Asia-Pacific Social Science Review 20(4) 2020, pp. 123–135

RESEARCH ARTICLE

Online Victimization, Social Media Utilization, and Cyber Crime Prevention Measures

Claudia San Miguel, Kristina Morales, and Marcus Antonius Ynalvez*
Texas A&M International University, USA
*mynalvez@tamiu.edu

Abstract: Engaging concepts germane to lifestyle-routine activities theory (LRAT), this study examines how social media (SM) utilization shapes online victimization experience. It also explores how considerations about online prevention measures play a moderating role between utilization and victimization. This study focuses on the Facebook® utilization of a subset of the U.S. population hitherto understudied in cybercrime prevention studies: Hispanics. An online survey was used to collect information pertaining to respondents' online victimization experience, social media utilization, and aspects of prevention measures. Logistic and negative binomial regression analyses were performed on two measures of online victimization (ever victimized and frequency of victimization). The findings demonstrate how LRAT can explain the link between SM utilization, prevention measures, and online victimization. The results highlight the role of two temporal aspects of utilization (intensity and extensity) in shaping online victimization experience along with the conditioning role of the salience of mutuality (i.e., the importance of mutuality—to an SM user—in deciding to accept an online friend request). Mutuality was found to be a critical moderating factor between temporal aspects of SM utilization and online victimization. The findings have important implications for online safety, cybercrime prevention, and online victimization awareness initiatives.

Keywords: Online victimization, social media utilization, salience of mutuality, cybercrime prevention

Social interaction via social media is rapidly outpacing face-to-face communication (Keller, 2013). With the increasing pervasiveness of the Internet in daily life, many have fallen victim to crimes on social media, such as Facebook® (FB), Twitter, and Instagram (Federal Bureau of Investigation [FBI] 2014, 2015a, 2015b; Reyns et al., 2011). Online offenders target these sites to carry out cyberbullying, hacking, identity theft, and cyberstalking. In 2014 alone, the FBI reported that ~9,800 individuals were victims of cybercrimes. Few studies have applied extant criminal justice theories to understand the nature and dynamics of these emergent crimes. However, skeptics argue that these theories are inadequate in explaining online victimization due to differences in the logic and opportunities between cyberspace and real space.

To date, criminal justice research on online victimization is still in its infancy. Most of the few extant studies have been exploratory in nature, focused on the adolescent population, and typically geared towards cyberbullying, given its high prevalence (Gilkerson, 2012). Scant attention has also been

devoted to understanding how social media utilization and considerations of cybercrime prevention measures link to online victimization (Henson et al., 2011). More importantly, studies focusing on minorities are very limited. Although there are a few studies on Hispanic victimization, these seldom relate to cyber activities (Sugarmann, 2014; FBI Law Enforcement Bulletin, 2015). Indeed, criminal justice research is sparse when it comes to cybercrimes committed on Hispanics, and this study fills this knowledge gap. Although online victimization is not exclusive to FB, this study focuses on this social media site, as it is the most popular site in the U.S. and the world (Milanovic, 2015).

The hypothesis that guides this study is that social media utilization influences online victimization experience, whereas considerations about prevention measures conditions utilization's impact on experience (Figure 1). By testing this hypothesis, we contribute to the criminal justice theory by adding to the scarce inventory of empirical studies on minorities and elaborating on the moderating role of prevention measures. This study follows a strand of research that combines routine activities theory (RAT) and lifestyle theory (LT*)* to elucidate online victimization experience better as it relates to micro-level antecedents and correlates such as intensity and extensity of utilization, and the role of mutuality in online social networks.

Literature Review

The Internet has provided people worldwide with vast opportunities, including criminal opportunities (Reyns et al., 2011). Not only does the Internet allow individuals to connect with others, communicate with family and friends, develop new relationships, build social capital, and expand social networks, it also gives people the opportunity for non-collocated and non-face-to-face interaction (Bossler & Holt, 2009). Arguably, the Internet has altered how people communicate and connect so much so that it has modified routines and lifestyles (Bossler & Holt, 2009; Bossler et al., 2012).

Indeed, the Internet has also paved the way and provided a space for new forms of criminal activities, such as cyberbullying, cyber impersonation, and identity theft, to mention a few. These activities occur in the various functionalities of the Internet, and social media sites such as Twitter, Instagram, and Facebook are not exempt (Reyns et al., 2012).

Facebook

Facebook connects users with colleagues, friends, relatives, and even strangers (Milanovic, 2015; Smith 2016). It also allows sharing pictures, thoughts, links, and affords the ability to support and like pages of organizations and brands (Milanovic, 2015). FB is the most popular social media site, averaging over a billion active users a day (Smith, 2016). In regards to online victimization on FB, privacy settings are critical, given the amount of personal information shared (Liu et al., 2011).

