Asia Pacific Journal of Information Systems
Vol. 30 No. 1 (March 2020), 53-71

ISSN 2288-5404 (Print) / ISSN 2288-6818 (Online)
https://doi.org/10.14329/apjis.2020.30.1.53

A Lifestyle-Routine Activity Theory (LRAT) Approach to Cybercrime Victimization: An Empirical Assessment of SNS Lifestyle Exposure Activities

Jihae Suh[a,*], Jiseon Choe[b], Jinsoo Park[c]

[a] *Research Professor, AI Institute at Seoul National University, Korea*
[b] *Master Student, MIS in the Business School at Seoul National University, Korea*
[c] *Professor, MIS in the Business School at Seoul National University, Korea*

ABSTRACT

The Internet and all of its possibilities and applications have changed individuals' lifestyles in relation to socializing, working, and how they spend their leisure time. Social networking sites (SNSs), such as Facebook or Instagram, are ideal settings for interacting with others but, unfortunately, they are also ideal settings for motivated offenders to commit cybercrimes. Thus SNS users may be more vulnerable to cybercrime. The purpose of this study is to investigate the occurrence of cybercrime victimization, specifically cyber-harassment, cyber-impersonation, and hacking. Self-report surveys collected from a sample of 147 respondents were examined using the moderated multiple regression analysis and a logistic regression analysis to determine possible relationships between SNS lifestyle exposure activities and cybercrime victimization. The results indicate moderate support for the application of lifestyle-routine activity theory (LRAT) to cybercrime victimization. Possible educational and managerial implications, as well as suggestions for future research, are discussed.

Keywords: Lifestyle-routine Activity Theory (LRAT), Cybercrime, Cyber Victimization, Social Networking Sites (SNS), Online User Behavior

Ⅰ. Introduction

As the number of Internet users has grown to more than half of the world's population (Wearesocial, 2017), and technology has advanced, the way people communicate has also evolved. Social networking sites (SNSs) have recently gained popularity, in comparison to other online communication platforms, especially among young adults, as they provide a cheaper and more interactive means of communication (Kokkinos, 2017). Despite the beneficial outcomes they provide, various hazards have also been

*Corresponding Author. E-mail: jihaesuh77@gmail.com

found to accompany this "wave of digital progressivism" (Choi and Lee, 2017; Leukfeldt et al., 2017). SNS users release personal information and pictures online without realizing that these actions may lead to an increased vulnerability to cyber-harassment and identity theft (Shin, 2010). For this reason, more researchers in IS field have explored the cause or the consequences of SNS usage and cybercrime victimization such as the types of information sharing, networking opportunities for criminals, information security, and validating effective measures and mitigation controls in collaboration with the private sector (Choo, 2011; Jaishankar, 2018). Previous research on this subject has shown a correlation between SNS users' activities and their chances of being victimized online. An earlier study conducted by Spitzberg and Hoobler (2002) found that 31% of undergraduate student participants experienced some kind of personal online victimization and, in a similar study conducted by Henson et al. (2011), 42% of social network users reported the same. A more recent study performed by Kokkinos and Saripanidis (2017), focusing on Facebook user activities, shows that "the victim's behavior may enhance the chances of getting victimized" (p. 235). There does, however, seem to be a widely-mistaken assumption that only these risky online activities result in an individual becoming a potential cyber-victim. Further, the classification of risky online behaviors has become unclear due to the convergence of the diverse types of activities available on SNSs. For example, one cannot simply judge an individual's act of exposing daily activities, or expressing feelings and opinions, on a SNS to be a risky behavior since it is the main feature provided by most of the SNS platforms.

Former studies that have assessed the influence of SNS activities on cybercrime victimization have focused on a variety of cybercrime types, so the categorizations and definitions of cybercrimes vary depending on the researcher's focus. Some researchers, such as Yar (2005), make a distinction between "computer-assisted crimes" and "computer-focused crimes." Computer-assisted crimes are characterized as crimes that existed before the internet, but have taken on a new life in cyberspace (e.g., theft, fraud), whereas computer-focused crimes are crimes that have emerged with the creation of the Internet (e.g., hacking, website defacement). Other researchers, such as Wall (2001), subdivided "cybercrime" into four established legal categories: cyber-trespass, cyber-deceptions and thefts, cyber-pornography, and cyber-violence. The present study focuses on two of Wall (2001)'s categories: cyber-trespass and cyber-violence. Within these, we examined specific subtypes of these cybercrimes: violent and sexual cyber-harassment (an example of cyber-violence) and cyber-impersonation and hacking (an example of cyber-trespassing).

The current study explores SNS activities to find answers to two main research questions: *1. Are people who use SNSs more often, and share their daily activities through SNS, more likely to be victimized by cybercrimes? 2. While using a SNS, would stricter privacy settings reduce the number of individuals being victimized by cybercrimes?* The theoretical approach is mainly based on the Lifestyle-Routine Activity Theory (LRAT), an integrated theory of Hindelang et al. (1978)'s Lifestyle Exposure Theory, and Cohen and Felson (1979)'s Routine Activity Theory, found in most of the related literature. LRAT is a representative theory in the criminal psychology literature, which states that victimization is a result of individual routine activities and behaviors (lifestyle exposure activities), which increase exposure to motivated offenders, and decrease exposure to capable guardianship (Cohen et al., 1981). The purpose of the current

study is to examine whether SNS lifestyle exposure activities increase the likelihood of cybercrime victimization. Data were collected through self-report surveys, and analyzed with moderated multiple regression and logistics regression. The reason for using logistics regression is the dependent variables are binary (victimized or not victimized).

Ⅱ. Theoretical Background and Hypotheses

Previous studies, mainly focusing on identifying the factors which increase the risk of cybercrime victimization, state that the victim's behavior may be as vital as the offenders' characteristics (Elias, 1986). Further, a number of studies have applied the Victim Precipitation Model (VPM) as a framework in order to examine how a victim's behavior is associated with being victimized online (Cappadocia, 2013; Dredge, 2014; Hinduja, 2008; Kshetri, 2016; Peluchette, 2015; Staksrud, 2013; Walrave, 2011). Traditionally, according to this criminology framework, there are certain spatial and temporal conditions in which individuals initiate some type of action that results in their subsequent victimization (Miethe, 1994). Overall, these studies consistently indicate that there is a connection between the victim's behavior and the risk of being victimized online (Peluchette, 2015).

