211-0007
378 Tenjinchou Kamimaruko Nakaharaku
Kawasakishi Kangawhken Japan

ISSN: 2423-8767

International journal of justice & law

2018 3(2)

<Index>

J-INSTITUTE

2018 3(2) 1-7 Submission: 2018/11/10, Peer review: 2018/11/20, Accepted: 2018/11/25, Published: 2018/12/30

International journal of justice & law

Publication state: Japan
ISSN: 2423-8767

Publisher: J-INSTITUTE
Website: http://www.j-institute.jp

Corresponding author
E-mail: pws7897@naver.com

Peer reviewer
E-mail: editor@j-institute.jp

http://dx.doi.org/10.22471/law.2018.3.2.01

Analysis of the Security Situation of the Republic of KOREA in Response to Cyber TERRORISM - From Legal Perspective

Park Woong-shin

SungKyunKwan University, Seoul, Republic of Korea

Abstract

Cyber terrorism has emerged internationally since the mid-1990s when networking began to take place. However, in most cases, the damage was localized by hacking the network of related organizations and hacking for economic gain in order to inform individual or organization claims. However, as we look at the year 2015, the s pread of computer networks and the dependence of the infrastructure on this network are not comparable to those of the 1990s. The fact that major broadcasting companies and financial institutions are temporarily paralyzed by the cyber terrorism incident on March 20, 2013 and June 25, 2013, revealing the vulnerability of the social infrastructure, reveals the danger of cyber terrorism It is imperative to prepare countermeasures.

In particular, major social infrastructures and services of the modern countries including Korea are gradually being connected and controlled by ICT technology. In case of facility and service failure caused by unauthorized access to such facilities, the impact on the normal operation of other core facilities may become very large. In particular, there is a serious problem in that the infringement of the network connecting the national infrastructure such as communication, finance, water supply, power, etc. and controlling each information system may cause obstacles in the whole country rather than simple cyber infringement. In this way, cyber terrorism cases against the state infrastructure have been actualized. In addition to the cases described above, there are many cases of cyber terrorism in Korea. In recent years, cyber terrorism targeting Korea has tended to occur in order to impose damage to national infrastructure such as GPS, telecommunications, broadcasting, and financial facilities. This is because the risk of individual criminal activity to threats to national security. In the ICT era, cyber terrorism is a new threat to national security and it is a new type of risk source that is discussed in modern risk society. Therefore, there is a need to cope with criminal policy and legislation.

[Keywords] ***Cyber Terror, Terror, National Security, Change of National Security Situation, Due Process***

1. Intro

The development of science and technology in late industrial society has changed human civilization rapidly. Particularly, due to the development of ICT technology, the world has lowered the barriers between countries to the point that the word "global village" is inexplicably brought about the free movement of manpower money and technology. This has a positive ripple effect such as economic co-growth, propagation of democracy and promotion of human rights come. On the other hand, not only economic damage such as abuse and abuse of nuclear energy caused by science and technology, serious environmental crime, unpredictable large-scale accident, and crimes that abuse ICT technology, but also adverse effects that can impose human life and body, It can be said that it is the dark side of. In particular, crime using ICT technology, such as cyber terrorism, has already spread to the masses through the media, and its severity is a direct threat to a

country's infrastructure beyond the level of individual criminal activity, it is changing situation.

Cyber terrorism has emerged internationally since the mid-1990s when networking began to take place. However, in most cases, the damage was localized by hacking the network of related organizations and hacking for economic gain in order to inform individual or organization claims. However, as we look at the year 2015, the spread of computer networks and the dependence of the infrastructure on this network are not comparable to those of the 1990s. The fact that major broadcasting companies and financial institutions are temporarily paralyzed by the cyber terrorism incident on March 20, 2013 and June 25, 2013, revealing the vulnerability of the social infrastructure, reveals the danger of cyber terrorism It is imperative to prepare countermeasures.

In addition, Korea has not only these internal risk factors but also risk factors according to the security environment surrounding the Korean Peninsula. That is, political and military conflicts with neighboring countries surrounding the Korean peninsula, as well as North Korea's political and military threats that have continued since the division. The problem is that Korea's external threat is not only caused by traditional security risks but also by new types of security risks. While the traditional concept of security is to look at security only by military threats, the new form of security concept, even if securing political and military security, is not reflective of its security, It is a concept that measures the degree of security by measuring the comprehensive quality of human life such as human rights, social development, economy, health and environment. Therefore, it is necessary to analyze Korea 's security situation not only from the external perspective of strengthening the national security capacity but also the minimum conditions in which the members of society can live like human beings.

2. Diagnosis of the Security Situation in Korea

2.1. Domestic factor(ⅰ) - contrast as a leading country in ICT technology

Rapid changes in modern society can be summarized as globalization and informatization. As I mentioned at the beginning, modern society has achieved political and economic development according to the progress of globalization, but the fundamental driver of globalization is due to ICT technology[1]. This information society is characterized in that capital for creating added value becomes knowledge and information, not real capital, like industrial society, and the essence of labor for production changes into mental activity rather than physical and physical labor. In addition, it is possible to spread knowledge freely beyond time and space by ICT technology, and it is also characterized by becoming a networked society beyond time constraints in the fields of politics and economy. With the advent of the information age characterized by this knowledge information society and network society, humanity is experiencing a breakthrough. In other words, the development of e-government and e-commerce, free communication due to the spread of the Internet, and the cultivation of political consciousness as a result are gifts not only for the people of a certain country but also for our people living in this era. In addition, the development of ICT technology accelerated the production and distribution of information, facilitating the disclosure of information, and disrupting the paradigm that governments or small numbers of people used to control or monopolize information. Another characteristic of informatization is that the state loses its dominant position of monopoly of information, while the capacity of non-state actors such as civic groups and individuals is strengthened. In summary, the use of ICT technology, rather than the accumulation of wealth by the human labor force of the past, is the production and redistribution of social goods, so that such digitized information has become a source of social wealth and a tool of new power. In Korea, social infrastructure such as public transportation, water supply, sewerage, telecommunications, and finance are integrated and managed by ICT technology, electronic financial

transactions are activated in private transactions, and ICT It is hard to imagine that there is no SNS utilizing technology, so our society is highly dependent on ICT technology[2]. Digital information, however, has emerged as a new economic, cultural and political value, but at the same time, it is the emergence of another new source of danger through industrialization[3]. In other words, all of the social organization is linked to the aggregation point of information and communication technology, and not only the structural weakness is highlighted, but also personal deviations (cyber terrorism, online pornography circulation, defamation, copyright infringement , Fraud, etc.) began to increase. As ICT technology has both the opportunity to make dramatic development in human civilization and the danger to threaten human life, there is a need to manage it systematically in terms of risk.