FB offers users two options to control privacy settings: basic and advanced (FB Help Center, 2015). Basic privacy settings allow users to select who can

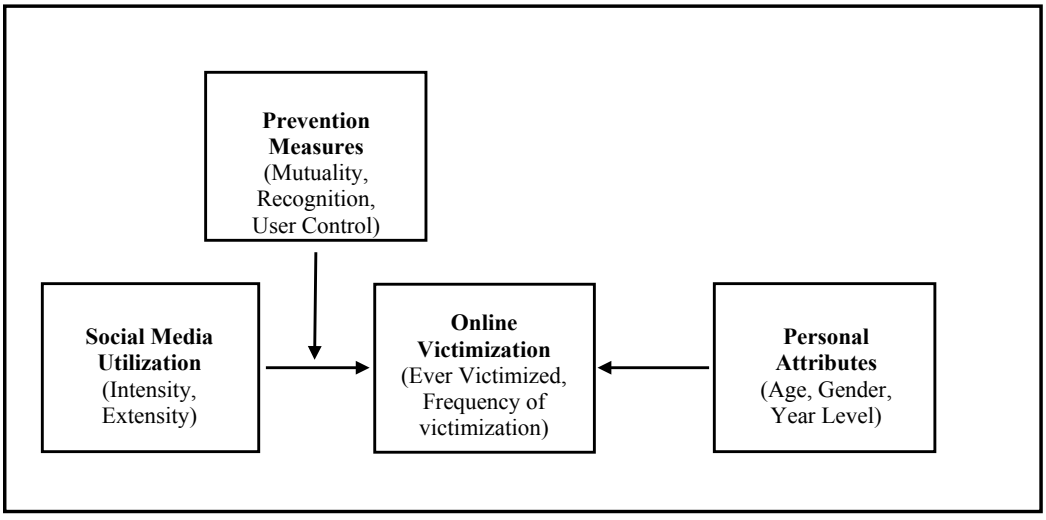

Figure 1. Conceptual Model

view their information, how they can connect with friends, who can add them, who can see their profiles, and remove posts they do not want to be linked/tagged to their profile pages (FB Help Center, 2015). Alternatively, advanced privacy controls allow users to remove posts they are tagged in, approve tags before allowing users' friends to view these posts, precludes others from posting on users' timeline, make finding users difficult, and allow certain posts to be hidden from others (FB Help Center, 2015).

Cybercrimes

Cybercrimes are offenses committed against an individual or a group of individuals using computer-based technologies such as the Internet, emails, chatrooms, or social media with the intent of purposefully causing harm, whether that be financial, legal, mental, emotional, or reputational (Halder & Jaishankar, 2011). Cybercrime is often committed against an individual without his/her knowledge because cybercriminals usually make such actions hard to discover (Oluga et al., 2014). There are many types of cybercrime, such as cyberbullying and harassment, cyber extortion, hacking, copyright infringement, online-romance scam, identity theft, and online fraud (Oluga et al., 2014). *Cyberbullying* occurs when an individual or a group of individuals, willfully using electronic technology, repeatedly harasses or threatens others by posting disturbing photos, texts, graphics, or by sending such information to others (Dilmac, 2009).

Computer hacking has wide significance in the world of computer networking and online communities (Jordan & Taylor, 1998). Computer hacking includes deceiving, downloading, or intruding into a person's communication and information systems (Oluga et al., 2014). Cyber impersonation is about a cybercriminal hacking into someone's account, posing as that someone and altering his/her status, comments, or sending messages that will make the individual look bad to ruin the victim's reputation, friendships, or to put the victim in trouble or in danger (Mann, 2015).

Online romance scams, also so-referred to as being cat-fished, are schemes whereby cybercriminals pretend to be someone else and may seek romance and companionship from a potential victim (Internet Crime Complaint Center, 2014). Such criminals search for potential victims through chat rooms, dating sites, and social media sites. They often use lies and manipulation to trick their victims (Internet Crime Complaint Center, 2014). Online romance scams do not only rob victims of money; victims are also often left to deal with the psychological trauma such as loss of confidence, depression, or a sense of betrayal (Whitty & Buchanan, 2012).

Online fraud is a criminal activity involving a computer or an Internet connection where a perpetrator may use sophisticated techniques to obtain personal information (Legal Information Institute, 2015). It may involve identity theft or financial fraud (National Crime Victim Law Institute, 2010). Fraud is an act of intentional deception to obtain personal gain or to cause a loss to an individual (Serious Fraud Office, 2015).

Identity theft is one of the fastest-growing crimes in the U.S. (Social Security Administration, 2015). It happens when someone unlawfully acquires an individual's personal data to use that individual's private information to commit theft or fraud (FBI, 2015a, 2015b). Furthermore, identity theft includes stealing information such as passwords, social security numbers, date of birth, passport numbers, death certificates, and other personally identifiable information (FBI, 2015a, 2015b).

Online Victimization Experience and Prevention Measures

Like other crimes, online victimization experience can vary in severity, frequency, and diversity. Depending on the cybercrime, victimization may require law enforcement, medical, or psychiatric assistance because victims may become suicidal, depressed, nervous, anxious, fearful, or afraid (Zhang et al., 2010). With respect to the frequency of victimization, it is possible that individuals experience repeated victimizations (Ybarra et al., 2012). Frequency is also important to study, as it is crucial to determine how long a user experienced being a victim or, for current victims, how long they have been experiencing online victimization as the severity of adverse effects from victimization experience typically from its frequency.

There are certain cybercrime prevention measures users can take in an online environment. Prevention measures or safety precautions include running and updating anti-virus programs, ensuring a running firewall, securing and using strong passwords, and installing updates (Anderson & Agarwal, 2010). Wall (2008) found that if users have a reliable security program installed and updated Internet browsers, their likelihood of experiencing online victimization is

reduced. In this study, the role of prevention measures is examined to determine whether such measures condition victimization experience. This is carried out by incorporating the importance of having mutual friends, number of mutual friends, recognition of a user's profile name and user profile photo, and the degree of user control in the analytical framework.

