Windows were made available in different operating systems as well as other internet browsers.

Websites that release information related to a government task is growing in numbers. Prism (www.Prism.go.kr) lists information about outsourced research opportunities and Alio (www.alio.go.kr) discloses information on management of public agencies. Clean Eye (www.cleaneye.go.kr) provides information on managements of local public companies. College Info (www.academyinfo.go.kr) and School Info (www.schoolinfo.go.kr) provide information on agencies related to education.

Examination of important changes as a result of the policy shows that a number of requests have significantly grew from 26,338 in 1998 to 398,163 in 2009. This data shows that a need for information documented, collected, and managed by the public agencies is growing constantly. Evaluation mechanism implemented in 2003 on the achievements of the policy have been conducted on different entities to raise

efficiency and transparency of the policy. Also, a committee comprised of professionals in academia, law, and public administration have been contributing to successful administration of the policy since August of 2004.[150]

However a frequent change of a public officer in charge of this issue led them to have shallow understanding of the work impeding the progress toward better quality of service. Also, some agencies are still using abstract interpretation of exceptions to deny request for information disclosure. Some requesters are demanding for abstract or broad information that are not in line with the principles of this polic y.[151] Some even request for information but refuse to receive information once it is provided. In cases like these, administrative cost that could have been spent on other individuals or public service; improvement is necessary.

D. Main contents of current version of Freedom of Information Act

According to Article 5.1 of the legislation, all citizens are the subjects of this right. Natural persons as well as legal persons are included. Although there may a dispute over the case of foreigners but an ordinance injunction with this legislation defines that an entity that resides in Korea with a permanent address or that is temporarily staying in Korea for an academic research are allowed to request for information disclosure.

The affected entity of this law is defined as public institutions. These institutions includes national agency, local self-governing agencies, agencies invested by the government, and other agencies defined by the presidential order. Administrative branch as well as legislative branch, judicial branch, the constitutional court, and all other state agencies are included. Local autonomous governments are also within the effects of this law. However, they can make its own ordinance specifying the delivery of services. Other entities defined by the presidential order has the same obligation enumerated in the law.

---

150) Ministry of Administration and Safety, *2009 Annual Report on Information Safety* (September, 2010). pg4-6

151) Ministry of Administration and Safety, pg 8-9.

The “Information” stated in the legislation refers to all information recorded in documents (electronic included), layouts, pictures, films, slides, and other medium that are created, collected, or managed by the public agency for work purposes. Broadly, it extends to all record that has a public characteristic. A concept of record in this case is inclusive of files, reports, evaluations, opinions, recommendations, agreements, statistic data, predictions, decisions and others. Especially, it reflects on the societal advancement toward telecommunication society and includes electronic records. “Disclosure” in information disclosure refers to allowing viewing or copying of a record based on the regulations or releasing information through telecommunication network based on Electronic Government Act Article 2 Clause 7.

A person requesting for disclosure can submit a form describing the information requested for disclosure. In this, information requested must be specific in its content and limit enough for an average person to recognize.

While the legislation outlines the principles of disclosure in article 3 and 9, article 9 clause 1 lists exceptions by their types. These non-disclosed information can be understood as information exempt after examining the relationship with individual basic rights or other principles listed in the constitution. Yet in 1996, it was criticized for shrinking citizen’s right to know by excessively expanding the area of exemptions. In 2006 the principle of disclosure was reinstated in article 9 and a significant part of exemptions are edited to state clearer definitions and specific limitations to suggest a stricter standard for exceptions. Furthermore, agencies and offices are obligated to state their own standard for exceptions with consideration for the characteristics of their work to make sure they do not interpret a standard more abstractly than it has already proclaimed.

The exceptions current legislation states are (1) information categorized as secret or non-disclosed by other legislations or orders such as codes of the parliament or the high courts, (2) information related to national security, defense, unification, and international relations that may severely endanger important benefits of the state, (3) information which disclosure may lead to significant impediment of protection of

citizen's rights, body or property, (4) information that may have an effect on ongoing court case and harms the neutrality of the court, (5) exams, inspections, human resource management and other information which there is a significant reason to believe a disclosure significantly disables work of a public official, (6) personal information such as name and social security number that risks violation of one's privacy (Yet, information specified in another legislations to disclose despite a concern for privacy based on a decision that a disclosure of private information holds great benefit for the society), (7) information about legal persons such as corporations and foundations which a disclosure has risk of harming one's rightful profit (But information required to protect citizens from the harms inflicted by the corporation or the foundation and those necessary to protect interest of the state and citizens can still be disclosed), and (8) information that can be abused by the predatory investors to gain unfair advantage in the real estate market or inflict unfair loss to others.

In reality, however, over forty-percent of the information denied for disclosure are done through reasons not stated in article 9 clause 9. Unless information does not exist, it is unfair to deny requests using reasons not stated in the legislation. Also in 2008, committee on information disclosure was reorganized from the president's office to Minister of Administration and Safety and their work has contracted severely in recent years.

E. Information disclosure policy based on Act on the Management of Public Archives

Categorized in the non-disclosed information based on the legislation above is a legislation on management of public records. This law was created to realize transparent and responsible administration of the public agencies and to outline codes necessary for safe preservation and effective use of public information. Since 2006, the law has gone through numerous revisions to take its current form. The law applies to information created or collected by the public agency for their work and those created or collected by individuals or groups that is recognized as worthy of

preservation. Public agency in this case refers to national apparatus, local authorities, and other entities selected by the president and record refers to data created or collected by a public agency regardless of their medium. Agencies affected by this law overlap with agencies affected by legislation on information disclosure.[152]

2) Resolving Digital Divide

A. Introduction

Digital divide generally refers to widening economic and social gap between those who have access to new telecommunication technology and those do not. However, Framework Act on National Informatization[153] states in its article 3 clause 9 that digital divide is "the difference in opportunities to access or use telecommunication services due to social, economic, geological, or physical condition".

Digital divide was first used in the U.S. during the mid-1990s and it highlights economic and social inequality in the era of digital economy. The concern in an advanced information state like the U.S. was that transformation into digital economy would intensify the digital divide in the process. Population of the developed countries that only amount to sixteen percent of the global population owns ninety percent of the computers and the number of phone lines installed in the city of New York outnumbers that of the entire African Continent. Also, the fact that 80 percent of information online is in English which only 20 to 30 percent of the world can understand. Therefore, there has been warnings that resolving the issue of digital divide will be the biggest issue in the American economy.

The U.S. government has been preparing a solution of its own with vice president Al Gore as the core by creating education and technology policy from 1993 to 1999. In February 2nd, 2000, President Clinton shared a "suggestions for resolving the digital divide". The main idea of the suggestion is that the government will provide all

152) Park, Jin-Woo, "On the Study of a Closed Information by the Law in the Freedom of Information Act", *Dong-a Law Review*, Vol.43. pg 49-50

153) Act No.9705, <Amended 2009. 5. 22, Enacted 2009. 8. 23>

citizens with an opportunity to use internet which is a common service like a telephone service. For this, the government guided lowering of prices of computers and services related to internet and facilitated competition among internet service providers. Also, 20 billion dollars-worth of tax benefits were to be handed out in the next ten years to private corporations become supporters of this plan by actions such as donating computers to schools. Corporations that donate to support school libraries and local information center are also given tax benefits. Also, a corporation conducting a training on information technology to its employees are given tax benefits. The plan was to install one thousand local information centers in low-income communities and to facilitate development of internet service accessible to the lower class. Training of new teachers to allow all children in the 21st century to fit into the information era is also one of the core programs of this suggestion.

South Korea is receiving similar warnings that digital divide between upper class who have advantages in accessing knowledge and information and lower class with relative disadvantage will intensify income gap between classes. By data retrieved in 2010, 82.2 percent of families have computers at home and 78.3% percent of the population use internet, which are high rates, yet only 67.2 percent of the information deprived population such as disabled, lower class, agrarian communities, and elderly have computers at home while only 44.2 percent of them use internet, which is significantly lower than that of the average citizens. An Index created to show the digital divide between information deprived communities and the rest have showed that from 55 in 2004 to 46.7 in 2005, 38 in 2006, 34.1 to 2007, 32 in 2008, 30.3 in 2009, 28.9 in 2010. Analysis of data from 2010 shows that access point was at 8.2, capability was at 49.2, quantity at 42.5 and quality was at 45.9. Moreover information level of the deprived community compared to the non-deprived revealed that disabled persons were at 81.3 percent level of the non-deprived persons. Low income class was at 80.5 percent, mid-to-elderly at 67.5%, and agrarian communities at 61.8%.[154] Although the digital divide between the deprived communities and the

154) Lee, Jae-Woong, 2010 Analysis and Suggestions regarding the status of Digital Divide.

rest have been narrowing every year, there still exists an undeniable gap. Especially the percentage of smartphone users among the deprived communities was at 1.3 while the same of the rest was at 15.6. The gap is projected to widen due to rapidly ascending trend of smartphone use. Therefore, continuous expansion of institutional foundation for the deprived population to utilize to access internet and the web is becoming ever important.

B. Policy to resolve the digital divide in South Korea

Efforts to resolve the digital divide at a policy level mainly started in the late 1990s. In 1999, the Second Plan for Facilitating Digitalization, known as Cyber Korea 21, was published and addressing the issue of digital divide was included in the clause on “creating the country with most apt computer uses”. The Fourth convention for strategies for digitalization in April 2000 produced a Plan to construct a strong information country. This plan had programs such as internet education using post offices, welfare centers, and local libraries, providing free personal computers as well as internet service for five years to students in low income families, expanding internet education for stay-home wives, and establishment of a comprehensive information website for persons with disabilities. In June of the same year, an education plan called Internet Education for ten million Citizens was created to conduct a large scale education sessions for all citizens.

For a systematic and effective facilitation of programs to address digital divide, Act on Resolving the Digital Divide was produced in January of 2001. This law was created with a purpose of providing free access to telecommunication network and guarantee enjoyment of information to groups such as low income class and disabled who are unable to do so due to economic, geological, physical or social circumstances. A comprehensive plan to resolve the digital divide was to be produced every five years while the delivery of these plans was monitored annually. Installing a commission on the digital divide, providing telecommunication devices to disabled

---

National International Society Agency, 2011. 3. pg 4-11

and recipients of National Basic Living Security Program, and establishment of information centers are among the programs addressed in the law.

It was revised in December 2002 to obligate government to come up with a solution to allow all citizens to have an access to high-speed telecommunication services in article 7.2. Article 11.2 calls for an installment of research body for establishment of policies, and article 16 created a government apparatus called Korea Agency for Digital Opportunity and Promotion to provide services for all citizens to freely access telecommunication services and improve qualities of lives.[155)]

On the other hand, in September 2001, A Comprehensive Plan to Resolve the Digital Divide suggested six main tasks including establishment of high speed telecommunication network, creation of environment suited for information access, revision of necessary legislations, engaging in international cooperation, foundation of policy background and improving public understanding.

The government initiated a large-scale digitalization education for deprived and non-deprived population to narrow the gap in information access as well as information utilization ability. From 2000 to June of 2002, Internet Education for Ten million Citizens (2000-2002) educated nearly fourteen million citizens. Following this in July 2002, "2 step plan for citizen digitalization (2002.7-2004)" was created with focus on practical uses and provided basic and intermediate classes to 5 million citizens in agrarian and fishing communities, disabled, and elderly groups.

Programs for management of knowledge and information resources was fully implemented as the government created a related law on January of 2001 and created a basic plan for management (2000-2004). This basic plan takes alleviating the digital divide as one of the policy objectives but with exception of a plan for creating an infrastructure for digitalization mainly focuses on enhancing potential for industrial utility of the digitalization. As a result of full implementation of a knowledge society through eKorea Vision 2002 and Broadband IT Korea 2007, importance of knowledge

155) Choi, Doo-Jin and Kim, Ji-Hee, "Shift in Paradigm of Digital Divide and Directions to Productive Information Utilization" *Issue Report on Digital Divide* Vol 1 (2), 2004, pg5-6

and information resource has been highlighted; as eBooks and others have become a center of a discussion for knowledge equality, management of the resource has broaden its horizon to abstract concepts in some areas and expanded concepts in others.[156)]

C. Contents of the Basic Law on National Informatization

Legislation on Resolving the Digital Divide from 2001 was replaced by the Framework Act on National Informatization in May 2009. Form article 31 to 36, this law outlines regulations related to development of policy and technology, guaranteeing access to information for disabled and elderly, provision of up-to-date telecommunication devices, and delivery of education all to address the issue.

A notable content of this legislation is in its provision of hardware and software to those including disabled persons defined by Act on Welfare of Persons with Disabilities and beneficiaries of National Basic Living Security Act who do not have access to information due to economic, geological, physical, and social circumstances. It makes emphasis on government obligation to resolve the issue. Furthermore, the government produced a standard or accessibility for disabled people on telecommunication technology and devices and have been disseminating the standard to website designers, developers, as well as managers. From 2006 to 2009, one national standard and nine organizational standard were produced.

D. Contents of the Disability Discrimination Act

To address the issue of the digital divide on disabled persons, Act on the Prohibition of Discrimination Against Disabled Persons, Remedy against Infringement of their Rights, Etc. installed in in 2007 prohibits discrimination in access to information, states a duty to provide rightful services in telecommunication and

156) Sim, Min-Suk, “Policy for Addressing the Digital Divide and Right of Access to Information - Library as a medium of socio-economic knowledge sharing system”, 2007 Fall Joint Seminar, pg 53-56

communication, and defines a national and local authorities' duty relating to access and communication. Details are as follows.

First of all, private individuals, companies, and public entities are prohibited from discriminating disabled person in using and accessing electronic and non-electronic information. Also, all person providing communication support on behalf of a disabled person cannot be stopped or impeded without a legitimate reason.

Moreover, a service provider must provide necessary support such as sign language and subtitles that allows equal access to information produced and disseminated to disabled and non-disabled persons. Public institutions must provide sign language interpreter, hearing aids, and other services in events hosted or managed by them. Media producer based on medial legislation as well as online contents producers must provide services such as hearing aids, voice service, sign language, and others to allow disabled persons to enjoy the content as equally as non-disabled persons do.