2.2. Domestic factor(ii) - a society in which new forms of mass risk coexist

According to a recent survey, the safety level of our society is not of high quality. In other words, the members of our society are perceived to have anxiety about various fields such as national security, natural disasters, environmental pollution, various talents, and new crimes. According to the survey, there is an anxiety about national security and crime occurrence without distinction between men and women. However, there is an anxiety about unpredictable dangers in modern scientific and technological society, such as natural disasters, environmental pollution and human resources. . Our society has a social infrastructure based on the developed ICT technology as described above, and the incidence of crime is significantly lower than that of advanced countries. Where does this anxiety come from? Is this anxiety merely a consequence of the subjective feelings of the members of the society or a defense instinct based on the dangerous media coverage, or is it actually an uneasy society? To find answers to these questions, it is necessary to review the concept of risk society presented by Ulrich Beck[4].

2.2.1. Concept and characteristics of dangerous society

It is difficult to uniquely define the concept of a dangerous society. According to Beck, a dangerous society is a society in which the dark aspects behind human social development are gradually leading social discussion, that is, a contradictory society in which the scientific civilization designed for human convenience threatens human existence itself. According to Beck, as modernization dismantled the feudal society of the nineteenth century and created an industrial society, today's modernization dismantles the industrialized society of the 20th century and dismisses the industrial society as “a modern society, A continuation of the continuous development of"[5]. In other words, he defines a dangerous society due to the change of society due to the change of the times. However, the notion of such a dangerous society is so abstract that it is unclear what the dangerous society Beck would like to discuss.

Eric Hilgendorf pointed out that the concept of risk society proposed by Beck is quite unclear in terms of philosophical, sociological and legal aspects. He pointed out that risk society is the destruction of the natural environment due to the rapid development of science and technology in late industrial society And threats to human survival, the disabling of the human sense system, and the arrival of fear society as a result of the assurance of industrial progress and the collapse of community consensus[6].

The concept of this abstract dangerous society became a hot topic in the Chernobyl nuclear power plant in 1986. Since the development of nuclear power in the West, the introduction of advanced science and technology, including global ecological risk, nuclear abuse and abuse, and social reflection on the danger have started in earnest in the 1970s and early 1980s. I was not interested in this[7]. However, in the late 1990s, the Sungsu Bridge, the collapse of Sampung Department Store, and the oil spill in Taean have led to the recognition of the possibility that a major catastrophe may occur due to the adverse effects of these technological developments. Discussions about risk have begun.

So what is the new form of risk that Beck suggests? There are two views in the country about the risk concept of Beck. In other words, it is a discussion of how to distinguish between traditional forms of risk and new forms of mass risk. (I)Beck distinguishes 'risk' from past threats (Gefährdung) and a new form of mass risk(Risiko), the former being a personal threat by wealth and political power, the latter by technological-economic development, Risiko, who has already used the notion of Risiko, Gefahr, and Gefährdung, which is translated into the same danger as Korean, implies a threat to the foreseeable legitimate interests(ie, nuclear power plants, Gefahr means the possibility of unexpected corruption of legal interests, and Gefährdung means the possibility of infringement of an individual's legal interests. It is a view interpreted as traditional danger. In other words, Beck distinguishes 'danger' from past threats(Gefährdung) and new forms of mass risk(Risiko)[8], the former being a personal threat by wealth and political power, the latter by technological-economic development, Risiko, in the sense that it uses the concept of Risiko, Gefahr, and Gefährdung, which translates into the same danger as the Korean language, which means a threat that can occur at the center of society itself,), Gefahr is an antagonism of unexpected legal interests, and Gefährdung is a traditional danger that means the possibility of infringement of personal interests[9]. The controversy is that the traditional form of risk (or crisis) is seen from the same point of view, but there is a difference in how the new type of risk is viewed. The risk is the possibility of occurrence, not the problem itself, Considering the possibility of human control over the future, it is reasonable to distinguish between risk and harm.

However, since the concept of Risiko, which is different from the traditional risk (Gefährdung), which means the possibility of infringement of the individual's legal interests by this division, is not a concept with its own limitations, The definition is still unclear. Therefore, the concept of a new form of risk must have an abstraction. Taking all of the above-mentioned arguments into consideration, the new form of risk is "to be expected based on human collective decisions in post industrial society, As well as a certain industrial mass risk that appears to be unavoidable in the unprotected state personally ". It is necessary to examine the conceptual features of the risk society based on the risk and the concept of risk society discussed above.

2.2.2. Our society as a new risk society

Korea has started to become a dangerous society based on the construction of Kori nuclear power plant in 1977[10]. However, Korea's risk society differs from the typical characteristics of risk society proposed by Ulrich Beck[11]. Risks are not only technological, socio-economic but also cultural aspects[12].

First, Beck 's risky society' s risks are inevitable products and fateful risks caused by the combination of development and industrialization of science and technology, which were key elements of the Western modernization process, We were able to avoid this if we were to switch from a flawed modernization strategy to a green development model as a result of the desperate need of the growth-oriented model chosen by the desperate need[13].

Second, it is a variation of danger personality. The dangers of Korean society are not only the new massive risk of late industrial society such as large scale environmental pollution, but also the danger of traditional society such as insolvency, industrial accidents, industrial society such as industrial society, transition society, school violence and sexual violence crime. It is showing the phenomenon. Furthermore, the adverse effects and risks associated with the development of science and technology are also showing signs of heightening social unrest.

Why did this dangerous society arise? I think there are various perspectives according to the writer, but basically it is because I stimulated the desire of safety for my existence. In other words, the subjective aspect of the emergence of new mass risk due to the development of science and technology, and the subjective aspect of increasing the anxiety and fear of the social members resulting from this competition. Of course, it is true that the traditional and natural dangers of our society have been reduced compared to

the industrial societies due to such economic growth and development of science and technology. However, objective safety has increased, but the subjective anxiety that the members of society have in the new form of mass dangerous danger poses a serious threat to objective safety. For this reason, members of our society are demanding active intervention in new risk factors, and the state and legislators have responded to the preemptive application of criminal law, not the traditional preventive law, the area of police law. In other words, according to the traditional liberal legal theory, it was virtue to abstain from intervening in the state, especially the state penal right, but in the dangerous society, it started the penal intervention enough to eliminate the anxiety of the risk of the social member.

2.2.3. Cyber terrorism in dangerous society

In this sense, the concept of cyber terrorism in our society is a traditional risk source such as murder and rape, but the approach to risk regulation is based on the necessity of social defense, or the cyber terror itself is a new form It is necessary to judge the risk cause.

Ulrich Beck explained that the new forms of risk have invisibility, equality, and boomerang effects, and cyber terrorism is consistent with these characteristics. In other words, ⅰ) cyber terrorism, unlike the traditional forms of terrorism, is a risk that goes beyond human cognitive ability, so it can be recognized through scientific knowledge, and ii)the traditional danger in terms of the exposure of crime is the status of social class Although the degree of exposure is different, cyber terrorism has the potential to be more vulnerable to the social middle class, which has a relatively high reliance on ICT technology, resulting in the disappearance of the line between the privileged and the non-privileged in terms of exposure. In other words, in terms of exposure to risk, cyber terrorism can be leveled differently from traditional risks. ⅲ)Cyber terrorism is also equivalent to the boomerang effect proposed by Beck, because ICT technology has a structure that allows people who see large and small gains to take risks and their negative consequences. ⅳ)Furthermore, social and political discussions on cyber security have been carried out with several serious cyber terrorism in the past, and the political and legislative debate that has arisen has led to the explanation that Beck's new type of risk is political explosive power I agree. In this respect, cyber terrorism is a typical example of the risk presented by Beck. Therefore, the top priority of the criminal policy for these risk sources is the construction of the social safety net to protect the safety of the members in response to the cyber terrorism which is a risk of social harm[14].

