Journal of Engineering and Applied Sciences 12 (Special Issue 3): 6498-6509, 2017
ISSN: 1816-949X

Establishing Cyberspace Norms using Bright Internet Principles: In the Case of the Korean Legal System

Sang Pil Yoon and HunYeong Kwon
Graduate School of Information Security, Korea University,
02841 Seoul, Republic of Korea

Abstract: This study aims to investigate why the internet began to be regulated and why companies and users oppose government regulation. We also study cyberspace norms and suggest solutions by analyzing the bright internet principles. This study derives the normative value from the beginning of the internet and the intentions of its designer. And we analyze the relation between technology and norm and suggest the necessity of the bright internet principles to reduce the risks faced in cyberspace because of new technologies. Subsequently, we derive the legal nature of the bright internet principles and introduce legal measures to realize the principles by analyzing the legal system of Korea. Norms make up the social order through stability and predictability. However, all information and phenomena are interconnected; cyberspace has become more difficult to predict and various dysfunctions have been occurring. How should the norms be addressed to solve these problems? First, the norms should be able to comprehensively cope with cyberspace because the cyberspace can give rise to complicated social phenomena. Second, the person who caused the risk must be responsible. Third, in cyberspace, communication and action are carried out without any concept of border; therefore, international principles need to be established through mutual agreement. The bright internet principles best take cares of these aspects. The role of law is crucial because these principles have a legal nature. The legal system about the internet in Korea should be able to respond from a global perspective, establish international governance that can promote domestic legislation of many countries and raise the autonomy of citizens. Finally, we briefly mention that it would be possible to enact a framework (tentatively) named "framework act on the internet users". In addition, "the internet user policy committee" could be formed to encourage citizens to participate voluntarily.

Key words: WWW, cyberspace, internet, law, norm, bright internet principle

INTRODUCTION

Norms are rules or standards that govern our behavior in the social contexts in which we participate (Bierstedt, 1970). These norms provide order and give stability and predictability to society. Individual human beings and communities inevitably encounter disputes in their social activities which arise from their respective conflict of interests. In other words, the absence of norms would lead to social confusion making it difficult for society to survive. In this sense, norms are essential for complex social relationships.

With the advent of computers and the development of the internet, the cyberspace was formed. When the internet was first designed, it was open, free and convenient for all users (Benedek and Kettemann, 2014). There were no rules governing the internet and it was driven by the core values of openness and freedom.

However, one consequence of this internet freedom was the production of spam mails, defamations, insults and copyright infringements (Cukier, 2005). Currently, additional issues have been included to this list such as hacking, cybercrime, terrorism and cyberwar (WEF, 2016). Furthermore, the political aggression through cyberspace is becoming more serious. China is conducting cyber retaliation by hacking the Lotte homepage with regard to South Korea's deployment of THAAD (Cone, 2017). And there has been a controversy over Russia's involvement in cyberattacks in the US elections (Clarke and Volz, 2017). As these side effects are related to the characteristics of cyberspace, it is necessary to agree on international norms to regulate cyberspace.

The Bright Internet (B.I.) principles were adopted as a research vision by the Association for Information Systems (AIS), International Telecommunication Union (ITU) and International Federation for Information

Corresponding Author: HunYeong Kwon, Graduate School of Information Security, Korea University, 02841 Seoul, Republic of Korea

Processing (IFIP). The researchers at Korea Advanced Institute of Science and Technology (KAIST) in Korea and Tsinghua University in China are also conducting related research (Brook, 2017). Joint research on the international level means that a consensus has been formed on the necessity for establishing norms for peaceful cyberspace use; various nations are actively seeking the ways for doing this. In particular, Korea has the best information infrastructure. In this sense, analyzing Korea's legal system will be a model for establishing norms for the elimination of internet dysfunctions in other countries.

Based on this background this study re-examines the fundamental meaning and the philosophical value of cyberspace by analyzing the initial design process of the internet. We will derive the role of norms by discussing the characteristics of norms and the present state of the deteriorated cyberspace. Consequently, our aim is to analyze the B.I. principles in a legal way, assign and classify the Korean legal system to each principle and propose the role of law to realize the principles according to the characteristics of norms.

PHILOSOPHICAL SIGNIFICANCE OF CYBERSPACE AND ITS CRISIS

Intrinsic meaning of the internet: The internet began with the development of computers in the 1950's with the exchange of packets for connections between machines. Scientists who realized the efficiency of point-to-point communication developed a protocol and created a packet-switched network. In 1969, the Advanced Research Projects Agency Network (ARPANET) allowed several unconnected networks to be combined into a single network (Leiner *et al*., 1997). However, other networks based on the packet-switching technology used different protocols; therefore, there was a problem in communication between the separate networks. The more open protocol developed by Cerf and Kahn in 1974 was initially called the internet transmission control program which led to the connection of different networks and the birth of TCP/IP (Leiner *et al*., 1997). Therefore, the internet began with the concept of communication between machines.

The problem of communication or connection was solved with the development of the standard protocol but the internet has another attribute, that is, "access". At the end of the Second World War, MIT professor Vannevar Bush proposed the concept of memory extension (or Memex) to systematically record rapidly increasing information and to develop new technology. The goal was to collect all the information that humans had and store it in one place so that anyone could easily access it. In 1963, Ted Nelson invented the concept of "hypertext" which became the main concept used for linking. Subsequently, in 1980, Tim Bernes-Lee from the Conseil Europeen pour la Recherche Nucleaire (CERN) created a system that allowed researchers to upload and manage information in a space to exchange data and ideas efficiently. This was called the "ENQUIRE" program. These inventions were continuously supplemented and in 1989, the World Wide Web (WWW) project was launched as a system in which users could freely access any kind of information by connecting to the web. Bernes-Lee created the current basic concepts of the internet such as Hyper Text Transfer Protocol (HTTP), Hyper Text Markup Language (HTML) and the Web Browser. The initial WWW was used only within CERN but it became the basis of the internet through its public release on August 06, 1991.