National and local authorities shall examine ways to develop and deliver telecommunication network as well as devices that take special needs of the disabled persons into account. A telecommunication device producer must work to allow equal access to the device to disabled and non-disabled persons in planning, manufacturing, and tailoring a product. National and local authorities must provide a service specifically tailored with consideration for different types and levels of disability and a service deliverer cannot force a recipient to receive service or aid in communication that is not considered for them.

In 2011, a percentage of subtitled, sign language, and commentary contents aired in central nation-wide television came out to be 96.5%, 5.2% and 6.2% respectively. Percentage of subtitled contents spiked up from 58% in 2006 while the others did not show much difference.[157] More proactive measures are required for them.

157) Korea Communications Commission, Status of Subtitle, Hand Signal, and Video Interpretation Service on National Television, 2011

E. Contents of Libraries Act

Libraries Act revised in 2006 defines library's social obligation in guaranteeing citizen's right to access information and right to know as well as measures necessary to carry out its role and has its goal in facilitating growth of libraries for effective dissemination of information to general public, alleviate the digital divide, provide secondary education, and contribute to national and societal cultural growth. This law has a separate chapter on alleviating the problem of unequal distribution of information and knowledge and makes relatively specific codes on role of libraries, establishment of national library for disabled persons, and others.

First of all, in relation to a role of libraries, its recommends establishment and management of facilities and libraries for narrowing the information gap. It take all measures for all citizens to receive information and knowledge services regardless of physical, geological, economic, and social circumstances. Facilities designed for narrowing the information gap must do all of its efforts to maximize access and convenience for deprived groups[158] defined by the presidential order.

Secondly, in relation to services to alleviate information gap, national and local authorities must come up with measures to allow deprived groups to freely use library facilities and services, libraries are allowed to use some of its funding purchasing materials, facilities, devices, and software to improve conditions for deprived groups, and cost paid to copyright holder can be provided by the library when a member of deprived group uses the material.

Furthermore, to aid members of deprived groups, especially those disabled, to access libraries, national aids center for libraries for disabled persons is established to make and distribute codes, learning materials, and manuals, training of special officers for the related duty, and other work required to provide library services to disabled persons.

Still, only 2% of all published material is provided in audiobooks and other modes

158) Disabled Person defined by "Act on Welfare of Persons with Disabilities" and beneficiaries defined by "National Basic Living Security Act", and Elderly over the age of 65

designed for disabled persons, and it is extremely low compared to other leading countries such as Sweden (10%) and Netherlands (10%). Database of original documents for visually impaired only amounts to just 229 PDF files and 732 VBF files. The government must expand its role as well as modes in providing alternative materials.[159)]

(2) Issues of Right of Access to Information

1) Access to the Web

Web accessibility refers to guaranteeing equal access of internet to groups such as disabled persons and elderly. As use of internet is increasing every day, one's proximity to the Web largely dictates level of right of access to information guaranteed.

The Web is especially important to disabled communities because it is essential in basic living activities such as public administrative works, online transactions, and online banking. Yet, according to the 2010 digital divide index, only 53.3% of the disabled persons have internet access at home while 78.3% of the entire population do. It shows nearly 25.0 % of difference existing between those two groups.[160)]

Most frequent inconveniences a disabled persons experiences in accessing the Web are visual, audio, difficulty accessing contents without a mouse, and inability to increase font. Addressing of those problems require unique and independent approaches and tools.

A legislation designed to guarantee right of access to the web in South Korea is Legislation on Alleviating the Digital Divide processed in 2001. Based on this law, a code on enhancing accessibility to the web for disabled and elderly persons was create in January of 2002. However, the former law was repealed and a Basic Law

159) Congressman Eun-soo Park, Midterm evaluation on 5 Year Plan for Development of Disability Policy, p 25-26.

160) Lee, Jae-Woong, 2010 Analysis and Suggestions regarding the status of Digital Divide. National International Society Agency, 2011. 3. pg. 14

on National Digitalization was created to manage solutions for alleviating the Digital Divide, guaranteeing the right of access to information for disabled and elderly persons, supplying and developing devices, provision of information devise, and others. In December 2005, national standard on Internet Web Contents Accessibility was approved and a subsequent guideline was created in March 2009.

Act on the Prohibition of Discrimination Against Disabled Persons, Remedy against Infringement of their Rights came into effect in April 2008 and mandates provision of tools for equal access to the information to all persons. A specific code from this law selects websites that are mandated to provide all necessary tools to allow full access to all contents on the website.

Level of web accessibility is rising after establishment of standardization law in 2005. According to 2009 report on web accessibility for disabled persons, most of the public websites such as central governance agencies, legislative bodies, and other local governments scored above 90 and especially those of local governments have scored 91.8 on average which was 8.5 points improvement from the previous year. Public corporations and semi-government agencies such as researching agencies scored 83.2, 8.6 points more than the year before; yet, it was still well below other agencies.

Also, a sample report on web accessibility on the agencies mandated by Act on the Prohibition of Discrimination Against Disabled Persons, Remedy against Infringement of their Rights shows that agencies such as public universities, public libraries, and welfare facilities have revealed they only scored 76.6.[161] On the other hand, similar research conducted by the ministry of administration and safety showed central agencies scored 94.6 points and local governments scored 94.7 points. Educational institutions scored 78.7 points. Medical institutions scored 77.9 while welfare facilities scored 80.4. It revealed that websites of the bodies most frequently visited by the disabled persons need to make the biggest improvements.

---

161) Ministry of Administration and Safety and National International Society Agency, Results of 2009 Web Accessibility Status, 2010. 3.

2) The End of Analogue Television and Transition to Digital Broadcast

Special Act on the Digitization of Terrestrial Television Broadcasting and the Promotion of Digital Broadcasting passed in 2008 had the president to set up a date for end of the analogue television service and analogue television contents providers to end their services by the designated date. According to this law, analogue television ceases exist in 2012 and a new era of digital broadcast will being in 2013. Once that happens, few household and groups who cannot afford digital television receiver cannot watch television.

This kind of transition to digital television means a complete prohibition of opportunity to access information from national television and it has a risk of violating right of access to information of impoverished communities. Even if they are allowed to watch analogue television as the government claims, those who receive information from analogue signal will unavoidable be subjected to less quality of information due to difference in video and audio quality. Of course, Korean Association Cable TV has promised to come up with a special solution to allow not only those under but also near the poverty line,[162] it is expected to have too much financial and technical resources to provide cable TV to all of them.

The government has recognized this problem and revised Enforcement Decree on the Digitization of Terrestrial Television Broadcasting and the Promotion of Digital Broadcasting on mandating national televisions to produce high definition contents and come up with a solution to the problem of lack of access for isolated locations. This ordinance, established in September of 2009, gives Korea Communications Commission authority to give out recommendations, warnings, prohibit operations, and eventually expel license of a broadcaster that does not abide by the duty or conditions enumerated. On the same ordinance, it gave national television broadcasters a duty to submit materials outlining a plan to facilitate transition to digital television and protection of viewer's rights and a new code on regulatory measures in case

162) Gil, Jongsub "Guaranteeing Benefits of Digitalization to All Citizens" *Yunhap News* 2009. 6. 4,

of their failure to comply with the rules.

Even if the digital contents providers are given duties associated with this transition, the curtailing of impoverished people's access to information through television from the end of analogue television service is inevitable. Especially for the disabled and elderly groups, expansion of opportunity to receive education and provision of financial support cannot fully close the information gap created by this. Therefore, a financial concern for periodic purchasing of new receiving devices, technical difficulties in stalling those devices, and problem of adopting to a new technology should be taken into consideration in providing services.

In this light, understanding and approach at the policy level is required for the deprived communities and a measure for disabled and elderly person to use to use its rights as viewers without discrimination. In the UK, the date for the end of analogue television was postponed by two years while a special measure was taken to provide support to citizens above 75 years old, recipients of support for disabled persons, and other deprived communities. Also, it plans to provide addition support to more groups if they require assistance.

A right to select medium and access of information are essential points of universal service of broadcast; hence, a policy is required to prevent creation of other deprived communities and provide assistance to allow citizens to successfully adapt to changing digital environment.[163)]

3) Decisions on digital certificates

Internet banking is financial system more advanced than PC banking in that it links customers and banks using a dedicated route. Internet service has an advantage in that it allows banks to provide services to people from all over the world and it has great potential as it primarily targets young and well off customers. Since, Security First Network Bank began its services as the world's first online bank, most banks

163) Kim Kwang-Ho, "Considerations for Disadvantaged Groups and Shift to Digital Broadcasting", *Telecommunication Technology Journal*, Vol 80 2009 pg 7

now created its own internet banking system to expand its customer base. All customers now have an opportunity to receive financial services online.

However, digital certificate from Korea Financial Telecommunications & Clearings Institute is an essential tool required for this system. Yet, it is only issued in Internet Explore which limits online banking services to Microsoft Windows' Internet Explore settings. It is a case unique to South Korea and it risks complete dependency on Microsoft in online banking.

Alternative operating system users such as those of Linux amounts to 50,000 and users of Macintosh including those in publishing and media producing industry amounts to 15,000. If they cannot use online banking using their computers, it is a violation of non-window users' right of access to information.

In 2007, civil society organization for web standardization named Openweb filed a law suit calling for Korean Financial Telecommunications & Clearings Institute to issue digital certificates in different browsers for users of different operations system to have access to related services. However, Seoul District Court ruled[164] in July 2008 that currently applicable laws do not specifically outline a duty to issue digital certificates in different browsers and that a private institution like Korea Financial Telecommunications & Clearings Institute does not violate related laws. Openweb has immediately appealed but Seoul High Court has decided not to hear the case, confirming the previous decision.[165]

In this case, the Supreme Court has ruled that it is up to private service providers such as KFT&C Institute to decide whether a services is provided in any medium. It also added that "most of the users are already using services provided by these private institutions and it cannot find any illegality in this transaction after considering the fact that each banks are already providing serviced tailored for their banking system."[166] This ruling endangers non-Window users' right of access to information it is a subject of a huge controversy.

---

164) Seoul Central District Court 2008.7.24. Decision 2007Ga-Hap114739
165) Seoul High Court 2009.3.25. Decision 2008Na82294
166) Supreme Court 2009.9.24. Decision 2009Da28998

In April 2010, Korean Communications Commission expressed that in a browser market in which 98 percent is using MS Internet Explorer, it limits internet service to those not using the Active X system in online banking and shopping thus the Commission will take a proactive measures to minimize user inconvenience and address security concerns from overuse of Active X tool. Also, the Commission plans to launch a diagnostic system to review websites for their compliance to the standard and file a statistical report on major one hundred websites including banks and online gaming websites to guide websites of public agencies to stop using Active X.

But in essence, a policy must be revised to discontinue digital certificate system that only provides services in Internet Explorer and guarantee right of access to information to all.

4) Discussion of Right of Access to Internet as Basic Right and Net Neutrality

Internet has opened a new horizon in media sector. Internet is unique in that it allows bilateral communication and has led to a surprising advancement in telecommunication sector. The birth of Web 2.0 services have allowed customers to be more than a passive receiver of information and work as an active contents creator. Individuals can share information and ideology across state borders at a low cost and internet has allowed individuals to access information and knowledge that was not impossible to acquire previously. It has contributed to the societal advancement.[167)]

However, an information gap from disability to access internet is creating a new type of discrimination. In developed countries 71.7 out of 100 people use internet while only 21.1 of 100 people from developing countries use internet.[168)] This type of gap exists in this country as well. Therefore, the society must invest its energy on guaranteeing rights of information weak by Open Access movement. Also, the state has a need to provide necessary infrastructure to discontinue this discrimination.

---

167) A/HRC/17/27 Article 19

168) Key Global Telecom Indicators for the World Telecommunication Service Sector", International Telecommunication Union, 2010. 10. 21.

The United Nations recommends that it must be a foremost goal for nation states to guarantee universal right of access internet.[169)]

As ability to access internet has become an important determinant factor of wealth, internet access has become an important right. In July 2010, Finland universalized a right to access internet broadband service at 1Mpbs speed, making right of access internet as a citizen's basic right for the first time in the world.[170)] Subsequently, other states are discussing the idea that difference in access to internet can cause class division and that high speed internet access must be recognized as a citizen's basic right.[171)]

In extension of this discussion, a survey[172)] conducted by GlobalScan revealed that 76 percent of the citizens form 26 countries consider access to information as a basic human right and 96 percent of citizens in South Korea, which has the second highest penetration rate of internet only behind Australia, think agreed.[173)] Net users in the world find the most value of internet in its searching ability and other valuable functions came out to be social communication, entertainment, and contents production and dissemination.

EU Congressr evised UE Regulatory Framework for Electronic Communications Networks and Services defining right of access to internet as a principle equal to freedom of expression.[174)] Also, it requires internet's openness and net neutrality while Netherlands became the first state to legally institutionalize net neutrality through its law in 2011. Citizens from states outside of the EU is bombarding their governments to guarantee net neutrality.

---

169) A/HRC/17/27

170) Communications Market Act, "Universal service obligation concerning network service (Section60d)".

171) BBC, "Finland makes broadband a 'legal right'(2010. 7. 1.).

172) BBC Global Poll 2010 Research was a survey jointly conducted by BBC, GlobeScan, Maeil Economy, East Asia Research Center on access to internet of 27,973 people from 26 countries.

173) Rate of Supply of Internet compared to total population is 77% (Internet World Stat, 2009. 9. 30)

174) Europa Press release(2009.11.5.), "Agreement on EU Telecoms Reform paves way for stronger consumer rights, an open internet, a single European telecoms market and high-speed internet connections for all citizen"(MEMO/09/491).

A concept similar to net neutrality is a non-discrimination principle, or also known as Caterfone principle,[175] was created during circuit-switching telephone era. However, internet, which is network of packets, with End-to-End design principle[176] further facilitates freedom, openness, and innovation is vulnerable to network provider's attempt to damage its net openness and it this vulnerability is inspiring demand to further regulate internet.