2.3. Foreign factors - changes in the security environment

Let's turn our perspective on the security environment out of the country. At the end of the 20th century, the end of the Cold War system under the US and the Soviet Union resulted in a reduction of the possibility of world wars. As a result, conflicts and conflicts between ideologies, systems, and institutions, which served as important criteria in determining the friendship and hostility between countries during the Cold War period, have been remarkably reduced, while the pursuit of core interests and political and economic interests[15]. The importance of peace and economic development through mutual cooperation is becoming more important. In this international situation, the concept of security is changing and our security environment based on this is also changing.

Traditionally, national security was based on military security. However, due to the end of the ideological confrontation between nations and the rise of non - state actors in accordance with the progress of information and globalization, Conflicts arise due to territorial and economic interests. In other words, the changed international situation calls for a new paradigm of national security. The recent national security paradigm is not focused on traditional ideology or military superiority but threatens and paralyzes the people, territory, sovereignty, Elements also appear as a concept of comprehensive security that can threaten national security[16].

The paradigm of this new security environment is characterized as follows. 1)As discussed above, in the setting up of the concept of security, not only from the military point of view, but also from the non-military elements such as politics, economy, society, environment and technology, The fundamental change of the subject and the threatened object is that the viewpoint of security has changed from the viewpoint of the state-oriented security concept to the center of the individual and the human community[17].

3)The emergence of transnational threats as a threat to national security is not a conventional concept of a nationality. Transnational threats are characterized by the fact that the source of the threat is done by non-state actors, while the threats by non-state actors are transcended beyond traditional borders. 4) Finally, each country in the world has reached a state where it can not guarantee the security of the state from the threat of terrorism. These threats are caused by traditional forms of terrorism, such as the September 11 attacks of 2001, but cyber terrorism using advanced ICT technology is also a potential threat to national security.

3. Conclusion - Cyber Terrorism as an Element of National Security

In general, national security means that the core values of a country are free from threats to core values. Traditional national security mainly refers to external military threats, and therefore, most of these threats are state actors. However, since the end of the Cold War, the security environment brought about various threats(eg, international crime, drugs, the environment, refugees, resources) other than military threats, and the inclusion of comprehensive security to cope with these various threats, . In particular, as the information society based on the innovation and development of ICT technology is settled, cyber-level security threats are added, and the security environment of that time is different from the security environment during the Cold War period. In particular, major social infrastructures and services of the modern countries including Korea are gradually being connected and controlled by ICT technology. In case of facility and service failure caused by unauthorized access to such facilities, the impact on the normal operation of other core facilities may become very large. In particular, there is a serious problem in that the infringement of the network connecting the national infrastructure such as communication, finance, water supply, power, etc. and controlling each information system may cause obstacles in the whole country rather than simple cyber infringement. In this way, cyber terrorism cases against the state infrastructure have been actualized. In addition to the cases described above, there are many cases of cyber terrorism in Korea. In recent years, cyber terrorism targeting Korea has tended to occur in order to impose damage to national infrastructure such as GPS, telecommunications, broadcasting, and financial facilities. This is because the risk of individual criminal activity to threats to national security. In the ICT era, cyber terrorism is a new threat to national security and it is a new type of risk source that is discussed in modern risk society. Therefore, there is a need to cope with criminal policy and legislation. However, on the grounds of the limitations, the concept of cyber terrorism as a basic premise for the response of cyber terrorism and the legal and philosophical grounds on which the state should prevent cyber terrorism will be published in the next issue.

4. Reference

4.1. Journal articles

[2] Kim HY & Oh JH. Present Status and Social Meaning of Domestic and Overseas SNS. *International Telecommunications Policy Review*, 24(12), 19-42 (2012).

[3] Ha TH. Challenges and Prospects of Korean Criminal Law in the 21st Century. *Anam Law Review*, 13, 133-154 (2001).

[4] Ryu CC. Risk Society and Risk Criminal Law. *Chonnam Law Review*, 18, 227-250 (1998).

[7] Roh JC. Risk Analysis in Modern Risk Society. *Crisisonomy*, 1(1), 33-48 (2005).

[8] Kang MS. Die Gesetzgebung in Der Risikogesellschaft -Die Aufgabe von Gesetzgebung unter der Risikogesellschaft. *Public Land Law Review*, 32, 321-356 (2006).
[9] Park KM & Lee SD. Countermeasures of the Criminal Law in Accordance with Appearance of Risikogesellschaft. *Sungkyunkwan Law Review*, 18(3), 513-533 (2006).
[11] Han SJ. Analysis of Risk Society and Critical Theory: Ulrich Beck's Seoul Lecture and Korea Today. *Society and Theory*, 12, 37-72 (2008).
[17] Lee JE. Changes in National Security Environment and National Crisis Management -National Crisis Types under Comprehensive Security Concept. *Crisisonomy*, 9(2), 177-198 (2013).

4.2. Books

[1] Joseph S. Nye J. The Paradox of American Power: Why the World's Only Superpower Can't Go It Alone. Sejong Institution (2002).
[5] Ulrich B. Risk Society, Saemulgyul (1997).
[6] Eric H. Strafrechtlich Produzen tenhaftung in der Risikogesellschaft. Duncker & Humblot (1993).
[10] Hong ST. ROK Risk Society. Dangdae (2007).
[12] Patrick T. O'Malley. Crime and Risk. Sage (2010).
[13] Park MS. Studies on the Risk-governing Criminal Law and Criminology in the Late-Modern Society(I): Modern Risk Society and Criminal Law of Law-governed State. Korean Institute of Criminology (2012).
[14] Kim HK. Studies on the Risk-governing Criminal Law and Criminology in the Late-Modern Society(I): Risk-governing Criminal Law & Criminology in the Contemporary Science-technology Society. Korean Institute of Criminology (2012).
[15] Chung CK. The National Crisis Manage ment in the 21st Century Comprehensive Security Era. DaeWangsa (2010).
[16] Kurt WR & Raymond F. Comprehensive Security in Asia. Brill Academic Pub (2000).

Author
Park Woong-shin / Sungkyunkwan University Post-Doc
B.A. Sungkyunkwan University
M.A. Sungkyunkwan University
Ph.D. Sungkyunkwan University

Research field
- A Study on the Problems and Improvement of the Investigation in the Act on Anti-terrorism, Sungkyunkwan Law Review, 29(2) (2017).
- A Study on the Darknet Crime Phenomenon and Criminal Countermeasures, Prosecution Service, 58 (2018).