The intention behind creating the WWW was to extend cyberspace from the individual domain to the public domain. The WWW also aimed to handle various kinds of information without any limits. It ensured smooth communication between tools and machines. To realize this, first, the information system needed to be able to associate all objects with one another. Second, each independent system needed to be incrementally connected around the link. Then, there would not be any need to perform unnecessary work such as the merging of databases. Third, it was pointless to restrict users to use a specific language or operating system. Fourth, the information needed to be available on all platforms. Fifth, people needed to be able to deal with information freely regardless of the device or the machine they used. Finally, the input and modification of information needed to be simple (Berners-Lee, 1996). Each of these principles could be summarized in terms of connectivity, accessibility, convenience, efficiency, autonomy and openness. The intent of the internet designer was that every user must be able to acquire, use and share various ideas and information without any restrictions. The main concept behind the internet was that it should be a place where anyone could access, connect and share information; this was the desire of all those who developed the internet.

We can "surf" the internet on the sea of information using hyperlinks. The information visible on the internet is the "public sphere" where users can share and communicate. The cyberspace is a place where anyone can have a conversation with anyone else and freely access and create programs or databases.

Philosophical value of expression

Relation of freedom of expression: The internet has various normative values in the light of its essential

design principles. The most prominent value is the freedom of expression. The internet is regarded as the most important "medium" after newspapers, radio and television (Dutton *et al*., 2010). The internet brought the greatest innovations in expression since the printing press (Ku, 2000). Freedom of expression is an essential value in a democracy. A democratic culture can be formed when all the members of society freely express their opinions, participate in the formation of culture and enjoy the interests of the community (Balkin, 2004). This can be done when all members of the society, not just the elite such as the politicians, lawyers, professors and doctors, can voice their opinions. It is noteworthy that the power of the "minority" who have not been able to voice their opinions in the traditional broadcast and print media is getting stronger by using cyberspace (Crump, 2003).

John Stuart Mill advocates and justifies the freedom of expression (Mill, 1869). According to him, freedom essentially means the power to resist political dominance, dictatorship and state violence (Mill, 1869). Therefore, the freedom of expression is not just a guarantee of freedom among private people but it is a guarantee of the freedom between the state and the individual. This means that the any type of act of suppressing the freedom of expression by state powers cannot be justified. In addition, individuals who express their views with one another (not with the state) should be open to criticism and suggestions as a means of finding the truth.

The opinions of certain members should not be ignored by the community because the role of the individual is very important while forming a diverse discourse. In this regard, John Stuart Mill emphasized the importance of the minority opinion. First, ignored or repressed opinions can be the truth (Mill, 1869). Second, even if opinions are not correct there may be some truth in the opinion (Mill, 1869). According to these two arguments, the freedom of expression seeks not only the formation of a democratic culture but also seeks the ultimate value of the discovery of truth. Even when there is only one different opinion that opinion cannot be said to be wrong it may be possible to reconcile with the disagreement or to obtain better results based on it. Third, even if the conventional views are certainly correct, most members can have a bias if they do not test these views using other opinions (Mill, 1869). Fourth, as a result of this, it is possible that the conventional views that many have sympathized with are recognized as dogmatic and prejudiced beliefs. This is because we cannot base our confidence on reason and experience (Mill, 1869). Therefore, we can conclude that public opinion formed without reviewing or reflecting on a minority opinion is not true or has not been evaluated for the truth. If social policy is enforced based on these pre-determined opinions, not only can there be various social costs but there would also be concerns about the damage to the essential value of democracy. It is necessary to supplement the majority opinion with minority views.

The function of freedom of expression can be summarized as the formation and development of personality through the self-realization of the individual, the maintenance and growth of democracy, the discovery of knowledge and truth and the balance between the stability and change of society (Emerson, 1970). The desire to express self-will is the most natural characteristic of humans. Therefore, freedom of expression has a superior position in most modern constitutions. Consequently, there is a strict criterion for judging the constitutionality for regulating the freedom of expression. In Korea, the constitutional court explained that the freedom of speech is a characteristic of the modern constitution and it has a superior position because it is the basis for the existence and development of the democratic state (Korea Constitutional Court in 1991). In addition, Article 1 of the United States Constitution (First amendment) provides freedom of expression without imposing any restrictions. Therefore, the freedom of expression is the central principle of the freedom and rights that are developed for the internet (Nak-In, 2009).

Diffusion of public sphere: Cyberspace forms a forum for enabling the freedom of expression in the course of deriving social consensus. The most important reason for the value of the public sphere is the fact that cyberspace has public domains such as internet cafes, blogs, social network services, work and conversation platforms, news articles and personal writings. Cyberspace expanded the public domain and constructed a new and more convenient public sphere (Jones, 1997). Jurgen Habermas defined the public sphere as "a space where the public is organizing itself as a bearer of public opinion as a space that mediates society and the state". He argued that free access to the public and the exclusion of privilege could lead to the rational legitimization of norms (Habermas *et al*., 1974). The post-medieval squares that existed for the sake of the status of the nobility and ruling classes, not for debates by citizens, could not be regarded as a public sphere. The origin of the public sphere can be said to be in early capitalism, in which newspapers emerged as a result of the development of media technology, the exchange of commodities and the active exchange of people. These changes were important because the media that could be accessed only by the intellectuals and elites became easily accessible to everyone; the common citizens recognized this and

questioned the status quo. Decisions were not being made only in the private domain with only a small number of members participating, discussing and deciding on the agenda. Discussion in the private domain was taken out on the public domain which had a great influence on the social consciousness. Therefore, cyberspace played a major role in the public sphere by expanding from the private domain to the public domain which was made possible by connectivity and free internet access. Through this, various opinions on diverse social issues could be converged quickly and easily this had a great influence on resolving various issues (Young, 2006).

