American Journal of Criminal Justice (2019) 44:63–82
https://doi.org/10.1007/s12103-018-9447-5

Opportunity and Self-Control: Do they Predict Multiple Forms of Online Victimization?

Bradford W. Reyns[1] · Bonnie S. Fisher[2] · Adam M. Bossler[3] · Thomas J. Holt[4]

Received: 26 March 2018 / Accepted: 23 July 2018 /
Published online: 28 July 2018

Abstract

This study investigates the predictors of four types of cybercrime victimization/experiences: online harassment, hacking, identity theft, and receiving nude photos or explicit content. The effects of victimization opportunity and low self-control are examined as the primary independent variables in logistic regression analyses of data collected from a large sample of undergraduates enrolled at two universities in the United States. Results suggest that opportunity is positively related to each of the four types of online victimization, and that low self-control is associated with person-based, but not computer-based, forms of cybercrime. These findings speak to the utility, and also the limitations, of these perspectives in understanding cybercrime victimization risk among college students, and to the potentially criminogenic nature of the Internet.

Keywords Online victimization · Cybercrime · Opportunity · Routine activities · Self-control

✉ Bradford W. Reyns
breyns@weber.edu

Bonnie S. Fisher
Bonnie.Fisher@uc.edu

Adam M. Bossler
abossler@georgiasouthern.edu

Thomas J. Holt
Holtt@msu.edu

[1] Department of Criminal Justice, Weber State University, 1299 Edvalson Street, Dept. 1206, Ogden, UT 84408-1206, USA

[2] School of Criminal Justice, University of Cincinnati, 650G Dyer Hall, ML 210389, Cincinnati, OH 45221-0389, USA

[3] Department of Criminal Justice and Criminology, University Hall, Room 226, Georgia Southern University, Armstrong Campus, 11935 Abercorn Street, Savannah, GA 31419, USA

[4] School of Criminal Justice, Michigan State University, 655 Auditorium Road, 434 Baker Hall, East Lansing, MI 48864, USA

Introduction

Victimologists examining the situational correlates and risk factors of victimization have frequently utilized routine activity theory, which argues that opportunities for victimization occur when a motivated offender, suitable target, and absent or ineffective guardianship converge in time and space (e.g., Cohen & Felson, 1979; Felson & Eckert, 2015; Wilcox & Cullen, 2018). These victimization opportunities are hypothesized to increase individuals' victimization risks. This theoretical premise has found substantial support with numerous empirical studies reporting links between opportunity-based risk factors and different forms of criminal victimization (e.g., McNeeley, 2015; Spano & Freilich, 2009), including partial support for the link between online opportunity and cybercrime or technology-enabled victimization (e.g., Holt & Bossler, 2016; Reyns, 2017; Vakhitova, Reynald, & Townsley, 2016).

Researchers also have integrated this theory with the general theory of crime (Gottfredson & Hirschi, 1990) to better understand the role that self-control may play in increasing the risk of victimization (e.g., Schreck, 1999; Schreck, Wright, & Miller, 2002; Stewart, Elifson, & Sterk, 2004). Though the general theory of crime was originally developed to account for offending, the central concept in the theory – low self-control – is also hypothesized to increase victimization risk by making individuals more vulnerable crime targets (e.g., Schreck, 1999). According to this vulnerability thesis, low self-control directly and indirectly affects the risk of victimization – a hypothesis that has been supported in studies examining traditional forms of victimization and in a more limited capacity in work examining cybercrime victimization (Pratt, Turanovic, Fox, & Wright, 2014).

Despite being empirically supported as an explanation for victimization, it has also been suggested that the effects of low self-control on victimization risk may be contextual (e.g., Pratt et al., 2014). Specifically, self-control may have a weaker direct relationship to victimization when individuals in criminogenic environments or situations perceive that they have little autonomy to choose what activities they may perform. For example, the elderly, children, prisoners, or those in abusive relationships may feel unable to affect their risk of victimization due to a perceived lack of control over the situation or their environment generally (e.g., Pratt et al., 2014; Kulig, Pratt, Cullen, Chouhy, & Unnever, 2017; Reyns, Woo, Lee, & Yoon, 2018).

This issue may also be evident in some forms of cybercrime victimization, as the very nature of the Internet can impact individuals' victimization risks in ways that may be otherwise hidden or hard to appreciate. Certain offenses such as online harassment may be directly influenced by both an individual's online routine activities as well as their individual attitudes and behaviors (e.g., Holt & Bossler, 2008; Leukfeldt & Yar, 2016; Peterson & Densley, 2017). The risk of computer hacking and fraud victimization may, however, be influenced more broadly by simply connecting to the Internet. Further, the web browser and operating system used by an individual may disproportionately increase their risk of being targeted for attack due to vulnerabilities in the software that may be unknown to the user (e.g., Maimon, Wilson, Ren, & Berenblum, 2015; Song, Lynch, & Cochran, 2016; Yar, 2005). In fact, prior research has found that the risk of malicious software infections and electronic credit card theft are unrelated to an individual's level of self-control (e.g., Bossler & Holt, 2010; Ngo & Paternoster, 2011).

To date, while the extant cybercrime scholarship supports the application of opportunity and low self-control as explanations for victimization, the majority of studies have considered only one form of cybercrime in isolation, with a disproportionate focus on interpersonal victimization (see Holt & Bossler, 2014; Reyns, 2017 for reviews). Thus, studies examining crimes that more directly affect either a computer or sensitive data (e.g., hacking, identity theft) are much less prevalent. A focus across multiple types of cybercrimes (i.e., person-based and computer-based) is needed to allow broader conclusions about the nature of cybercrime victimization – including its common determinants – to be reached. The current study takes this necessary next step in evaluating the relationship between victimization opportunity, low self-control, and online victimization by estimating the impact of these theoretical concepts upon the risk of four different types of cybercrime victimization/experiences. These four types of cybercrime were chosen because they loosely correspond to Wall's (2001) cybercrime typology, and because they include those that are both person-based and computer-based.