Lifestyle-Routine Activity Theory (LRAT)

LT is a type of personal victimization theory (Jensen & Brownfield, 1986) where lifestyle refers to an individual's way of life and indicates activities across extended periods. These activities include those in the home, school, leisure, and at work. These also include evening recreational activities (Myrstol & Chermak, 2005). LT's centerpiece hinges on time—intensity and extensity—people spend in public places, their personal characteristics (e.g., age, gender, etc.), and their interaction with others, which may include potential offenders (Jensen & Brownfield, 1986). LT argues that lifestyle is critical because it determines the extent to which an individual interacts with motivated offenders in the absence of capable guardians (Jensen & Brownfield, 1986). In essence, LT focuses not only on activities but also on the characteristics of individuals that make them vulnerable targets of crimes (Myrstol & Chermak, 2005).

RAT extends LT and posits that an individual's daily routines put that individual at high risk of victimization (Frailing & Harper, 2013). In RAT, three elements are necessary for a crime to take place: a motivated offender, a potential target, and the absence of a capable guardian (Cohen & Felson, 1979). Crimes are highly likely when a motivated offender encounters a suitable target in the absence of a capable guardian.

Applied to online victimization, a motivated offender may lurk in a variety of cyber locales, such as social media sites, whereas potential targets may be anyone who spends time online. The absence of capable guardianship can be manifested by not having a firewall, a security program installed in a user's computer, or both (Reyns et al., 2011). This can also be manifested when one fails to apply appropriate privacy settings, prevention measures, or both. Similar to LT, RAT posits that the more time online one spends, the greater his/her chances of being victimized. Reyns et al. (2011) reported that an increase in Internet usage increases a target's susceptibility; that susceptibility increases when one posts personal information such as relationship attributes, e-mail addresses, and sexual orientation.

The idea of fusing LT and RAT—referred to as LRAT—to explain cybercrimes is creative, and there are proponents and opponents. Proponents such as Holt and Bossler (2008) reported a positive correlation between the number of hours an individual spends online and the likelihood of victimization. Reyns (2013) applied LRAT to crimes where the offender and the victim were never in direct contact. He examined victims of identity theft and their daily routines while also considering their personal characteristics and perceived risks of identity theft victimization. Reyns (2013) found support for the application of LRAT in explaining online victimization. The study highlights that crimes do not only occur during direct contact but may also occur indirectly through Internet connections and exchanges in cyberspace.

It is worth noting that there are also researchers who argued that elements of LRAT might not be suitable for the study of online victimization (Reyns et al., 2011). For example, Yar (2005) contended that spatial and temporal aspects are critical in explaining the criminal activity. As such, LRAT might not explain cybercrimes, given that these crimes occur in non-linear time and space of flows (Reyns et al., 2011; Yar, 2005). Because victims and offenders must connect for a crime to occur in cyberspace, victim and offender do not come together in the same real space, many researchers take this non-alignment to imply that LRAT may not be apply to cybercrimes (Reyns et al., 2011).

With these seemingly opposing views, two divergent views have emerged, namely: (a) LRAT is applicable to only place-based crimes; and (b) LRAT simply needs revision to include other crimes where victim and offender do not have contact with one another in a physical and real environment (Reyns et al., 2011; Tillyer & Eck, 2009).

This paper forwards the argument that it is possible to revise LRAT to include online contact between offender and victim. This happens when the offender's and the victim's "network devices" connect in cyberspace (Reyns et al., 2011). This thinking is in keeping with criminal justice scholars who recognize that advancements in information and communication technologies trigger processes of creating and re-creating new opportunities for crime and victimization to occur. As Reyns (2013) stated, the Internet has created new opportunities for crime to take place,

not only in the traditional physical environment but also in a completely new environment—the online environment.

Methods

Study Location

This study was conducted at Texas A&M International University (TAMIU), located in Laredo, Texas. Laredo is a city along the U.S. southwest border with Mexico. It has a population of ~255,473, of which 96% are Hispanics (United States Census Bureau, 2015) and an average crime rate of 331 per 100,000; this is higher than the national average of 257 per 100,000. Cybercrime statistics for the city are not yet available, but as of 2014, Texas ranked third among the top 10 states in terms of the total number of complaints and financial losses amounts resulting from cyber victimization (Internet Crime Complaint Center, 2014). TAMIU is a 4-year public regional university. It is mainly (86%) an undergraduate institution. As of fall 2019, current enrollment was over 8,000. Its student population comprised ~59.4% female, ~40.6% male, ~92.7% Hispanic, ~56% low income.

Data Collection Method

A Survey Monkey online survey was used to collect information pertaining to respondents' sociodemographic characteristics, online victimization experience, social media (i.e., FB) utilization, and aspects of prevention measures. TAMIU's Institutional Review Board reviewed, approved, and had oversight over this study's research protocol.

Target Population

This study focuses on undergraduate students' online victimization because 93% engage social media sites at significantly higher rates than any other age group (Lindsay & Krysik, 2012). Majority of undergraduate students are millennials. Recent statistics indicate that 91% of millennials utilize FB, with the average user spending at least 20 minutes per day on FB (Smith, 2016). Although undergraduate students are disproportionately susceptible to identity theft (Identity Guard Resource Center, 2015), there are very few studies conducted on undergraduate students.

Although Marcum et al. (2010) reported that adolescents and young adults subpopulations have the fastest-growing rates of Internet use, it is equally important to consider undergraduate students because they are also identified as an at-risk group for cybercrime (Reyns et al., 2011). This high risk is largely due to undergraduates routinely using the Internet to do course requirements such as assignments, term papers, and so forth (Reyns et al., 2011). Further exacerbating this is that undergraduate students are prone to not having computer-security software (Choi, 2008).

Sampling and Sample

TAMIU undergraduate Hispanic students enrolled in criminal justice and psychology programs were surveyed in spring and summer 2016. A combination of two samples, one with students enrolled in the University's SONA system, and the other sample involved face-to-face recruitment in two criminal justice courses. SONA is a cloud-based software environmental management system, which aids universities in managing research studies and recruiting participants online (SONA Systems, 2016).