In addition to forming a public domain, another important function of the cyber public sphere was diffusion. The various discussion fields in cyberspace function by selecting various agendas of society and spreading them through interactions. Therefore, cyberspace played the role of a medium. The media fulfills the fundamental thirst of humankind to share ideas and knowledge. If we think back to Marshall Mcluhan's theory that "the medium is a message", cyberspace itself can eventually become a message. Furthermore, with the development of the Internet of Things (IoT) which includes smartphones, tablet PCs and fixed spaces such as desktops, cyberspace has come into contact with human beings in all spaces. These changes mean that a human being's thoughts can be expressed in cyberspace at any time and opinions become diversified and spread quickly. However, it is well known that these features often have negative effects in the real life and in cyberspace.

Influence of cyberspace on reality: Ultimately, cyberspace should aim at realizing the value of democracy. Open spaces enable free access and efficient sharing of information and opinions; consequently, it contributes to the promotion of freedom of expression by forming the public sphere. Furthermore, the characteristics of cyberspace ultimately lead to the stability of society and the formation and development of knowledge and truth.

Given these circumstances, it was earlier thought that there should not be any regulatory system for cyberspace which would secure maximum freedom for users. Governments recognized cyberspace as a place that they could not regulate; users could freely express their opinions on this medium (Lessig, 1996). Even laws were perceived to be useless because of the emergence of cyberspace (Lessig, 1996). However, cyberspace has been causing side effects for a long time. In contemporary society, the problems that arise in cyberspace including the internet have enormous influence on the real lives of human beings; therefore, the situation needs to be regulated. This is because behavior on cyberspace inevitably affects individuals and organizations in reality. In fact, the distinction between cyberspace and real space is becoming blurred (Lessig, 1999).

Cyberspace affects reality in different ways. Shapiro mentions three major changes arising from the internet (Shapiro, 1999). First, power is shifting from organizations such as the state governments to individuals; second, these changes lead to conflicts between organizations such as the government, corporations and the media, Third, the confusion hinders predictability, resulting in life changes in which various side effects occur. Furthermore, these uncertainties bring new challenges and threats to internet users, regulators and legislators (Farrell and Weiser, 2003).

Risks of cyberspace and role of norms

Relationship between technology and norms: A norm is a rule or standard that all members of society identify with and it is a concept that governs our actions in society (Hun-Yeong, 2009). Norms are built up by experiences and customs. However, the nature of technology and its rapid evolution pose a range of unforeseen problems that cause a variety of social and ethical dilemmas (Tene and Polonetsky, 2013). Even before norms such as customs, morality, ethics or law are formed, new technologies are pouring in and causing fresh problems.

Thus, norms face serious challenges because of the arrival of the technology-oriented society. In the case of laws that most closely affect reality before the essential norm like ethics, there is a kind of normative lag in that the enactment procedure cannot avoid the coordination of various interests, social consensus and political relations (Tene and Polonetsky, 2013).

The reason for this situation is the problem caused by the characteristics of the technology itself. Legislative procedure is based on discipline through prognosis; therefore, besides fact-finding, it requires diagnosis and evaluation of the subject matter of the legislation and determining the future prospects of legislative processes. However, in the case of technology, it is difficult to predict the social impact of technological advancement; therefore, it is impossible to investigate, diagnose and evaluate it. Furthermore, legislators generally have limited knowledge of technology; therefore, they cannot predict the side effects of introducing and using technology. Therefore, participation of experts in each field is essential. The process of legally interpreting and accepting these technical opinions requires agreement through a process of public involvement because it is tied

to various interests. Eventually, the set of processes for legislation includes normative uncertainties arising from the absence or lack of expertise.

In addition, the rapid development of technology causes two major problems. The first problem is the effect of the speed of the development of technology on the establishment of norms and laws. In this case, the pace of technological development necessarily accompanies the absence or distortion of laws when examining the process of establishing norms and laws. Moore's law explains that the density of microchips doubles every 18 months and technology is growing exponentially (Moore, 1965). In addition, Ray Kurzweil's law of acceleration says that the development that took place in 100 years in the 21st century is equivalent to the rate of technological development of the past 20,000 years. Moore's law refers to the singularities in information technology, especially the influence of artificial intelligence (Kurzweil, 2004). Therefore, in the legislation process, it is becoming harder to respond to the development of technology. The second problem pertains to the attributes of the development process of technology and law. Technology is fundamentally fluid and has the property of continuous development. However, the law remains relatively fixed in that it seeks legal stability or some degree of permanence in its procedures. It is reasonable that norms and laws should also be changed to meet the demands of society; however, trust in the normative role of the law is derived from its legal stability. Therefore, the nature of the law is inevitably confronted by changing technologies.

The development of technology and the crisis of cyberspace

Conflict between state and individual: Traditionally, we have been able to express opinions freely through the Web because of its promptness, openness and anonymity. However, these characteristics have also given rise to other problems such as disagreements on the views expressed by certain members on cyberspace. As a result, the state governments began to regulate certain expressions and there arose controversies as to whether the freedom of expression was being excessively limited or distorted (Spinello, 2001). The side effects of internet freedom such as fraud, insult, defamation, false information, impersonation and hacking, need to be restricted; however, restrictions would inevitably involve state control. In particular, even though all individual opinions must be respected, it is not necessary to permit malicious, abusive or offensive expressions. For example, the Constitution of the Republic of Korea states certain restrictions on the press and publishing in light of this: Article 21(4) "Neither speech nor the press shall violate the honor or rights of other persons nor undermine public morals or social ethics. Should speech or the press violate the honor or rights of other persons, claims may be made for the damage resulting therefrom". In such cases, the restriction must be based on laws and should not unduly invade the essence of freedom of expression. And Article 37(2) "The freedoms and rights of citizens may be restricted by act only when necessary for national security, the maintenance of law and order or for public welfare. Even when such restriction is imposed, no essential aspect of the freedom or right shall be violated". (The Constitution of Korea). However, legal measures for the stabilization of cyberspace invariably limit the freedom of expression either intentionally or unintentionally. It is clear that appropriate restrictions on some expressions can enhance the expression of sound thoughts and opinions. However, the freedom of expression in the media and the normative value of the public sphere are clearly perceived to be fundamentally threatened by the intervention of the state.