Major career
- 2017~present. Dongseo University, Lecturer
- 2017~present. Sungkyunkwan University, Post-Doc

2018 3(2) 8-12
Submission: 2018/11/10, Peer review: 2018/11/20, Accepted: 2018/11/25, Published: 2018/12/30

International journal of justice & law

Publication state: Japan
ISSN: 2423-8767

Publisher: J-INSTITUTE
Website: http://www.j-institute.jp

Corresponding author
E-mail: cieletmoi@kic.re.kr
Peer reviewer
E-mail: editor@j-institute.jp

http://dx.doi.org/10.22471/law.2018.3.2.08

International Co-Operation and KOREAN Situation about Non-Conviction Based CONFISCATION

Kim Kyoung-chan

Korean Institute of Criminology, Seoul, Republic of Korea

Abstract

The general tendency of contemporary Crime in the 21st century is transnational, intelligent, difficult to prove, related to much illicit money and collaborative among criminals especially in North East Asia. It is difficult to recover criminal assets in North East Asia not only because of the lack of the necessity recognition for the criminal asset recovery but also the limitation of the governance for the efficient mutual legal assistance in criminal matters including the incompletion of the legislation for the Asset Recovery. Non-Conviction Based Confiscation is also based on the completion of the legislation and the willingness for the substantial collaboration among the judicial organizations in Northeast Asian countries.

[Keywords] ***Asset Recovery, Confiscation, Victim Protection, Mutual Legal Assistance, Criminal Proceeds***

1. The Lack and Limitation for the Crime Prevention and the Victim Protection through the Criminal Asset Recovery

The increase of the International Trade and exchange have also brought us the necessity for the global performance on the crime prevention and the transnational protection of Crime Victims. The International Co-operation in the Criminal Asset Recovery is very important for the crime prevention and the protection of the victims, but it is very much difficult to have successful results because of the difference between venue and jurisdiction including the lack of understanding of the legislation from the each countries[1].

It may be important to increase the understanding of the situation of each countries for the success of the international co-operation of the confiscation of the criminal proceeds and asset recovery. The international co-operation for asset recovery may depend on the agreement, treaties, recommendations, (in)formal information toward the Common goal based on mutual trust and understanding.

2. Mutual Understand and Encouragement for the Asset Recovery

2.1. The difference of the domestic law and crime response system

Many Crimes like Economic Crime, Corruption Crime, Cyber Crime, Organized Crime, Narcotic Crime[2] and Terrorism are supernational and based on the criminal proceeds and assets.

People, Parliament and Government in each country need to know the crime phenomenon and the characteristics of criminals about the criminal proceeds and assets, it can lead to the proper legislation for the Crime Response.

Each Country has the different background about their own domestic law[3], it has the dissimilar Crime Response System including the (im)possible Investigation method and the different ways of Co-operation with other

counties and the international organization in spite of the agreements and some recommendations[4].

There are many special laws related with the confiscation of criminal proceeds and Asset recovery in Korea, but the enforcement of the law is not conducted well, the default of paying under the confiscation is estimated at 21 billion dollars by 2015 in Korea.

2.2. The unsuccessful cases of the asset recovery

The case of former president known as a corrupt offender, Chun Doo-Hwan, has still been in default of paying under the confiscation of about 100 million dollars even if he paid about 100 million as a confiscation for 20 years. He said “I have only about 250 dollars” but he has lead luxurious lives until now.

The case of Corrupt Businessman infam ous for Sunken Ship –Sewol ferry- Yoo, Byung-Eun died as a fugitive criminal on 2014. Although the ministry of Justice of Korea has frozen his asset, the asset recovery about him has been through the Civil litigation, but it is not so effective and it is also difficult to get the evidence related with the corrupt money.

The case of big fraud like the pyramid scheme fraud, the amount of the damage is about 3 billion dollars, Cho Hee-Pal died in China on 2011, his death was officially recognized in China on 2016. The 30 victims even committed suicide, many victims hope to get their money back.

Although there are many laws including criminal law that related with confiscations in Korea, the laws have no specific regulations on Non-Conviction Based Confiscation especially about the fugitive and the death of the criminal, it is also impossible to confiscate the criminal proceeds when the statute of limitations on the crime has expired.

2.3. The efforts and endeavor of the supreme prosecutor’s office in Korea

Supreme Prosecutor’s Office in Korea tried to establish a Network for Asset Recovery with a plan to have an annual meeting from 2013.

It has established an on-line system(ISF) for the improvement of the information utilization about Criminal proceeds and Asset Recovery from 2009.

It is important to start with the recognition and detailed understanding of the difficulty about the law and the regulation[5], it may also significant to have mutual respect and trust in the Co-operation through the Sympathy and Encouragement for the common safety and the stable development.

3. Difficulty, Necessity and Discussion for the Asset Recovery

3.1. Sharing the criminal cases and the criminal statistics

Firstly, it may be necessary to share the Crime cases and the statistics[6] about the confiscation of the criminal proceeds and Asset including the problems of the success and failure of the Asset Recovery. It is also for the mutual understanding about the real situation about the phenomenon of the crimes including the prevention of the crimes internationally. The statistics on crimes based on the different legal system may be difficult and inaccurate but it can be useful for interactional approach[7].

The productive and practical ways for Asset Recovery may need to have the estimation about the Co-operation with the investigation teams and judicial authorities in each country, but it may also be difficult to have the proper estimation from each other, nevertheless the results about the estimation from the each party may be necessary to be used for the improvement of the procedure and the sharing of the investigation methods including the revision of the legislation in some counties.

3.2. The effort for the legislation and international judicial co-operation

Secondly, it is essential for the Government and the Parliament in each country to have the willingness by making appropriate efforts for the confiscation of the criminal proceeds and Asset Recovery. The integrity and the meaningful independence of the judge and the court can be the basement for

the international Co-operation from the evidence-based viewpoint despite the difference of the power structure[8].

But it may also be difficult to recommend on the judicial reformation towards some directions, but the importance of the evidence can be emphasized in each country.

It may be necessary to discuss on the reasons about the problems of the enforcement and ineffective regulations of confiscation in Korea, the investigative authorities in Korea can investigate into financial transactions about the offenses of the public officials with or without warrant, but it may be necessary to discuss on the scope and the propriety of the issuing the warrant and the order of court comparing with G20 about the criminal proceeds in Korea.

Furthermore, it may be very helpful and critical to have opportunity to have comprehensive understanding on the real situation and problems about law enforcement and law reform with G20.

3.3. The modification of the presumption and the burden of proof

Thirdly, one of the main difficulty about the confiscation of the criminal proceeds is related with the presumption of illegal profits and the burden of proof. The special laws like "Act on Special Cases Concerning Confiscation illegal political funds" "Act on Special cases concerning Forfeiture for offenses of public officers" "Act on special cases concerning the prevention of illegal trafficking in narcotics, etc." have the clauses about the presumption of illegal profits, but the other special laws like "Act on regulation and Punishment of criminal proceeds concealment" "Act on Special Cases Concerning Confiscation and Recovery of Stolen Assets" don't contain the clause about the presumption of illegal profits[9].