Theoretical Framework

Opportunity, Self-Control, and Online Victimization

Studies that have tested an opportunity perspective on online victimization have adapted the building blocks of opportunity (i.e., exposure, target suitability, guardianship) to online contexts and generally supported the application of the theory of explain cybercrime victimization. Among studies utilizing samples of college students, research has consistently found that routine activities related to online communications and/or social networking increase students' likelihood of experiencing different forms of cybercrime victimization (e.g., Choi, 2008; Bossler & Holt, 2009; Henson, Reyns, & Fisher, 2013; Marcum, Higgins, & Ricketts, 2010; Reyns, Henson, & Fisher, 2011). Similar results also have been identified in both adolescent samples (e.g., Holt, Bossler, Malinski, & May, 2016; Näsi, Räsänen, Kaakinen, Keipi, & Oksanen, 2017; Navarro & Jasinski, 2013; Räsänen et al., 2016; Van Ouytsel, Ponnet, & Walrave, 2016) and general population studies (e.g., Leukfeldt & Yar, 2016; Pratt, Holtfreter, & Reisig, 2010; Reyns, 2013, 2015; Reyns & Henson, 2016; Van Wilsem, 2011).

Factors beyond opportunity also influence victimization risk – in particular, low self-control. Research has demonstrated that low self-control is related to offline violent and property victimizations (e.g., Holtfreter, Reisig, & Pratt, 2008; Piquero, MacDonald, Dobrin, Daigle, & Cullen, 2005; Pratt et al., 2014; Schreck, 1999; Stewart et al., 2004). Additionally, research suggests that low self-control has a direct effect on victimization that is not explained by opportunity-based risk factors (e.g., Schreck, 1999; Stewart et al., 2004; Turanovic, Reisig, & Pratt, 2015). In online studies, the published research testing the effects of low self-control upon different forms of online victimization has produced encouraging results supportive of its continued exploration (e.g., Bossler & Holt, 2010; Holt, Bossler, et al., 2016; Reyns, Burek, Henson, & Fisher, 2013; Reyns, Fisher, & Randa, 2018; Van Wilsem, 2011).

Together, these two perspectives have significant explanatory power in identifying the predictors of a variety of types of offline and online victimization. Yet, studies that

jointly test these two frameworks as explanations of victimization also suggest that their utility may be limited in some ways by the environmental context in which the crime takes place. This is a possibility implied by the extant cybercrime literature, but one that has not been fully explored. Put differently, there may be domain-specific dynamics in play when applying these frameworks to online contexts.

Opportunity and Low Self-Control: Online-Specific Dynamics

There is a notable dynamic present between the predictive power of self-control, opportunity, and victimization surrounding the individual as the target of the offense as opposed to their computer or their personal information as the target. In the case of the former, greater opportunities and lower self-control are hypothesized to heighten victimization risks as suggested in the offline victimization literature. In the case of the latter, however, these forms of victimization (e.g., hacking, identity theft), may not be impacted by opportunity and low self-control as traditionally predicted. To illustrate, Bossler and Holt (2010) argued that the absence of a relationship between low self-control, fraud, and malware infections in their study may have been due to the random nature of these offenses.

The lack of consistent risk factors also has been noted across the literature regarding the personal and protective factors (i.e., opportunities) at play in malicious software infections that target an individual's operating system or installed software (e.g. Bossler & Holt, 2009; Choi, 2008; Holt & Bossler, 2013; Ngo & Paternoster, 2011; Reyns, 2015). Overall, these issues may be a function of the potentially criminogenic nature of the Internet as a whole – affecting the association between self-control, opportunity-producing routine activities, and victimization risk. To elaborate, the open nature of the Internet and the protocols that support its functionality enable computer hackers and data thieves to scan computer networks for potential targets at all times. By virtue of simply connecting a computer or device to the Internet, an individual increases his or her risk for compromise by a cybercriminal (Brady, Randa, & Reyns, 2016).

Beyond this, the security tools individuals need to employ in order to reduce their risk of compromise may neither be fully understood by average users nor configured or implemented properly to ensure full protection. Further, the risk of experiencing certain forms of cybercrime victimization could also be influenced by factors beyond the individual victim's control. To illustrate, there has been a substantial increase in the number of mass data breaches occurring in the EU and U.S. over the last decade, where individuals' financial and personal information is acquired by compromising payment systems or data maintained by retailers and third-party organizations (Ponemon Institute, 2016; Symantec, 2016). In these instances, the entity responsible for data management is at fault for the incident, not the individual victim, as they had no responsibility in securing or storing their data. An individual may still experience victimization, however, as the information acquired from breaches are frequently sold to others via online markets for use in fraudulent online purchases or identity crimes (e.g., Holt, Smirnova, & Chua, 2016; Leukfeldt, Kleemans, & Stol, 2017).

Taken as a whole, cybercrimes involving data stored on an electronic device, or the device itself, may occur regardless of one's online activities or level of self-control, compared to those cybercrimes that specifically target an individual. A person may not

perceive or realize that their victimization risks while online could be affected by factors beyond their control. Thus, they may place faith in protective software programs and tools that may only partially mitigate risks (e.g. Bossler & Holt, 2010; Holt & Bossler, 2013; Leukfeldt, 2015). The nature of the Internet may be similar to the conditions described by Pratt et al. (2014, p. 105) as to the diminished value of self-control relative to routine behaviors in certain forms of victimization when they asked: "When such autonomy to choose among behavioral alternatives is severely reduced, is there any room left for self-control to play a role in the explanation of victimization?"

The Present Study

Considered together, the previously reviewed theoretical arguments suggest that research questions related to the roles of victimization opportunity and low self-control have yet to be fully answered in the extant cybercrime literature. Accordingly, the present study addresses two primary research questions:

RQ1: What is the effect of victimization opportunity on cybercrime victimization risk?
RQ2: What is the effect of low self-control on cybercrime victimization risk?

Regarding the first research question, we hypothesize based on previous research that victimization opportunities will be predictive of each of the four types of cybercrime victimization/experiences. With respect to the second research question, we hypothesize that the effect of low self-control will vary according to the cybercrime outcome under consideration. In particular, low self-control should theoretically have a greater impact upon person-based forms of cybercrime, as compared to its computer-based forms (Bossler & Holt, 2010). Our cybercrime outcomes are operationalized using Wall's (2001) well-established typology for cybercrimes, and these research questions are examined through analyses of data from a large sample of college students drawn from two U.S. universities.

Method

Data

The data were collected as part of a larger five-year project, Consortium to Evaluate a Novel Violence Prevention Program on College Campuses, which examined interpersonal victimization and perpetration among college students. The National Institutes of Health funded the project through a R21 Advancing Novel Science in Women's Health Research grant. The institutional review board at the second author's school approved the study's research protocol. Data collection occurred at two large, urban, public universities, with one located in the Midwest and the other in the South in the United States, during the Spring 2015. Both universities have Carnegie Classifications as R1 doctoral universities, with undergraduate student populations of approximately 33,000 and 22,000, respectively. The two

universities are within 100 miles of each other. The field period lasted almost four weeks from 12:00 pm on April 13th to 11:59 pm on May 11th.