Until these problems are solved, the influence of the individual in cyberspace will get bigger with the development of internet of things based on big data. Therefore, it will be difficult to control individuals; however, government intervention in the market has been further strengthened such as by the control of internet Service Providers (ISPs). Furthermore, with advanced technologies such as deep packet inspection and server monitoring, it is possible to track individuals, thereby increasing concerns of state control over citizens. For example, Edward Snowden and NSA surveillance case on June 10, 2013 caused global controversy over the country's surveillance issue. Furthermore, recently, the WikiLeaks exposed CIA hacking tool (Pagliery, 2017).

Increasing the malicious infringement on rights: With the development of big data technology, all digitized information including personal information is treated as property. Digital data is expanding the economic scale and scope in terms of both supply and demand because of its characteristic of being able to be quickly collected and used without being destroyed (OECD, 2015).

As a result, cybercrimes such as hacking and information leakage through cyber attacks are increasing rapidly. According to Symantec's internet security threat report, cybercriminals are becoming increasingly focused and are strategically targeting high-value-added intellectual property based on professional and organizational behavior. It is difficult to respond to cybercrime because it is not easy to prove it and there is no concept of border in cyberspace. This leads to legal problems like investigative coordination and

responsibility attribution. As part of the response, the Budapest Treaty was signed in November 2001 to enable countries to work together to tackle cybercrime but the technical barriers remained. For example, the results of the cyber attack analysis of 2016 revealed that 33.1% of the attacks were unknown, 15.1% of the accounts were hijacked, 11.6% of the target attack and 11.3% attacks were the Distributed Denial of Service (DDoS). It is difficult even to grasp the techniques used for the new attacking methods. Information leakage accidents are also becoming very large. In 2015, there were nine major security accidents involving more than 10 million personal information leaks. Companies tend not to disclose incidents; therefore, the estimated number of leaks in 2015 was approximately 5 billion.

Cyber terrorism and cyber war are also becoming a real threat. The concept of cyber war has come about because of the Stuxnet attack on Iran's nuclear facilities in 2010. Attacks on the national infrastructure are also increasing (Hathaway *et al*., 2012). Hacktivists use hacking as a political struggle. Cyber attacks by countries have also shown that issues pertaining to international politics and ideology are surfacing on cyberspace. Behind the e-mail hacking case of the US presidential election in 2016, CIA concluded that Russia intervened to help Donald Trump. And the North Korea was involved in the SWIFT hacking case with suspicion of specific state involved in Yahoo case. Cyber attacks are spreading to material damage. In addition, well-designed malicious code can be used to paralyze the internet at wartime (Aldesco, 2002). The development of IoT has enabled the hacking of smart phones, smart TVs, self-driven cars and so on which has resulted in the invasion of privacy and property and has caused personal injuries. For example, Chinese researchers have proven that hacking Tesla's cars can actually cause confusion (UN, 2017).

Proliferation of normative confusion: In addition to cyber attacks such as hacking, there is also a problem of content layers between users. An individual can express various thoughts and opinions or make content using internet broadcasting. In internet broadcasting, various contents are generated regardless of the genres such as literature, comedy, report, contest or drama. However, objectionable contents such as obscene content and live broadcasting of suicides have also become a social issue. For example, due to the suicide broadcasting on the Facebook, there are social discussions that taking place to introduce technical or institutional regulation to prevent this (Kelion, 2017; Tae-Yeong and Kyu, 2015). Other problems include malicious comments, cyber defamation, the spread of false news, extreme political disputes, online recruitment of terrorists and so on. Furthermore, now it has become imperative to reevaluate human inputs because of the development of artificial intelligence technology which includes autonomous robots and their copyrights, contracts, jobs, damages and distribution of responsibilities. It is becoming increasingly difficult to resolve normative confusion.

Necessity of establishing fundamental principles: The greatest threat posed by science and technology to our normative consciousness emerges from the discussion on the emergence of the "autonomous robot" based on "Strong AI". This does not imply a problem such as the trolley dilemma or who should be responsible when the "autonomous robot" becomes too universal. Rather, it is a question that challenges Descarte's philosophical proposition that "man is human only when he thinks". In other words, nature is a huge and precise machine; if the human body is the part of this nature, the development of intelligent information raises the fundamental philosophical question "what will you do now?" We are now faced with a big and threatening confusion of identity. The overall normative issues including ethics and law are on the surface (Zeng, 2015). If we suppose that normative entropy is maximized in the dilemma of conflict between efficiency and ethical norms, just like a dissonance between capitalism and democracy, then we need a guarantee of trust and safety. Therefore, we need to urgently establish a principle based on it.

Direction of norms

Construction of comprehensive response system: Crisis in cyberspace does not remain isolated and it causes bigger and more diverse damages. The fundamental nature of the internet affects the outcome. Also, it is fundamentally difficult to respond to changes in technology. Even if legislation has been adopted as a normative response, technology continues to evolve and requires constant revision. Furthermore, there are problems such as whether or not industrial development is hindered because of excessive regulation of technology.

In the midst of various problems of how to respond, the crisis of cyberspace grows out of control. In particular, the problems in cyberspace are connected to one another and the inherent limitations of normative responses and the different ways of institutional responses of different countries cause other problems. For example, in the case of the problem of personal information transferred abroad, the European Court of Justice declared that the Safe Harbor Agreement was void

in October, 2015 and it has made the United States accept the EU's enhanced privacy standards. In addition, a normative system needs to be established that can respond in a comprehensive manner; this needs to include cooperation systems and organizations for prompt legal responses.