Korean criminal law and special laws about the confiscation and asset recovery do not include the reversal of the burden of proof, but the introducing it has been controversial and much discussed for the effective confiscation and recovery[10].

3.4. International victim protection through the asset recovery

Lastly, it is important to give the criminal proceeds and Asset back to the legal owner and the rightful person for the material restoration of the victims internationally[11].

When it is impossible or very difficult to restore them in some cases, it may be necessary to discuss on the using the Criminal Asset for finding ways for preventing the similar crimes and the protection of the victims as a common fund.

4. Co-Operation and Leadership

4.1. The role of G20 for the asset recovery

The effectiveness and efficiency for the confiscation of the criminal proceeds and Asset Recovery between countries may be enhanced by the process transparency and the reciprocal trust through the agreement or joint(investigative) organization.

G20 countries may be necessary to show a good leadership for the prevention and the response of the crime.

Firstly, the countries G20 may make a plan to issue the present condition about the asking and requested situation about the criminal proceeds and assets with some explanation for sharing.

It may be useful to share the systematic statistics and the analysis of the cases about the criminal proceeds and assets including the related victims, it also will assist joint confrontation and joint response system that can be established despite the difficult of the statistics of the crimes and victims from a world wide view.

4.2. Education and programme for the asset recovery

Secondly, it can be necessary to analyse the performance and categorize the crimes about the confiscation of the criminal proceeds, it may need to follow the review the domestic law and the implementing law from a comparative perspective for the enhanced Co-operation.

It may be necessary for G20 to consider on the global education programs about the prevention of the crimes including the confiscation of the criminal proceeds and asset recovery[12]. It can not only share the ways of the investigation and the understanding of the legal system in each country, but also offer some information about the domestic difficulty and the improvement of the international co-operation. The programs may have especially about the pending issue and problem about the confiscation of the criminal proceeds and asset recovery.

4.3. The importance of the international cooperation and proper legislation

Thirdly, it is not easy to have successful results for the criminal asset recovery internationally because it may be the deficiency of the proper procedure that holding a binding effect, therefore it may be necessary to reform the inadequate legislation and revise the unestablished or unprepared distribution structure about the Co-operation with the requested counties for the confiscation of the criminal proceeds and criminal asset recovery.

4.4. Leadership and community for the prosperity

Finally, G20 may show the good leadership toward the stability and the international cooperation through the preparing for community about the confiscation of the criminal proceeds and asset recovery, it may narrow the difference of the perspective for the response about the Criminal proceeds from each country. It may lead G20 to peaceful development and common prosperity

5. Asset Recovery as the Foundation and the Source for the Crime Prevention and the Deterrence of the Crime

Criminal proceeds and criminal assets are the source and the foundation of many crimes like money laundering, terrorism, organized crime, smuggling, cyber crime and corruption crime and so on.

The present crimes in one region or one country has become international and co-operative, the criminal proceeds and asset is very difficult to find and search with the effort of only one organization or one country.

It is necessary for G20 countries to share the information about the effective and efficient ways for the asset recovery in spite of the difference of the law and the crime response.

Regardless of the effort of the related organizations for the asset recovery in Korea, Korean criminal law for the confiscation and asset recovery is not so effective now shown as the absence of Non-Conviction Based Confiscation.

Asset recovery may be a tough labor through co-operative working by many organizations and countries, it also takes a very hard and complicated task. If we make an effort for the deterrence of crimes together basically, we need to eradicate the source of the crime, it may start with the confiscation of the criminal proceeds, the asset recovery is related with having the same goal toward the Common prosperity that considering on the criminal victims.

6. Reference

6.1. Journal articles

[1] Jeong OS. A Device on the Introduction of the Confiscation without Guilty-sentence. *Prosecution Service*, 46, 182-242 (2015).

[3] Park WS & Lee KL. A Study on the Dark net Crime Phenomenon and Criminal Countermeasures. *Prosecution Service*, 58, 219-256 (2018).

[4] Kim JH. Operational Status of 「Act on Special Cases Concerning Confiscation of Offenses of Public Officials」 and Its Improvement Direction. *Korean Journal of Comparative Criminal Law*, 20(3), 27-55 (2018).

[5] Shin HY. A Study on the Income Tax Consequence of the Confiscation of the Proceeds of Crime. *Anam Law Review*, 50, 243-277 (2016).

[7] Kang JH. Die Rechtsvergleichende Arbeit zur Einziehung im Strafrecht. *Chonnam Law Review*, 38(3), 83-107 (2018).
[8] Kim ME & Sung KS. Criminal Sanction for Organized Crime: Confiscation of Criminal Proceeds. *Soongsil Law Review*, 25, 31-58 (2011).
[9] Roh SH. Several Review Points for Necessary Forfeiture and Confiscation in Foreign Exchange Transactions Act. *Sungkyunkwan Law Review*, 29(2), 145-178 (2017).
[10] Kim HK. A Study on the Introduction of Civil Forfeiture, *Korean Journal of Victimology*, 19(1), 57-80 (2011).
[11] Kim HK. The Interpretation and Execution Procedure of Forfeit without Prosecution in a New Criminal Law Amendment. *Korean Criminological Review*, 26(2), 59-94 (2015).
[12] Kang MK & Park SK & Lee BG. A Study on the Problems and Improvement of the Seizure and Search System of Digital Evidence Liable to Confiscation. *The Journal of Police Sciencem*, 18(1), 115-142 (2018).

6.2. Books

[2] Kim KC. The Research and Legal Studies on the Policy and the Trends of Drug and Voice Phishing Crime Related to Korean in Northeast China. Korean Institute of Criminology (2013).
[6] Yoon HS. Building Crime Prevention System Utilizing Big Data. Korean Institute of Criminology (2015).

Author
Kim Kyoung-chan / Korean Institute of Criminology Researcher
B.A. Korea University
M.A. Korea University
Ph.D. Korea University

Research field
- The Legal Study and Research on the Policy and Trends about the Secret Trade Infringement Cases Related with China, Korean Institute of Criminology (2016).
- The Research on the Law about the Deportation of Foreign Countries, Korean Institute of Criminology (2018).

Major career
- 2012~2013. Korea University, Post Doc
- 2013~present. Korean Institute of Criminology, Research Fellow

2018 3(2) 13-20 Submission: 2018/11/10, Peer review: 2018/11/20, Accepted: 2018/11/25, Published: 2018/12/30

International journal of justice & law

Publication state: Japan
ISSN: 2423-8767

Publisher: J-INSTITUTE
Website: http://www.j-institute.jp

Corresponding author
E-mail: sung9987@hanmail.net

Peer reviewer
E-mail: editor@j-institute.jp

http://dx.doi.org/10.22471/law.2018.3.2.13

Protecting VICTIMS by Infringing Personal Information on SNS

Yoon Hae-sung

Korean Institute of Criminology, Seoul, Republic of Korea

Abstract

With the spread of smartphones and tablet PCs beyond the users of personal PCs connecting the Internet, cyber space has become an existential stage that directly affects our life rather than a simple virtual space. The first level of SNS ripple effect is that it functions as a media medium for marketing, publicity, and entertainment due to the network function that makes it easier to build so-called connections. On the other hand, the other attribute of SNS is exposed to the negative aspect which is used as a means of various crimes. Among the characteristics of SNS, since the location information service is accompanied and the personal privacy information is exchanged, exposure of location information and personal information eventually leads to privacy violation it is likely to lead to other crimes.