Using student enrollment data from the last week of January 2015, the registrar at each school drew a random sample of 5000 undergraduate matriculating students aged 18–24 years old,[1] by four year-in-school strata (first-year, sophomore, junior, and senior) and two gender identities (male and female). Each of the year-in-school stratum represented 25% of the total sample ($n = 1250$ respectively at each school). Within each year-in-school stratum, the percent of females and males were equally split, 50/50 ($n = 625$, respectively at each school).

An initial email was sent to each student in the sample on April 13th inviting them to participate in a web-based survey about the prevention of dating violence and sexual violence. The student's email address on file with the respective school's registrar was used to send the invitation. Following Dillman's (2007) tailored design method, students received an original invitation and subsequent follow-up emails approximately 3–4 days apart at noon over the four-week period. To attract students' attention, each email had a different subject heading, such as: "First reminder: Followup: Please complete (school name) Survey" and "Last reminder: Last chance: Please complete (school name) survey."

To increase the likelihood of participation, each follow-up email was sent on a different day of the week and over the course of the field period; each day of the week had an email sent. Students who decided to participate were instructed to click on the survey link, which opened a webpage explaining the purpose of the study and providing informed consent. Students could then decide to complete the survey or to opt out. Students who participated received a $5 Amazon e-gift card sent to the email address that the invitation email had been sent within a week of submitting their responses. The overall response rate was 40.63% ($N = 4063/10{,}000$). Excluding cases for which a valid response on each variable used in the analyses ($n = 829$) was not available resulted in an analytical sample of 3234 students, for a response rate of 32.34%. This sample was predominantly female and White, with an average age of 20.

Measures

Outcome Measures In the early years of cybercrime scholarship, Wall (2001) introduced a typology of cybercrime that included four distinct types: cyber-violence, cyber-trespass, cyber-deception/theft, and cyber-pornography/obscenity. While originally developed to categorize types of cybercrime events, the present study conceptualizes the typology from a victimization perspective and investigates a representative type of cybercrime victimization from each of these categories. Four online experiences are examined as dependent variables and based upon Wall's (2001) typology. In particular, online harassment (i.e., cyber-violence), hacking (i.e., cyber-trespass), identity theft (i.e., cyber-deception/theft), and receiving nude photos or explicit content (i.e., cyber-pornography/obscenity) are examined as online experiences representative of the typology categories.

[1] Conventionally, students aged 18 to 24 years are considered to be traditional college students, whereas older students (i.e., over age 25) are viewed as non-traditional. The survey was administered only to traditional college students, as they are a homogeneous group in terms of their lifestyles and routine activities, whereas non-traditional students, by definition, often have differing home and work responsibilities.

Online Harassment Cyber-violence was operationalized as online harassment. To measure online harassment, participants were asked: "*Since the beginning of Fall 2014 term how many times have you experienced any of the following behaviors online?*" Those who indicated that they had experienced harassment any number of times (i.e., one or more) were classified as victims of online harassment.[2] As Table 1 illustrates, approximately 10% of students had such an experience during the academic year.

Hacking Victimization Hacking victimization represents Wall's (2001) cyber-trespass category. Respondents who indicated that they had experienced hacking any number of times (i.e., one or more) since the beginning of the Fall semester were coded as victims of cyber-trespass. Amongst members of this sample, 8% had been hacked during the academic year (see Table 1).

Online Identity Theft Victimization Identity theft, representing Wall's (2001) category of cyber-deception/theft, measured whether students had their identity stolen online since the beginning of the Fall 2014 term. Measured with the same survey prompt as harassment and hacking, persons self-identified as victims of online identity theft. Findings suggest that 5% of students were victims of cyber-deception/theft since the beginning of school year (see Table 1).

Receiving Nude Photos or Explicit Content The operationalization of cyber-pornography/obscenity (Wall, 2001) from the victim's perspective is not straightforward. However, a focus on the receipt of sexually explicit content is within the spirit of Wall's (2001) description from his typology. Accordingly, this variable was measured with a survey item asking respondents the following question: "*Since the beginning of the 2014 Fall term, have you ever received a nude, nearly nude or sexually explicit photograph or video of someone?*" As Table 1 indicates, 32% of our sample disclosed that they had been the recipient of this kind of online content since the beginning of the academic year. It is important to note that the "victimization" label may not be accurate in all cases, such as when the nude photos or explicit content were solicited.

Theoretical Variables

Opportunity The opportunity variable[3] reflects the mean number of hours in an average day that individuals spent engaged in 10 different online routine behaviors, with response choices ranging from 0 to 10 or more hours (0 = 0, 1 h = 1, 2 h = 2, 3–5 h = 3, 6–9 h = 4, and 10 or more hours = 5). These routines have been identified in

[2] As with the other outcome variables, the measure of online harassment was dichotomized to examine the likelihood of experiencing victimization, rather than to explain the frequency of victimization. Doing so also simplified the analyses while aiding in interpretation of the results.

[3] Reliability analysis for the opportunity construct produced a Cronbach's alpha of 0.69. Thresholds for interpreting acceptable α coefficients vary, and should largely be based upon theoretical knowledge of the scale. Based on past research, and existing theory, we contend that an α of 0.69 is acceptable under the circumstances (see Holt & Bossler, 2016 for review of literature linking online behaviors to victimization). A similar approach was taken and explained by Koss and colleagues in their discussion of the reliability and validity of the Sexual Experiences Survey (see Koss et al., 2007).