Hypothesis

The hypothesis that guides this study is FB utilization influences online victimization. However, considerations about prevention measures (i.e., number of mutual friends, recognition of friend requests, and degree of user control) moderate the influence of FB on victimization.

Dependent Variables

Online victimization experience was cast in two dimensions: "ever victimized" and "frequency of victimization." The measure for ever victimized is derived from six binary items answerable by either a yes (1) or a no (0). Each binary variable stems from questions that asked respondents whether they were a victim of (a) hacking, (b) cyber-impersonation, (c) cyberbullying, (d) identity theft, (e) an online romance scam, or (f) online fraud on FB. The sum of responses to these six binary items was calculated. The resulting sums were then further recoded as either "1" if response was between 1 to 6, inclusive, or "0" if zero. This recoded variable served as the final measure of ever victimized.

There are six items to measure the frequency of victimization, which had the generic interrogative phrase: "How many times did you experience this

type of cyber-crime?" This phrase was used for all the six types of cybercrimes (mentioned above). These questions were asked only to those who have responded "yes" to the question: "have you ever experienced being victimized online?" Because the original response categories to each of these questions were in ranges (i.e., 1 to 2 times, 3 to 4 times, 5 to 6 times, 7+ times), the midpoint was used in the analysis. If, for example, a respondent answered "1 to 2 times," the midpoint 1.5 was used; for "3 to 4 times," 3.5 was used; for "5 to 6 times," 5.5 was used; and for "7+ times," 7 was used.

Independent Variables

The following variables were used as multivariate controls: age (in years) male (male=1; female=0), and senior level (1=senior, 0=non-senior). FB utilization was cast in two dimensions: extensity and intensity. The extensity of utilization was measured by the question, "For how many years have you been using FB?" The intensity of utilization was measured by the question, "On average, how many hours/minutes a day do you spend on FB?" With the original response categories expressed in ranges, the midpoint was calculated and used in the analysis.

Aspects of prevention measures included mutuality, recognition, and control settings. Constructing a measure of salience of mutuality involved two questions. The first question was, how important was the number of mutual friends in accepting an FB friend-request? This was answerable using the following scale: 1=not important, 2= important, 3=very important. The second was how many mutual friends should there be in accepting an FB friend-request? Response categories were 0, 1–5, 6–10, and 11+. The second step was to subject responses to these questions to a principal component analysis (PCA).

PCA is a statistical technique to reduce a set of correlated items to a parsimonious and trackable set of mathematically derived variables called PCs. PCs are linear combinations of the original correlated items (Alani, 2014). The two correlated items subjected to PCA were the number of mutual friends between the respondent and FB friend requester, and the importance of having mutual friends in deciding whether to accept or reject an FB friend request (1=not important, 2=important, 3=very important). PCA generated one PC, which was referred to as salience of mutuality (i.e., the importance of mutuality to a social media user in accepting an online friend request). High scores on this PC indicate that mutuality was an important consideration in a user's decision to accept an online friend-request, whereas low scores indicate the converse.

Questions about the importance of recognizing a user's FB profile and the importance of recognizing a user's FB name had similar response categories to those mentioned above. In regards to the degree of user control, types of personal information that respondent sets to either private (0) or public (1) were used. More specifically, "who can view your posts? Videos? Personal information? Status Updates? Photos?" Each of these five items was answerable by either 1= public or 0=private, with the average computed and used in the analysis. However, another binary variable used was whether a respondent has his or her FB postings set to either private (0) or public (1).

Analytical Strategy

For ever victimized (1=yes, 0=no), a binary logistic regression analysis was performed. For the frequency of victimization, which exhibited a positively skew frequency distribution and overdispersion, a negative binomial regression analysis was carried out. In analyzing ever victimized, the entire sample size of n=209 was used. For the frequency of victimization, only respondents who had ever experienced online victimization were included (n=90).

Results

Table 1 shows that majority of respondents were female (74%), non-senior (53%), 19 to 22 years of age (43.3%), inclusive. In terms of FB utilization, a plurality of respondents spent less than an hour per week on FB (34%) and had been on FB for six years (23%). In terms of mutuality, most respondents viewed it very important to have mutual friends (66%) and indicated they needed to have between one and five friends (42%) in common before they would accept an FB friend request.

In terms of recognition, respondents said it was not only important (46%) but also very important (46%) to recognize a friend requester's profile name. In addition, respondents said it was very important (56%) to recognize an FB friend requester's profile

Table 1

Descriptive Statistics

Variables of the Study	Min.	Max.	Mean	SD
Age (in years)	20.50	27.0	23.30	2.63
Senior (1= Senior, 0= Non-Senior)	0.00	1.00	0.47	0.50
Male (1= Male, 0= Female)	0.00	1.00	0.26	0.44
Intensity (No. of hours per week using Facebook)	0.50	5.00	2.49	1.84
Extensity (No. of years using Facebook)	0.00	10.00	5.67	2.41
Importance of Having a Mutual Friend (1= Not Imp, 2= Imp, 3= Very Imp)[a]	1.00	3.00	2.56	0.67
Number of Mutual Friends (1=0, 2 = 1 to 5, 3 = 6 to10, 4 = 11 and over)	0.00	11.00	6.49	3.82
Mutuality Score (PCA-Derived; centered)	-2.57	1.16	0.00	1.00
Recognition of User Name (1= Not Imp, 2= Imp, 3= Very Imp)	1.00	3.00	2.38	0.63
Recognition of User Profile Photo (1= Not Imp, 2= Imp, 3= Very Imp)	1.00	3.00	2.53	0.57
Recognition Score (Mean; centered)	-1.52	0.48	0.00	0.40
Posts are set to (1= Public, 0= Private)	0.00	1.00	0.14	0.35
Personal Information are set to (1= Public, 0= Private)	0.00	1.00	0.68	0.47
User Control (Mean; centered)	-0.37	0.63	0.00	0.40
Has Ever Been Victimized (1=Yes, 0=No)	0.00	1.00	0.52	0.50
Frequency of Victimization[b]	7.00	126.00	12.83	16.64