Establishing clear responsibility structures: The problem of responsibility is an essential element in discussing normative responses. Legal relationships that are represented by rights and obligations necessarily require responsibility for actions taken by the subject. In this regard there may be various problems in cyberspace.

For example, it may seem reasonable to take direct responsibility for a hacker in case of a personal information leak caused by his or her act. However, if an individual is a hacker, there is a problem of whether he or she can pay damages for personal information leaked in large quantities. In reality, the question arises whether or not the hacker's country should compensate in terms of technical difficulties introduced by national laws which make it difficult to identify the hacker. If this conflicts with the relationship of power between nations, it will be necessary for nations and companies that have relatively low military or economic strength to assume responsibility. In this respect, there is a liability problem of the domestic company, especially the ISP. Recently, there has been a tendency to introduce punitive damages (punitive damages are system intended to reform or deter the defendant and others from engaging in conduct similar to which formed the basis of the lawsuit) but this does not help solve the fundamental problems. Therefore, the norms should set the accountability principles and should be able to provide standards for the countries to comply with. Furthermore, it is necessary to prepare measures to enable the smooth collection of evidence when proper and transparent procedures are used as procedural issues for the identification of responsibility.

Seamless international cooperationl: The internet has made globalization real by having a profound impact on the whole world (Ferdinand, 2000). When considering the characteristics of cyberspace, the relationship with other countries must also be considered to establish a comprehensive response and a clear accountability structure. Without cooperation between nations, the problem of comprehensive response or responsibility cannot be solved.

In essence, these normative directions presuppose mutual trust. The question arises as to whether international laws such as international common law and treaty have force in this area. Nonetheless, international norms are required because they provide directions for the implementation of justice in the international community. International norms are required as a minimum norm and they should be accompanied by an endeavor to comply with the principles based on mutual trust and consensus. Therefore, the internet will ultimately contribute to the improvement of democracy when mutual trust among users is guaranteed (Schwartz, 1999).

BRIGHT INTERNET PRINCIPLES AND THE APPLICATION OF LAW

Background and concept of bright internet principles: In December 2015, Professor Lee Jae-Kyu of the KAIST announced the B.I. principles at the Association for Information Systems (AIS); the goal was to establish international organizations and global internet principles using technology and policy. In particular, the MOU between the AIS and International Telecommunication Union (ITU) was a concrete move to realize internet peace (Brook, 2017). The B.I. principles are the blueprints of the internet they are designed to eliminate the side effects of the internet. They consist of six principles: origin responsibility, deliverer responsibility, identifiable anonymity, global digital search, privacy protection and peaceful internet society (Lee, 2016). We briefly explain these six principles in the following paragraphs. For more details, please refer to Lee (2015).

First, the principle of origin responsibility states that a person who has committed malicious acts in cyberspace must be responsible for the outcome of his or her actions. It is a very basic principle but it is a completely different concept if we think about the accountability structure currently built in cyberspace. In the current cyberspace, the person or organization whose information was leaked is supposed to be responsible. For example, if a company's customer information is leaked by an attacker, the company is penalized for not taking the appropriate measures to protect the information. However, this is essentially the same as distributing elsewhere the responsibilities of the attacker. This does not mean that the company does not have an obligation to protect information. This principle seeks to establish the concept of preventive security and make the attacker responsible. Therefore, it is the most important principle.

However, the application of the principle of origin responsibility is not practical. The principle of deliverer responsibility seeks to overcome these limitations. Most cyber attacks are not done by attackers directly through their own IP addresses but by bypassing the IP addresses several times through various paths. In other words, after

acquiring rights to another PC by bypassing the security system of the PC or the computer system, a large amount of packet transmission or spam mail is sent for the cyber attack (Raiyn, 2014). However, the measures to cope with this are simple. Even if the attackers are not sending mail from their own addresses, the receiver should be able to block the message if it plays the role of a mediator in the middle of network. Therefore, it is necessary for the subjects of cyberspace to have certain powers and duties such as giving the ISP the right to deny service to spammers.

To realize these principles, there should be confirmation of objective facts. According to the origin responsibility, even if the IP that provided the cause is found, attackers do not use their real names to commit the crimes. Therefore, if a criminal act is confirmed, it should be possible to trace the real name of the attacker without impinging on the right to remain anonymous. This is the principle of identifiable anonymity.

Malicious codes are often sent to countries on the other side of the globe. Therefore, if a cyber attack is detected and its source and sender are identified, tracking and investigation should be possible in real time without delay. It is difficult to respond to the billions of spam e-mails and cyber attacks using the existing criminal cooperative system. Therefore, real-time digital investigation rights should be made internationally based on rules through the principle of global digital search.

In the course of the investigation, the privacy of innocent users must be protected. Sensitive information is directly linked to privacy in a big data environment and it is easy to use in criminal activities. Furthermore, the problems related to privacy are likely to lead to the problem of surveillance by the state in the course of the investigation. These problems are accompanied by a breach of privacy in the enhancement of national security. Therefore, the principle of privacy protection must be followed to minimize information breaches and enhance security.

Finally, the norms at the national level should be established through the principle of peaceful internet society. This can be composed of any entity such as individuals, corporations, criminal groups, terrorists and nations. In particular, cyber warfare at the national level should be strictly regulated. Therefore, the internet should not be used as a way to attack other users of cyberspace.