Several theories mainly focusing on the victims' characteristics and conditions such as lifestyle and backgrounds have been introduced (Cohen and Felson, 1979; Cohen et al., 1981; Hindelang et al., 1978) in order to explain the factors that precipitate victimization. Cohen et al. (1981)'s LRAT, a widely used theoretical approach to study criminal victimization, is a theory that integrates Hindelang et al. (1978)'s lifestyle exposure theory and Cohen and Felson (1979)'s routine activity theory. This integrated theory states that victimization is a result of individual routine activities and behaviors, which increase exposure to motivated offenders, and decrease exposure to capable guardianship (Cohen et al., 1981).

2.1. Lifestyle and Routine Activity Theory

According to Ngo and Paternoster (2011), both the lifestyle exposure theory (Hindelang et al., 1978) and the routine activity theory (Cohen and Felson, 1979) explained "how routine activities of the victims are related to the risk of victimization and how criminal opportunities develop out of the routine activities of everyday life" (Kokkinos, 2017, p. 773).

The LRAT is based on the idea that individuals may encounter criminal events depending mainly on the kind of settings in which they spend their free time, and what kind of activities they engage in during their free time (Svensson, 2010). The routine activity element incorporates the lifestyle theory concepts of vocational and leisure activities. According to LRAT, an individual's lifestyle routine activities and behaviors are what defines him or her to be a suitable target of cybercrime social bullying (Choi and Lee, 2017; Cohen, et al., 1981).

Cohen et al. (1981)'s LRAT theory includes the following major components: exposure to potential offenders, proximity to crime, guardianship, and target attractiveness. They were originally defined based on the relationships of each component with the physical/real world. First, the "exposure to potential offenders" component refers to the physical visibility and accessibility of persons or objects to potential offenders at any given time or in any given place. Second, "proximity to crime" is defined as the physical

distance between areas where potential targets of crime reside and areas where a relatively large population of potential offenders are found. Third, "guardianship" is defined as the effectiveness of persons (e.g., housewives, neighbors, security guards) or objects (e.g., burglar alarms, locks, barred windows) in preventing violations from occurring, either by their presence alone, or through direct or indirect action. Fourth, "target attractiveness" is the material or symbolic desirability of human or property targets to potential offenders. LRAT Theory mostly gives theoretical concepts for explaining the risk of cyber victimization. It is possible that the variables selected on the basis components of LRAT may be reflective of the characteristics of the environment in which cybercrimes occur (Vakhitova et al., 2019). The theoretical application of the LRAT to cybercrime victimization, specifically on SNS platforms, will be discussed in the following section with the details of each component.

2.2. Applying LRAT to Cybercrime Victimization

Previous studies have used the routine activity theory or the LRAT to explain cybercrime victimization related to online activities (Choi, 2008; Ngo, 2011; Yar, 2005; Yucedal, 2010) and some have applied the assumptions from the theories in a number of empirical studies (Alshalan, 2006; Choi, 2008; Holt, 2009). These studies have set their research settings as the cyberspace as a whole; however, more recent studies have incorporated SNSs as a separate environment (Back, 2016; Choi and Lee, 2017; Phillips, 2015), and some have focused on the relationship between cybercrime victimization and specific SNS platforms such as Facebook (Dredge, 2014; Kokkinos, 2017; Peluchette, 2015).

Since Facebook is different from traditional online platforms, disclosure of one's profile information to the public is possible (Gross and Acquity, 2005). In one's profile, including real name, date of birth, one's affiliation to the specific group membership such as school, workplace and even relationship status can be exposed. Thus, many previous literatures have explored Facebook by highlighting its specific effects of the openness (Kim et al., 2018). The other stream of research is to focus on the personal motives to disclosure one's information on Facebook. However, as Staksrud et al. (2013) suggested, rather than the specific aspect of SNS platform, the vulnerability of users may depend more on how individuals interacts in the Facebook. Especially, one's degree of self-disclosures can be a critical factor to be a target of a cybercrime considering the non-anonymity in the Facebook (Buglass et al., 2017).

In order to explain the theoretical application of the LRAT to cybercrime victimization, each of the four major components described in Cohen et al. (1981)'s study need to be dealt with independently. First, the current study assumes that proximity to crime is a given, as with most of the previous studies (Choi and Lee, 2017; Phillips, 2015), since the infinite and anonymous nature of the Internet means that all users are potentially proximal to crime. As the component "exposure to potential offenders" is closely related to the proximity to crime, this is also assumed. Choi and Lee (2017) argue that "given the rise of digital technology, the physical convergence of potential offenders and victims in time and space are no longer quintessential elements to engender victimization" (Pratt, 2010, p. 395). Thus, the current study will focus on the other two components, namely "target attractiveness" and "capable guardianship."

For "target attractiveness," Cohen et al. (1981) state that individual routine daily behaviors and activities, (i.e., lifestyle characteristics including vocational

and leisure activities), determine whether or not an individual is a suitable target. Previous studies have introduced risky online behavior as a concept of vocational and leisure activities. For example, Phillips (2015) conceptualized social networking itself as a risky online behavior, and Kokkinos and Saripanidis (2017) posited that a risky lifestyle on Facebook could include the time victims spend online, the number of Facebook friends, the Facebook content posted, etcetera. Choi and Lee (2017) assessed three variables of risky online behaviors, namely cyber risky SNS activities, cyber risky leisure activities, and cyber risky vocational activities. However, considering the peculiarities of SNS platforms, it is difficult to find a clear distinction between users' vocational, leisure, and risky activities within SNS. Therefore, the current study does not distinguish between the three but, instead, differentiates the types of routine activities using SNS, which will be explained in detail in the hypothesis section.

For "capable guardianship," previous studies on cybercrime attacks, such as malware or hacking, have mainly focused on physical or technological guardianship (i.e., anti-virus and firewall software; Yar, 2005; Yucedal, 2010). SNS guardianship is conceptualized as online privacy settings on personal networking sites (Choi and Lee, 2017; Phillips, 2015), which will be the focus of the current study.

2.3. Types of Cybercrime

Cybercrime can be defined as "offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS, Halder, 2011, p. 15). According to Yar (2005), the term "cybercrime" may refer to a range of illicit activities whose common distinction is the central role played by networks of information and communication technology (Phillips, 2015).