N=209

[a] Imp = Important

[b] Computed for respondents who reported having ever been victimized (N=90)

photo prior to accepting a request. In regards to user control, five items were used to construct the scale to measure user control. These items were (a) postings, (b) personal information, (c) videos, (d) photos, and (e) status updates. In analyzing the data, however, only responses relating to postings and personal information were usable because there were many missing values for the other three items. Majority of respondents had their postings set to private (86%) and their personal information set to public (68%).

For ever victimized, the overall regression equation was statistically significant ($p<0.01$), but no interaction terms were significant (Table 2). There were three significant main effects, namely: males, intensity of FB utilization, and user control. Without any significant interaction terms, these results indicate that gender, intensity of utilization, and user control directly and independently shaped victimization experience. Specifically, the odds of males experiencing online victimization was 0.21 times [i.e., exp(B) = 0.21; p = .0010] that of females.

Put another way, the odds of experiencing victimization were 79% less likely for males. These results also underscore that as the number of hours per week spent on FB (intensity of use) increased by one hour, the odds of experiencing online victimization increased by 1.25 times [i.e., exp(B) =1.25; p = .0170]. Lastly, the results show for user control, the odds of experiencing online victimization of those who set their privacy settings to public are ~3.00 times

Table 2

Binary Logistic Regression for Ever Been Victimized (N=209)

Predictors	B	SE(B)	exp(B)	p-value	
Constant	-2.67	1.63	0.07	.1009	
Age (years)	-0.10	0.07	0.91	.1764	
Senior (1=senior, 0=non senior)	-0.02	0.37	0.98	.9531	
Male (1=yes, 0=no)	-1.54	0.46	0.21	.0008	***
Intensity (hrs. per week; centered)	0.23	0.10	1.26	.0174	*
Extensity (yrs. Centered)	-0.04	0.09	0.96	.6545	
User Control (UC; 0=private, 1=public)	1.05	0.45	2.87	.0188	*
Mutuality (PCA-derived score; centered)	-0.07	0.20	0.93	.7242	
Recognition (Mean-derived score; centered)	-0.71	0.49	0.49	.1467	
Intensity X UC	0.02	0.11	1.02	.8411	
Intensity X Mutuality	-0.27	0.28	0.76	.3298	
Intensity X Recognition	-0.03	0.24	0.97	.8866	
Extensity X UC	-0.20	0.23	0.82	.3904	
Extensity X Mutuality	0.14	0.09	1.15	.1386	
Extensity X Recognition	-0.34	0.24	0.71	.1561	
R^2 (Nagelkerke)	.21				
p-value	.0100				
df	152				

*p<0.05, **p<0.01,***p<0.001

[exp(B) = 2.80; p = .0190] compared to those who set their privacy settings to private.

For the frequency of victimization, the overall regression equation was statistically significant (p = 0.0480), meaning that at least one of the predictors influenced the frequency of victimization (Table 3). Clearly, males exhibited higher victimization frequency than females (B = +1.60; p = .0000). Results also indicated a significant interaction between intensity and salience of mutuality (B = -0.25; p = .0020). In other words, when the salience of mutuality was low, high intensity of use was associated with a high frequency of victimization. When salience of mutuality was high, the high intensity was associated with low levels of victimization frequency. A similar pattern was observed between the extensity of use and salience of mutuality (B = -0.17; p = 0.0190), with the caveat that the regression coefficient was smaller compared to that for the intensity of use and salience of mutuality.

Discussion

The research question this study sought to answer was, "does social media utilization impact online victimization experience, and does such an impact, if it exists, moderate considerations about prevention measures?" In regards to the first part of this question, results suggest that the answer is yes. The amount of time (intensity not extensity) a user spends online determines one's chances of victimization. As to the

Table 3

Negative Binomial Regression Results for Frequency of Victimization (N=90)

Predictors	+B	SE(B)	95% Wald CI		p-value	
			Lower	Upper		
Constant	-18.24	0.183	-18.598	-17.882	0.000	***
Year level (1=senior, 0=non-senior)	-2.95	0.309	-3.561	-2.348	0.000	***
male (1=yes, 0=no)	1.60	0.433	0.754	2.451	0.000	***
Intensity (hrs. per week; centered)	-0.05	0.080	-0.207	0.105	0.522	
Extensity (yrs.; centered)	-0.14	0.088	-0.316	0.030	0.105	
User Control (UC; 0=private, 1=public)	0.36	0.383	-0.389	1.111	0.345	
Mutuality (PCA-derived score; centered)	0.17	0.148	-0.121	0.458	0.254	
Recognition (Mean-derived score; centered)	-0.47	0.395	-1.244	0.305	0.234	
Intensity X UC	0.03	0.218	-0.401	0.454	0.903	
Intensity X Mutuality	-0.25	0.082	-0.413	-0.090	0.002	**
Intensity X Recognition	0.08	0.258	-0.426	0.585	0.758	
Extensity X UC	0.32	0.215	-0.100	0.742	0.135	
Extensity X Mutuality)	-0.17	0.072	-0.310	-0.028	0.019	*
Extensity X Recognition	0.41	0.276	-0.133	0.948	0.140	
(Scale)	1[a]					
(Negative binomial)	1[a,b]					

[a] Fixed at the displayed value.