In 2010, the U.S. Federal Communications Commission created its open-internet regulation to prohibit discrimination and blockage committed by network providers and especially in wireless broadband services ordered prohibition of blockage implemented against competitions such as mVoIP[177] services. According to the example described by the FCC, all individuals and corporations should be free of discrimination by those who have the authority over the network in accessing the internet and enjoying contents. In relation to net neutrality, Japan also have suggested in relation to net neutrality that a user should be able to easily access and use network based on IP, network should be accessed through all devices and should support End-to-End communication, and a user should be guaranteed equal access to communication and platform levels.[178]

Various discussions surrounding the net neutrality is happening in South Korea and they include an argument between internet network providers and smart television

175) "No Harm to Public Network" and "Open Network" : Sparked by 1950 Husa-a Phone Incidnet and 1968 Catefone Incident, it is a regulatory policy which illegalize discriminatory access to connection to telecommunication devices or network in a public network infrastructure. Open Network was suggested in 1986 'Computer Inquiery III' which states that a network is a social necessity and that even a network created by a different network company should allow inter-communication, moving services without changing a phone number, and establishment of a private network.

176) It is a principle introduced by Jereome H. Saltzer, David P. Reed, and David D Clark in 1981 which suggests that continuity of internet service is realized by a device and that a network simply functions a mode of transfer.

177) mVoIP(Mobile voice over Internet Protocol) service refers to a technology that carries audio signal through an internet network through a mobile device such as smartphones. Unlike regular telephones, transmits audio packets through an IP network and VoIP is a term describing a solution related to sending an audio data to internet or an IP network.

178) Internet Freedom Coalition, WC Docket No. 07-52

producers, discussions about internet messenger, and a clash between mVoIP service providers and cellular network managers. In the midst of these discussions, Korean National Human Rights Commission received a petition on the case where a cellular network provider actively screened data used by the users using deep packet inspection to selectively block the use of mVoIP services thus violate the user's privacy.

Estonian congress passed a legislation which declares internet access as a basic human right in 2000.[179] French Constitutional Commission practically made a declaration which recognized internet access as a human right in 2009.[180] Costa Rican Constitutional Court also made a similar decision in 2010. As citizens of an information apt state,[181] 96 percent of the citizens of South Korea consider internet access as a universal basic right. Since international community as well as the UN unanimously recommends expansion of infrastructure for internet access, a discussion of internet access and net neutrality shall be held more frequently.

Section 4. Right to Enjoy Information and Culture

1. Meaning of the Right to Enjoy Information and Culture

The concept of the right to information and culture is still forming. However, this does not mean that such a right has not been existed and is an entirely new concept. The International Covenant on Economic, Social and Cultural Rights (so called "A-Covenant") adopted in December 1966 by the United Nation's General Assembly mentioned, at Article 15, everyone's rights "to take part in cultural life" and "to enjoy the benefits of scientific progress and its applications" as one of the basic human

179) Colin Woodard, "Estonia, where being wired is human right", Christian Science Monitor, 2003.7.1
180) A.HRC/17/27, Korea Internet & Security Agency, Online Law Trend Vol 25 (2009-10)
181) Ranked 1st in UNE-Government Development Index for two consecutive years (2010, 2011), 1st in ITU ICT Development Index (2011) and etc.

rights, and the Universal Declaration on the Human Rights of 1948 prescribes, at Article 27, substantially the same right, i.e., “the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits.” These rights are the main elements of the right to enjoy information and culture. Therefore, it can be said that the right to enjoy information and culture mainly consists of two rights: the right to take part in the cultural life; and the right to enjoy the benefits of scientific progress and its applications. In addition, the right to enjoy information and culture may also include the states’ obligations of ‘conservation, development and diffusion of science and culture’ and ‘respecting the freedom of scientific research and creative activity’, which stem from Article 15(2) of the A-Covenant, saying “the steps to be taken by the States Parties to the present Covenant to achieve the full realization of this right shall include those necessary for the conservation, the development and the diffusion of science and culture” and from Article 15(3) of the A-Covenant saying “the States Parties to the present Covenant undertake to respect the freedom indispensable for scientific research and creative activity.” However, given the multi-vocal and variable nature of the term “culture,” it is not easy to specify and codify the right to information and culture into national legislations and such a right has been one that has failed to draw much attention so far.

One of the events that provoked concrete discussion over the right to enjoy information and culture was the World Trade Organization’s agreement on the Trade Related Aspects of Intellectual Property Rights (TRIPS) of 1995, which represent the global expansion and one-size-fits-all model of the intellectual property rights. When TRIPS became obligatory for the developing countries in 2000, ardent debates on the access to medicines, patents on pharmaceutical products, and relations to rights to health were provoked in connection with the price of HIV/AIDS drugs in Sub-Saharan Africa, India, South American and eastern Asian countries. As the IPRs protection has been expanded in global scale, the right to information and culture

became one of the most important principles to counterweigh the overly broad IPRs protection under the regime of human rights laws. The right to enjoy information and culture, infringement of which has not been specifically identified, became to be concretely conceptualized by the strengthening of copyright protection.

2. International Trends and Standards

(1) International Movements Concerning the Conceptualization of the Right to Enjoy Information and culture

1) The Right to Take Part in Cultural Life

The Committee on Economic, Social and Cultural Rights of the UN first discussed the right to take part in cultural life of the Article 15(1) (a) of the A-Covenant from May 2008, and adopted the General Comment No. 21 in December 2009. According to the General Comment No. 21, “culture” of “the cultural life” is defined as something that “shapes and mirrors the values of well-being and the economic, social and political life of individuals, groups of individuals and communities.” The Committee explains through the General Comment No. 21 that the right to take part in cultural life consists of three main components: (a) participation in, (b) access to, and (c) contribution to cultural life.

In terms of equality and non-discrimination, the necessary conditions for the full realization of the right of everyone to take part in cultural life should include (paragraph 16 of the General Comment No. 21): (a) availability, i.e., the presence of cultural goods and services that are open for everyone to enjoy and benefit from; (b) accessibility, i.e., effective and concrete opportunities for individuals and communities to enjoy culture fully, within physical and financial reach for all in both urban and rural areas, without discrimination; (c) acceptability, i.e., the laws, policies, strategies, programs and measures being adopted by the State party for the enjoyment of cultural rights being formulated and implemented in such a way as to be acceptable to the individuals and communities involved; (d) adaptability referring to the

flexibility and relevance of strategies, policies, programs and measures adopted by the State party in any area of cultural life; and (e) appropriateness referring to the realization of a specific human right in a way that is pertinent and suitable to a given cultural modality or context, that is, respectful of the culture and cultural rights of individuals and communities, including minorities and indigenous peoples.

From the states' obligation of human rights, the obligation to respect, protect and fulfill the right to enjoy information and culture includes: the obligation to refrain from inappropriately restricting the enjoyment of the right (obligation to respect); the obligation to take steps to prevent third parties from interfering with the right (obligation to protect); and the obligation to actively take legislative, administrative, judicial, and budgetary measures necessary for the protection of the right (obligation to fulfill).

2) The Right to Enjoy Benefits from Scientific Progress and its Applications

The UNESCO held annual expert meeting from 2007 and released the Venice Statement on the Right to Enjoy the Benefits of Scientific Progress and its Applications in 2009. The Venice Statement shares the concerns that the acceleration of the production of knowledge has increased the effects on human rights in both positive and negative ways, with consequences for inequalities among and within States and across generations. Advances in information and communication technologies have expanded opportunities for education, freedom of expression and trade, but they have also widened the "digital gap," and facilitated infringements of privacy, incitement to hatred and censorship. Significant disparities are increasing among States concerning the availability of resources, capabilities, and infrastructure necessary for research and development, and therefore the acceleration of scientific progress is widening the divide between the most and least scientifically and technologically advanced societies.

The Venice Statement views that the science may impose significant challenge for human rights in the world today, and requires attention to five main issues. First, it is necessary to clarify the nature of scientific knowledge, progress or advancement

and who decides on goals, policies, allocation of resources and possible conflicts between freedom of research and the protection of other human rights and human dignity. In addition, whereas the individual right to enjoy the benefits of scientific progress and its applications must be respected, the rights of communities to share in these benefits must be recognized as equally important. Second, freedom of inquiry is a vital element in the development of science as the science is not only about advancing knowledge of a specific subject matter, nor merely about procuring a set of data and testing hypotheses that may be useful for some practical purpose. Third, States, commercial enterprise and the scientific community have a responsibility to ensure support for scientific inquiry and dissemination of scientific knowledge, and to actively pursue capacity building on a global scale, particularly in those countries which are relatively inactive in this regard. Fourth, the right to enjoy the benefits of scientific progress and its applications may create tensions with the intellectual property regime, which is a temporary monopoly with a valuable social function that should be managed in accordance with a common responsibility to prevent the unacceptable prioritization of profit for some over benefit for all. Fifth, in the context of Article 15 1(b) of the A-Covenant, enjoyment as "participation" is distinct from enjoyment as actual "sharing" in the benefits of scientific progress and its applications. "Enjoyment" means actual enjoyment of the scientific progress and applications thereof.

According to the Venice Statement, in connection with the States' obligation to respect, protect and fulfill the human rights, the duty to "respect" the right to science should include: (a) to respect the freedoms indispensable for scientific research and creative activity, such as freedom of thought, to hold opinions without interference, and to seek, receive, and impart information and ideas of all kinds; (b) to respect the right of scientists to form and join professional societies and associations, as well as academic autonomy; (c) to respect the freedom of the scientific community and its individual members to collaborate with others both within and across the country's borders, including the freed exchange of information, research ideas and results; and

(d) to take appropriate measures to prevent the use of science and technology in a manner that could limit or interfere with the enjoyment of the human rights and fundamental freedoms. The duty to "protect" the right to science should include: (a) to take measures to prevent and preclude the utilization by third parties of science and technologies to the detriment of human rights and the dignity of the human person by third parties; and (b) to take measures to ensure the protection of the human rights of people subject to research activities by entities, whether public or private, in particular the right to information and free and informed consent. The duty to "fulfill" the right to science should include: (a) to adopt a legal and policy framework and to establish institutions to promote the development and diffusion of science and technology in a manner consistent with fundamental human rights; (b) to promote access to the benefits of science and its applications on a nondiscriminatory basis including measures necessary to address the needs of disadvantaged and marginalized groups; (c) to monitor the potential harmful effects of science and technology, to effectively react to the findings and inform the public in a transparent way; (d) to take measures to encourage and strengthen international cooperation and assistance in science and technology to the benefit of all people and to comply in this regard with the States' obligations under international law; (e) to provide opportunities for public engagement in decision-making about science and technology and their development; and (f) to institute effective science curricula at all levels of the educational system, particularly in the State-sponsored schools, leading to development of the skills necessary to engage in scientific research.

(2) Conflict between the IPRs and the Right to Enjoy Information and Culture

As interactive production and consumption of culture are growing and the open and sharing ideology is emerged and realized in Web 2.0 era, the conflict between the movement for strengthening IPRs protection and the counter-action against the excesses of IPRs by making use of the right to enjoy information and culture is raging.

1) Development Agenda of the World Intellectual Property Organization (WIPO)

The WIPO Development Agenda was negotiated by the joint proposal of Argentina and Brazil in 2004. The proposal was subsequently supported by 12 other developing countries, collectively called "Friends of Development (FoD)." In a nutshell, the FoD's Development Agenda has two proposals: the impact of IPR protection may vary from country's level of development of each countries and such a level of development has to be taken into consideration in developing countries and LDCs where the social cost may outweigh the benefits of the IPR protection; and while access to information and knowledge sharing are regarded as essential elements in fostering innovation and creativity in the information economy, adding new layers of IPR protection to the digital environment would obstruct the free flow of information and scuttle efforts to set up new arrangements for promoting innovation and creativity, through initiatives such as the 'Creative Commons,' and thus the provisions of the IPR related international agreements need to strike balance with the benefits of consumers and the general public. To this proposal, the industrialized countries such as the U.S. kept opposition on the grounds that the current IPR regime has no problem.

After years of debate, WIPO established the Committee on Development and Intellectual Property in 2007 for further discussion and actions for the FoD's Development Agenda. In this course, 111 proposals have been submitted, which were grouped into 6 clusters with 45 recommendations, and adopted at the 2007 General Assembly. The 6 clusters include: (1) technical assistance and capacity building; (2) norm-setting, flexibilities, public policy and public domain; (3) technology transfer, information and communication technology and access to knowledge; (4) assessments, education and impact studies; (5) institutional matter including mandate and governance; and (6) other issues. How to implement the 45 recommendations categorized in the six clusters has been actively discussed within WIPO, and efforts such as studies on patent and public domain, IPRs and competition policy, digital

divide and access to knowledge, socio-economic development and IPRs, open collaborative versus IPR-based R&Ds, and the limitations and exceptions of IPRs have been made.

2) Spread of Access to Knowledge Movements

Access to knowledge (A2K) refers to a global movement against the expansion of IPRs and has provided the momentum for the official discussion of the Development Agenda within the authoritative international body. A2K is one of the efforts to afford a comprehensive counter discourse that can embrace various concepts such as human rights and its keywords includes public domain, commons, openness, and public interests. The Medical R&D Treaty discussed in the World Health Organization, free software movements, Creative Commons, Information Sharing License, patent pool of UNITAID are typical examples of A2K movements.

In August 2011, more than 180 professionals, scholars and activists from 35 countries gathered in Washington DC asked to re-articulate the public interest dimension in IPR system, criticizing the on-going movements to expand and strengthen the IPR protection and enforcement through the trade pacts. They made public two recommendations via the Washington Declaration: IPR policy and institution affects a broad range of interests within society, not just those of rights holders and therefore IPR policy making should be conducted through transparent and open mechanisms that encourage broad public participation; and markets alone cannot be relied upon to achieve a just allocation of information goods — hence it is required: to seek a counter-balance against the reckless expansion of IPR based on the internationally established legal principles such as human rights, to promote open access to information and knowledge; to put priority the public interests in reforming the patent system for the purpose of incentivizing innovation in diverse ways; to support the cultural creativity by seeking new mechanisms for remuneration for authors in a way that does not run counter to the opportunity of information sharing provided by the progress of information and communication technology; to

check enforcement excesses to ensure that the excessive enforcement of IPR in courts, cross-border and over Internet does not undermine the proportionality and procedural fairness; to implement the WIPO Development Agenda in consideration of the social, economic, and cultural developments of each country; and to require the policy making of IPR be based on empirical study not on faith or ideology.