The legal nature of bright internet principles and the Korean Internet Legislation

Legal analysis of bright internet principles: The content of the Bright Internet Principles (B.I. Principles) have a legal nature which includes punishment, prevention and mutual cooperation; therefore, the role of the law is essential. These principles can be roughly classified into four types according to legal characteristics. The principles of origin and deliverer responsibilities concern responsible conduct on the internet. The legal liability is very diverse but largely classified as criminal, civil and administrative. The principle of identifiable anonymity and global digital search are the procedural principles to substantiate the relationship of rights of the first and second principles and introduce various procedural problems and technical requirements. This can be divided into traditional procedural law like the criminal procedure act, the civil procedure act and the related laws that regulate technical requirements. The principle of privacy protection may be applicable to laws and regulations governing the obligation to comply with confidentiality including privacy. The last principle (Peaceful Internet Society) is the domain of international public law but in Korea, it can be specified in various laws dealing with national security.

Environmental and geopolitical implications of Korean Internet Legislation: Korea has the world's best ICT development index and the most well-developed information infrastructure. According to ITU's ICT Development Index 2016, Korea ranks 1st in both 2015 and 2016 (ITU) and Korea ranked 1st in the UN e-Government evaluation for 6 years (UN, 2017). However, a well-established information infrastructure means that Korea is more prone to cyber attacks and other side effects. For example, China produced the highest cyber attacks in 2015 including Botnet and Zombie PC. These attacks happened because in 2013, the Chinese government announced plans to expand the bandwidth for computer distribution, expand all networks and increase internet speeds throughout China including the rural areas. This exposed Korea to the most cyber attacks. In the second half of 2015 according to APT exposure rates by region, the exposure of Korea is 38% which is approximately 15% of the world average and approximately 2-3 times more than that of the United States (FireEye, 2016).

From the viewpoint of international relations, Korea is a very important nation. Korea is still the only country at war and it has close relations with China, Russia, the United States and Japan. Therefore, analyzing Korea's legislative system about the internet can have implications for developing countries that are in the process of informatization and these countries can adopt the B.I. principles.

Table 1: The relationship between the B.I. principles and Korean internet and ICT legislation

B.I. principles	Legal nature	Legislative classification	Legislation
Origin responsibility	The responsibility of the actions	Criminal responsibility	Criminal act, juvenile protection act, act on promotion of information and communications network utilization and information protection, etc., personal information protection act, national security act, military secret protection act, copyright act, act on the protection of information and communications infrastructure, act on prevention of divulgence and protection of industrial technology, framework act on telecommunications
		Civil responsibility	Civil act, act on promotion of information and communications network utilization and information protection, copyright act, broadcasting act, personal information protection act, act on the development of cloud computing and protection of its users
Deliver responsibility		Administrative responsibility	Monopoly regulation and fair trade act, act on the consumer protection in electronic commerce, etc., act on promotion of information and communications network utilization and information protection, etc., framework act on consumers, personal information protection act, broadcasting act, framework act on national informatization, act on the protection of information and communications infrastructure
Identifiable anonymity	Procedural and technical requirements to prove the relationship of substantive rights	Traditional procedures	Criminal procedure act, civil procedure act
Global digital search		Technical regulations	Act on promotion of information and communications network utilization and information protection, internet address resources act, framework act on telecommunications, telecommunications business act, law and regulations on standard, technology and safety
Protection of privacy	The obligation to protect various secrets and privacy	Protection of privacy	Personal information protection act, act on promotion of information and communications network utilization and information protection, protection of communications secrets act, act on the protection, use, etc. of location information, framework act on national informatization, act on the development of cloud computing and protection of its users, internet address resources act
		Obligation of confidentiality	Protection of communications secrets act, military secret protection act, attorney-at-law act, medical service act, act on the protection, use, etc. of location information, act on prevention of divulgence and protection of industrial technology, framework act on national informatization, act on anti-terrorism for the protection of citizens and public security, act on special cases concerning the punishment, etc. of sexual crimes, sexual violence prevention and victims protection act, regulations on the security affairs
Internet peace	International public law and national security	International cooperation	National security act, act on the protection of information and communications infrastructure, act on anti-terrorism for the protection of citizens and public society, national intelligence service act, act on the performance of duties by police officers, law and regulations on cyber security

The relationship between B.I. principle and Korean Internet Legislation: Table 1 shows the results of analyzing Korea's internet legal system according to the B.I. principles. First, the principles of origin and deliverer responsibilities that govern liability for conduct are classified into laws that regulate individual fields in addition to criminal and civil law. The laws regulating criminal liability include the Criminal Act, the Juvenile Protection Act and Act on Promotion of Information and Communications Network Utilization and Information Protection. Other laws, except for the Criminal Act are classified by checking the penal clauses of individual laws and regulations. Typically, the act on promotion of information and communications network utilization and information protection have penalty provisions associated with the collection of personal information, notice and consent, transfer, leakage, insufficient technical and administrative protection measures, contents related to harmful media, pornography, defamation, commercial advertising information and so on. The civil liability is regulated by the Civil, Copyright and Broadcasting Act and these acts contain the civil penalties on copyright infringement in cyberspace related to broadcasting regulations in the field of information and communication. In the case of administrative responsibility, we identified and classified the provisions of administrative measures such as fines and the suspensions of businesses and laws and regulations of individual sectors. When there is a lack of safety measures, the personal information protection act makes it obligatory for the personal information protection manager to notify the public after taking various measures to protect the personal information.

The principle of identifiable anonymity and global digital search includes procedural and technical requirements. In addition to the Criminal Procedure act and Civil Procedure act, the individual sectors have various legislations. For example, the various technical

standards and safety standards are regulated by Internet Address Resources Act, Framework Act on Telecommunications, Act on the Protection of Information and Communications Infrastructure and so on. For example, the Act on the Protection of Information and Communications Infrastructure includes analysis of vulnerabilities, criteria for evaluation and guidelines for protection. The Internet Address Resources Act includes the allocation of internet protocol address and the prohibition of registration of malicious domain names.

The principle of privacy protection includes the Personal Information Protection Act, the act on promotion of information and communications network utilization and information protection, the act on the protection, use, etc. of location information and so on. These laws include obligations for revealing personal information such as the residence number and other sensitive information and taking appropriate information protection measures. Laws related to confidentiality include the Protection of Communications Secrets Act, Military Secret Protection Act, Attorney-at-Law Act and Medical Service Act.