[b] Poisson-based model revealed over dispersion; the omnibus test for this negative binomial-based model yielded the following results: LR chi-square = 122.2; df = 13; p-value = 0.000.

*p<0.05, **p<0.01,***p<0.001

second part of the question, results point to a more complex answer.

In terms of ever victimized, results suggest no detectable moderating effects; none of the elements of prevention measures considered by users conditioned the impact of FB utilization on ever victimized online. In other words, FB utilization and prevention measures directly and independently influence the likelihood of ever victimized. Although no moderating effects were observed, ever victimized, results on the frequency of victimization revealed the moderating role of the salience of mutuality on the impact of intensity of FB utilization.

Specifically, under conditions of low salience of mutuality, the high intensity was associated with high victimization frequency. In contrast, under conditions of high salience of mutuality, high-intensity associate with low victimization frequency. These results are suggestive of the importance of both salience of mutuality and intensity of utilization with regard to online victimization experience. These same results signal that intensity of utilization is not necessarily a risk factor for victimization experience for as long as mutuality was of high importance in the decision to accept an online friend-request.

The statistical significance of mutuality in terms of both direct and moderating effects is consistent with Coleman's (1988) idea regarding the protective mechanism afforded by social networks that exhibit trust and closure along with a high number of mutual ties among members (i.e., high network density). Network closure is exemplified by the following

example whereby children who are friends and whose parents are also friends are less likely to be involved in deviant behavior compared to children whose parents are not friends (Zou, Ingram, & Higgins, 2015).

The results also highlight the importance of intensity over extensity in terms of online victimization, which may be suggestive of the greater impact of routine over lifestyle. In concrete terms, the number of hours in a week (intensity) compared to the number of years (extensity) using FB has consequences that were more impactful on the online victimization experience. These results are insightful as they stress the salience of both routine and lifestyle in regards to understanding online victimization experience. These results hammer the point that two individuals may have very similar lifestyles (e.g., having an active online lifestyle), but may actually manifest these at varying levels on a day-to-day basis (i.e., one might be surfing the web for one hour a day, and the other six hours a day). This difference has detectable, real, and impactful consequences such as frequency of victimization or even health status. The observed finding between time spent online and victimization is consistent with the findings of Marcum (2008), who reported that respondents who spent more time online increased their exposure to a motivated offender and their likelihood of experiencing online victimization.

In thinking about the degree of user control, previous studies have not directly addressed the link between privacy settings on social media and online victimization. This study revealed that the odds of experiencing online victimization for individuals who have their privacy settings set to public are almost three times higher than those who have their privacy settings set to private. Consistent with this result, Loong (2014) reported that FB users who had their privacy settings set to public were significantly more likely to experience cyberstalking. Mathiyalakan et al. (2012), and Williams et al. (2011) reported that users who had their privacy settings set to public were more vulnerable online as a result of broadcasting information to potential online predators.

To our knowledge, the ideas of mutuality (more specifically salience of mutuality) and recognition have not yet been largely considered in modeling online victimization. Cruz-Cunha and Portela (2015) examined the relationship between a person's privacy settings and the likelihood of accepting a friend request, but not the roles that salience of mutuality and recognition might play in determining the likelihood of online victimization. Although these researchers found that individuals who did not have mutual friends had greater chances of victimization, neither the moderating role of mutuality nor salience of mutuality in the decision to accept an online friend-request were explored. Altogether, the aforementioned discussion indicates that LRAT is a promising approach to modeling, understanding, and explaining cybercrime victimization. This observed efficacy of LRAT is in keeping with previous studies such as Bossler and Holt (2009), Reyns et al. (2011), Yar (2005), Taylor et al. (2006), Choi (2008), Bossler and Holt (2009), and Ngo and Patermaster (2011).

This study provides support to a growing literature in criminal justice, suggesting that when a motivated offender and a potential target intersect within a network—including cyber networks—victimization is likely to take place (Reyns 2013). This study also highlights the temporal aspects of social media utilization such as intensity and extensity as critical in shaping the frequency of victimization; and that this shaping is conditioned by the importance of mutuality. In other words, the temporal aspects of social media utilization and the mutuality aspect of prevention measures work in tandem to better understand online victimization.

Conclusion

With cybercrimes rife, it is critical to understand their nature and dynamics if their adverse effects are to be mitigated and controlled. To this end, this study underscores the applicability of LRAT in advancing knowledge about online victimization in social media. The role of gender, intensity and extensity of utilization, and considerations of prevention measures such as user control and mutuality in online victimization, provides support for the applicability of LRAT in understanding cybercrimes. In terms of ever victimized, being male, having high intensity and extensity of use, along with a high degree of user control, play protective roles. As to the frequency of victimization, being male and high salience of mutuality are protective factors whereby mutuality moderates the influence of intensity and extensity on the frequency of victimization.

Specifically, users who viewed mutuality as not important (salience of mutuality is low) in the decision to accept an online friend-request were prone to

frequent victimization compared to those who viewed mutuality to be important (salience of mutuality is high). In other words, high importance placed on mutuality enhances protection against recurrent victimization. Though, it is worthy to note that salience of mutuality exhibits a stronger moderating role on the intensity-victimization link than on the extensity-victimization link. Nonetheless, both intensity and extensity of social media utilization are critical predictors of frequency of victimization.