3) Global Opposition against ACTA

The Anti-Counterfeiting Trade Agreement (ACTA) was first developed by Japan and the U.S. proposing a new trade regime to block a widespread international circulation of counterfeits and IPR infringing goods in 2006. Eleven countries including South Korea, the U.S. Japan, the European Union, Canada, Singapore, Switzerland, Mexico, Morocco, and New Zealand reached, after 11th rounds of talks, a preliminary agreement on October 2010, and released the final text on December 2010, which was signed by eight ACTA negotiation partners (South Korea, the U.S., Singapore, New Zealand, Canada, Japan, Morocco) on October 2011 in Tokyo, Japan.

As written in the Preamble, ACTA views that effective enforcement of IPR is critical to sustaining economic growth across all industries and globally, and that the proliferation of counterfeit and pirated goods undermines legitimate trade and sustainable development of the world economy, causes significant financial losses for right holders and for legitimate businesses, and, in some cases, provides a source of revenue for organized crime and otherwise poses risks to the public. To combat such proliferation, ACTA says, enhanced international cooperation and more effective international enforcement is required, and the USTR made clear that ACTA is a groundbreaking initiative by key trading partners to strengthen the international legal framework for effectively combating global proliferation of commercial-scale counterfeiting and piracy.

However, ACTA, unlike the aims of combating the IPR infringing activities, tries to establish special rules in civil and criminal proceedings, reinforce the border measures by the customs authority, impose overly broad legal responsibility on ISPs

for the activities of their users, and force ISPs to monitor their users. As a result, many commentators condemned ACTA as denying the principle of presumption of innocence, which applies to even a criminal suspect, leading to the presumption of guilty for alleged infringers of IPRs, encroaching the right to fair trial, bring about conflicts with basic human rights such as right to health, privacy, and freedom of expression, contradicting with existing international treaties, and rather hampering legitimate trade.

In June 22, 2011, the Senate of Mexico approved a resolution urging the Mexican government not to sign ACTA. For the resolution the Mexican Senate formed the ACTA Working Group on November 2010 to study whether the negotiation has been conducted in a transparent way and if there is any provision that runs counter to the protection of basic rights under the Mexican constitution. The Working Group indicated needs of further study for alternative legislative measures that could provide IPR protection without undermining the right to freedom of expression, the right to information and the privacy right. The Senate members concerned about criminalization of transmission of documents, books or songs over Internet by young people, which could impede youngers' access to information and culture. Not only members of the Senate, the Federal Telecommunications Commissions, telecommunication industries, and ICT service providers also expressed their opposition to ACTA. In the European Union, ACTA was criticized as threatening the Internet freedom of expression, strengthening censor on Internet in the name of crackdown of piracy, and undermining the access to medicine. Responding to those concerns, the European Parliament finally rejected ACTA in July 4, 2012.

3. Domestic Situation and Issues of Concern Relating to the Right to Enjoy Information and Culture

(1) Constitutional Foundation of the Right to Enjoy Information and Culture

As discussed above, the right to enjoy information and culture is still forming and therefore is not necessarily corresponding to existing constitutional rights. Yet the

right to freedom of expression of Article 21(1), the right to academic freedom of Article 22(1), and the right to education of Article 31 of the Constitution may form a constitutional foundation for the right to enjoy information and culture. The main topics domestically arising in connection with the right to enjoy information and culture are about excessive protection of copyright, which is also observed internationally. The followings show some of those issues.

(2) Domestic Issues of Concern Related to the Right to Enjoy Information and Culture

1) Korea–EU FTA

The Korea-EU FTA, which provisionally entered into force from July 2011 requires Korea to protect the copyright for at least 70 years after the author's death (Article 10.6), and protect television signals by banning retransmission of television signal *itself* on the Internet not merely the contents of the signal (Article 10.7:2). The protection of television signal itself is problematic because the Copyright Act is to protect works, i.e., expressive results of creative activity and provides protection for broadcasting as a form of use of works, not the television signal itself.

And the Korea-EU FTA introduced a so-called "showing right", granting an exclusive right to broadcasters to allow or ban the communication to the public of their television broadcasts if such communication is made in places accessible to the pubic against payment of an entrance fee (Article 10.9:5(c)). Here the communication to the public includes broadcasting sounds (Article 10.9:1(b)). By these provisions, the Copyright Act, which only recognized broadcasters' right to reproduction of broadcast (Article 84) and right to simultaneous relay broadcasting (Article 85), was revised.

On the other hand, during the negotiation of the trade pact, the EU demanded so-called "public performance compensation right" by which those who make communication to the public sounds fixed in a phonogram have to pay performers or phonogram producers. Reportedly, the South Korean government explained the

public performance compensation rights refer to IPR protection rule in connection with music, and when a phonogram is played in public places such as restaurant or café, compensation has to be paid to singers and phonogram producers not only to composers and lyric writers. What the Korean negotiating teams were worried about was that if the EU's demand was accepted the small-scaled undertakings had to bare no small burden, resulting in no or little music in café or restaurant or in a worst case the burden being passed on to consumers. After that, the Korean government announced that the EU withdrew the demand of the public performance compensation right at the sixth round (January 28 to February 1, 2008) and in return for it the Korea committed to expand the border measures to apply all of the IPRs not restricted to copyright and trademark. By the way, in March 25, 2009 when the FTA talks were still undergoing, the Korean National Assembly amended the Copyright Act to introduce the compensation rights of performers and phonogram producers against the public performance (this amendment was introduced by members of the National Assembly, and its apparent purpose was to protect the Korean wave).

Concerning the technological protection measures, the Korea-EU FTA prohibits, unlike the Copyright Act, a circumvention itself (Article 10.12(1)), and provides an extensive protection for TPMs to cover access control (Article 10.12(3)).

The EU put a particular emphasis on geographical indications, and demands of EU were entirely reflected into the FTA text, expanding the protection scope and applicable subject matters of the geographical indications than TRIPS (Articles 10.18 to 10.26). Now in addition to wines and spirits, almost all of the agricultural products and foodstuffs become to be protected, and the scope of protection is extended to ban use of the geographical indications on similar products, even when the true origin of the product is indicated or the geographical indication is used in translation or transcription or accompanied by expressions such as "kind", "type", "style", "imitation" or the like (Article 10.21:1(b)). This protection is tantamount to an absolute protection in a sense that the protection reaches to areas where likelihood of confusion of misleading of consumers does not occur. And the limitations under

TRIPS are narrowed. According to TRIPS, the protection of geographical indications is limited in three cases: prior use (Article 24(4)); prior use or registration of trademark (Article 24(5)); and common name (Article 24(6)). But the Korea-EU FTA only permits person's own name not in such a manner as to mislead consumers (Article 10.21:2), and the prior use or registration of trademark (Article 10.21:5), removing the common name exception. The rationale of TRIPS limiting the right of geographical indications to the common name is that it would be unrealistic to enhance the protection to cover the customarily used names such as "Champaign" and "Cognac".

The FTA also requires legislation on data exclusivity for pharmaceutical products (Article 10.36) and for agricultural pesticides (Article 10.37) for at least five years or ten years, respectively. The way of protection is that data on safety and efficacy for a new pharmaceutical product submitted to the drug approval authority should not be used in another approval process. And tests, study reports or information submitted to obtain a marketing authorization of agricultural pesticides shall not be used by third parties or relevant authorities for the benefit of any other person aiming at obtaining a marketing authorization. On the other hand, unlike the Korea-US FTA, the Korea-EU FTA does not obligates the Parties to protect data on new indication of pharmaceutical products. Further, differently from the Korea-US FTA, the EU FTA excludes disclosed data and protects data origination of which involves a considerable effort.

The enforcement chapter, one of the main targets of the EU, was concluded by verbatim copying of laws of European Union. The Korea-EU FTA introduces every special rules for the benefit of IPR holders, ignoring the underlying judicial principles such as a fair trial. When pegged as an infringer by the IPR holders, the defendant has to provide every information and is forced to be in a position that any materials and implements used in infringing activity or even documents related to the infringement are to be seizure or destroyed. Moreover the alleged infringer may pay for damages, even when the amount of which is not proved, unlike the principle of civil code.

The Judicial Yearbook of 2005 published by the Ministry of Justice revealed that the number of civil lawsuits on the merits handled by the first instance courts in IPR related cases was only 87. Among these, while the decisions in favor of plaintiffs (IPRs holders) were 19 (total win of 2 and win in part of 17), the IPR holders were lost in 21 cases. In criminal cases for patent infringement, as much as 33% cases were ended up with innocence of defendant, indicating that alleging patent infringement was wrong. What was worse was that patent rights registered through a strict scrutiny of the patent office were found invalid at the court or tribunal in more than 50% cases. And even the infringing patent rights were conducted without imitating patented products or methods in majority cases-most of defendants being "innocent infringers". There has been no exact statistical data in South Korea, but studies on the U.S. patent litigations show 1.76% or around 4% of willful patent infringements. In other words, those who have no intention to free-ride or imitate the patents have been involved in patent suits.

The Korea-EU FTA allows an injunction against intermediaries whose services are used by third parties in infringing IPRs that include copyright, trademark and geographical indications, excluding patent rights (Article 10.46:1). The scope of "intermediaries" may be determined in each Party's legislation, but shall include those who deliver or distribute infringing goods and also where appropriate, include online service providers (Footnote 21 of Article 10.46:1). If deliverers or distributors are intermediaries under the meaning of this Article, an injunction against courier service or postman who tries to convey allegedly copyright infringing products, and against delivery enterprise who transports wines or cheese products bearing marks identical or similar to other's geographical indications becomes possible. This scenario came from the real story. In September 17, 2009, the German Federal Supreme Court granted an injunctive relief against a shipping agent who had delivered allegedly patent infringing MP3 players imported from China.

2) Korea-US FTA

When compared with the Korea-EU FTA, the Korea-US FTA provides more rigorous protection and enforcement rules for the sake of IPRs holders by: linking a drug approval process to patent; allowing shutting down an Internet site that permits unauthorized reproduction or transmission of copyrighted works; deleting domestic provision that enables revocation of patent registration when the patent has not been worked for two years after the issuance of a compulsory license (Article 18.8:4); introducing a patent term extension due to a delay in patent examination procedure by the patent office (Article 18.8:6); providing a trademark protection for non-visually perceptible mark such as sound or scent, differently from the current Trademark Act; expanding the protection of encrypted program-carrying signal to criminalize individuals when they willfully receive and make use of the signal knowing that it has been decoded without authorization of the lawful distributor of the signal (Article 18.7:1); putting temporary storage of copyrighted works under the control of copyright holders' reproduction right (Article 18.4:1); increasing criminal investigation against unauthorized text book copying on university campus (Side Letter); in connection with IPR enforcement, introducing pre-established damages, seizure of allegedly infringing goods and documentary evidence, and destruction of materials and implements that have been used in the manufacture or creation of infringing goods regardless of their predominant use in infringement; allowing preliminary injunctions without hearing the alleged infringers; transforming copyright criminals to be actionable *ex officio*; disabling passing through customs of suspected goods even when importers post a bond or other security to obtain possession of suspected trademark or copyright infringing goods; and recommending imposition of criminal penalties "sufficient to provide a deterrent to future infringements", leading to an encroachment of legislative and judicial discretions in criminal policy. Further, not only copyright infringing activity conducted by knowingly using a camcorder in a cinema, but also even an act of preparation, say, attempting to use an audiovisual recording devices is subject to a criminal action.

Among others, the patent-approval linkage has been pointed out by the Korean government as the most harmful provision. This provision is highly problematic because the linkage system is not for legitimate protection of patent, rather it pointlessly compels waste of public resources for the sake of protection of private interests and undermines patients' right to access to medicines by delaying market entering of affordable generic medicines. There are many products that have to obtain a prior approval for marketing or to pass a certain safety test before they are sold. One typical example is an automobile. Any car can be put into market when it meets a statutory safety criteria and an environment standard. There is no reason to ban the marketing of automobiles on the basis that they would infringe a patent right of someone else. The reason why the unique and odd system that links a patent with a drug approval process was born in the U.S. was simply because of a successful lobby of the U.S. Congress by the multi-national pharmaceutical giants. On the earth, the U.S. is the single country that introduced the patent-approval linkage of their own accord, and another countries have merely introduced such a system in the course of signing FTAs with the U.S. by the way, according to the study of the U.S. Federal Trade Commission, of all the patent infringement suits between brand-name pharmaceutical companies (holding patent rights) and generic pharmaceutical companies, the generic companies found prevailed in 73 percent of the cases. Of the decisions favoring the generic companies, non-infringement decisions were 56 percent and patent invalidity decisions were 46 percent. Similar story was found in South Korea. The generic companies won in 37 cases of total 48 cases where 14 generic companies filed invalidation trials against brand-name companies from 2000 to 2008 for product patents for active pharmaceutical ingredients-success rate of the generic companies is as much as 77.1 percent. In other words, approximately 80 percent of pharmaceutical patents that are to be protected under the patent-approval linkage system are patents that should not have been registered. When a patentee is injured from an unauthorized sale of infringing pharmaceutical products, the patentee can bring a civil suit and can fully recover the injury including litigation expenses. In

contrast, there is no way to recover the injury the general public suffers, which caused from the delay of entrance of cheaper generic medicines due to the linkage of originally invalid 80 percent patents. Eventually, the loss arising from implementing the patent-approval linkage has to be borne by patients who need medicines and the whole people who have statutory duty to pay national health insurance premium.

The side letter entitled “Online Piracy Prevention” is unique, never included in any other FTAs the U.S. has signed. It permits shutting down an Internet site that allows unauthorized reproduction and transmission of copyrighted works, and the obligation is unilaterally given by South Korea to the U.S. As the side letter uses the phrases “Internet sites that permit the unauthorized reproduction, distribution, or transmission of copyright works”, the target is not confined to a site whose operators themselves conduct a copyright infringing act. Rather it aims at Internet sites that fail to actively prevent or prohibit the unauthorized circulation of copyrighted works. Such sites may include Internet portal sites, search engines, and even email service providers, not only sites providing the P2P or webhard services. In addition, the side letter is not drafted in such a form intending to give an authority to courts (in that case, the agreement usually says “judicial authorities shall have the authority to …”). So the obligation to crack down websites can be implemented by an order of administrative bodies.

3) P2P Service and ISPs’ Liability

The scope of liability of Internet service providers (ISPs) including P2P service providers has been settled by the Supreme Court in Soribada case.