Table 1 Descriptive statistics, scale, and coding for study variables

Variables	Scale and Coding	*M*	*SD*
Dependent Variables			
Harassment	0 = no, 1 = yes	0.10	0.30
Hacking	0 = no, 1 = yes	0.08	0.28
Identity Theft	0 = no, 1 = yes	0.05	0.23
Nude Photo	0 = no, 1 = yes	0.32	0.47
Independent Variables			
Opportunity	0 to 5 (mean time spent engaged in online routine activities)	0.83	0.48
Low Self-Control	1 = more self-control to 4 = low self-control	2.01	0.45
Control Variables			
Female	0 = male, 1 = female	0.56	0.49
Age	Age in years	20.22	1.38
White	0 = non-White, 1 = White	0.85	0.35
Relationship Status	0 = single, 1 = non-single	0.45	0.49
Sexual Orientation	0 = non-heterosexual, 1 = heterosexual	0.85	0.35
Live on Campus	0 = off campus, 1 = on campus	0.37	0.48
Full Time	0 = no, 1 = yes	0.97	0.14
Athlete	0 = no, 1 = yes	0.05	0.22
Greek Membership	0 = no, 1 = yes	0.22	0.41
Campus Location	0 = South, 1 = Midwest	0.54	0.49
N		3234	

prior research as theoretical or empirical correlates of online victimization, and include: (1) sending/responding to email, (2) social networking (e.g., Facebook, Twitter), (3) communicating through instant messaging, (4) video chatting (e.g., Skype), (5) blogging (reading or writing), (6) downloading (music, films, podcasts), (7) communicating in chat rooms or forums, (8) watching TV (or YouTube or listening to the radio), (9) participating in class discussions (e.g., on Blackboard), or (10) visiting pornographic websites.

Self-Control The low self-control variable was constructed using Grasmick and colleagues' (1993) 24-item scale for measuring self-control. Respondents were provided with 24 statements and asked to rate their level of agreement, with answer choices ranging from strongly disagree (1) to strongly agree (4). As a representative example, one of these statements read: "*Sometimes I will take a risk just for the fun of it.*" Answers to these statements were combined by calculating a mean level of self-control, with higher values denoting lower self-control. A Cronbach's α of 0.91 indicated high internal consistency among these items, and an average level of self-control of 2.01 (0.45).

Control Variables Following prior research, several known correlates of online victimization were included in the analyses as control variables. Among these, age was

measured in years, while the rest were measured dichotomously, including: female, race, relationship status, sexual orientation,[4] lives on campus, full time student, student athlete, Greek member, and campus location. The coding and descriptive statistics for the control variables are provided in Table 1.

Analytic Strategy

Prior to examining the cybercrime variables within our theoretical framework, correlation analyses were performed. These analyses suggested that there are significant relationships between both opportunity and cybercrime and low self-control and cybercrime, thus supporting further analyses. Following this, binary logistic regression models were conducted to estimate the effects of online opportunity (as a construct), low self-control, and the control variables on the four different cybercrime outcomes. The results of these analyses are provided in Table 2 for the four models. Further analyses also were conducted to provide a view of how individual routine activities influence these cybercrime outcomes. Thus, Table 3 provides binary logistic regression results for four models in which the opportunity construct was separated into the various online routine activities to examine the effects of specific behaviors, in addition to the effects of low self-control and the control variables.

Results

Binary Logistic Regression Analyses

Opportunity Construct Table 2 provides results from the logistic regression analyses for the four types of cybercrime; of primary interest are the effects of the opportunity construct and low self-control. Across the models in Table 2, opportunity is a significant and positive predictor of harassment, identity theft, and receiving nude/explicit content. Likewise, low self-control was significantly related to harassment and receiving nude/explicit content. Amongst the control variables, several significant relationships emerged. First, for online harassment, being female, White, non-heterosexual, and a student at the Southern university were all associated with elevated victimization risks. Second, for hacking, age and Southern campus status were both associated with increased risks, as neither of theoretical variables impacted the likelihood of hacking victimization. Third, for identity theft victimization, age and being a part time status student were both related to heightened victimization risk, although the strength of the relationships was modest. Finally, in examining receiving nude/explicit content, males,

[4] Students were asked about their sexual attraction to other people and asked to select an orientation that best described them from a list including: only attracted to females, mostly attracted to females, equally attracted to females and males, mostly attracted to males, only attracted to males, and not sure. Females who indicated they were only attracted to males, and males who indicated they were only attracted to females were coded as heterosexual. Low frequencies amongst the other combinations necessitated collapsing the remaining individuals into a "non-heterosexual" category.

Table 2 Binary logistic regression models: online victimization, by opportunity, low self-control, and control variables

	Model 1: Harassment			Model 2: Hacking			Model 3: Identity Theft			Model 4: Nude Photo		
Variables	Coefficient	*SE*	Exp(B)	Coefficient	*SE*	Exp(B)	Coefficient	*SE*	Exp(B)	Coefficient	*SE*	Exp(B)
Opportunity	0.58***	0.11	1.78	0.23	0.12	1.26	0.37**	0.13	1.45	0.48***	0.08	1.62
Low Self-Control	0.43**	0.14	1.55	0.25	0.14	1.29	0.15	0.16	1.16	0.41***	0.08	1.52
Female	1.02***	0.13	2.79	−0.03	0.13	0.96	0.17	0.15	1.19	−0.55***	0.08	0.57
Age	0.05	0.05	1.05	0.20***	0.05	1.22	0.13*	0.06	1.14	0.01	0.03	1.01
White	0.34*	0.17	1.41	−0.09	0.17	0.91	−0.23	0.19	0.78	0.53***	0.11	1.70
Relationship Status	−0.07	0.12	0.92	0.14	0.12	1.15	0.02	0.15	1.02	0.29***	0.07	1.34
Heterosexual	−0.53***	0.14	0.58	−0.11	0.17	0.89	0.04	0.20	1.04	−0.69***	0.10	0.49
Live on Campus	0.01	0.14	1.01	0.09	0.15	1.09	−0.10	0.18	0.90	−0.08	0.09	0.91
Full Time	0.49	0.45	1.64	0.58	0.52	1.79	−0.83*	0.35	0.43	0.05	0.27	1.06
Athlete	−0.31	0.30	0.72	0.36	0.24	1.44	0.12	0.31	1.13	0.22	0.16	1.25
Greek Membership	−0.00	0.14	0.99	0.20	0.15	1.23	0.01	0.18	1.01	0.11	0.09	1.12
Campus Location	−0.83***	0.12	0.43	−0.49***	0.13	0.61	−0.26	0.15	0.76	−0.13	0.07	0.87
Constant	−5.26***	1.23	0.00	−7.57***	1.29	0.00	−5.19***	1.42	0.00	−2.03**	0.77	0.13
−2 Log-likelihood	2007.43			1857.72			1433.67			3911.63		
Model χ^2	180.03**			42.73***			28.62**			199.77***		
Nagelkerke R^2	0.10			0.03			0.02			0.08		
N	3234			3234			3234			3234		

*$p \leq .05$; ** $p \leq .01$; *** $p \leq .001$

Table 3 Binary logistic regression models: online victimization by routine activities, low self-control, and control variables