Intriguingly, the initial hypothesis that "users who do not recognize friend-requesters' profile picture or profile name, and yet accept their friend-requests were more likely to experience victimization than users who considered these elements prior to accepting" was not supported. Meaning, non-recognition of a requester's profile was not a risk factor for ever victimized and for frequency of victimization. It was both mutuality and user control that proved critical to online victimization.

Based on extant studies, users who spend a great deal of time online (high intensity) tend to be victimized more (Bossler et al., 2012), especially so under conditions of low mutuality. That said, heeding campaigns aimed at reducing such adverse online experiences might be a strategy to consider seriously. As digital technologies advance, so do platforms of social media sites. Thus, it would be prudent for users to continuously re-think and re-examine how they engage others online to keep themselves safe from becoming victims of cybercrimes.

Aside from ensuring that mutuality is construed as important in online friendship request decisions, users also apply practices and settings that reduce the chances of online victimization. The U.S. Department of Homeland Security has a campaign blog called *Stop. Think.Connect*. This blog assists users in staying safe while enjoying the benefits of the Internet (Department of Homeland Security, 2016). There is also a campaign called *Take a Bite out of Cyber Crime*, which helps users to protect themselves from online predators (CMO Council 2016). With this study focused on FB victimization experience, users need to be made aware of FB-related prevention campaigns such as *Bullying Prevention Hub*. This hub focuses mainly on cyberbullying and provides teenagers, parents, and educators with information on how to prevent victimization (FB, 2016).

Declaration of ownership

This report is our original work.

Conflict of interest

None.

Ethics approval

The study was approved by the Institutional Review Board of Texas A&M International University (IRB protocol # 2015-11-10; approved on 12/4/2015).

References

Alani, A. S. A. (2014). *Principal component analysis in statistics*. Eastern Mediterranean University.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *Mis Quarterly*, *34*(3), 613–643.

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, *3*(1), 400–420.

Bossler, A. M., Holt, T. J., & May, D. C. (2012). Predicting online harassment victimization among a juvenile population. *Youth & Society*, *44*(4), 500–523.

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

CMO Council. (2016). Take a bite out of cybercrime campaign. The peer-powered network. https://www.cmocouncil.org/media-center/press-releases/569

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588–608.

Coleman, J. S. (1988). Supplement: Organizations and institutions: Sociological and economic approaches to the analysis of social structure. *American Journal of Sociology*, *94*, S95–S120.

Cruz-Cunha, M. M., & Portela, I. M. (2015). *Handbook of research on digital crime, cyberspace security, and information assurance* (Advances in Digital Crime, Forensics, and Cyber Terrorism (ADCFCT) Book Series). IGI Global.

Department of Homeland Security. (2016). *Protect Yourself from Online Fraud this Tax Season*. https://www.census.gov/quickfacts/table/PST045216/4841464,00

Dilmac, B. (2009). Psychological needs as a predictor of cyber bullying: A preliminary report on college

students. *Educational Sciences: Theory & Practice*, *9*(3), 1307–1325.

Facebook. (2016). *Bullying prevention hub*. https://www.facebook.com/saf-ety/bullying/

Facebook Help Center. (2015). *Advanced privacy controls*. https://www.-facebook.com/help/466544860022370/?helpref=hc_fnav

FBI Law Enforcement Bulletin. (2015, April 8). *Hate crime victimization statistics* (Bulletin Report). https://leb.fbi.gov/2015/april/bulletin-reports

Federal Bureau of Investigation. (2015a). *Identity theft*. https://www.fbi.gov/-about-us/investigate/cyber/identity_theft

Federal Bureau of Investigation. (2015b). *Identity theft overview*. https://-www.fbi.gov/about-us/investigate/cyber/identity_theft/identity-theft-overview

Federal Bureau of Investigation. (2014). *Internet of things poses opportunities for cybercrime*. https://www.ic3.gov/Media/PDF/Y2015/PSA150910.pdf

Frailing, K., & Harper, D. W. (2013). *Fundamental of criminology: New dimensions.* Carolina Academic Press.

Gilkerson, L. (2012). *Bullying statistics: Fast facts about cyberbullying*. Retrieved from http://www.covenanteyes.com/2012/01/17/bullying-statistics-fast-facts-about-cyberbullying/

Halder, D., & Jaishankar, K. (2011). *Cybercrime and the victimization of women: Laws, rights, and regulations*. IGI Global.

Henson, B., Reyns, B. W., & 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.

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, *30*(1), 1–25.

Identity Guard Resource Center. (2015). *Why your college student is especially vulnerable to identity theft*. http://www.identityguard.com/identity-theft-resources/articles/why-your-college-student-is-especially-vulnerable-to-identity-theft/

Internet Crime Complaint Center. (2014). Internet Crime Report. Federal Bureau of Investigations. https://www.fbi.gov/news/news_blog/2014-ic3-annual-report

Jensen, G. F., & Brownfield, D. (1986). Gender, lifestyles, and victimization: Beyond routine activity. *Violence and Victims*, *1*(2), 85–99.

Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review*, *46*(4), 757–780.

Keller, M. (2013). Social media and interpersonal communication. *Social Work Today*, *13*(3), 10.

Legal Information Institute. (2015). *Computer and internet fraud*. Cornell University Law School. https://www.law.cornell.edu/wex/computer_and_internet-_fraud#

Lindsay, M., & Krysik, J. (2012). Online harassment among college students. *Information, Communication & Society*, *15*(5), 703–719.