Finally, the principle of internet peace is related to international cooperation between nations and organizations. For example, the act on the performance of duties by police officers includes the application of confidential information provided by the United Nations forces and foreign countries. This information needs to be applied in relation to national security, secret management, restrictions for national security and the prohibition of leakage in the National Security Act, Act on Anti-Terrorism for the Protection of Citizens and Public Society and so on.

Legal response to realize the B.I. principles: Legislators need to be aware of the following to realize the B.I. principles. First, the contents of the principles should be addressed from a global perspective, considering international politics, international consensus and the role of international organizations. Although, the contents of the general statutes set the actual contents in accordance with the international convention and standards, it is difficult to respond effectively to procedural problems. For example, the personal information protection act specifies eight principles in accordance with the OECD guidelines on the protection of privacy and transborder flows of personal data, 1980. In addition, Article 14 of the act stipulates that "The government shall establish necessary policy measures for improving the protection level of personal information in an international environment and to ensure that the transborder transfer of personal information does not infringe on the rights of an owner of information". However, the content of this law covers the information protection of the people in the international environment rather than the contents of international cooperation in general. Of course, user protection is important. However, it is time to reconsider what is necessary to protect and to what extent. In addition, the contents of general laws concerning international cooperation such as the National Security Act and the National Intelligence Service Act, mainly consist of the security point of view. Eventually, the issues to be solved must be reanalyzed and agreed between governments and this takes additional time and money.

Second, domestic legislation should be swiftly implemented to ensure that Korea has strong international links. While implementing domestic legislation, priority should be given to forming consensus for the establishment of legislative realization. In other words, various public and private organizations should work together organically to form a discussion framework and it is essential to establish a control tower that can integrate the interactions. The control tower must be situated at an international organization or an international community. The global debate environment and the consensus of nations can be formed through this and it will be possible to promote the governance structure to the highest level in individual countries.

Third, as a fundamental problem, laws and institutions should aim not only to protect users but also to interact autonomously and subjectively with internet technology. As in the case of the above-mentioned personal information protection act, a blind protective structure constitutes a structure in which only the rights to a country or an ISP are sought without having any obligations. In fact, these problems are based on the overall Korean internet legal system. Korea has failed to cope with the side effects of the process of informatization whenever problems have arisen, some quick solutions have been provided by state-led workers. Basically, users should be able to solve problems that occur in the field by voluntarily using technology. To do this, users have the right to be supported so that they can raise their basic competencies. Along with these initiatives, ethics and education are also needed. Furthermore, progress can be made with development by referring to the various privacy infringements including the problems about information protection occurring in each country.

Recently, in celebrating the 28th anniversary of the birth of the World Wide Web, its founder Tim Bernes-Lee expressed grave concern (Bernes-Lee, 2017).

Today marks 28 years since, I submitted my original proposal for the World Wide Web. I imagined the web as an open platform that would allow everyone everywhere to share information, access opportunities and collaborate across geographic and cultural boundaries. In many ways, the web has lived up to this vision though it has been a recurring battle to keep it open. But over the past 12 months, I've become increasingly worried about three new trends which I believe we must tackle in order for the web to fulfill its true potential as a tool which serves all of humanity.

Tim Bernes-Lee has warned of three threats. The first is that web users lose their control over data. Second, the web is flooded with false information. Third, there is insufficient transparency of politics on the internet. In this regard, people must face the government's surveillance and portal companies that are building large platforms should delete illegal or false information. To do this, users must directly check the transparency of processes and request that the public environment be rebuilt.

CONCLUSION

The internet provides an open space where anyone can participate, thereby ensuring free communication among users, enhancing the efficiency of human life and contributing to the realization of democracy. Recently, however, the internet environment has been facing a normative crisis because of cyber attacks, cyber terrorism, warfare, illegal content and ideological confusion caused by national regulation to create a sound cyberspace. In such a situation, norms should be able to present a comprehensive response system that can cope with problems that are interlinked and an international consensus is needed to establish and realize a clear responsibility structure.

The B.I. principles propose preventive measures and countermeasures against the side effects of the internet in a confused cyberspace. The principles of international communication and consensus are set in order to replace the self-defense concept with a preventive concept and to advance the procedure. Through this, it will be possible to create an environment in which users or members can freely and securely communicate through the internet by retaining the essential nature of the internet mentioned above.

It is clear that laws play an important role in realizing a desirable cyberspace. However, there needs to be sufficient social consensus so that everyone cooperates. Further efforts need to be made so that individuals can take responsibility and establish and observe the norms to overcome the chaos of the information age. In this regard, the B.I. principles assign the responsibility to the source of malicious code or the sender of information and suggest that the person who attacks is responsible.

Therefore, the most important thing is both the acceptance of the principles and the realization that the contents should be accompanied by autonomous efforts to build the trust of cyber space members. If citizens and netizens want to make their own decisions, their rights can be strengthened. Ethical issues, information gaps and flaws in professionalism can be problematic in the process. A system can also be created that solves the problems. For example, by establishing the (tentatively) named act "framework act on the internet users", it is possible to form "The committee on the internet user policy" which can flexibly reflect the internet and the information technology policies with representation from citizens. The committee's functions may include a citizen's reporting system for internet technology policies and trends aimed at information equality. It can also include a civic education program to support user autonomy besides identity enhancement to make subjective decisions about information technology.

Using the suggestions given in this study, people can act as the main agent for the formation and improvement of the internet environment, technology and legal systems. Consequently, the rights of users will grow naturally in the process of carrying out the responsibilities and the cyberspace can be normalized.

ACKNOWLEDGEMENT

This research was supported by the National Research Foundation of Korea Grant funded by the Korean Government (NRF-2014S1A3A2044645).