In terms of criminal policy, privacy is important and constitutionally recognized rights, and personal information infringement is also closely related, so personal information and privacy violation are not related to crime. Therefore, it is necessary to pay attention to the crime prevention aspect from the viewpoint of the users, and it is considered that the responsibility should not be overlooked from the viewpoint of the business operator.

In other words, if you understand the nature of SNS and understand the awareness and danger possibility, you can be protected from SNS crime damage. Therefore, it is important to pay attention to how well SNS users understand the attributes of SNS. Considering that cybercrime using SNS is mainly based on weakness of personal information protection, we use social networking service(SNS) so that personal information management can be carried out under self responsibility by educating and educating SNS users. It is necessary to establish clear guidelines on the limitations on the use of location information and surrounding information as the type and scope of personal information required for SNS subscription, and as linkage information.

[Keywords] ***SNS, Personal Information, Location Based SNS, Blog-Based SNS, Networking SNS***

1. Intro

With the spread of smartphones and tablet PCs beyond the users of personal PCs connecting the Internet, cyber space has become an existential stage that directly affects our life rather than a simple virtual space. The first level of SNS ripple effect is that it functions as a media medium for marketing, publicity, and entertainment due to the network function that makes it easier to build so-called connections[1]. On the other hand, the other attribute of SNS is exposed to the negative aspect which is used as a means of various crimes. Among the characteristics of SNS, since the location information service is accompanied and the personal privacy information is exchanged, exposure of location information and personal information eventually leads to privacy violation it is likely to lead to other crimes.

On the other hand, the other attribute of SNS is exposed to the negative aspect which is used as a means of various crimes. Among the characteristics of SNS, since the location information service is accompanied and the

personal privacy information is exchanged, exposure of location information and personal information eventually leads to privacy violation it is likely to lead to other crimes.

In this way, since the exposure and leakage of the user's personal information on the SNS exposes the location without knowing the privacy infringement as well as the lifestyle of the user, the criminal establishes the criminal environment that can combine the behavior radius and the life pattern of the users it is the price to offer. Therefore, the characteristics of the SNS, that is, the positive aspects (such as personal information and privacy disclosure) related to the trust connection of the human relationship can be exploited as means of criminality by linking with personal information, location information, and security achievement, Which can lead to more serious problems in that it is used as an off-line crime rather than a cyber problem.

2. Examination of Normative Control of Personal Information Leakage in SNS

2.1. Possibility of crime due to leakage of personal information and location information

2.1.1. Possibility of leakage of personal information including location information and additional crimes

As the phenomenon of SNS integration with social media and devices is accelerated by the spread of smart phones and the development of various application webs, the crime aspect in cyberspace based on SNS, for example, 'location based SNS' The location information of the subscriber is disclosed to the user on the SNS on the assumption that the subscriber agrees with the terms and conditions of the subscription process in cooperation with the existing SNS account. Accordingly, it is possible to recognize the location information of the contact person as well as the acquaintances of neighboring persons, as well as acquaintances of the acquaintances and many others. Of course, location-based SNS can be used as an advertising or marketing technique to recommend restaurants nearest to their current location, or provide sales information of stores near their favorite brands to visitors, it is not[2]. However, the personal information exposed by the SNS can be a serious problem as it can be seen by not only marketing and advertising companies but also criminals. For example, if you compare Twitter and Facebook, which are representative SNSs, Twitter is a bridge type(weak ties) or an open network centered on exchanging information and opinions through a unidirectional relationship with a follow- Facebook can be regarded as a cohesive or closed network in that it emphasizes emotional exchange such as exchanges and relationships among family members or acquaintances[3].

Based on this analysis, if we assume that the level of exposure of personal information is similar, we will be more open to the bridge-type SNS in facebook, which is a closed-type SNS operated with status confirmed based on the existing friendship It is possible to predict that Twitter is more likely to engage in personal information infringement and derivative illegal activities[4].

2.1.2. Possible crime related to account theft and hacking

There is a possibility that users may fall into crime objects and objects due to the disclosure and exposure of personal information in SNS on the basis of 'self-exposure'. Because of this, account theft of SNS is happening frequently. I experimented with the validity of such a fake account. I replicated the ID of the boss who was aiming to create a fake Facebook account. From that account, I sent a friend to the 432 friends of this boss' s friend. A request was made for the barrel. Moreover, most people are already "friends" with the boss. He sent a request to 436 direct friends of his boss and reported that he was finally able to become a "friend" with the permission of 14 people in an hour.

2.1.3. Review criminal policy direction based on exposure and disclosure of personal information

Social network services are defined as distribution of information by individuals, com-

munication between individuals(communication), and information exchange through network connection. This concept definition can be deduced from the form of exposing personal information and privacy to self - satisfaction voluntarily by criminal policy, and the form in which personal information is leaked for hacking or commercial purposes without exposing it voluntarily. Ultimately, from the viewpoint of the user, personal information and privacy information can be classified into exposure for self-satisfaction and unwanted leakage, and personal information(big data problem) There is a possibility of leakage to exploit a crime. On the other hand, criminal offenders may use hacking, malicious codes, apps, etc. to steal personal information with intention or purpose, which they intend to use for crime, or to divulge personal information directly or indirectly in a trust relationship for other purposes. The criminal law issues caused by the disclosure of personal information include theft through social networking, joint cyber casings, and the use of personal information. Fake accounts and account theft, which are closely related to the problem with Big Data. On the other hand, criminal law issues related to the leakage of personal information may lead to crimes such as phishing, social engineering, malware, fraud, use of personal information, and theft. In addition, both the exposure and disclosure of personal information on SNS over indirect networks need to be discussed in relation to the legal liability of ICT providers[5].

2.2. Personal information disclosure and security issues

SNS is not only personal information, but also various personal information such as personal connections, tendencies, opinions, daily life are posted and disclosed. "Inattentive disclosure" on SNS mainly refers to the case where an address or telephone number is disclosed without knowing it is disclosed, or the user updates his / her life or family composition. If information on the SNS accumulates, it may lead to future problems. In particular, when it is common to disclose all information, information disclosed on the SNS is permanently left on the Internet, which may lead to leakage of personal information, and personal information leakage may lead to various crimes. As such, even after the withdrawal of a service member, it is possible that the user's right to self-determination may be infringed because it is stored and disclosed continuously. In addition, the information disclosed on the SNS is easily and rapidly spreading forgery, alteration, and abuse, and there is a high risk of crimes such as defamation and intimidation[6].

For this reason, the user himself / herself needs to be aware of the problem and select the contents and scope of disclosure[7].