	Model 5: Harassment			Model 6: Hacking			Model 7: Identity Theft			Model 8: Nude Photo		
Variables	Coefficient	*SE*	Exp(B)	Coefficient	*SE*	Exp(B)	Coefficient	*SE*	Exp(B)	Coefficient	*SE*	Exp(B)
Routine Activities												
Emailing	−0.10	0.08	0.89	0.16*	0.08	1.17	0.19*	0.09	1.21	−0.08	0.05	0.92
Social Networking	0.10	0.06	1.10	0.15*	0.07	1.16	0.13	0.08	1.14	0.12**	0.04	1.12
Instant Messaging	0.07	0.04	1.07	−0.11*	0.05	0.89	−0.02	0.06	0.97	0.17***	0.03	1.19
Skyping	−0.17	0.10	0.83	−0.32*	0.12	0.72	−0.15	0.13	0.85	0.05	0.06	1.05
Blogging	0.14*	0.06	1.15	0.07	0.07	1.07	−0.00	0.09	0.99	−0.07	0.05	0.93
Downloading	0.07	0.08	1.07	0.06	0.08	1.06	−0.01	0.10	0.98	−0.03	0.05	0.96
Chatting	0.19	0.10	1.20	0.07	0.11	1.08	0.13	0.13	1.14	−0.12	0.07	0.88
TV	0.08	0.05	1.08	−0.06	0.06	0.93	0.09	0.07	1.09	0.02	0.03	1.02
Class Work	0.07	0.05	1.07	0.15*	0.06	1.16	0.06	0.07	1.07	0.05	0.04	1.06
Porn	0.06	0.09	1.06	−0.00	0.09	0.99	−0.12	0.13	0.88	0.22***	0.06	1.25
Low Self-Control	0.44***	0.14	1.55	0.29*	0.14	1.33	0.17	0.17	1.19	0.37***	0.09	1.45
Female	1.05***	0.15	2.86	−0.13	0.14	0.87	0.04	0.17	1.04	−0.57***	0.09	0.56
Age	0.06	0.05	1.06	0.18**	0.05	1.20	0.11	0.06	1.12	0.03	0.03	1.03
White	0.25	0.18	1.29	−0.11	0.18	0.89	−0.24	0.20	0.78	0.51***	0.12	1.66
Relationship Status	−0.03	0.12	0.97	0.18	0.13	1.20	0.05	0.15	1.05	0.27***	0.08	1.31
Heterosexual	−0.51***	0.14	0.60	−0.12	0.17	0.87	−0.03	0.21	0.96	−0.75***	0.11	0.47
Live on Campus	0.03	0.14	1.04	0.12	0.15	1.13	−0.09	0.18	0.90	−0.11	0.09	0.88
Full Time	0.40	0.45	1.50	0.47	0.52	1.60	−0.96**	0.36	0.38	0.02	0.27	1.02
Athlete	−0.23	0.30	0.79	0.38	0.24	1.47	0.17	0.31	1.18	0.20	0.16	1.22
Greek Membership	0.02	0.15	1.02	0.14	0.15	1.15	−0.02	0.19	0.97	0.09	0.09	1.09
Campus Location	−0.83***	0.12	0.43	−0.48***	0.13	0.61	−0.25	0.15	0.77	−0.13	0.08	0.87

Table 3 (continued)

	Model 5: Harassment			Model 6: Hacking			Model 7: Identity Theft			Model 8: Nude Photo		
Variables	Coefficient	*SE*	Exp(B)	Coefficient	*SE*	Exp(B)	Coefficient	*SE*	Exp(B)	Coefficient	*SE*	Exp(B)
Constant	−5.43***	1.24	0.00	−7.15***	1.30	0.00	−4.81***	1.44	0.00	−2.22**	0.78	0.10
−2 Log-likelihood	1994.31			1832.16			1422.64			3863.16		
Model χ^2	193.15***			68.29***			39.65**			248.24***		
Nagelkerke R^2	0.11			0.04			0.03			0.10		
N	3234			3234			3234			3234		

*$p \leq .05$; ** $p \leq .01$; *** $p \leq .001$

Whites, persons in a relationship, and those categorized as non-heterosexual were all more likely to have such an experience.

Specific Routine Activities Table 3 provides an alternative view of opportunity by providing estimates of the effects of individuals' specific online routine activities upon their likelihood of experiencing these four types of cybercrimes. In Model 5, the only routine behavior significantly associated with harassment victimization is blogging, but interestingly, the effect of blogging on online harassment was somewhat weak. Importantly, low self-control continued to be a significant predictor of victimization, and while most of the control variables from Model 1 remained significant, race (White) became non-significant in this model.

Model 6 of Table 3 provides a more nuanced view of the predictors of hacking victimization than did Model 2. Here, five specific routine activities were associated with victimization, including emailing, social networking, and doing class work, which positively impacted victimization risk, and instant messaging and skyping, which negatively affected this risk. It is notable that low self-control became a significant predictor of victimization in this model, whereas it was not in the prior hacking model (Model 2). Age and campus location retained their effects from the previous model.

Changes were also observed across the models of identity theft victimization. As Model 7 demonstrates, only emailing was significantly related to victimization, with greater email use corresponding with an increased odds of identity theft. Being a full-time student remained a significant predictor of victimization across these two models, while age became non-significant in Model 7.

In Model 8 of Table 3, particular routine activities were significant indicators of the likelihood of receiving nude/explicit content. Specifically, social networking, instant messaging, and viewing pornography each increased the odds of this outcome. Further, like the previous model of this dependent variable, low self-control remained a significant factor. Likewise, the previously significant control variables of male, White, in a relationship, and non-heterosexual retained their significance.

Discussion

Research examining criminal victimization has found substantial support for the role of low self-control as a direct and indirect risk factor for violent and property crimes (Pratt et al., 2014). This dynamic also has been partially supported for cybercrime victimization, though more research is needed both replicate and validate the limited body of scholarship that currently exists. In particular, there is a need to understand the extent to which the criminogenic nature of the Internet may disproportionately increase the risk of victimization, thereby decreasing the potential explanatory role of self-control (e.g., Pratt et al., 2014; Kulig et al., 2017; Reyns et al., 2018). The present study sought to address an open question related to the effects of victimization opportunity and low self-control upon four types of cybercrime victimization/experiences. Examining four distinct types of cybercrime based on Wall's (2001) typology allows for comparisons of the relative effects of these two prominent victimization theories. Based on the results from our analyses, four conclusions are warranted.