Liu, Y., Gummadi, K. P., Krishnamurthy, B., & Mislove, A. (2011). *Analyzing Facebook privacy settings: User expectations vs. reality*. Paper presented at the ACM SIGCOMM Conference on Internet Measuremment. http://www.ccs.neu-.edu/home/amislove/publications/Privacy-IMC.pdf

Loong, A. C. J. (2014). *Cyberstalking on Facebook: Examining the relationship between Facebook usage characteristics and cyber stalking victimization among young Malaysian Facebook users* (Unpublished doctoral dissertation). Universiti Tunku Abdul Rahman, Kapar, Perak, Malaysia.

Mann, B. L. (2015). Social networking websites- A concatenation of impersonation, denigration, sexual and aggressive solicitation, cyber-bullying and happy slapping videos. In P. Leith (Ed.), Privacy in the information society (Vol. 2, pp. 493–503). Ashgate Publishing. http://www.ucs.mun-.ca/~bmann/0_ARTICLES/Mann_Social_Netg_PrivInfoSoc_15.pdf

Marcum, C. D. (2008). Identifying potential factors of adolescent online victimization for high school seniors. *International Journal of Cyber Criminology*, *2*(2), 346–367.

Marcum, C. D., Ricketts, M. L., & Higgins, G. E. (2010). Assessing sex experiences of online victimization: An examination of adolescent online behaviors using routine activity theory. *Criminal Justice Review*, *35*(4), 412–437.

Mathiyalakan, S., Heilman, G., & White, S. (2013). Gender differences in student attitude toward privacy in Facebook. *Communications of the IIMA*, *13*(4), 35–44.

Milanovic, R. (2015, April 13). The world's 21 most important social media sites and apps in 2015. *Social Media Today*. http://www.socialmediatoday.com/social-networks/2015-04-13/worlds-21-most-important-social-media-sites-and-apps-2015

Myrstol, B. A., & Chermak, S. M. (2005). Victimology. In L. Glick (Ed.), *Criminology*pp. 452-495). Pearson. http://wps.ablongman.com/wps/media/objects/1893/1938583/CH_15_web.pdf

National Crime Victim Law Institute. (2010). *What is "online fraud"? Protecting, enforcing, & advancing victims' rights*. https://law.lclark.edu/live-/news/6855-what-is-online-fraud

Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology*, *5*(1), 773–793.

Oluga, S. O., Ahmad, A. B. H., Alnagrat, A. J. A., Oluwatosin, H. S., Sawad, M. O. A., & Muktar, N. A. B. (2014). An overview of contemporary cyberspace activities and the challenging cyberspace Crimes/Threats. *International*

Journal of Computer Science and Information Security, 12(3), 62–100. http://search.proquest.com/-docview/1534315580?accountid=7081

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyber lifestyle-routine activities theory to cyber stalking victimization. *Criminal Justice and Behavior*, *38*(11), 1149–1169.

Reyns, B. W., Henson, B., & Fisher, B. S. (2012). Stalking in the twilight zone: Extent of cyberstalking victimization and offending among college students. *Deviant Behavior*, *33*(1), 1–25.

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime & Delinquency*, *50*(2), 216–238. https://doi.org/10.1177/0022427811425539

Serious Fraud Office. (2015). *What is fraud?* http://www.sfo.gov.uk-/fraud/what-is-fraud.aspx

Smith, C. (2016). *By the numbers: 200+ amazing Facebook statistics*. Digital Stats/Gadgets (DMR). http://expandedramblings.com/index.php/by-the-numbers-17-amazing-facebook-stats/

Social Security Administration. (2015). *Identity theft and your social security number*. Social Security Administration. https://www.ssa.gov/pubs/EN-05-10064.pdf

SONA Systems. (2016). *Sona System Experimental Management System: Master documentation et.* SONA Systems Ltd.

Sugarmann, J. (2014, December 5). Murder rate for Hispanics is twice the murder rate for whites. *HuffPost.* http://www.huffingtonpost.com/josh-sugarmann/murder-rate-for-hispanics_b_5309973.html

Taylor, R. W., Caeti, T. J., Loper, D. K., Fritsch, E. J., & Liederbach, J. (2006). *Digital crime and digital terrorism.* Pearson Prentice Hall.

Tillyer, M. S., & Eck, J. E. (2009). Routine activities. In J. M. Miller (Ed.), *21st century criminology: A reference handbook* (pp. 279–287). Sage.

United States Census Bureau. (2015). *QuickFacts. Laredo City, Texas*. https://www.census.gov/quickfacts/table/PST045216/4841464,00

Wall, D. S. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law Computers & Technology*, *22*(1-2), 45–63.

Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. *CyberPsychology, Behavior, and Social Networking*, *15*(3), 181–183.

Williams, J., Field, C., & James, C. (2011). The Effects of a Social Media Policy on Pharmacy Students' Facebook Security Settings. *American Journal of Pharmaceutical Education, 75*(9) 1-6.

Zou, X., Ingram, P., & Higgins, E. T. (2015). Social networks and life satisfaction: The interplay of network density and regulatory focus. *Motivation and Emotion 39*, 693–713.

Yar, M. (2005). The novelty of "cybercrime": An assessment in light of routine activity theory. *European Journal of Criminology*, *2*(4), 407–427.

Ybarra, M., Boyd, D., Korchmaros, J., & Oppenheim, J. (2012). Defining and measuring cyberbullying within the larger context of bullying victimization. *Journal of Adolescent Health*, *51*(1), 53–58.

Zhang, A. T., Land, L. P. W., & Dick, G. (2010). Key influences of cyberbullying for university students. *Pacific Asia Conference on Information Systems (PACIS) Proceedings*. PACIS.