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


5.2. Books


Author

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

Research field

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