Further, cybercrime can be further divided into "computer-assisted crimes" (those crimes that pre-date the Internet but take on a new life in cyberspace, e.g. fraud, theft, money laundering, sexual harassment, hate speech, pornography) and "computer-focused crimes" (those crimes that have emerged in tandem with the establishment of the Internet and could not exist apart from it, e.g. hacking, viral attacks, website defacement) (Wall, 2001; Yar, 2005). The above definitions may be socio-technically helpful, but they have a limited criminological utility. In criminological function, cybercrime is generally classified by the subject of itself. In detail, it is categorized by three categories; against individuals, against organization, against society at large (Dashora, 2011). In case of against individuals, the subject can be person and property of an individuals, and against organization, it can be government, firm, group of individuals. The types of crime in against individuals and individual property are harassment via e-mails, defamation, cheating and fraud, transmitting virus, and unauthorized control/access over computer system etc. The types of crime in against organization are cyber terrorism against the government organization and distribution of pirated software etc. The types of crime in against society at large are online gambling, sales illegal article and forgery etc. (Dashora, 2011). Also, Wall (2001) categorized the cybercrime into four categories; cyber-trespass, cyber-deceptions and thefts, cyber-pornography, cyber-violence and it seems to better describe

cybercrime. Recently, cyber-trespass have received more attention, because social network media becomes a part of daily life and increases the users, which permits the users to share information, and can connect well with recognized friends (Wall, 2001; Yar, 2005). Therefore, the current study will focus on "cyber-trespass", which signifies crossing boundaries into other people's property and/or causing damage (e.g., hacking, defacement, viruses), and "cyber-violence", which refers to doing psychological harm to or inciting physical harm against others, thereby breaching laws pertaining to the protection of the person (e.g., hate speech, stalking). Specific cybercrime variables and measures will be described in the methodology section.

Ⅲ. Research Hypotheses and Research Model

3.1. Hypotheses

Social networking sites create an environment for both positive and negative interaction with peers. While SNSs, such as Facebook, have been found to enhance interpersonal relationships and build social capital, they have also provided a place for cybercrime offending (Kowalski, 2014). As the LRAT argues, the possibility of cybercrime offending is closely related to victims' behaviors on SNSs. Peluchette et al. (2015) have suggested that "how individuals use social networking and the type of profile content they choose to post is likely to be influenced by the level of concern that they have for what others think of them but may also unknowingly be placing them at greater risk for cyberbullying." Although their research focused on cyberbullying, there always is a possibility for other types of cybercrime.

Furthermore, self-disclosing through SNSs could enhance the chances of victimization (Wilson, 2012), since those who disclose more personal information such as his or her age and academic ability through SNSs are more likely to become victims (Peluchette, 2015). Kokkinos and Saripanidis (2017) have defined "self-disclosure" on SNSs as the willingness to discuss personal information with other users on Facebook. Choi and Lee (2017) have included "expressing opinions and feelings through SNS" as a measure of their "cyber risky SNS activities" variable. As with the above research findings, the current study assesses the influence of SNS use on cybercrime victimization, cyber harassment, cyber impersonation and cyber hacking, (Hypothesis 1 ~ Hypothesis 3) via different types of SNS activities.

Choi and Lee (2017) have stated, digital capable guardianship is conceptualized as online privacy settings on personal networking sites. Back (2016)'s study included security applications on SNSs as additional means of guardianship. However, the current study only assesses the privacy settings on SNS as capable guardianship. The privacy setting on SNS is a technical tool designed to permit users to control the amount of information they expose on their SNS profile. For example, it can be used to modify the visibility of user's profile or of certain information. Based on the above theoretical application to cybercrime, the following hypotheses have been developed for this study.

H1: Individuals who use SNSs frequently are more likely to be victims of cybercrime.

H1a: Individuals who use SNSs frequently are more likely to be victims of cyber harassment.

H1b: Individuals who use SNSs frequently are more likely to be victims of cyber impersonation.

H1c: Individuals who use SNSs frequently are more likely

to be victims of cyber hacking.

H2: Individuals who disclose preferences through SNSs are more likely to be victims of cybercrime.

H2a: Individuals who disclose preferences through SNSs are more likely to be victims of cyber harassment.

H2b: Individuals who disclose preferences through SNSs are more likely to be victims of cyber impersonation.

H2c: Individuals who disclose preferences through SNSs are more likely to be victims of cyber hacking.

H3: Individuals who express their opinions or feelings are more likely to be victims of cybercrime.

H3a: Individuals who express their opinions or feelings are more likely to be victims of cyber harassment.

H3b: Individuals who express their opinions or feelings are more likely to be victims of cyber impersonation.

H3c: Individuals who express their opinions or feelings are more likely to be victims of cyber hacking.

H4: Individuals who have stricter SNS privacy settings are less likely to be victims of cybercrime.

H4a: Individuals who have stricter SNS privacy settings are less likely to be victims of cyber harassment.

H4b: Individuals who have stricter SNS privacy settings are less likely to be victims of cyber impersonation.

H4c: Individuals who have stricter SNS privacy settings are less likely to be victims of cyber hacking.

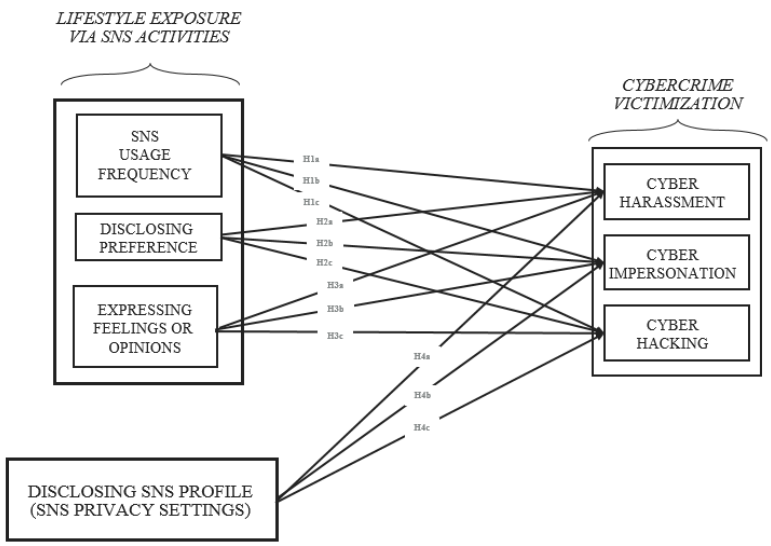
3.2. Research Model

Along with the above hypotheses, <Figure 1> depicts the research model in more detail.

Ⅳ. Research Methodology

4.1. Data and Sample

Data were collected from self-report surveys given to a random sample of respondents. 173 survey responses were initially collected from the Prolific Academic (https://prolific.ac). When the participants completed the survey, they received $1 dollar of financial reward and the period of data collection was from 2019 July 25th to 27th, for three days. Responses



<Figure 1> Research Model

<Table 1> Demographic Characteristics of Sample

Demographic Characteristics	Categories	Study Sample (N = 147)
Age	10 ~ 19	4% (n = 6)
	20 ~ 29	53% (n = 78)
	30 ~ 39	26% (n = 38)
	40 ~ 49	11% (n = 16)
	50 ~ 59	6% (n = 9)
Gender	Female	59% (n = 87)
	Male	41% (n = 60)
Occupation	Engineering / technician / IT-related	31% (n = 46)
	Student	25% (n = 37)
	Business management / finance	35% (n = 35)
	Art / entertainment / sports	5% (n = 5)
	Education / research / law / medical	21% (n = 21)
	Other	3% (n = 3)

with error, such as missing or inconsistent responses, were removed, and a final total of 147 respondents participated in the study. The demographic characteristics are presented in <Table 1>.