The Soribada court found that users’ electronic storing MP3 files transmitted over the Soribada platform into their own computers’ hard disks is reproduction under the meaning of the Copyright Act, and that the users’ acts of downloading music files and putting them into a sharing folder set by the program’s default function is tantamount to making the music files available to another P2P service users, not a private copy permitted under the Copyright Act. On this base, the court held the

operators of the Soribada service is liable as aiding users' unlawful behaviors. This decision broadens the scope of secondary liability of ISPs. However the materials shared by users through the Soribada service are not limited to copyrighted works. They may include materials created by users. Nonetheless the Soribada court does not require concrete knowledge on the infringement and found the ISPs liable when they can anticipate and facilitate the potential infringement of the reproduction right. Some commentators criticize this decision by comparing the Soribada case with adultery and hotel keepers case. Even when the hotel keepers can expect that adultery may happen in their hotel rooms, an obligation cannot be imposed upon the hotel keepers to examine conjugal relations of guests or to look into each room and failure of such an examination cannot be led to closure of the hotel.

In a case involving the updated version of Soribada (version 5), the Seoul High District Court rendered a surprising decision. The court held that the Soribada service is one of the special ISPs having to take a certain technological measures as defined in the revised Copyright Act, and therefore the service provider is obliged to take active filtering measures, not passive ones. If the active filtering are compulsory measures, music files that can be exchanged through the P2P services are confined to sounds authorized by copyright holders, completely banning users created contents.

4) Technological Protection Measures

Paragraph 28 of Article 2 of the Copyright Act defines the technological protection measures as including: "technological measures by a rights holder or a person who has obtained consent from such a rights holder to effectively prevent or restrict access to works protected under this Act with respect to the exercise of copyrights and other rights protected according to this Act" (subparagraph a); and "technological measures by a rights holder or a person who has obtained consent from such a rights holder to effectively prevent or restrict the infringement on copyrights and other rights protected according to this Act" (subparagraph b). This definition is to add protection for TPMs for access control, and Article 104*bis* introduces prohibition of circumvention of TPMs.

Such a stronger protection of TPMs is problematical because it allows continuous control by copyright holders beyond the statutory term of protection and may weaken fair use permitted in certain circumstances under the Copyright Act. Therefore, protection of TPMs under the rubric of laws may go beyond the limitation of copyright protection and bring a conflict with fundamental rights.

5) Three-Strikes-Out Rules against Copyright Infringement

The Copyright Act revised and went into force in April 22, 2009 created Article 133*bis* for so-called "three-strikes-out rule". Now the Ministry of Culture, Sports and Tourism (MCT) can order online service providers to suspend Internet users' accounts for up to 6 months, after giving three warnings to remove or block allegedly infringing contents, information or computer programs or information enabling circumvention of TPMs. And according to 133*ter*, the Korea Copyright Commission (KCC) can make requests to online service providers: to send a warning to repeat infringers; to delete or stop transmission of allegedly infringing material; or suspend their users' accounts for a non-defined period.

Against the similar rules of the French law, the Constitutional Court, on June 2009, considered the law unconstitutional. The four reasons for this finding can be summarized as: (1) the three-strikes-out rule is in direct conflict with the right to freedom of expression and communication protected by the Declaration of Human and Civic Rights of 1789, which encompasses the right to access to an internet connection; (2) granting powers to administrative authorities to impose sanctions having a nature of criminal punishment is contrary to the principle of division of powers; (3) the Parliament cannot delegate her power to the administrative body to restrict the right to Internet connection for the protection of copyright and neighboring rights; and (4) the three-strikes-out rule is in violation with the provision of the French Declaration of Human and Civic Rights of 1789 presuming innocence until found guilty by courts. These reasons of the unconstitutionality can be applied to the Korean model.

6) Criminal Sanction for the Protection of Copyright

Reckless criminal enforcement of copyright has become social problems, mass-creating law-breakers and producing a newly-coined word “copyright suicide.” Differently from another countries where copyright infringement is subject to a criminal action as in Korea, the criminal enforcement has become a sort of new business model for copyright holders. They or lawyers acting for them monitor Internet users and send warning letters to suspected individuals threatening a criminal sanction (imprisonment of shorter than five years or fine of less than KRW fifty million). In exchange of not taking the criminal action, they ask a cash settlement. Criminal enforcement procedure provide copyright holders with a leverage using the threat of criminal action as any act of copying or transmission of copyrighted material no matter how serious or minor can trigger the criminal action.

The table below shows the criminal cases handled by the Prosecutors Office. Criminal complaints of copyright infringement skyrocketed from 2007. But the actual indictments by the prosecutors are very small, less than 5%. The cases brought to the formal court trial is so minute, 0.1% in 2007, 0.0088% in 2008, and 0.075% in 2009. Absolute majority cases ended up with “Withdrawal” because of the cash settlement out of the court. This reveals that the criminal enforcement of copyright has turned into one of the profit sources rather than a means of criminal policy for copyright protection, provoking widespread resistance to the copyright system.

〈Table 12〉 Data on Criminal Copyright Infringement Cases

Year		2005	2006	2007	2008	2009
Complaints Received		14,838 (290)	18,227 (611)	25,027 (2,832)	90,979 (21,953)	89,410 (22,169)
Indictment	Demand for a Trial	19 (0)	23 (0)	26 (0)	8 (0)	67 (0)
	Summary Indictment	1,486 (19)	1,473 (31)	1,637 (76)	3,975 (118)	3,956 (17)

Year		2005	2006	2007	2008	2009
Non-Prosecution	Dismissal	1,013 (19)	1,445 (20)	3,836 (313)	12,446 (1,575)	24,702 (13,707)
	Withdrawal	9,481 (155)	11,426 (389)	15,195 (1,865)	51,255 (11,855)	27,150 (2,936)
	Suspension	215 (33)	1,865 (118)	1,986 (379)	16,520 (6,056)	24,676 (4,243)
	Etc.	2,624 (64)	1,995 (53)	2,347 (199)	6,775 (2,349)	8,859 (1,266)

Another tragic and unintended consequence is found in an increase of victims of teenagers. According to the Analysis of Crime 2009 of the Supreme Prosecutors' Office, 15% of under-age crime is related to the copyright infringement (among the total suspected under-age, the suspected copyright infringers occupy around 15%. While the under-age crime occupies 6%, the copyright crime by the under-age amounts to 23%. Perceiving this problems the Prosecutors Office launched from July 2008 a program to suspend prosecution upon copyright education for juveniles (extended to adults from March 2009), and from 2009 a temporary program to dismiss the complaints against the first offenders was introduced. Partly due to those programs, the complaints against juveniles decreased in 2010 to approximately one tenth of cases in 2009.

7) Damages on the Excessive Enforcement of Copyright

On February 2, 2009, a five-year-old danced to her own humming of "I am Crazy", a popular song of a singer Sohn Dahmbi, and a video clip of her singing of its lyrics in the refrain part was posted on a user's blog to which a link appeared on Naver's video site. Korea Music Copyright Association, a trustee of the copyright to the song, requested Naver to stop reproducing and transmitting the blog post which was promptly blocked. The user filed a damages suit against Korea Music Copyright Association for requesting a takedown without lawful cause pursuant to Article 6, 2014. The court granted 200 hundred Korean won.[182] This judgment is significant

in that it ruled that even a rights-holder's practice of making excessive claims for copyright enforcement has been unlawful.

8) Game Shut-Down

Article 23-2 Paragraph 1 and Item 2 of Article51-6 of Youth Protection Act, promulgated on May 19, 2011 (Act No. 10659), provided for the game shutdown rule, according to which a provider of real-time game through information and communication network is banned from doing so to any minor below 16 years old during 0 AM to 6 AM at the penalty of up to 2 years of imprisonment or up to 10 million Korean won. The game shutdown was adopted in China and Thailand but later abandoned for not being effective and currently Korea is the only country that has adopted it.[183] Even in our country, according to a report on the Status of the Rule Encouraging Youths' Sound Use of Internet Game (Shutdown), the effect of decreasing game use is merely 0.3%.[184]

The main purpose of game shutdown rule is to protect the sleep time of youths addicted to internet games. However, it has been pointed out in opposition that the means adopted for that legislative purpose violates the youths 'constitutional right to pursuit of happiness, family autonomy, and parents' right to educate children, principle of equality, etc.[185] Due to the controversies of unconstitutionality, youths and youths' parents have filed on October 28, 2011 and Korean Game Industry Association and game companies have filed in similar periods constitutional challenges respectively. The game shutdown rule is different from other copyright issues in that it exists only in Korea but generates similar debates as other rules that excessively restrict peoples' right to participate in formation and development of culture and enjoy the result.

---

182) Seoul High Court 2010.10.13 Announced 2010나35260
183) "China-Thailand Abandon Ineffective Shut-down", <Hankuk Gyeongje>, November 20, 2012
184) Jun Byung-heon, "Survey Shows only 3% Decrease in Youths Late Night Gaming after Shutdown," http://blog.daum.net/bhjun/5509059
185) Hwang Sung-gi, "Constitutional Conformity of Online Game Shutdown", <Hanlim Bubhak Forum>, November 2005, p. 139-156

Chapter 3

National Human Rights Commission's Contributions related to ICTs and Human Rights

- **Section 1.** Current Data on Petition, Consultation, and Appeal
- **Section 2.** Petitions, Consultation, Appeal, and Guidance Cases

Section 1. Current Data on Petition, Consultation, and Appeal

1. Current Data on Appeals related to ICTs and Human Rights

A number of petitions, consultation, appeal, and guidance cases related to information human rights has dramatically increased from 31 in 2001 to 6,386 in 2012 and the number of appeals during seven year period prior to 2012 has continuously increased from 2,716 in 2008 to 5,142 in 2010 to 6,836 in 2012 which is nearly 250% increase from 2006. Also, the number of cases related to information human rights reviewed by the NHRC since its installment accumulates to 37,000. Data sorted by its types revealed that as of December 2012, cases related to information privacy accounts for 85.3 percent of that number and the next frequent cases were those of right of access to information and freedom of expression in online settings.

〈Table 13〉 Data on Appeals According to Different ICTs and Human Rights

as at 2012.12.31. (number, %)

Year	Data Privacy	Online Freedom of Expression	Data Accessibility Rights	Right to Enjoy Information Culture	Total
2001	30	-	-	1	31
2002	315	20	42	0	377
2003	904	55	129	3	1,091
2004	1,518	99	229	6	1,852
2005	2,665	139	271	17	3,092
2006	2,332	140	237	7	2,716
2007	2,719	191	312	13	3,235
2008	3,261	182	374	32	3,849
2009	3,854	187	371	27	4,439
2010	4,357	266	482	37	5,142
2011	4,235	220	545	32	5,032
2012	5,559	279	512	36	6,386
Total	31,749	1,778	3,504	211	37,242
Ratio	85.3	4.8	9.4	0.6	100.0

〈Table 14〉 Types of Complaints

	Petitions	Counsel	Complaints	Guidance	Total
Data Privacy	4,703	10,105	9,579	7,092	31,479
Online Freedom of Expression	178	510	1,052	38	1,778
Data Accessibility Rights	983	704	1,139	678	3,504
Right to Enjoy Information Culture	22	62	119	8	211
Total	5,886	11,381	11,889	7,816	36,972
Ratio	15.9	30.8	32.2	21.1	100.0

2. Right of Information Privacy

The right of information privacy includes cases involving surveillance, wire-tapping, circulation of crimes inflicted or committed, discrimination or harm from excessive gathering or release of personal information. Searching for cases of right of information privacy using the keywords, “Personal Information”, “Privacy”, “CCTV”, “Location Information”, “Surveillance”, “Wire-tapping”, “Public Circulation”, “Release of Identity”, “Leak”, and “Portrait Rights” has revealed that between 2001 and December of 2012 there were 4,703 cases of petition, 10,105 cases of consultation, 9,579 cases of appeal, and 7,092 cases of guidance which all added up to be 31,479 cases.

Data organized by its date showed that there were 31 cases in 2001, 315 cases in 2002, 1,518 cases in 2004, 1,695 cases in 2006, 3,261 cases in 2008, 4,357 cases in 2010, and 5,559 cases in 2012 which points to continuously rising trend. In 2012, the number of cases increased by 30 percent compared to the previous year and it was 3.7 times more than that of 2004 and 2.5 times more compared that of 2006.

Especially from 2001 and late 2012, 6,120 cases about CCTV could be broken down in to 1,485 cases of petition, 3,010 cases of consultation, 1,434 cases of appeal, and 191 cases of guidance. This accounts for 20 percent of the appeals made regarding right of information privacy and the most frequent.

〈Table 15〉 Number of Complaints on Rights of Information Privacy

as at 2012.12.31. (number)

Year	Petitions	Counsel	Complaints	Guidance	Total
2001	19	10	1	0	30
2002	114	196	5	0	315
2003	131	445	70	258	904
2004	195	521	273	529	1,518
2005	337	791	869	668	2,665
2006	235	655	637	805	2,332
2007	449	680	829	761	2,719
2008	518	953	823	967	3,261
2009	628	1,096	915	945	3,584
2010	823	1,442	1,167	925	4,257
2011	567	1,416	1,469	783	4,235
2012	687	1,900	2,521	451	5,559
Total	4,703	10,105	9,579	7,092	31,479
Percentage	14.9	32.1	30.4	22.5	100.0

3. Freedom of Expression in the Cyber Space

Cases involving freedom of expression in the cyber space includes cases involving use of commentary sections or discrimination or human rights violation inflicted due to one's online posting. Statistical data retrieved keywords "Online Forums", "Comments", and "Posting" revealed between 2001 and late 2012, there were 178 cases of petitions, 510 cases of consultation, 1,052 cases of appeal, and 38 cases of guidance, which adds up to be 1,778 cases in total.

Sorted by years, 20 cases in 2002, 55 cases in 2004, 140 cases in 2006, 182 cases in 2008, 266 cases in 2010, and 279 cases in 2012 have been filed on the issue of freedom of expression in the cyber space, the number is in a steadily increasing trend, doubling from 2006 to 2012.