In the case of personal information collected and used in the SNS under the current law, the Information and Communication Network Act may apply, but in the case of other privacy information, it may be difficult to apply the information network regulation.

In addition, most of the SNSs operate in a manner that discloses information basically to earn revenue from advertising and data licenses. As such, a large number of online ads appear on the SNS, but online advertising is not generally reviewed. Because of this, even software that is considered to be a fake security program, and ads that can be seen at a glance that fraud is likely to occur, also appears as unauthorized advertisements. In Japan, there is a device that reports problematic advertisements, and the problematic advertisement is operated with a policy of coping quickly. However, in Korea, there are many problems because the institutional devices like Japan are not implemented.

3. Infringement of Personal Information in SNS and Countermeasures

3.1. ICT service providers and privacy protection

3.1.1. Significance of ICT service provider

Among social media, SNS such as Facebook has a large amount of personal information on a global scale, circulating a vast amount of information. Providing ICT services including

SNS. Because it deals with personal information including personal information of users, or is in contact with information requiring security, it can not be independent of legal liability. These operators are regarded as providing "telecommunication services", so they are regarded as "telecommunication carriers", and those telecommunication carriers can be regulated by the Telecommunications Business Act[8].

3.1.2. ICT service provider responsibilities

① Responsibility for personal information leak related business

Since ICT service providers often deal with personal information in the provision of services, there are occasions when they are obliged to take responsibility for protecting them or for damages caused by information leakage. The content and form of ICT services vary widely, so the legal obligations of providers vary according to the content and type of service, but most cases correspond to telecommunication service providers in the Telecommunications Business Act. In this sense, the obligation of operators in the Telecommunications Business Act is the responsibility of providing ICT services, paying attention to the risks arising from the nature of these services, and focusing on social media centering on social networking services(SNS).

② Legal risk due to the nature of the service

In social media such as SNS today, there are many forms in which information is distributed to the unspecified majority and exchanged. When illegal information (pirated copyright infringement information) or harmful information using SNS is distributed, damages due to contents or legal problems arise. Social media is also trying to prevent crime by the cyber security department of the National Police Agency or the internet patrol of the local government because it is easy to be a crime such as illegal drugs, sales of bank accounts, Such a problem is basically a problem of the user, but the provider may be requested to disclose distributor information from the authorities on the basis of criminal investigation or preventive cooperation. In such cases, it is a question of how operators should respond to distributor information disclosure requests. Depending on the degree of involvement of SNS providers in the exchange of information among members, the legal liability that they have as a business operator is also different. When discussing the legal responsibilities of these operators, it is necessary to consider the role or position of the service provider in the service, which can be divided into two cases. The first is the position where the operator can freely adjust or control the information exchanged. In other words, the operator has the authority to operate and manage the information on the service because it is possible to restrict the information, edit it, and delete it[9]. The second is the case that there is only the so-called "conduit" role in the role of delivering the information, not the operation and management authority such as processing, processing and deleting the information on the service to the business operator. Such a position is a structure that cannot be modified or deleted because it does not know the contents of the information distributed on the service at all. Therefore, in discussing the responsibilities of ICT service providers, it is necessary to examine the roles and positions of ICT service providers, such as the extent to which they have the authority to operate and manage information distributed on the services.

3.2. Personal information infringement measures in SNS

3.2.1. Threat factors and countermeasures for general SNS service

As we have seen, the most common problem when using SNS is the invasion of privacy caused by information collection. Another problem that is related to SNS is the domestic legal system of overseas SNS providers. Since foreign SNS providers often do not comply with domestic laws and regulations, measures are taken to protect SNS personal information as well as relevant laws such as the Information and Communications Network Act. However, unless domestic companies are actually regulated, there is a concern. If the SNS collects the address book information of the subscriber and uses it as a

friend recommendation to others, the subscriber does not go through the consent procedure. In the case of SNS, in addition to the simple collection of the phone book, there may be possession of. Therefore, differences in the handling of personal information are problematic in that operators set arbitrary policies such as the scope of disclosure of personal information. In addition, excessive personal information disclosure default settings such as postings by users and protection of minors when using SNS may be a problem. As a countermeasure to this, first, it may be difficult to apply information network regulation in case of other privacy information collected / used by SNS. Therefore, it is necessary to set the concept and scope of privacy information(including legal definition against institutionalization) Separate measures are needed such as notification and agreement procedures. Second, in relation to the problem of reverse discrimination in the application of the domestic legal system to foreign SNS operators, it is necessary to prevent the relative contraction of domestic SNS industry by establishing measures for enhancing the trust level of users for domestic operators, And the fact that more information than sensitive information is collected by domestic operators should be actively promoted to users. Third, it considers the paradigm shift in accordance with the SNS, examines the consent process, strengthens protection measures in accordance with the personal information life-cycle from the viewpoint of the operator, and recognizes that the unwanted information can always be leaked through the SNS There is a need to make appropriate action choices.

3.2.2. Threat factors and countermeasures for each SNS service

① Blog-based SNS

As a threat factor, first, there is not enough consent procedure to collect personal information. Second, the information that is disclosed on Twitter's followers is collected and distributed through the portal's search engine. Third, the user reveals his / her personal information and information to be used for his / her life indiscriminately. As a countermeasure against this, first, it is necessary to promote the disclosure of the risk of privacy infringement to the users of SNS's privacy service provider. Second, there is a need to provide institutional safeguards in the case where information disclosed in SNS is provided to third parties, and plans for discarding public information according to the user's intention. Third, it is necessary to enforce technical and administrative protection measures such as hacking and malicious code blocking, illegal spam, defamation monitoring and filtering system. Fourth, it is necessary to encourage compliance with the personal information protection measures of service providers through the provision of guidelines for operators and to promote the risks of using SNS to users.

② Location-based SNS

First, the location information of a specific user can be profiled, so that an empty house can be abused for crimes such as theft. Second, location-based SNS provides common SNS functions like Twitter, so there are similar risks such as excessive exposure and sharing of personal information. First, it is necessary to develop and disseminate anti-abuse technology of location information application program using 3G, GPS, and wireless LAN AP. Second, it is necessary for the location-based SNS provider to provide the user with a personal location information self-control system or similar function to ensure the user's control. Third, it is necessary to periodically investigate and disclose known location information or personal information related vulnerabilities for each SNS service.

③ Networking SNS

First, it is relatively easy to gather information about human network without user's consent. Second, it is more complicated and difficult for users to delete accounts or use the dormant function than the service registration procedure, and there is a risk of continuous exposure and misuse of personal information. Third, illegal spam can be sent in large quantities by exploiting the human network. To cope with this, first, it is necessary for the service provider to take measures such as allowing access only with mutual con-

sent in order to prevent spread of privacy information due to unlimited interconnection between users. Second, there is a need to mandate technical protection measures, such as sending large amounts of illegal spam emails. Third, there is a need to promote awareness and limit information collection on vulnerable people who are inadequate to recognize and manage personal information protection such as children and adolescents.