4.2. Independent Variables

Four independent variables related to the relationships among SNS, SNS usage frequency, disclosing preference, expressing feelings or opines and disclosing SNS profile were assessed (Back, 2016; Choi and Lee, 2017; Phillips, 2015). For SNS usage frequency, three survey items were operationalized: (1) accounts on any SNS platform (Facebook, Instagram, KakaoStory, Naver Band, or Twitter; multiple responses available); (2) amount of time spent on SNS daily and (3) number of posts, including images and video clips, uploaded daily. For statements (1), the respondents were asked to indicate their answers by selecting the box that best fit toward the given statement, and these scores were added separately for each individual. The numbers of accounts the participants indicated for statements (1) was summed and calculated as the number of total accounts, which was from 1 to 5. For statement (2), the respondents were asked to state the number of minutes spent on SNS per day, which was re-operationalized from 1 to 5. For statements (3), the respondents were instructed to estimate their number of posts and comments, which was re-operationalized from 1 to 5. The responses were integrated as one variable measuring SNS usage frequency (SNS_V1) by re-operationalizing these three sub-groups of statements. The scale had a minimum score of 1 (indicating a low level of SNS usage frequency) and a maximum score of 5 (indicating a high level of SNS usage frequency).

Three survey items covered user preferences regarding SNS activities: (1) Do you “follow” persons and pages in which you are interested? (2) Do you “like” the posts that you like or in which you are interested? (3) Do you “share” the posts in which you are interested? The respondents were asked to respond on a scale from 1 (Strongly disagree) to 5 (Strongly agree). The responses were integrated as one variable measuring whether the respondent discloses their preferences via SNS activities (SNS_V2).

To do this, all responses were summed and then re-operationalized on a scale from 1 to 5. The scale has a minimum possible score of 1 (indicating a low level of preference disclosure through SNS), and a maximum score of 5 (indicating a high level of preference disclosure through SNS).

For whether the respondent expresses feelings/opinions through SNS (SNS_V3), the survey items "whether user expresses opinions with honesty through SNS", "whether user expresses feelings on SNS" and "whether express myself on sensitive issues through SNS" were used. The respondents were asked to respond on a scale from 1 (Strongly disagree) to 5 (Strongly agree). The scale has a minimum possible score of 1 (indicating the absence of exposing feelings/opinions via SNS activities), and a maximum score of 5 (indicating the presence of exposing feelings/opinions via SNS activities)

For disclosing SNS profile, the following question was used: "To what extent do you set your privacy settings?" Respondents were asked to select the box that best fit their situation, ranging from "strongly close" to "strongly open" The scale was 1 to 5 and the responses were analyzed as one variable constituting SNS privacy settings (SNS_PS). The scale has a minimum possible score of 1 (indicating a high level of SNS privacy settings), and a maximum score of 5 (indicating a low level of SNS privacy settings)

4.3. Dependent Variables

Three dependent variables were assessed regarding cybercrime victimization (CV): (violent) cyber-harassment (CV1), cyber-impersonation (CV2), and hacking (CV3). As mentioned previously, this study focuses on the two legal categories classified by Wall (2001), namely "cyber-trespass" and "cyber-violence". The cyber-harassment measured here is related to cyber-violence, and cyber-impersonation and hacking are related to cyber-trespass. The three dependent variables are all examples of the crime victimization variable (CV). Respondents were asked to answer either "yes" or "no" to if they have ever been victimized by any of the cybercrimes mentioned (CV1 to CV3). Using a binary scale for each dependent variable ("yes" or "no"), the items were summed to create one CV variable. If the respondent was victimized by any of the four cybercrimes, the response is "yes" (1) and, if the respondent was not victimized by any, the response is recorded as "no" (0).

First, for CV, the scale represents a possible minimum score of 0 indicating no victimization, and a maximum score of 1 indicating that the respondent has been victimized. For CV1, the scale has a possible minimum score of 0 (indicating no violent cyber-harassment victimization), and a maximum score of 1(indicating that the respondent has been victimized by violent cyber-harassment). For CV2, the scale has a possible minimum score of 0 (indicating no violent cyber-impersonation victimization), and a maximum score of 1 (indicating that the respondent has been victimized by violent cyber-impersonation). For CV3, the scale has a possible minimum score of 0 (indicating no hacking victimization), and a maximum score of 1 (indicating that the respondent has been victimized by hacking).

For each construct and their measures, this study go through an extensive literature review and find evidence for our survey items from previous empirical studies in the field cybercrime. These are presented in <Table 2>.

The descriptive statistics for the study measures including the demographic variables, the independent variables, and the dependent variables are described in <Table 2>.

<Table 2> Measures for the Analysis of Cyber Crime

Constructs	Items	Scale	Reference
SNS Usage Frequency **SNS_V1**	**SNS_V1_1** Accounts on any SNS platform (Facebook, Instagram, Kakao Story, Naver Band, or Twitter; multiple responses vailable)	Range: 1-5 The number of total accounts	(Shin, 2010; Wilson, 2012)
	SNS_V1_2 Amount of average time spent on SNS daily	Range: 1-5 1: Less than 30 minutes 2: 30-60minutes 3: 60-90 minutes 4: 90-120 minutes 5: More than 120 minutes	(Shin, 2010; Wilson, 2012)
	SNS_V1_3 Number of average post including images and video clips, uploaded weekly	Range: 1-5 1: 0 Posts 2: 1 Posts 3: 2 Post 4: 3 Post 5: More than 4 Post	(Shin, 2010; Wilson, 2012)
Disclosing Preference **SNS_V2**	**SNS_V2_1** Clicked on "follow" persons and pages	Range: 1-5 1: Strongly disagree 2: Disagree 3: Neutral 4: Agree 5: Strongly agree	(Yar, 2005; Pereira et al., 2016; Kokkinos and Saripanidis, 2017)
	SNS_V2_2 Clicked on any "like" button		(Yar, 2005; Pereira et al., 2016; Kokkinos and Saripanidis, 2017)
	SNS_V2_3 Clicked on "sharing" button		(Yar, 2005; Pereira et al., 2016; Kokkinos and Saripanidis, 2017)
Expressing Feelings or opinions **SNS_V3**	**SNS_V3_1** Express my opinions with honesty on SNS	Range: 1-5 1: Strongly disagree 2: Disagree 3: Neutral 4: Agree 5: Strongly agree	(Choi and Lee, 2017; Phillips, 2015)
	SNS_V3_2 Express my feelings on SNS		(Choi and Lee, 2017; Phillips, 2015)
	SNS_V3_3 Express myself on sensitive issues through SNS		(Choi and Lee, 2017; Phillips, 2015)
Disclosing SNS Profile (SNS privacy settings) **SNS_PS**	What extent do you set your privacy setting? (Such as in Facebook, Everyone, Friends of Friends, and Friends)	Range: 1-5 1: Strongly disagree (Friends) 2: Close 3: Neutral 4: Open 5: Strongly open (Everyone)	(Choi, 2008)
Cyber Harassment **CV1**	Hate speech, meaning language that denigrates, insults, threatens or targets an individual	Range: 0-1 0: No 1: Yes	(Wall, 2001)
			(Wall, 2001)
Cyber Impersonation **CV2**	Commit something illegal while posing as you		(Wall, 2001)
Cyber Hacking **CV3**	Modifying or altering computer software and hardware		(Wall, 2001)