〈Table 16〉 Number of Complaints on Freedom of Expression on the Internet

as at 2012.12.31. (number)

Year	Petitions	Counsel	Complaints	Guidance	Total
2001	-	-	-	0	-
2002	3	17	-	0	20
2003	3	36	13	3	55
2004	9	37	49	4	99
2005	8	34	94	3	139
2006	14	28	96	2	140
2007	25	35	128	3	191
2008	19	45	108	10	182
2009	26	53	105	3	187
2010	22	65	174	5	266
2011	15	67	136	2	220
2012	34	93	149	3	279
Total	178	510	1,052	38	1,778
Percentage	10.0	28.7	59.2	2.1	100.0

4. Right of Access to Information and Right to Enjoy Information and Culture

Petition cases related to right of access to information in totality have been searched and studied by searching with keywords “Information Release”, “Web Accessibility”, “Digital Divide”, and “Internet Access” have revealed from 2001 to late 2010, there were 983 cases of petitions, 704 cases of consultation, 1,139 cases of appeal, and 678 cases of guidance which sum up to be 3,504 cases.

Sorted by years, 42 cases in 2002, 229 cases in 2004, 237 cases in 2006, 374 cases in 2008, 482 cases in 2010, and 512 cases in 2012 relates to the issue which show an ascending trend as it doubled from 2006 to 2012.

〈Table 17〉 Number of Complaints on Right to Enjoy Information and Culture

as at 2012.12.31. (number)

Year	Petitions	Counsel	Complaints	Guidance	Total
2001	-	-	-	0	-
2002	26	15	1	0	42
2003	57	36	29	7	129
2004	84	47	44	54	229
2005	83	60	84	44	271
2006	67	35	90	45	237
2007	119	33	114	46	312
2008	112	58	158	46	374
2009	109	82	120	60	371
2010	107	100	143	132	482
2011	137	97	187	124	545
2012	82	141	169	120	512
Total	983	704	1,139	678	3,504
Percentage	28,1	20,1	32,5	19,3	100.0

Moreover, appeals related to right to enjoy information culture have been searched using keywords including “Copy Right”, “Shut-down”, and “Intellectual Property Rights” revealed between 2001 and late 2010, there were 22 cases of petitions, 62 cases of consultation, 119 cases of appeal, and 8 cases of guidance, summing up to 211 cases. Sorted by years, there were 4 cases in 2004, 17 cases in 2005, 7 cases in 2006, 13 cases in 2008, 27 cases in 2009, 37 cases in 2010, 32 cases in 2011, and 36 cases in 2012. In this category, appeals are the most frequent types of cases with 56 percent and the number of cases is slowly trending.

Section 2. Petitions, Consultation, Appeal, and Guidance Cases

1. Examples of Petitions, consultation, appeal, and guidance cases

(1) Right of privacy of information

1) Privacy Intrusion involving CCTV (Visual Information)

In installing a CCTV for security purposes at the office, consent of the interest party was not obtained; also, a sign indicating that they are being monitored was not posted which led the commission to recommend the perpetrator to receive education from human rights commission or ministry of administration and safety in regards to an appeal for one's violation of privacy as well as right to decide one's personal information.

2) Full-body Scanners (Physical Information)

The Ministry of Land, Transport and Maritime Affairs' decision to install a full body scanner at the airports has a clear risk of infringing upon one's privacy and leakage of collected personal information, and discrimination based on religion or nationality. While the equipment may be used to search for materials previous indistinguishable through other equipment, it is unclear whether such device significantly improves capacity to prevent terrorist activities. Also, the legal foundation for using this equipment is unclear which violates the principle against excessive measures; therefore, the commission has recommended against using the device.

3) Unauthorized access of personal information

Upon the appeal claiming that the National Pension Service collected private information of internet users, civilians who have been engaging in "Anti-National Pension" programs, and friend and families, the commission conducted an independent research to find that public workers that the Service indiscreetly accessed private information and visited residents of specific contributor. The commission has

decided those are violating one's right to control private information, privacy, and other human rights and recommended the service to discipline engaged workers and receive mandatory education sessions to prevent further incidents and come up with a structural solution.

4) Fingerprint Identification (Biometric Information)

A central library at a public institution's decision to require fingerprint identification of students was brought the commission which then decided that it has a high risk of violate students' privacy and recommended the Minister of Education to take necessary actions.

5) Electronic Surveillance at Businesses

Regardless of public or private, electronic surveillance using CCTV, IC chip cards, GPS, and other technology is happening and all employees under such surveillance can be subjected to violation of privacy. Therefore, the committee recommended the minster of employment and labor to come up with a special law, amend current employment acts, and tighten the monitoring of each businesses for the matter. Core tenets of the recommendation includes a call for a distinct sphere where such surveillance is authorized, a legal tool to protect employee's rights in installing and using electronic surveillance, a detailed description of the laws regarding the private data collected, and a measure to provide an adequate level of compensation if the surveillance was abused or excessively conducted.

(2) Freedom of Expression in the Cyber Space

1) The Committee's opinion on cyber defamation law

Regarding the telecommunication law which attempts to create a cyber-defamation law that can be enacted regardless of the victim's opinion, the committee expresses that making the law applicable regardless of the victim's opinion allows policing

bodies to engage in investigations without the victim's law suit and penalize the perpetrator without confirmation of the inflicted harm which are both conflicting with the current policing principles. Also, it opens up a room for an investigator's opinion in deciding on which case to investigate which may lead to a biased policing. As a result, it may eventually lead to major contraction of freedom of expression in the cyber space and the committee advised to do the otherwise.

2) UCC videos during pre-elections period

Current law allows simple expression of support or opposition for a person who plans to run for an election. However, repeated expression is sought as a political campaign during a pre-election period during which political campaign is prohibited. This "repeat" is unclear as exactly how many repetitions fall into this "repeat". Also, prohibiting posting or dissemination of satirical humor videos about a political figure or a situation is an excessive prohibition. Elections Committee's standard for decision is vague and unclear and is susceptible to subjective enactment of the law which can conversely impede impartiality of the committee. Human Rights Commission discourages the elections committee to excessively prohibit UCC videos and recommends to revise its codes to allow citizen's right to express political opinions and engage in political campaigns to the maximum level within the boundaries the related laws permit.

3) Opinion submitted to the court regarding the "Minerva Case"

On the Framework Act on Electronic Communication Article 47 Clause 1 which binds "a person who publically engage in a deceptive electronic communication with a purpose of harming public good" to be imprisoned for up to five years and the law's possible violation of freedom of expression, the commission submitted a report to Seoul Local Court to strictly determine the laws unconstitutionality and illegality for its possible contribution to contraction of fundamental rights because of the law's vague wording in "false electronic communication" and "a purpose of harming public good".

Concerning this, the court has decided that in a case where an internet user named "Minerva" is charged for posting a deceptive information on an online board on the topic of economy, he did not have an intention of posting wrongful information nor a purpose to harm public good and therefore free of charge.

4) Consultation on expulsion from school for posting an opinion on personal webpage

"During my 3rd year of school A, I wrote a passage on my personal webpage (mini-homepage) and I was expelled from school because what I wrote was too left. Until the decision to expel me, I was never given a change to explain myself and it happened in just two weeks span."

"After getting expelled, I tried to enroll at school B but I was denied enrollment because of this event. Because I was expelled just three months before the graduation, I have to serve in the military next Monday. I visited NHC to see if they can help me reclaim my honor through investigation."

5) Consultation regarding a case involving a request to delete a blogpost

"I wrote a blogpost expressing my anger toward military draft dodgers. It was mostly criticizing those who engage in illegal activities to make use of a loophole in the military conscription system. Military Manpower Administration sent out a request to the portal website to delete my blogpost claiming that the methods described on my blogpost, despite the fact that they were already introduced via national television, could be abused by future draft dodgers.

"MMA acknowledged that my posts are not illegal but they are open to controversy, has an unfitting title, and has statements that are not true.

"I am confident that anyone with reasonability would decide to obey the conscription instead of dodging it. However, MMA claims that the title is unfitting and denying to revive my posts. Portal website, scared of the MMA's request, is telling me they will repost it if MMA agrees to do so. Truthfully, it is a violation

of citizen's basic right due to state and corporate abuse of power."

(3) Right of Access to Information

1) Recommendation to correct discrimination in using company intranet board

In a petition on the case involving Korean Broadcasting Station's decision not to give permission to access company's intranet for its orchestra member claiming the access is not related to the direct work of the employee, the Commission has decided that because the intranet is a cyberspace serving as a central ground for information and online transaction and an essential component in providing fluid communication for its employees, it is an unfair discrimination as free formation of opinion is possible through adequate guarantee of access to information.

2) Recommendation regarding violation of right to know by denying disclosure of information

A request for disclosure of public information regarding county chief and deputy county chief's expenditure was denied and taken to the high court which ordered disclosure of information. However, the recipient of the order destroyed the document claiming it has passed the designated period of storage and the case was taken to HRC for violation of right to know and right to pursuit happiness. The Commission recommended the chief to penalize related officials, come up with measure to prevent similar incidents, and conduct an education on their duties. Also, a recommendation was given to minister of administration and local authority and heads of related of officials to produce a plan to prevent similar incidents from happening.

3) Human Rights Violation by destruction of information

A request for disclosure of information on applicants of job openings for professors at universities related to their list of academic achievements, research records, and

evaluations was denied and was taken to the court to achieve partial win on the case. Yet, the school destroyed all related records and notified denial of disclosure. The Commission recommended minister of education, science, and technology to give warning to the institution and recommended the chairman of the institution to penalize and educate the officials involved in the case.

4) On the Results of Survey on Web Accessibility

Legislation on prohibition of discrimination against disabled persons and protection of rights defines national and local state's duty related to access and provision of assistance for information and communication to tackle the issue of information deprivation of disabled persons. According to the Commission's survey on web accessibility, websites of public institutions are still difficult to access for disabled persons and were especially lacking in providing access to the visually impaired.

2. Data on Recommendations Related to ICTs and Human Rights

Related to information privacy, opinions and submissions made by the Commission in many cases involved human rights violation from state and public institution's intrusion of privacy and excessive collection of data. There were also policy recommendations related to communication secrecy, CCTV, QR Code, and full body scanners and collection of personal information.

The following are exemplary cases of policy recommendations, opinions, and submissions related to freedom of expression in the cyberspace made by the Commission. Opposition against mandate use of real names online, excessive restrictions on UCC videos, cyber defamation law, national security law and others are discussed.

〈Table 18〉 Recommendations related to ICTs and Human Rights

as at 2011.12.31.

1. **Protection of Communication Secret Act** (June, 10, 2002) : Recommended deleting a provision allowing up to 12 hours of emergency wiretapping
2. **Occasional aptitude tests for driving licenses** (July 30, 2002): Recommended amending the Law Regarding Protection of Personal Information Held by Public Agencies to avoid privacy infringement; reviewing the disqualification conditions under the Roads Traffic Act; and conducting periodic human rights education on the workers of the related agencies
3. **Telecommunications Business Act amendment** (August 13, 2002): Recommended converting to self-regulation of the information and communication businesses; deleting or amending the ambiguous provisions
4. **Insurance Business Act amendment** (September 25, 2002): Recommended deleting a provision allowing acquisition personal data from the related agencies as part of insurance fraud investigations
5. **Police acquisition of facial photographs of individual residents** (March 10, 2003): Recommended legislating a provision limiting data requests and production of such data in relation to probation of youths
6. **Enforcement Decree of the Act Regarding Lapse of Criminal Sentence** (May 12, 2003) : Recommended legislating a provision limiting data requests and production of such data in relation to probation of youths
7. **NEIS** (May 12, 2003) : Recommended improving upon the provisions concerning academic affairs, admissions and advancements, health, and teachers' personnel records
8. **Educational Civic Servants' Personnel Records Rules amendment** (October 22, 2003) : Opined deleting the fields for blood type, name, relationship, birthdate, occupation in the personnel cards
9. **Terrorism Prevention Act amendment** (October 22, 2003): Opposed the amendment for the following reasons: The current laws and institutions are sufficient for preventing terrorism; The procedure for requesting deployment Special Forces is unconstitutional; The strengthening of the intelligence agencies' powers can restrict people's basic rights; Several provisions may violate constitutional law and international human rights law
10. **The Act Regarding Protection of Personal Information Held by Public Agencies amendment** (November 10, 2003) : Recommended collecting and using personal data in a manner sufficiently protective of people's right to informational self-determination set forth in Articles 10 and 17 of the Constitution
11. **"Political Relations" Act amendment** (February 16, 2004) : Recommended aborting adoption of the real-name rule on the bulletin boards on the internet media; lowering the age threshold for voting; lowering the entry barrier for new political candidates; and building a method for obtaining representation from diverse sectors and classes
12. **Anti-theft CCTV installation** (April 19, 2004) : Recommended legislating a new law or amending the Act Regarding Protection of Personal Information Held by Public Agencies to provide a statutory basis for installing anti-theft CCTV
13. **Rules on Collecting and Managing Public Officials' Election Candidates' Personal Data** (July 5, 2004) : Recommended limiting the scope of protected persons from "those desiring a position within public agencies including state, local, and state-sponsored agencies" to that of Article 19-3 Item 3; and requiring approval from or notice to the data subjects before transfer of the data to other agencies and destruction of the data after the use

14. **The Act Supporting Finding of Missing Children** (September 6, 2004) : Opined limiting to the necessary minimum the scope of children to be subjected to genetic testing; and converting into statutory provisions those rules on management of the test results, protection of genetic data, data base building, etc.
15. **Framework Act on Education amendment** (October 11, 2004) : Recommended amending the Primary and Secondary Education Act Articles 60-3 and 25, School Health Act Article 7-2 to conform to the Human Rights Commission' recommendations on NEIS; and requiring prior notice for creating and managing school activities records and physical examination records for the Primary and Secondary Education Act Article 25 and School Health Act Article 7-2.
16. **Personal background checks** (February 14, 2005) : Recommended legislating a statutory basis for personal background checks; limiting the checks of people to the extent necessary for national security; abrogating the provisions concerning family ideologies which may violate the rule against guilt by association
17. **Protection of Youths' Sex Act amendment** (February 28, 2005) : Opined for clearing detail-level data registration of the potential unconstitutionalities vis-à-vis the rule against excessive restriction, due process, the rule of statutory punishment, and the rule against blanket delegation; Recommended limiting disclosure of the detail-level data of the perpetrator only upon the request of the victimized youth or his/her family; and Opined for permitting variances on the employment restriction in proportion to the severity of the crime committed, the relationship between the restricted jobs and the crime, and the risk of recidivism.
18. **Disruption of Order Regulation Act bill** (August 31, 2005) : Opined for overhaul of the bill because, although a general law non-criminally enforcing light administrative duties is needed, the bill allows a fine up to 30 million KRW to be fulfilled in lieu by restriction on participation in government-licensed projects, provision of credit information, or jail time, thereby excessively restricting people's basic rights.
19. **Provision of data on out-of-school youths** (April 10, 2006) : Opined that, although protection and support of out-of-school youths is needed, disclosing the data on them without their consent or statutory bases violates their informational self-determination rights and possibly violates Article 30-6 Paragraph 1 of the Primary and Secondary Education Act.
20. **Youths' Sex Protection Act overall amendment** (January 8, 2007) : Agreed with including male children in the victim categories, defining quasi-rape acts, and abolishing public disclosure of the personal data in favor of limited inspection; and Recommended abolishing the bans on deferred sentence or deferred judgment and the provision on genetic data registration
21. **Enforcement Decree and Enforcement Rules of Medical Benefits Act, amending** (February 15, 2007) : Recommended improvements and careful implementation in view of the fact that the bill may violate medical care beneficiaries' rights to health, medical care, life, and data protection, and may unreasonably discriminate against them in comparison to ordinary health care insurance beneficiaries, and in some respects violate the state's duty to guarantee minimum standard of living and the principle of public aid.
22. **Passport Act, overall amendment** (April 12, 2007) : Opined that the definition of passport data must be further concretized; that collecting fingerprints data upon passport issuance is not the minimum necessary; that the thus collected biometric data needs not be stored or managed and therefore their management should be limited to the extent necessary for accomplishing the purpose; that marking residential registration numbers on the passports is not the minimum necessary use of personal data and therefore the relevant provision in the Decree must be abolished; and that

what is shown on the passport are important and therefore must be based on statute.