3.3. Suggestion of criminal policy issues in SNS

As such, the use of social network services is likely to expand in the future. It is a convenient system and it is possible to expand the living space significantly, but the problem of personal information is surfacing. This problem can not be avoided by understanding the characteristics of the SNS and setting it appropriately. The JNSA SNS Security WG enumerates the following items as a device to avoid problems with SNS. ① Be conscious of the fact that it is always open, quoted, and recorded. ② Use complex passwords to increase security. ③ Set the scope of disclosure and avoid unnecessary exposure. ④ Make sure that you do not become friends with someone you do not know, even if you know someone. ⑤ Make a setting that does not hurt "friend". ⑥ Deletion from "friend" is considered carefully, and the use of limitation list is considered. ⑦ Understand the technical risks such as location information of photographs and check-ins and use them properly. ⑧ Do not add "friends" tag. ⑨ Countermeasures Reduce the risk of using dangerous sites by using software. ⑩ In organizations such as corporations, SNS guidelines should be created and followed through education. There are also some precautionary measures regarding how social networking can severely damage a company or company. ① Do not use social networking sites on company computers. This behavior is like opening a back door to hackers directly to your company's accounts, files, and other information. ② Avoid posting specific information about work, absenteeism, and other information that could open up opportunities for crime. ③ Hackers use the answer to the "secret question" of the user's account to figure out the password and penetrate the account. Do not answer secret questions with answers that you can easily find on social networking sites, such as the logical answer, your mother's name, or where you were born. If the secret question is "Which city were you born in?", The answer should be a city in another country, preferably a city you have never visited before. ④ Never give confidential company information to people you can not identify. It is good to be careful even if the person is the right person.

4. Outro

As we have seen, the SNS now has access to the attributes of the SNS, that is, PCs or mobile devices(smart phones) that contain personal information, and the networks in the SNS tend to be built on the basis of real networks Therefore, the risks and vulnerabilities that SNS may be used for crime can be exposed. For this reason, behavioral patterns such as spoofing and theft, as well as privacy infringement, have now become the subject of controversy in the world of social networking. For example, a Facebook profile may include name, birth date, education and career experience, Sexual and social status, online and offline contact information, political and religious perspectives, music, books and cinematic symbols, as well as pictures, and more. Once you have completed a typical social networking profile, anyone can build a fairly detailed database of information about others. This makes it possible not only to know who the other person is but also to know who knows the other person, and to access information about the other person as well as the other person's friend. Recently, in New York, Charles Schumer has asked the Federal Trade Commission to provide guidance on how to use social networking sites and how to use their personal information[10].

On the other hand, a Canadian law firm is pushing for a potential class action lawsuit against Facebook, saying that the Facebook site "is deliberately or inadvertently designing its own privacy policy and tricking users into putting their privacy and privacy at

greater risk "We are now preparing a lawsuit against him. And in Germany, the Hamburg Data Protection Office says it is in violation of the German Privacy Act by storing non-user personal information on third parties without permission from Facebook.

As we observe all these processes, we have to click on more than fifty buttons on your profile and personal information on a site like Facebook and ask you to select over 170 different options, so concerns about privacy breaches It is always present. For those concerned about their privacy, at least special attention should be paid to the three settings. It is now necessary to consider whether (i) you can see what you share(such as status updates or photos), (ii)who can see your personal information, and (ii)what Google can see.

Facebook founder and CEO Mark Zuckerberg said that people no longer want "complete privacy," saying they need a generational change in privacy. However, in terms of criminal policy, privacy is important and constitutionally recognized rights, and personal information infringement is also closely related, so personal information and privacy violation are not related to crime. Therefore, it is necessary to pay attention to the crime prevention aspect from the viewpoint of the users, and it is considered that the responsibility should not be overlooked from the viewpoint of the business operator. In general, SNS users are aware of the privacy and security issues associated with SNS, but are not well aware of the dangers of disclosing personal information[11].

In fact, according to a study of Chinese university students, 34.0% of students lacked knowledge of laws or regulations related to Internet management, and 18.7% of students answered that they are willing to respond to negative information or convey it to others Respectively[12].

In other words, if you understand the nature of SNS and understand the awareness and danger possibility, you can be protected from SNS crime damage. Therefore, it is important to pay attention to how well SNS users understand the attributes of SNS. Considering that cybercrime using SNS is mainly based on weakness of personal information protection, we use social networking service(SNS) so that personal information management can be carried out under self responsibility by educating and educating SNS users. It is necessary to establish clear guidelines on the limitations on the use of location information and surrounding information as the type and scope of personal information required for SNS subscription, and as linkage information.

5. Reference

5.1. Journal articles

[2] Kim DS & Cho TY. A Strategy on the Use of Space Media as Location based SNS. *Journal of Basic Design & Art*, 11(3), 35-45 (2010).

[3] Choi Y & Park SH. The Effects of Social Media Usage on Social Capital. *Korean Journal of Broadcasting and Telecommunication Studies*, 25(2), 241-276 (2011).

[4] Lee SS. Illegal Behavior in Social Network Services and Social Capital as Its Cause and the Point at Issue: Comparison between Twitter and Facebook. *Korean Criminological Review*, 94, 261-290 (2013).

[5] Kim BS. A Review on the Meaning of SNS Crime. *Chonnam Law Review*, 33(3), 169-193 (2013).

[6] Ji YH. Criminal Liability for Defamation on the SNS. *Kyunghee Law Journal*, 48(2), 117-148 (2013).

[7] Park SM. The Limitation of the Criminal Act on Minor Copyright Infringements and the types of Copyright Infringement on SNS. *Journal of Criminal Law*, 26(3), 149-177 (2014).

[8] Lee SH. Research on Criminal Legislations against Identity Theft & Impersonation through Social Network Services. *Korean Criminological Review*, 99, 127-159 (2014).

[9] Hur JS. A Study on the Problem of SNS's Infringement of Personal Information

and its Countermeasures. *Journal of Media Law*, Ethics and Policy, 9(2), 75-103 (2010).
[11] Kate Raynes Goldie. Alias, Creeping and Wall Cleaning: Understanding Privacy in the Age of Facebook. *First Monday*, 15(1), 1-22 (2010).
[12] Ji YH & Chun HW. Criminal Policy on Using Open Type SNS for Election Campaign. *Kyunghee Law Journal*, 48(4), 83-106 (2013).

5.2. Books

[1] The National White Collar Crime Center, Criminal Use of Social Media. NW3C (2013).
[10] John G. Browning. The Lawyer's Guide to Social Networking: Understanding Social Media's Impact on the Law. Thomson Reuters (2010).

Author
Yoon Hae-sung / Korean Institute of Criminology Researcher
B.A. Seowon University
M.A. Sungkyunkwan University
Ph.D. Sungkyunkwan University

Research field
- The Current Trends of Voice Phishing Fraud, Korean Association of Criminology, 25(2) (2013).
- A Review on National Security Criminal Justice of Republic of Korea in the New Security Situation, Korean Police Studies Review, 14(2) (2016).

Major career
- 2014~2015. Yongin University, Lecturer
- 2016~present. International Society for Justice & Law, Vice President