<Table 3> Descriptive Statistics for Study Measures

Variables	Mean	Std. Deviation	Min	Max
Independent Variables				
SNS Usage Frequency (SNS_V1)	3.01	0.73	1.00	4.67
Disclosing Preference (SNS_V2)	3.28	0.53	2.00	5.00
Expressing Feelings or Opinions (SNS_V3)	3.14	0.85	1.00	5.00
SNS Privacy Setting	2.68	1.05	1.00	5.00
Dependent Variables (CV)				
Cyber harassment (Violent) (CV1)	0.29	0.45	0.00	1.00
Cyber impersonation (CV2)	0.26	0.44	0.00	1.00
Cyber Hacking (CV4)	0.31	0.47	0.00	1.00

Upon the descriptive statistics on the independent variables, SNS usage frequency, disclosing preference, expressing feelings or opinions, SNS privacy setting showed relatively higher mean scores with 3.01, 3.28, 3.14, and 2.68 points out of 5 points, respectively. In case of dependent variables, cyber harassment (violent), cyber impersonation, and cyber hacking showed mean scores with 0.29, 0.26, and 0.31, respectively, which tells the maintenance less than 50% in view of statistical concept.

Ⅴ. Analysis and Results

5.1. Analysis

A logistic regression analysis was considered to be the most appropriate technique in the research, because all the dependent variables were binary responses and don't have to be normally distributed as well as the output of a logistic regression is more informative than other classification algorithms.

The following models describe how the logistic regression analyses were carried out depending on the hypotheses.

For Hypothesis 1a:

$$\ln(CV1) = \beta 0 + \beta 1\, x\, 1(SNS\_V1\_1) + \beta 2\, x\, 2(SNS\_V1\_2) + \beta 3\, x\, 3(SNS\_V3) + \varepsilon$$

First, in order to find out whether the chosen independent variable, namely SNS usage frequency (SNS_V1), is related to cyber harassment (CV1), the dependent variable CV1 was analyzed. Furthermore, in order to find out which specific cybercrime(CV), cyber harassment (CV1), cyber impersonation(CV2) and cyber hacking(CV3), was related to the independent variables, SNS usage frequency(SNS_V1), disclosing preference(SNS_V2), expressing feeling or opinions(SNS_V3), the logistic regression model was analyzed with each separate independent variable (SNS_V1 to SNS_V3) and dependent variable(CV1 to CV3)

For Hypothesis 4a:

$$\ln(CV1) = \beta 0 + \beta 1\, x\, 1(SNS\_PS) + \varepsilon$$

Next, in order to find out whether the SNS privacy settings was related to cyber harassment (CV1), the above regression model was used. The logistic regression model was analyzed with each dependent variable(CV1 to CV3).

5.2. Results

Moderated multiple regression analysis was performed to investigate the relationships of SNS usage frequency, disclosing preference, expressing feelings or opinions, and SNS privacy setting to cybercrime victimization.

Relationship with cybercrime victimization was reviewed under the considerations of gender and age in the first model; and then relationships of SNS usage frequency, disclosing preference, expressing feelings or opinions, SNS privacy setting to cybercrime victimization were reviewed under the controlling state of gender and age in the second model.

Controlled regression analysis demonstrated 18% of explanatory power and collinearity statistics value upon multicollinearity hypothesis was close to 1 and lower than 10 which met the basic hypothesis. With respect to Durbin-Watson value to review independency of residuals, it was 2.01 which was close to 2 to meet the hypothesis.

Upon the analysis results, only SNS privacy setting ($p < 0.01$) showed to influence to cybercrime victimization except fort SNS usage frequency, disclosing

<Table 4> The Relationships of SNS Usage Frequency, Disclosing Preference, Expressing Feelings or Opinions, and SNS Privacy Setting to Cybercrime Victimization

Model		Model Ⅰ					Model Ⅱ				
		Standardized Coefficients	*t*	*Sig.*	Collinearity Statistics		Standardized Coefficients	*t*	*Sig.*	Collinearity Statistics	
		Beta			Tolerance	VIF	Beta			Tolerance	VIF
(Constant)			3.36	0.001				0.93	0.352		
Female (Male)		0.04	0.49	0.624	0.94	1.06	0.02	0.26	0.799	0.94	1.06
20s (Teenage)		-0.23	-1.10	0.273	0.15	6.57	-0.19	-0.92	0.357	0.15	6.70
30s (Teenage)		-0.30	-1.55	0.124	0.18	5.49	-0.18	-0.96	0.338	0.18	5.70
40s (Teenage)		-0.19	-1.28	0.203	0.31	3.27	-0.10	-0.67	0.501	0.29	3.45
50s (Teenage)		-0.08	-0.65	0.515	0.43	2.35	-0.04	-0.36	0.720	0.41	2.47
SNS Usage Frequency							-0.07	-0.81	0.421	0.88	1.14
Disclosing Preference							0.01	0.12	0.901	0.93	1.08
Expressing Feelings or Opinions							-0.06	-0.80	0.425	0.92	1.08
SNS Privacy Setting							0.39	4.82	0.000***	0.93	1.08
F		0.65					3.29				
Sig.		0.662					0.001				
R Square		0.02					0.18				
Adjusted R Square		-0.01					0.12				
Change Statistics	R Square Change	0.02					0.16				
	F Change	0.65					6.46				
	Sig. F Change	0.662					0.000***				
Durbin-Watson							2.01				

Note: Dependent Variable: Cybercrime Victimization, * $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$

preference, and expressing feelings or opinions. Therefore, cybercrime victimization can be explained to be increased as SNS privacy setting is strongly open to everyone.