First, opportunity, which was conceptualized in the initial analyses as a construct denoting time spent in opportunity-producing routine activities, appears to increase online victimization risk. The opportunity construct was predictive of three of the four types of online victimization/experiences: harassment, identity theft, and receiving nude/explicit content. However, this measure of opportunity was not a significant predictor for hacking victimization. Yet, in the supplemental routine activities analyses that examined the specific routines rather than an overall opportunity variable, four distinct activities were significantly related to hacking victimization.

Regarding the routine activity analyses, online behaviors generally differentially affected victimization risk depending upon the type of cybercrime under examination. That is, certain routine activities had crime-specific effects. Namely, blogging was only related to online harassment, and likewise, viewing pornography online was only correlated with receiving nude/explicit content; skyping was only related to hacking (inversely). Conversely, emailing, social networking, and instant messaging had effects across victimization types. Emailing was related to hacking and identity theft; social networking impacted risks for hacking and receipt of nude/explicit content; instant messaging affected hacking (negatively) and nude/explicit content (positively). Some of these variable effects have a clear-cut explanation. For instance, perhaps more time using email equates with a greater likelihood of falling prey to scams or fraudulent emails that lead to identity theft. On the other hand, other findings do not have a straightforward explanation, such as the negative relationships between instant messaging, skyping, and hacking victimization.

Overall, these findings suggest that in some cases, a global view of opportunity may be helpful toward understanding victimization risk, while in other instances it is specific behaviors that are of greater explanatory use. As a theoretical concept, there is fairly compelling evidence based on our analyses that opportunity increases online victimization risk, particularly for those types of victimization/experiences involving interactions with others. Meanwhile, a routine activities-specific analysis brings depth to an understanding of online victimization in some cases, but it also adds opacity in other cases in that certain variable effects are not immediately interpretable.

Second, low self-control was directly related to harassment, hacking, and receiving nude/explicit content – depending on modeling of opportunity. Across models, persons with low self-control were at approximately 50% greater risk of being harassed or receiving nude/explicit content. In the routine-specific model, low self-control was also significantly, but somewhat weakly, related to hacking victimization. These findings are similar to those reported by Bossler and Holt (2010) whose analyses found significant relationships between low self-control and online harassment, low self-control and hacking victimization, and a null effect of low self-control and credit card fraud.

With respect to the impact of low self-control on harassment and receipt of nude/explicit content, it could be argued that persons with low self-control have personal interactions with others online that predispose them to experiencing these outcomes. Schreck (1999) suggested that individuals with low self-control were often pugnacious, which would heighten one's likelihood of being involved in negative online encounters, both as the aggressor and victim. It is noteworthy that several studies have reported an overlap between offending and victimization, including within online victimization research (e.g., Holt & Bossler, 2008; Reyns et al., 2011; Van Wilsem, 2013).

Regarding the nude/explicit content variable, as was previously noted, describing this experience as a victimization may not be entirely accurate. While receiving unwanted nude/explicit content is considered a form of visual sexual victimization (see Fisher, Cullen, & Turner, 1999), the wording of the survey item used to construct this variable does not make this clear. It may be that individuals solicited nude or explicit content, as would be the case if someone were engaged in sexting with their partner. This contention is supported by the effect of the relationship status variable. At the same time, the results indicate that opportunity and low self-control both significantly and positively affect this experience, which is a finding supported in the sexting research literature (e.g., Reyns, Henson, & Fisher, 2014; Wolfe, Marcum, Higgins, & Ricketts, 2016).

Third, it is noteworthy that low self-control was not significantly related to either hacking (in Model 2) or identity theft victimization. Based on these results and prior research and theory, we propose that hacking and online identity theft victimization are crimes for which the victim's level of self-control plays only a minor role in their victimization risk (Bossler & Holt, 2010). Implicit in the self-control perspective is the assumption that individuals have the ability and freedom to make choices that either guard against, or expose them to, victimization risk. Hence, self-control plays a more limited role for crimes and in situations where individuals' ability to exercise decision making is either restricted or irrelevant. This supports Pratt et al.' (2014) arguments regarding the potential utility of low self-control as a factor in the risk of victimization. With respect to hacking, cybercriminals often look for vulnerabilities in systems, and steal data on a rather large scale. This makes the individuals' routine activities or level of self-control essentially immaterial in the commission of the crime – depending on the method of theft. Instead, the onus must be placed on the organizations that are tasked with protecting these data to ensure their security – rather than on the potential victim.

Fourth, although our primary interest was in examining opportunity and low self-control frameworks as predictors of cybercrime victimization/experiences, several findings related to the control variables merit mentioning. To begin, sex was consistently related to both harassment and receipt of nude/explicit content. It may be that there are some sex-specific correlates of victimization within the opportunity perspective, in particular, and it would be beneficial if future research explored this possibility. Additionally, age was a predictor of both hacking and identity theft, and given the relatively truncated range for this variable, it would be interesting to further explore the reasons for this effect. Further, persons who identified as a sexual orientation other than heterosexual were consistently at greater risk for harassment and receipt of nude/explicit content. Again, this finding warrants additional attention, and in the case of each of these findings, sex, age, and sexual orientation should not be theoretically meaningful from an opportunity perspective (e.g., Hindelang, Gottfredson, & Garofalo, 1978). This suggests that these individuals may have been targeted *because* of these characteristics – a proposition supported by target congruence theory, which argues that offenders seek victims with characteristics representative of their ideal target (Finkelhor & Asdigian, 1996).

Limitations

Efforts were made to conduct a methodologically rigorous study, but there are some limitations that are nevertheless important to note. First, while it is very common to test

opportunity and self-control perspectives within college student samples, doing so limits the generalizability of the findings to college populations. It would be valuable to replicate these analyses within adolescent or general population samples.

Second, it is somewhat difficult to measure certain types of victimization through victimization surveys. For this study, three measurement issues are noteworthy. Among them, asking individuals to self-identify as victims of hacking may have underestimated its extent, particularly in instances where the victim does not know they have been hacked. Further, prior research has identified personal deviance and peer deviance as correlates of cybercrime victimization. These measures may have yielded similar results if included in the present study, but measures of these concepts were not available in the data. Additionally, the measure for receiving nude photos or explicit content does not necessarily reflect a criminal victimization, as the behavior may have been consensual. Yet, prior research suggests that analogous behaviors, such as sexting, have similar predictors to online victimization (e.g., Reyns et al., 2014). Considering this, and its place in Wall's (2001) typology, its inclusion in the present study adds value to the cybercrime literature.