23. **Managing 'Environmental Watchers' in the Five Big Rivers area and use of personal geolocation data** (July 19, 2007) : Recommended establishing the prior consent procedure for collection and use of the watchers' geolocation data and other safeguards for rights such as the procedures for notifying the watchers of the use of their personal data, the management and security measures for using and processing the geolocation data, and the watchers' rights to inspect and correct the data.
24. **Providing conscription physical examination records to the current employers** (August 16, 2007) : Opined that the employing agencies need receive the minimum necessary data for the agents rated for the diseases qualifying them for public interest duties; and that public interest agents' pathological or penal records, if needed for work-related purposes, can be in principle collected by the employing agencies only though separate procedure.
25. **State Property Act, amendment** (September 13, 2007) : Recommended deleting the provisions for collecting tax data or financial transactions data on those delinquent on the fees for using state properties due to the concerns for privacy infringement.
26. **Administrative Data Pooling Act bill** (November 1, 2007) : Opined that financial agencies must be excluded from the agency pool; that the scope of the agencies in the pool and the scope of data subject to the pooling must be specified in statute; and that, for protection of data subjects, the data subjects must be given prior consent rights before their data are used as the Minister of Government Administration and Home Affairs.
27. **Electronic surveillance at workplace** (November 12, 2007) : Recommended to the Department of Labor legislating a special law regulating the growing electronic surveillance at workplaces and amending the Labor Standards Act in order to prevent the infringement on workers' rights.
28. **Protection of Communication Secrets Act amendment** (December 17, 2007) : Opined that the new bill goes against the legislative intent of the Act and has problems with communicational freedom and privacy, data protection, and the warrant doctrine.
29. **Defense Personnel Certificate Act bill** (April 3, 2008) : Opined that the safeguards for privacy of the defense personnel certificate holders must be more concretely specified in the bill to ensure efficient management and operation of the certificate program.
30. **Car earing program** (May 15, 2008) : Opined that attaching plastic stickers on the cars to mark the facts of Roads Traffic Act violations and overdue fines may infringe the car owners' privacy and impose a new obligation of not removing the stickers, and therefore that the program must be supported by a statutory basis in the Road Traffic Act.
31. **National Intelligence Service's personal background check affidavit forms** (July 31, 2008) : Opined to the Chief of NIS for deleting the fields for the resident registration numbers, workplaces, and positions of the affiant's parents, spouses, and children.
32. **Wandering seniors badges program** (November 6, 2008) : Opined that, although the program has greatly contributed to prevention of accidents and missing incidents of seniors suffering from dementia, the personal data collected as part of the program, if breached, can make the seniors the targets of crimes, and therefore, that the databases of the personal data must be centrally managed and supervised under the responsibility of the Ministry of Health and Welfare to stronger data protection, and must be operated in accordance with the Government Administration and Public Safety Ministry's 2008 Guidelines on Protection of Personal Data Held by Public Agencies.
33. **National Tax Service's inquiries on personal data use** (December 24, 2008) : Opined that the incumbent soldiers' service records (service period, name, resident registration number) constitute

personal data, and therefore the data requests for those records, even if related to public interest, must be as specific as possible to be acceptable.

34. **Protection of Communication Secrets Act amendment (Lead Sponsor: MP YI Han-Sung)** (January 22d, 2009) : Opined that adding geolocation data as the data to be included in the "communication records" violates people's privacy; that imposing the obligations of user notification, data retention, and wiretapping facilities installation on the service providers on the penalty of fines violates freedom of business and people's informational self-determination, and therefore that the relevant provisions must be deleted.
35. **Information Communication Network and Data Protection Act amendment (Lead Sponsor: MP NA Kyung-Won)** (February 5, 2009) : Opined that adoption of cyber-insult law should be carefully reconsidered; and that in any case it should be a crime prosecutable upon victims' complaint as in Penal Code.
36. **Criminal Code amendment (Lead Sponsor: MP Chang Yoon-Suk)** (February 5, 2009) : Opined that the provision cyber defamation is superfluous on top of the Information Communication Network Act provision, the cyber insult provision overlaps with MP Na Kyung-Won's ICNA bill, and therefore both provisions must be withdrawn.
37. **Communicable Disease Prevention Act amendment** (March 19, 2009) : Opined that the power of requesting data from other public agencies, which the Chief of the Center for Disease Control has, must not cover personal data and be limited to the extent necessary to prevention of infection.
38. **Act Supporting and Protecting Missing Children amendment (Lead Sponsor: MP KIM So-Nam)** (June 4, 2009) : Opined for maintaining the current law except the provisions on collecting fingerprints of missing seniors suffering from dementia, which must be improved upon by specifying concretely the selection standard of applicable seniors and the collection procedure thereof.
39. **Framework Act on Telecommunication Article 47 Paragraph 1** (June 8, 2009) : Opined to the Constitutional Court that the provision must be strictly scrutinized in view of the importance of freedom of speech, the nature of Internet space, the provision's chilling effects, and therefore the provision's potential for human rights infringement.
40. **Homeless and other low-income people's identity theft prevention measures** (August 27, 2009) : Opined that collection and management of personal data upon the homeless and others deepens social discrimination against them, and the Seoul City's identity theft prevention measures be thoroughly reconsidered also in view of freedom of privacy and informational self-determination.
41. **Election-related UCC Use Standards** (October 29, 2009) : Recommended that, in view of the nature of Internet medium, excessive restriction on election-related UCC must be avoided, and the Standards must be reconsidered to avoid infringement on freedom of speech.
42. **Act Regarding Lapse of Crime amendment** (November 6, 2009) : Opined that the new provisions defining 'public security criminals' and authorizing the Minister of Justice's segregated management and usage of the data concerning them are too vague and delegate major issues for disposition by the Presidential Decrees, thereby excessively restricting informational self-determination and right to equality, and it is not desirable to legislate them.
43. **Information Communication Network Act's amendment concerning online posters' identity verification rules** (November 19, 2009) : Opined that removing the 100,000 average daily user per service type threshold of the applicable service providers violates people's freedom of speech and the information and communication service providers' freedom of business, in contravention of the rule of statutory reservation and the rule against blanket delegation.
44. **Personal Data Protection Act amendment concerning CCTV (government-sponsored bill)** (December

3, 2009) : Opined that some provisions on video recording equipment delegate too broad authorities to regulations to guarantee the effective management of CCTV; that the installation and management of anti-theft CCTV should not be outsourced to civilians except technical aspects; and that governance of civilian CCTVs should not be left to *ex post* regulation but subjected to *ex ante* regulation such as licensing and registration.

45. **Personal Data Protection Act provisions concerning personal data protection agency** (December 24, 2009) : Opined that "The government bill lacks the element of independence of the data protection agency, and MP YI Hye-Un's and MP Byun Jae-il's bills need improvement on the provision authorizing work-related individual suits and the proposals for strengthening parliamentary participation in appointment of the Commissioners and otherwise reinforcing the institutional and budgetary independence of the agency."
46. **Proposal to show on military service certificates the fact of past evasions** (March 25, 2010): Opined that the proposal unilaterally discloses the matters subject to people's general right of personality and right of privacy.
47. **Police Officers' Duties Administration Act amendment (National Assembly's Public Administration and Safety Committee's bill) concerning suspicion-less questioning** (May 13, 2010): Opined that the bill's provisions on inspection of the items carried personally or by vehicles violated bodily freedom and privacy and freedom of personal life, and the mandatory provisions on identity verification violate the right to silence and informational self-determination excessively and therefore need be replaced with voluntary provisions.
48. **Domestic airport full-body scanning** (June 10, 2010) : Recommended aborting the National Lands and Oceans Ministry's proposal to install the full-body scanner violates the rule against excessive restriction and the rule of statutory reservation, thereby risking human rights infringement.
49. **Public "Wanted" notice program and related laws, regulations, and practices** (June 17, 2010) : Recommended to the Minister of Justice creating statutory bases for public "Wanted" notices and the Internet versions of such, and to the Chief of the National Police (1) observing the rules and procedure of public "Wanted" notices; (2) deleting the photographs of the wanted persons on the Internet immediately upon arrest; (3) installing technical safeguards to prevent, and warn against, the wanted persons' photos from being copied and distributed; and (4) include outside personnel in the committee selecting the persons to be publicly "wanted".
50. **Criminal Procedure Act amendment, Protection of Communication Secrets amendment, concerning search and seizure or wiretapping of electronic mails** (August 19, 2010) : Recommended to the Chairperson of the National Assembly creating statutory bases for search and seizure or wiretapping of e-mails; limiting the scope of seizure or wiretapping by the specifying the "dates created" of the applicable e-mails; otherwise avoiding excessive acquisition; and guaranteeing the suspects such rights as advance notifications, attendance during execution, request for removal of unrelated material, and return of the medium.
51. **Act Regarding Lapse of Crime Article 8-2 Paragraphs 1 and 2** (September 9, 2010) : Recommended to the Minister of Justice expunging all investigation records except on the cases closed upon deferred prosecution or insufficiency of evidence
52. **Internet censorship** (September 30, 2010) : Recommended to the President of the Communications Commission transferring to private self-regulation bodies the current censorship system which suffers from the lack of prior notice and hearings and the vagueness of the censoring standards, thereby allowing arbitrary suppression of expressions and postings by administrative power.
53. **Private sector CCTV installation and operation** (November 25, 2010) : Recommended to the Minister

of Health and Welfare implementing the standards for CCTV installation and operation on public sanitation facilities and zoning the premises of public baths to keep cameras off the zones where people reveal 'special' or all body parts; and to the Minister of Government Administration and Safety and the Communications Commission administering prior licensing of private CCTVs, banning voice-recording CCTVs, and creating guidelines for security systems.

54. **Special Act for Punishment of Sexual Violence Crimes amendment** (December 30, 2010) : Opined that including in the disclosure provisions the photographs of the convicts' residences and the information on the neighborhood may infringe upon the human rights of the perpetrator, his or her family and the neighbors, and the disclosure should be limited to the publicly available level such as the official address and the actual residential address .
55. **In-house benefits electronic management systems** (April 28, 2011) : Opined that checking the service periods using QR Code and the resulting geolocation data does not constitute human rights infringement; that using personal data or personal geolocation data of the care-givers should be consented to by the care-givers; that attaching RFID tags to the beneficiaries should be explained, consented to, and vetted for any expression of objection, and the tag numbers should be encrypted; and that using the care-givers' mobile phones runs the risk of restricting informational self-determination and an alternative should be sought.
56. **City library reading space CCTV installation** (July 14, 2011) : Opined for running CCTA-installed reading spaces separately from non-installed ones and for seeking alternative methods of preventing thefts and property losses and installing CCTV as the last resort under full compliance with the relevant rules and regulations
57. **The former DNA Identity Verification Act bill** (related to 2011Hun-ma28 constitutional complaint) (July 25, 2011) : Opined that the constitutional complaint case is "an important case gravely influencing human rights protection and promotion" in relation to the inmates' informational self-determination under Articles 10, 17 and 37(1) of the Constitution
58. **Companies' mandatory personal data collection** (October 27, 2011) : Recommended investigating Cacao Inc.'s mandatory personal data collection and considering imposition of a fine; reviewing all companies' personal data collection practices; and implementing the data collection guidelines established on the users' informational self-determination rights.
59. **Smart schools' fingerprint-based identity verification system** (October 27, 2011) : Opined to the Chief of the Multifunctional Administrative City Construction Agency against installing fingerprint-based identity verification systems to check students' attendance.

Chapter 4

Suggestions for Promotion of ICTs and Human Rights

- **Section 1.** Reinforcement of Protection of Right of Information Privacy
- **Section 2.** Reinforcement of Freedom of Expression on the Internet
- **Section 3.** Reinforcement of Right of Access to Information
- **Section 4.** Reinforcement of Right to Enjoy Information and Culture

Section 1. Reinforcement of Protection of Right of Information Privacy

1. Alignment of Laws Related to Protection of Personal Information

- Unification of laws related to Protection of Personal Information Law such as, Telecommunications Law and Credit Information Law
  - Coherent application of a law bypassing the danger of double restrictions and monitoring
- Forerunning states have already proved that the principle of protection of personal information does not require separate application in online or offline, manufacturing or service industry, or any other sector of economy.