Logistic regression was performed to review the relationship of SNS usage frequency, disclosing preference, expressing feelings or opinions and SNS privacy setting to cyber harassment (violent). Upon the analysis results, prediction accuracy was shown to be 74.15% to meet the appropriateness of the model. Only capable guardianship ($p < 0.01$) showed to influence to cyber harassment (violent) except fort SNS usage frequency, disclosing preference, and expressing feelings or opinions. Therefore, cyber harassment (violent) can be explained to be increased as capable SNS privacy setting is strongly open to everyone.

Logistic regression was performed to review the relationship of SNS usage frequency, disclosing preference, expressing feelings or opinions and SNS privacy setting to cyber impersonation. Upon the analysis results, prediction accuracy was shown to be 76.87% to meet the appropriateness of the model. Only capable guardianship ($p < 0.01$) showed to influence to cyber impersonation except fort SNS usage frequency, disclosing preference, and expressing feelings or opinions. Therefore, cyber impersonation can be explained to be increased as SNS privacy setting is strongly open to everyone.

Logistic regression was performed to review the relationship of SNS usage frequency, disclosing preference, expressing feelings or opinions and SNS privacy setting to cyber hacking. Upon the analysis results, prediction accuracy was shown to be 72.79% to meet the appropriateness of the model. Only expressing feelings or opinions ($p < 0.01$) showed to influence to cyber hacking except fort SNS usage frequency, disclosing preference, and capable guardianship. Therefore, cyber hacking can be explained to be increased as expressing feelings or opinions is stronger.

<Table 5> The Relationships of SNS Usage Frequency, Disclosing Preference, Expressing Feelings or Opinions, and SNS Privacy Setting to Cyber Harassment (Violent)

Items	B	S.E.	Wald	Sig.	Exp(B)
20s (Teenage)	-1.38	1.40	0.98	0.323	0.25
30s (Teenage)	-1.39	1.45	0.93	0.336	0.25
40s (Teenage)	-2.65	1.73	2.35	0.126	0.07
50s (Teenage)	-1.65	1.71	0.93	0.334	0.19
Female (Male)	0.30	0.50	0.35	0.552	1.35
SNS Usage Frequency	-0.13	0.35	0.14	0.713	0.88
Disclosing Preference	-0.73	0.51	2.07	0.150	0.48
Expressing Feelings or Opinions	0.20	0.29	0.45	0.500	1.22
SNS Privacy Setting	2.00	0.35	31.95	0.000***	7.37
Constant	-3.45	2.41	2.05	0.152	0.03
- Omnibus Tests of Model Coefficients : Chi-square = 66.66, Sig. = 0.000 - Model Summary : -2 Log likelihood = 109.23, Cox & Snell R Square = 0.36, Nagelkerke R Square = 0.52 - Percentage Correct = 74.15					

Note: Dependent Variable: Cyber harassment (Violent), * p < 0.1, ** p < 0.05, *** p < 0.01

<Table 6> The Relationships of SNS Usage Frequency, Disclosing Preference, Expressing Feelings or Opinions, and SNS Privacy Setting to Cyber Impersonation

Items	B	S.E.	Wald	Sig.	Exp(B)
20s (Teenage)	-1.20	1.01	1.41	0.236	0.30
30s (Teenage)	-0.75	1.06	0.50	0.479	0.47
40s (Teenage)	-0.81	1.16	0.48	0.487	0.45
50s (Teenage)	-1.38	1.32	1.09	0.296	0.25
Female (Male)	-0.13	0.43	0.09	0.764	0.88
SNS Usage Frequency	-0.22	0.29	0.55	0.458	0.80
Disclosing Preference	0.46	0.41	1.24	0.265	1.58
Expressing Feelings or Opinions	0.09	0.25	0.12	0.729	1.09
SNS Privacy Setting	0.84	0.22	14.29	0.000***	2.31
Constant	-3.55	2.02	3.07	0.080	0.03
- Omnibus Tests of Model Coefficients : Chi-square = 20.15, Sig. = 0.017 - Model Summary : -2 Log likelihood = 147.87, Cox & Snell R Square = 0.13, Nagelkerke R Square = 0.19 - Percentage Correct = 76.87					

Note: Dependent Variable: Cyber impersonation, * $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$

<Table 7> The Relationships of SNS Usage Frequency, Disclosing Preference, Expressing Feelings or Opinions, and SNS Privacy Setting to Cyber Hacking

Items	B	S.E.	Wald	Sig.	Exp(B)
20s (Teenage)	0.09	0.92	0.01	0.925	1.09
30s (Teenage)	-0.51	0.98	0.27	0.606	0.60
40s (Teenage)	0.29	1.05	0.08	0.782	1.34
50s (Teenage)	1.07	1.14	0.89	0.347	2.92
Female (Male)	0.23	0.39	0.34	0.558	1.25
SNS Usage Frequency	-0.20	0.27	0.53	0.466	0.82
Disclosing Preference	0.08	0.36	0.05	0.822	1.08
Expressing Feelings or Opinions	-0.43	0.22	3.72	0.054***	0.65
SNS Privacy Setting	-0.25	0.18	1.91	0.167	0.77
Constant	1.41	1.80	0.62	0.433	4.10
- Omnibus Tests of Model Coefficients : Chi-square = 9.93, Sig. = 0.356 - Model Summary : -2 Log likelihood = 172.77, Cox & Snell R Square = 0.07, Nagelkerke R Square = 0.09 - Percentage Correct = 72.79					

Note: Dependent Variable: Cyber Hacking, * $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$

Ⅵ. Conclusion

The current study sought to explore how SNS lifestyle exposure activities, and the absence of SNS privacy setting, affect the likelihood of cybercrime victimization specially cyber harassment, cyber im-

personation, and cyber hacking. We hypothesized that SNS activities that expose users' lifestyles, and less strict privacy settings, would increase the likelihood of cybercrime victimization. The logistic regression analysis yielded three significant results and, in this section, the results will be discussed relative to the original hypotheses, as well as possible implications that lead on from them.

According to the findings from this study, the LRAT elements that had significant effects on the likelihood of cyber harassment and cyber impersonation was SNS privacy setting. Also, expressing feeling and opinions had significant effects on the likelihood of cyber hacking.

Some results are consistent with the original hypotheses, whereas others do not support them. Among the results, those that are consistent with the presented hypotheses are the following: Individuals who have stricter SNS privacy settings are less likely to be victims of cyber harassment and cyber impersonation than those who strongly open to everyone. And individuals who express their opinions or feelings are more likely to be victims of cyber hacking than those who rarely express their opinion.