REFERENCES

Aldesco, A.I., 2002. The demise of anonymity: A constitutional challenge to the convention on cybercrime. Loy. L.A. Ent. L. Rev., 23: 81-86.

Balkin, J.M., 2004. Digital speech and democratic culture: A theory of freedom of expression for the information society. NYUL. Rev., 79: 1-4.

Benedek, W. and M.C. Kettemann, 2014. Freedom of expression and the internet. Council of Europe, Strasbourg, France, Pages: 173.

Berners-Lee, T., 1996. WWW: Past, present and future. Comput., 29: 10-70.

Bernes-Lee, T., 2017. Three challenges for the web, according to its inventor. WWW Foundation, Francisco.

Bierstedt, R., 1970. The Social Order. McGraw-Hill Kogakusha, Tokyo, Pages: 208.

Brook, P., 2017. AIS bright internet ties with UN ITU. AIS, Tokyo.

Clarke, T. and D. Volz, 2017. Trump acknowledges Russia role in U.S. election hacking: Aide. Reuters, Canary Wharf, London, UK.

Cone, A., 2017. Website of Korea retail giant Lotte hacked in China. Unified Payments Interface, Maguindanao.

Crump, C., 2003. Data retention: Privacy, anonymity and accountability online. Stanford Law Rev., 56: 191-229.

Cukier, K.N., 2005. Who will control the Internet-Washington battles the world. Foreign Aff., 84: 7-10.

Dutton, W.H., A. Dopatka, M. Hills, G. Law and V. Nash, 2010. Freedom of connection freedom of expression. UNESCOs, Paris, France.

Emerson, T.I., 1970. The system of freedom of expression. Random House Trade, New York, USA.

Farrell, J. and P.J. Weiser, 2003. Modularity, vertical integration and open access policies: Towards a convergence of antitrust and regulation in the internt age. Harv. J.L. Tech., 17: 85-134.

Ferdinand, P., 2000. The internet, democracy and democratization. Democratization, 7: 1-17.

FireEye, 2016. Domestic cyber attacks and ransomware trends. FireEye, Milpitas, California, USA. https://www.fireeye.kr/company/press-releases/2016/fireeye-announces-trend-of-cyber-threats-to-south-korea.html.

Habermas, J., S. Lennox and F. Lennox, 1974. The public sphere: An encyclopedia article (1964). N. Ger. Critique, 3: 49-55.

Hathaway, O.A., R. Crootof, P. Levitz, H. Nix and A. Nowlan *et al*., 2012. The law of cyber-attack. California Law Rev., 100: 817-885.

Hun-Yeong, K., 2009. Conditions for legitimacy of internet regulation in Korea. Public Land Law Rev., 46: 207-207.

Jones, S.G., 1997. The internet and its social landscape. Virtual Culture Identity Commun. Cybersociety, 7: 22-35.

Kelion, L., 2017. Facebook artificial intelligence spots suicidal users. BBC News, London, UK.

Ku, R.S.R., 2000. Open Internet access and freedom of speech: A first amendment catch-22. Tul. L. Rev., 75: 88-127.

Kurzweil, R., 2004. The Law of Accelerating Returns. In: Alan Turing: Life and Legacy of a Great Thinker, Christof, T. (Ed.). Springer, Berlin, Germany, ISBN:978-3-642-05744-1, pp: 381-416.

Lee, J.K., 2015. Research framework for AIS grand vision of the bright ICT initiative. MIS. Q., 39: 3-12.

Lee, J.K., 2016. Invited commentary: Reflections on ICT-enabled bright society research. Inf. Syst. Res., 27: 1-5.

Leiner, B.M., V.G. Cerf, D.D. Clark, R.E. Kahn and L. Kleinrock *et al*., 1997. The past and future history of the internet. Commun. ACM., 40: 102-108.

Lessig, L., 1996. The zones of cyberspace. Stan. L. Rev., 48: 1403-1403.

Lessig, L., 1999. The limits in open code: Regulatory standards and the future of the net. Berkeley Tech. L. J., 14: 759-760.

Mill, J.S., 1869. On liberty. Longmans, Green, Reader and Dyer, London, UK.

Moore, G.E., 1965. Cramming more components onto integrated circuits. Electronics, 38: 114-117.

Nak-In, S., 2009. Internet and freedom of expression. J. Media Law Ethics Policy Res., 8: 104-104.

OECD., 2015. Data-Driven Innovation: Big Data for Growth and Well-Being. OECD Publishing, Tokyo, ISBN:9789264229358, Pages: 456.

Pagliery, J., 2017. Wikileaks claims to reveal how CIA hacks TVs and phones all over the world. CNN, Atlanta, Georgia, USA.

Raiyn, J., 2014. A survey of cyber attack detection strategies. Intl. J. Secur. Appl., 8: 247-247.

Schwartz, P.M., 1999. Privacy and democracy in cyberspace. Vand. L. Rev., 52: 1607-1653.

Shapiro, A.L., 1999. The control revolution: How the Internet is putting individuals in charge and changing the world we know. Public Affairs, New York, USA.

Spinello, R.A., 2001. Code and moral values in cyberspace. Ethics Inf. Technol., 3: 137-150.

Tae-Yeong, C. and L.J. Kyu, 2015. Bright Internet campaign spread to the world. Information Technology University, Lahore, Pakistan.

Tene, O. and J. Polonetsky, 2013. A theory of creepy: Technology, privacy and shifting social norms. Yale J.L. Tech., 16: 59-100.

UN., 2017. E-government survey. United Nations, New York, USA.

WEF., 2016. Global risk report. World Economic Forum, Cologny, Switzerland.

Young, B., 2006. A study on the public sphere and promotion of public interest in cyberspace. J. Cybercommunication Acad. Soc., 17: 1-48.

Zeng, D., 2015. AI ethics: Science fiction meets technological reality. IEEE. Intell. Syst., 30: 1-5.