Third, the variance explained in the models, while fairly typical in victimization research, is still somewhat low, and this is after considering low self-control, a wide range of routine behaviors, and many student characteristics. These potential limitations offer opportunities for future research to build and improve on our work, and despite any shortcomings, the results of the present study have implications for research and theory.

Implications for Research and Theory

Meta analyses of the effects of self-control on criminal behavior and criminal victimization underscore the usefulness of the theory in explaining these outcomes (e.g., Pratt & Cullen, 2000; Pratt et al., 2014). Yet, recent research, including the present study, suggests that low self-control may also have limits to its application. Our results, for example, support its continued use when examining person-based cybercrime victimization/experiences, but mixed or null support for computer-based outcomes. Should future research replicate these findings, it would further suggest that self-control is most meaningful in situations in which the individual has the freedom to make decisions resulting in increased vulnerability. For crimes such as hacking or identity theft, it appears that the criminogenic nature of the Internet automatically makes users vulnerable to victimization, irrespective of their decision making.

Our results also indicate that a more holistic view of opportunity yields theoretically meaningful results. By contrast, a routine-specific examination of opportunity produces a more practical view of victimization risk. Both of these approaches have value, and future research might more purposefully consider these competing interests when testing the opportunity perspective, the routine activity approach, or lifestyle-exposure theory. While each framework shares common assumptions, the empirical results generated across these approaches suggest differing uses for theory and/or practice.

Related to this, the results suggest possible means for preventing online victimization. Together, our analyses indicate that opportunity increases cybercrime risk, and that particular routines are directly related to online victimization. Situational prevention methods may prove effective if they are devised to address these particular risky

behaviors (e.g., Cornish & Clarke, 2003). Yet, it seems unrealistic to simply advise potential identity theft victims to avoid emailing, for example, because it is a risk factor for victimization. Instead, there is a need for interdisciplinary research combining computer security methods of automated threat detection and mitigation to better minimize the risk of victimization (see also Bossler & Holt, 2009; Holt & Bossler, 2013). Such techniques could help to better minimize the risk of victimization without the need for user interaction with security tools or protocols they do not understand. At the same time, cybercrime scholarship would greatly benefit from research exploring both the technical and social forces that play a role in the risk of certain forms of victimization, such as the ways that blogging is related to harassment, or how social networking is related to hacking, along with our other significant findings related to specific routine activities and victimization. Such research would provide valuable insights that could be used to develop very specific situational crime prevention strategies that lead to meaningful reductions in online victimization.

References

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*, 400–420.

Bossler, A. M., & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice, 38*, 227–236.

Brady, P. Q., Randa, R., & Reyns, B. W. (2016). From WWII to the World Wide Web: A research note on social changes, online "places," and a new online activity ratio for routine activity theory. *Journal of Contemporary Criminal Justice, 32*, 129–147.

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

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

Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime Prevention Studies, 16*, 41–96.

Dillman, D. A. (2007). *Mail and internet surveys: The tailored design method*. Hoboken, NJ: Wiley.

Felson, M., & Eckert, M. A. (2015). *Crime and everyday life* (5th ed.). Thousand Oaks: Sage.

Finkelhor, D., & Asdigian, N. L. (1996). Risk factors for youth victimization: Beyond a lifestyles/routine activities theory approach. *Violence and Victims, 11*, 3–20.

Fisher, B., Cullen, F. T., & Turner, M. G. (1999). *The extent and nature of the sexual victimization of college women: A National Level Analysis*. Washington, DC: National Institute of Justice.

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford, CA: Stanford University Press.

Grasmick, H. G., Tittle, C. R., Bursik Jr, R. J., & Arneklev, B. J. (1993). Testing the core empirical implications of Gottfredson and Hirschi's general theory of crime. *Journal of research in crime and delinquency, 30*, 5–29.

Henson, B., Reyns, B. W., & Fisher, B. S. (2013). Does gender matter in the virtual world? Examining the effect of gender on the link between online social network activity, security, and interpersonal victimization. *Security Journal, 26*, 315–330.

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization*. Cambridge, MA: Ballinger.

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

Holt, T. J., & Bossler, A. M. (2013). Examining the relationship between routine activities and malware infection indicators. *Journal of Contemporary Criminal Justice, 29*, 420–436.

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35*, 20–40.

Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. New York: Routledge.

Holt, T. J., Bossler, A. M., Malinski, R., & May, D. C. (2016). Identifying predictors of unwanted online sexual conversations among youth using a low self-control and routine activity framework. *Journal of Contemporary Criminal Justice, 32*, 108–128.

Holt, T. J., Smirnova, O., & Chua, Y. T. (2016). Exploring and estimating the revenues and profits of participants in stolen data markets. *Deviant Behavior, 37*, 353–367.

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

Koss, M. P., Abbey, A., Campbell, R., Cook, S., Norris, J., Testa, M., Ullman, S., West, C., & White, J. (2007). Revising the SES: A collaborative process to improve assessment of sexual aggression and victimization. *Psychology of Women Quarterly, 31*, 357–370.

Kulig, T. C., Pratt, T. C., Cullen, F. T., Chouhy, C., & Unnever, J. D. (2017). Explaining bullying victimization: Assessing the generality of the low self-control/risky lifestyle model. *Victims and Offenders, 12*, 891–912.

Leukfeldt, E. R. (2015). Comparing victims of phishing and malware attacks. *International Journal of Advanced Studies in Computer Science and Engineering, 5*, 26–32.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*, 263–280.

Leukfeldt, R., Kleemans, E., & Stol, W. (2017). The use of online crime markets by cybercriminal networks: A view from within. *American Behavioral Scientist, 61*, 1387–1402.

Maimon, D., Wilson, T., Ren, W., & Berenblum, T. (2015). On the relevance of spatial and temporal dimensions in assessing computer susceptibility to system trespassing incidents. *British Journal of Criminology, 55*, 615–634.

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory. *Deviant Behavior, 31*, 381–410.

McNeeley, S. (2015). Lifestyle-routine activities and crime events. *Journal of Contemporary Criminal Justice, 31*, 30–52.

Näsi, M., Räsänen, P., Kaakinen, M., Keipi, T., & Oksanen, A. (2017). Do routine activities help predict young adults' online harassment: A multi-nation study. *Criminology & Criminal Justice, 17*, 418–432.