According to above results, leaving the privacy setting open so that it can be viewed by everyone makes the individual, without any reason, more likely to become a target for hate speech, meaning language that denigrates, insults, threatens or targets an individual, and highly likely to be involved in something illegal by impersonating him/her on SNS. In addition, it means that expressing the individual's opinion or feeling with honesty on SNS makes the hardware and software of his/her computer vulnerable for hacking. Based on above results, disclosing SNS profile on SNS makes the individual more vulnerable for the cybercrime. In other words, it means that if an individual does not want to be a victim of cybercrime, he/she should open your SNS only for his/her friends.

The unexpected results are as follows: That individuals who use SNSs frequently and who disclose preferences through SNSs is more likely to become a victim of cybercrime is not significant. That is, it shows that although an individual has many SNS accounts, lots hours of using SNS and lots of postings, he/she is not likely to become a victim of cybercrime, and no matter how much he/she follows SNS of others, presses the like and sharing button, he/she does not likely become a victim of cybercrime. As a result, although the individual has many accounts and spends lots of time, engaging in simple SNS activity, that is, not writing the opinion or feeling of an individual with honesty is not likely to make him/her a victim of cybercrime. Intuitively, people think that an individual having many accounts and spending lots of time with them makes the individual to become a target of cybercrime easily, the actual results showed against it.

As a result, these findings are meaningful because they can be interpreted to indicate that people may not be vulnerable to cybercrime even if they actively show in what they are interested on SNS. Moreover, these findings imply that it might be easier for cybercriminals to target those actively express feeling or opinions on SNS and those strongly open their SNS to anyone.

Ⅶ. Discussion

With growing concerns about big social media firms already possessing a large amount of personal data, the current study adds more importance to exploring the possible outcomes of using social media carelessly. Not only should individuals be more cau-

tious about what personal information to share but, also, the SNS companies need to find discrete solutions to protect their users.

Using techniques supported by existing literature, this study applied the LRAT to cybercrime victimization, specifically violent assaulting harassments, impersonation and hacking, by means of a self-report survey. We found moderate support for the application of the LRAT to cybercrime victimization. While the study yielded significant results, both consistent and inconsistent with the original hypotheses.

One limitation of this study is the limited type of cybercrime that were included. We only investigated those who were the victims of three types of cybercrime (violent assaulting cyber-harassments, cyber-impersonation, and hacking). However, there may be individuals who were victimized by other cybercrimes such as cyber-stalking, sexting, or other kinds of sexual assault online. The scope of cybercrime should be defined more broadly in future research.

There are also opportunities for future research regarding possible privacy policy changes within social media companies. As most of the SNS companies make revenue by providing ad products, it is crucial for them to acquire more online users, as well as maintaining the uses on their services. Therefore, it would be meaningful to find out the effect of cybercrime victimization users and, thus, whether or not being victims of cybercrimes would make them leave the platform. There would be useful managerial implications if future research focused on possible policy changes on SNS users' privacy settings.

This study is important in building current and emerging literature because researchers and policymakers, or even companies, can use this results as a base on which to understand which lifestyle factors may contribute to cybercrime victimization. By analyzing these factors, education and prevention policy efforts can be made to reduce the risk of victimization, and therefore make the internet a safer place for individuals to engage in with their daily routine activities, such as social networking and communicating with others. Also, this study included different types of SNS platforms rather than focusing on only one.

Hopefully, the current study will help develop the understanding of, and literature on, cybercrime victimization, as well as encouraging further discussion on how to prevent such crimes from harming individuals.

Acknowledgement

This study was supported by the Institute of Management Research at Seoul National University.

<References>

[1] Aguinis, H. (2004). *Regression analysis for categorical moderators*. Guilford Press.

[2] Alshalan, A. (2006). *Cyber-crime fear and victimization: An analysis of a national survey*. Mississippi.

[3] Back, S. (2016). *Empirical assessment of cyber harassment victimization via cyber-routine activities theory*. Master of Criminal Justice. Bridgewater State University.

[4] Berry, W. D. (1993). *Understanding regression assumptions*. London: Sage.

[5] Buglass, S. L., Binder, J. F., Betts, L. R., and Underwood, J. D. (2017). Motivators of online vulnerability: The impact of social network site use and FOMO. *Computers in Human Behavior, 66*, 248-255.

[6] Cappadocia, M. C., Craig,W., and Pepler, D. (2013). Cyberbullying: Prevalence, stability, and risk factors during adolescence. *Canadian Journal of School*

Psychology, 28, 171-192.

[7] Cho, S., and Lee, J. M. (2018). Explaining physical, verbal, and social bullying among bullies, victims of bullying, and bully-victims: Assessing the integrated approach between social control and lifestyles-routine activities theories. *Children and Youth Services Review, 91*, 372-382.

[8] Choi, K. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology, 2*(1), 308-333.

[9] Choi, K., and Lee, J. R. (2017). Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory. *Computers in Human Behavior, 73*, 394-402.

[10] Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security, 30*(8), 719-731.

[11] Cohen, L. E., and Felson, M. (1979). Social change and crime rate trends: A routine activities approach. *American Sociological Review, 44*(4), 588-608.

[12] Cohen, L. E., Kluegel, J. R., and Land, K. C. (1981). Social inequality and predator victimization: An exposition and test of a formal theory. *American Sociological Review, 46*, 505-524.

[13] Dashora, K. (2011). Cyber crime in the society: Problems and preventions. *Journal of Alternative Perspectives in the Social Sciences, 3*(1), 240-259.

[14] Dredge, R., Gleeson, J., and de la Piedad Garcia, X. (2014). Presentation on Facebook and risk of cyberbullying victimisation. *Computers in Human Behavior, 40*, 16-22.

[15] Eck, J. E., and Clarke, R. V. (2003). Classifying common police problems: A routine activity theory approach. *Theory and Practice in Situational Crime Prevention, Crime Prevention Studies, 16*, 7-39.

[16] Elias, R. (1986). *The politics of victimization: victims, victimology, and huma rights*. New York: Oxford Press.

[17] Gross, R., and Acquisti, A. (2005). Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on Privacy in the Electronic Society*, 71-80. New York, NY: ACM. November 2005.

[18] Halder, D., and Jaishankar, K. (2011). *Cyber crime and the victimization of women: Laws, rights and regulations*. India: Manonmaniam Sundaranar University.

[19] Henson, B., Reyns, B. W., and Fisher, B. S. (2011). Security in the 21st century examining the link between online social network activity, privacy, and interpersonal victimization. *Criminal Justice Review, 36*(3), 253-268.