2. Revision of Administrative Structure for Protection of Personal Information

- Commission for Protection of Personal Information shall be reorganized into an independent and able body and compilation of all works related to protection into the commission.
  - Because the works are divided among various commissions and bodies, funding is wasted through unnecessary operation cost for bodies that concern same jobs
  - Different bodies have varying opinions on a same issue and they monitor each other which disables responsible propulsion of policies
  - Funding for the commission for protection of personal information is not independent and it only has the right to review and decide on issues without authority to conduct investigation which impedes them from work as independent protective body
- All 27 states in the EU have focused all works related to protection of personal information in a uniform body and the U.S. is running a similar apparatus.

3. Minimization of Risk of Human Rights Violation in Establishment and Running of Comprehensive CCTV Controlling Centers by Local Governments

- Problems occurred related to establishment of comprehensive CCTV controlling centers jointly initiated by ministry of administration and safety and local governments.
  - Unclear source of responsibility for the centers, multiple use of CCTV, lack of codes, conditions, and process related to sharing of information by local governments, police, and military, and lack of measure to prevent hacking and leakage of information have been pointed out as possible problems.
- Minimization of components that may violate human rights by creating a collaborative body comprised of human rights groups, NHC, and relate administrative bodies that installs and runs these centers
  - Specifying the purpose of installment and running of the centers
  - Minimization of sharing personal video footage and establishment of codes and conditions for sharing
  - Annual disclosure of results of operation to media and local communities.
  - Guarantee of participation to local residents, human rights groups, and local professionals in deciding on installment and operation goals, creation of codes and conditions, and use of funding

4. Protective Measures for Families and Close Ones of Offenders of Serious Crimes

- Creating measures to protect privacies of families, relatives, and neighbors of convicted criminals whose personal information have been publically released.
  - Statement of duty to protect family, relatives, and other close ones in special legislations on designated crimes and police operation codes for protection of human rights

- Establishment of duty to protect privacy and guidelines for interviews and reports for media producers

- Make consideration for Korean sentiment which upon public disclosure of personal information of criminals sees the crime not as a personal problem but as a product of family heritage or defective parenting

5. Improvements in Cyber Investigation and Collection of Digital Evidence

- Specification of basis and limits of seizure and searching for digital evidence to align them with principles of constitution.
  - Use of filtering system which mechanically choose and collect only information related to the case
  - Use of system in which mandates system managers to only choose and submitted ordered information upon specific and documented orders.
  - Establishment of duty, process, and method to return or destroy copied or collected digital information
  - Installment of a principle not to recognize validity of an evidence if information was collected through clearly illegal methods regardless of search warrants.
  - Application of principles of search warrants in provision of telecommunication information based on the related law
- Despite previous principles on criminal law on selective collection and collection of unusual medium, operational norm to collect whole of the data for the data's characteristic still persists.
  - Review the need for an institution to seek for an approval for collection and search for digitally stored information

6. Establishment of a Tool to Guarantee Transparency of Criminal and Legal Information System

- Establishment of a tool for transparency and stability of criminal and legal information system which has great risk of abuse and human rights violation
  - Disclosure of accurate information about types, range, and stored period of criminal and legal information recorded and stored in the system
  - Measure to protect privacy such as restriction of access to information that is prohibited from collection and storage
  - Establishment of operation codes specifying authority and range of access stored information which can easily be abused by a staff in charge
  - Differentiation of storage period and access based on the sensitivity of material
  - Establishment of codes for technical and managerial protection of database and a tool manage and monitor them
- As there are concerns for possible occurrence of the big brother and violation of privacy, minimization of types of information allowed to collected and recorded into the system for protection of human rights and private information

7. Revision of Operational Norm in Processing Private Information Based on Real Names and Restructuring of National ID System

- Change national ID number which indicates age, place of birth, and sex to random numbers and establishment of procedures to grant changes in ID number upon the court's approval
  - Alleviation of problems through unlimited generation of national ID numbers and checking for duplicate numbers using computer technology
  - Once the number is changed, it will be noted on the ID to disable identity theft of laundering
- Revision of legislations which mandates companies to collect real name and national ID numbers

- Complete revision of all laws that mandate or allow excess collection of national ID numbers.
- Constitution Court has unanimously decided mandating use of real names as unconstitutional (2012.8.23. Decision 2010Hun-Ma47, etc.)

- Stopping ministry of administration and safety's plan to use electronic ID
  - To tackle the issue of abuse and excess use of national ID, the ministry must lower dependency on the IDs rather than use electronic IDs

8. Establishment of Principles Regarding Collection and Use of Biological Information and Prevention of Abuse

- Advocating institutionalization of general principles on collection and use of biological information such as DNA à establishment of codes on protection and use of biological information based on article 12 of Personal Information Protection Law.
  - Although biological information is treated with extreme care for its unique, unchangeable, and continuous characters, South Korea lacks codes on processing these information
  - Recently, DNA databases are competitively compiled, collection and processing method of DNA sample, method of protection and storage of DNA information, methods of destruction of information, and other related methods lack adequate level of regulations and guidelines.
- Revisions on laws related to biological information such as legislation on use and protection of DNA identification and information
  - Penalty for abuse of DNA information is seriously lighter than that for cases involving general abuse of personal information, which can cost up to 5 years in prison or 50,000 dollar fine

9. Establishment of guidelines, restrictions, and procedures regarding Deep Packet Inspection

- Stop indiscriminate approval of deep packet inspection and find a suitable mechanism to effectively control range and method of deep packet inspection
  - Principle prohibition of deep packet inspection, and further limitation of crimes subjected to this inspection based on communication privacy law
  - Legal institutionalization of required conditions, procedures, range, method, period, and others
  - Institutionalization of disclosure of information of technological specifications of DPI
- Because DPI happens at in a comprehensive way, e-mails, searching, electronic transactions, and other private records are subjected to inspection
  - It is possible to look into use of internet by family members who share one computer and those who use same internet router on different computers
  - The Secretariat of National Assembly also pointed out DPI can be used to monitor entire privacy of citizens and is against principle of minimal intrusion

10. Reinstatement of Principles on Protection of Personal Information Regarding Big Data

- Modernization of the principle to fit current situation where big data and cloud computing are a reality to practically protect rights of owners of information
  - Establishment of guidelines, procedures, and preconditions for synchronization or compilation of data or database
  - Installment of Do-Not-Track function, Privacy by Default, Privacy by Design, Right to be Forgotten and others
- Although big data is considered to have a new IT technology that may contribute to efficient operation of governments and companies, it may have a huge cost of giving up private life and secrecy

- Therefore a mixture of facilitation of the technology and protection of privacy is required

11. Guidelines for Protecting Personal Information on Social Media

- Guidelines for disclosure and sharing of personal information to unspecified public or specific groups.
  - Restrictions on service providers from arbitrarily making personal information public
  - Giving information subjects the authority to control range and components of private information that is made public
  - Requiring provision of Do-Not-Track function that an information subject may use at anytime

Section 2. Reinforcement of Freedom of Expression on the Internet

1. Application of the Principle of Self-Regulation and Revision on the Mechanism to Review Illegal Online Contents

- As the second Universal Periodic Review, the first and second National Action Plan recommendation, report from UN Special Rapporteur, and recommendation from the National Human Rights Commision have recommended, the principle of self-regulation shall be allowed in regards to reviewing online contents to eventually make the commission a civilian organization
  - Despite NHC and international community's recommendations, censoring bodies such as Korea Communications Standard Commission for internet censorship still exists
  - Therefore, as advised in the second Universal Period Review, the state should

guarantee freedom of expression online, transfer powers of the Standard Commission, and suppress investigations, confinements, and criminal convictions that restrict freedom of expression and encourage self-censorship by individual citizens

- Description of illegal content in Act on Promotion of Information and Communications Network Utilization is too vague. It needs to be specified and limited.

2. Reinforcement in Guarantee for Freedom of Anonymous Expression

- Limited Identity Verification System based on Information and Communications Network Act in 2012 is declared unconstitutional for its violation of right to control one's information and freedom of expression
- However, mandatory use of real names on threads on elections based on Public Official Election Act and Internet Address Resources Act still exist
- The Constitutional Court decided unlike regular posts and threads, those discussing elections may require use of real names based on elections law; yet, it still added that freedom of anonymous expression is protected by article 21 of the constitution
- Considering that freedom of anonymous expression has historically contributed to advancement of democracy, strengthening of the power to do so in telecommunication network is needed

3. Protecting Freedom to Tell Truth

- Just like offline, online space should implement restrictions on principle against expressions that defame others
- Yet, if an information is disseminated only for the public good, despite its possible harm on others reputation, its illegality can be reconsidered. Therefore,

a broader interpretation of public good is required

- Although the High Court has consistently been broadly interpreting the cases with considerations for the information's publicness, contribution to public good, and reason to believe it is true, freedom to tell truth shall be consider for its own importance

4. Expansion of reasonable solutions for clash with right of information privacy

- Freedom of expression on the Internet should be guaranteed to the maximum level with a premise that it is an essential component for digital democracy
- Along with this, right of information privacy which is often violated with malicious online comments should be guaranteed to the maximum level
- If those two conflict, a settlement should be made in a way that is most fair and balanced

5. Abiding by the Principles of Restrictions on Freedom of Expression

- According to article 37 clause 2 of the constitution, limitations on basic rights should follow the principle of statutory reservation. This principle also applies online.
- UNHRC's general guideline also states that restrictions on freedom of expression shall only be implemented through a law, a state shall not give full authority to the policing body, and the law shall be in line with purpose and goals of international covenants.
- As for restrictions for obtaining national security, restrictions on information related to rightful public good without clear and practical harm to the national security would be breaking the principle of minimal restriction on human rights
- In case of restrictions, it shall be proceeded with very specific and careful application of laws

6. Revisions on Service Provider's authority to Delete or Blind uploaded contents

- Unless its original intent to quickly block out malicious online comments, it should be revised for its risk of blinding and deleting rightful criticisms on social public figures.
- In cases of constructive criticisms, if a normal citizen can fully understand the general customs and legal knowledge, allowing the dissenter to post an opposing opinion shall be considered

Section 3. Reinforcement of Right of Access to Information

1. Expansion of Guarantee of Right to Request Disclosure of Public Information

- With a Official Information Disclosure Act in place the right is guaranteed in at limited level, reasons and parameter of nondisclosure need to be specified
- Considering the criticisms that relocation of the commission to the office of minister of administration and safety from the office of the president has resulted in contraction of the commission's authority, the issue needs be considered
- Information managed under Act on the Management of Public Archives and those under information disclosure law greatly overlap. Overlapping parts need to be reorganized

2. Measures to Address the Digital Divide

- With definition of the digital divide through Framework Act on National Informatization, a legal foundation for measures to close the digital divide has been established. Yet, there are still undeniable gap because of sheer number of information deprived groups

- A measure must be taken to especially address the issues arising among elderly, disabled, and other social minorities.
- Despite the Act on the Prohibition of Discrimination Against Disabled Persons, REmedy Against Infringement of Their Rights and following measures to provide easy access to digital and non-digital information to disabled persons, there should be more proactive expansion in providing sign language and other services in national televisions
- Libraries Act of 2006 is serving as a clear legal foundation for citizen's right of access to information and right to know, unlike for non-disable persons, contents for disabled persons such as audiobook is extremely limited and therefore requires assistance in developing and producing contents in an alternative medium
- Based on Special Act on the Digitization of Terrestrial Television Broadcasting and the Promotion of Digital Broadcasting of 2008 regarding facilitation of digital broadcasting, all analogue television broadcasts will come to an end starting 2013. However, welfare recipients and those in similar situation will face difficulty benefitting from this change and the state must come up with a comprehensive plan to provide assistance
- Expansion of general service regarding disabled person and elderly persons' right to choose contents is also needed

3. Expansion of Right to Access Internet and Protection of Net Neutrality

- In an internet era, the digital divide or information gap comes from lack of access to information and the international community is also recognizing right to access internet as a new human right
- Counsel of Europe also in 2009 revised its Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services to recognize right to access internet as a basic right equal to freedom of expression.

It drafted and adopted a law that places a ban on website access restrictions and mobile application restrictions and guarantee of net neutrality to eventually add the concept to the European Commission's declaration.

- Korea-US FTA article 15.7 stated "as long as a customer does not impose harm to the network and the activity is not restricted to the state of event, one shall be allowed to connect a device of choice to internet."
- In South Korea's case in relation to net neutrality, as long as a customer does not impost harm to the telecommunication network, right to connect to internet through a device of choice and enjoy applications or contents shall be included into the right to internet access
- Also, the court shall make improvements on its websites to change current internet environment which only allows access through Internet Explorer

Section 4. Reinforcement of Right to Enjoy Information and Culture

1. Realization of the concept of right to enjoy information and culture.

- New installment of clauses regarding public use of contents in copyright laws
- Legalization of right to respond to excessive application of copyrights
- Guarantee public to access and remake information contents created with public funding
- Balanced harmony between intellectual property rights and right to enjoy information and culture.
  - Along with development of information technology, the right is on its way to becoming an important human right which enables access, production, and dissemination of information
  - As the second ASEM Human Rights Seminar recommended to its member

states, intellectual property rights and excessively strict protection of copyright can threaten enjoyment of human rights and suppress creativity in online spaces. Therefore, public benefit should always be considered in making and revising copyright laws

- As copyright was created with recognition of these types of human rights, it shall be implemented to recognize the rights of the users

2. Survey on Effects of Current Restrictions that Violate the Right to Enjoy Information and Culture

- Because most of copyright laws are created and imposed internationally, efforts made by sovereign states to guarantee the right is inherently limited
- Despite this, it is difficult to discern the right in any of the currently effective laws. Rather unique copyright protection laws and the game shutdown law are in place
- Three-Strike policy, technical protection, and game shutdown laws, which the effects are still unclear, shall be studied and examined for their harmful effects on the right and if the survey is conducted at an adequate level, the commission will possibly need to make recommendations to repeal those laws

ICTs and Human Rights

| Printed | November, 2014
| Issued | January, 2013

| Published by | Byung-chul HYUN
| Address | Gumsegi Bldg., Mugyoro 6, Jung-gu,
Seoul, Korea (100-842)
National Human Rights Commission of Korea
| TEL | +82-2-2125-9835 | FAX | +82-2-2125-0919
| Homepage | www.humanrights.go.kr
| Printed by | Hanhak Munhwa
| TEL | +82-2-313-7593 | FAX | +82-2-393-3016

ISBN 978-89-6114-359-2 93330