Navarro, J. N., & Jasinski, J. L. (2013). Why girls? Using routine activities theory to predict cyberbullying experiences between girls and boys. *Women and Criminal Justice, 23*, 286–303.

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

Peterson, J., & Densley, J. (2017). Cyber violence: What do we know and where do we go from here? *Aggression and Violent Behavior, 34*, 193–200.

Piquero, A. R., MacDonald, J., Dobrin, A., Daigle, L. E., & Cullen, F. T. (2005). Self-control, violent offending, and homicide victimization: Assessing the general theory of crime. *Journal of Quantitative Criminology, 21*, 55–71.

Ponemon. (2016). *2016 Cost of Cyber Crime Study.* Available at: www.hp.com/us/en/software-solutions/ponemon-cyber-security-report/.

Pratt, T. C., & Cullen, F. T. (2000). The empirical status of Gottfredson and Hirschi's general theory of crime: A meta-analysis. *Criminology, 38*, 931–964.

Pratt, T. C., Holtfreter, K., & 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*, 267–296.

Pratt, T. C., Turanovic, J. J., Fox, K. A., & Wright, K. A. (2014). Self-control and victimization: A meta-analysis. *Criminology, 52*, 87–116.

Räsänen, P., Hawdon, J., Holkeri, E., Keipi, T., Näsi, M., & Oksanen, A. (2016). Targets of online hate: Examining determinants of victimization among young Finnish Facebook users. *Violence and Victims, 31*, 708–726.

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

Reyns, B. W. (2015). A routine activity perspective on online victimization: Results from the Canadian general social survey. *Journal of Financial Crime, 22*, 396–411.

Reyns, B. W. (2017). Routine activity theory and cybercrime: A theoretical appraisal and literature review. In K.F. Steinmetz & M.R. Nobles (Eds.), Technocrime and criminological theory (pps. 35–54). New York: Routledge.

Reyns, B. W., Burek, M. W., Henson, B., & Fisher, B. S. (2013). The unintended consequences of digital technology: Exploring the relationship between sexting and cybervictimization. *Journal of Crime and Justice, 36*, 1–17.

Reyns, B. W., Fisher, B. S., & Randa, R. (2018). Explaining cyberstalking victimization against college women using a multitheoretical approach: Self-control, opportunity, and control balance. *Crime and Delinquency*, https://doi.org/10.1177/0011128717753116.

Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *International Journal of Offender Therapy and Comparative Criminology, 60*, 1119–1139.

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

Reyns, B. W., Henson, B., & Fisher, B. S. (2014). Digital deviance: Low self-control and opportunity as explanations of sexting among college students. *Sociological Spectrum, 34*, 273–292.

Reyns, B. W., Woo, Y., Lee, H. D., & Yoon, O. K. (2018). Vulnerability versus opportunity: Dissecting the role of low self-control and risky lifestyles in violent victimization risk among Korean inmates. *Crime and Delinquency, 64*, 423-447.

Schreck, C. J. (1999). Criminal victimization and low self-control: An extension and test of a general theory of crime. *Justice Quarterly, 16*, 633–654.

Schreck, C. J., Wright, R. A., & Miller, J. M. (2002). A study of individual and situational antecedents of violent victimization. *Justice Quarterly, 19*, 159–180.

Song, H., Lynch, M. J., & Cochran, J. K. (2016). A macro-social exploratory analysis of the rate of interstate cyber-victimization. *American Journal of Criminal Justice, 41*, 583–601.

Spano, R., & Freilich, J. D. (2009). An assessment of the empirical validity and conceptualization of individual level multivariate studies of lifestyle/routine activities theory published from 1995 to 2005. *Journal of Criminal Justice, 37*, 305–314.

Stewart, E. A., Elifson, K. W., & Sterk, C. E. (2004). Integrating the general theory of crime into an explanation of violent victimization among female offenders. *Justice Quarterly, 21*, 159–181.

Symantec. (2016). *2016 Internet Security Threat Report.* Available at www.symantec.com/security-center/threat-report?inid=globalnav_scflyout_istr.

Turanovic, J. J., Reisig, M. D., & Pratt, T. C. (2015). Risky lifestyles, low self-control, and violent victimization across gendered pathways to crime. *Journal of Quantitative Criminology, 31*, 183–206.

Vakhitova, Z. I., Reynald, D. M., & Townsley, M. (2016). Toward the adaptation of routine activity and lifestyle exposure theories to account for cyber abuse victimization. *Journal of Contemporary Criminal Justice, 32*, 169–188.

Van Ouytsel, J., Ponnet, K., & Walrave, M. (2016). Cyber dating abuse victimization among secondary school students from a lifestyle-routine activities theory perspective. *Journal of Interpersonal Violence*, https://doi.org/10.1177/0886260516629390.

Van Wilsem, J. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology, 8*, 115–127.

Wall, D. S. (2001). Cybercrimes and the internet. In D. S. Wall (Ed.), *Crime and the internet* (pp. 1–17). New York: Routledge.

Wilcox, P., & Cullen, F. T. (2018). Situational opportunity theories of crime. *Annual Review of Criminology, 1*, 123–148.

Wilsem, J. V. (2013). Hacking and harassment—Do they have something in common? Comparing risk factors for online victimization. *Journal of Contemporary Criminal Justice, 29*, 437–453.

Wolfe, S. E., Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2016). Routine cell phone activity and exposure to sext messages: Extending the generality of routine activity theory and exploring the etiology of a risky teenage behavior. *Crime Delinquency, 62*, 614–644.

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

Bradford W. Reyns is an associate professor in the Department of Criminal Justice at Weber State University.His research focuses on different dimensions of criminal victimization, particularly victimological theory,victim decision making, and the relationship between technology use and victimization.

Bonnie S. Fisher is a Professor at the School of Criminal Justice at the University of Cincinnati in the Schoolof Criminal Justice. Her research agenda spans victim-centered issues from estimating the extent of differenttypes of interpersonal and cyber victimization to identifying their predictors to evaluating the effectiveness ofbystander intervention programs to reduce victimization and perpetration among high school and collegestudent populations.

Adam M. Bossler is a Professor in the Department of Criminal Justice and Criminology at Georgia SouthernUniversity. His research interests focus on the application of traditional criminological theories to cybercrimeoffending and victimization, the police response to cybercrime, and rural policing.

Thomas J. Holt is a Professor in the School of Criminal Justice at Michigan State University. His researchspecializes in cybercrime and the police response to these offenses. He received his PhD in 2005 from theUniversity of Missouri Saint Louis.