[20] Hindelang, M. J., Gottfredson, M. R., and Garofalo, J. (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization*. Cambridge, Mass: Ballinger Pub. Co.

[21] Hinduja, S., and Patchin, J. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. *Deviant Behavior, 29*, 129-156.

[22] Holt, T. J., and Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior, 30*, 1-25.

[23] Holtfreter, K., Reisig, M. D., and Pratt, T. C. (2008). Low self-control, routine activities, and fraud victimization. *Criminology, 46*, 189-220.

[24] Jaishankar, K. (2018). Cyber criminology as an academic disipline: History, contribution and impact. *International Journal of Cyber Criminology, 12*(1), 1-8.

[25] Kim, Y., Park, Y., Lee, Y., and Park, K. (2018). Do we always adopt Facebook friends' eWOM postings? The role of social identity and threat. *International Journal of Advertising, 37*(1), 86-104.

[26] Kokkinos, C. M., and Saripanidis, I. (2017). A lifestyle exposure perspective of victimization through Facebook among university students. Do individual differences matter? *Computers in Human Behavior, 74*, 235-245.

[27] Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., and Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin, 140*, 1073.

[28] Kshetri, N. (2016). Cybercrime and cybersecurity in India: Causes, consequences and implications for the future. *Crime, Law and Social Change, 66*(3), 313-338.

[29] Leukfeldt, E. R., Kleemans, E. R., and Stol, W. P. (2017). Origin, growth and criminal capabilities of cybercriminal networks: An international empirical analysis. *Crime, Law and Social Change, 67*(1), 39-53.

[30] Long, S. J., Long, J. S., and Freese, J. (2006). *Regression models for categorical dependent variables using Stata*. Stata Press.

[31] Messner, S. F., and Blau, J. R. (1987). Routine leisure activities and rates of crime: A macro-level analysis. *Social Forces, 65*(4), 1035-1052.

[32] Miethe, T. D., and Meier, R. F. (1994). *Crime and its social context : toward an integrated theory of offenders, victims, and situations*. Albany: State University of New York Press.

[33] Ngo, F. T., and Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology, 5*(1), 773.

[34] Peluchette, J. V., Karl, K., Wood, C., and Williams, J. (2015). Cyberbullying victimization: Do victims' personality and risky social network behaviors contribute to the problem? *Computers in Human Behavior, 52*, 424-435.

[35] Pereira, F., Spitzberg, B. H., and Matos, M. (2016). Cyber-harassment victimization in Portugal: Prevalence, fear and help-seeking among adolescents. *Computers in Human Behavior, 62*, 136-146.

[36] Phillips, E. (2015). *Empirical assessment of lifestyle-routine activity and social learning theory on cybercrime offending*. Master of Criminal Justice. Bridgewater State University.

[37] Pratt, T. C., Holtfreter, K., and Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency, 47*(3), 267-296.

[38] Shin, D. H. (2010). The effects of trust, security and privacy in social networking: A security based approach to understand the pattern of adoption. *Interacting with Computers, 22*(5), 428-438.

[39] Spitzberg, B. H., and Hoobler, G. (2002). Cyberstalking and the technologies of interpersonal terrorism. *New Media & Society, 4*(1), 71-92.

[40] Staksrud, E., Olafsson, K., and Livingstone, S. (2013). Does the use of social networking sites increase children's risk of harm? *Computers in Human Behavior, 29*, 40-50.

[41] Suh, J., Park, J., Kim, B., and Rahman, H. A. (2018). How practitioners perceive a ternary relationship in ER conceptual modeling. *Asia Pacific Journal of Information Systems, 1*(1), 75-92.

[42] Svensson, R., and Pauwels, L. (2010). Is a risky lifestyle always "risky"? The interaction between individual propensity and lifestyle risk in adolescent offending: A test in two urban samples. *Crime & Delinquency, 56*(4), 608-626.

[43] Vakhitova, Z. I., Alston-Knox, C. L., Reynald, D. M., Townsley, M. K., and Webster, J. L. (2019). Lifestyles and routine activities: Do they enable different types of cyber abuse? *Computers in Human Behavior, 101*, 225-237.

[44] Wall, D. (2001). Cybercrimes and the internet. In D. Wall (ed.) *Crime and the internet*. London: Routledge.

[45] Walrave, M., and Heirman, W. (2011). Cyberbullying: Predicting victimization and perpetration. *Children & Society, 25*, 59-72.

[46] Wearesocial. (2017). *Digital in 2017: Global overview*. Retrieved from https://wearesocial.com/special-reports/digital-in-2017-global-overview

[47] Wilson, R. E., Gosling, S. D., and Graham, L. T. (2012). A review of Facebook research in the social sciences. *Perspectives on Psychological Science, 7*, 203-220.

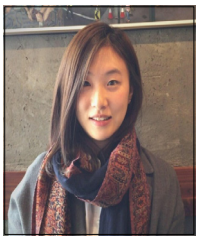
[48] Yar, M. (2005). The novelty of 'cybercrime' an assessment in light of routine activity theory. *European Journal of Criminology, 2*(4), 407-427.

[49] Yucedal, B. (2010). *Victimization in cyberspace: An application of routine activity and lifestyle exposure theories*. Doctor of Philosophy. Kent State University.

◆ About the Authors ◆

Jihae Suh

Jihae Suh is the corresponding author of this paper and received a Ph.D. degree in Management Information Systems from the Seoul National University in 2017. She received her Master degree from Carnegie Mellon University and B.A. from Kyung Hee University. Currently, she is a research professor at Seoul National University Big Data Institute.



Jiseon Choe

Jiseon Choe received a Master degree in Management Information Systems from Seoul National University in 2018. Formerly, she received her B.A. degree in History and Business Administration at Korea University. Her interest area was social big data, data analysis, and cybercrime.

Jinsoo Park

Jinsoo Park is Professor of MIS in the Business School at Seoul National University. He was formerly on the faculties of the Department of Information and Decision Sciences in the Carlson School of Management at the University of Minnesota and the Department of Management Information Systems in the College of Business Administration at Korea University. He received a PhD degree in Management Information Systems from the University of Arizona in 1999. His research interests are in the areas of ontology, semantic interoperability and metadata management in interorganizational information systems, schema matching, and data modeling. His research has been published in *MIS Quarterly, IEEE Transactions on Knowledge and Data Engineering* (TKDE), *IEEE Computer, ACM Transactions on Information Systems* (TOIS), *Data & Knowledge Engineering, Journal of Database Management*, and several other journals and conference proceedings.

Submitted: December 6, 2018; 1st Revision: February 24, 2019; 2st Revision: September 14, 2019; Accepted: November 29, 2019