ABSTRACT Existing research on cyberbullying has consistently overlooked the role of victims in online offending, as well as victim behaviour as both a facilitator and predictor of digital predation. This article offers an interdisciplinary critique of existing research and proposes a new framework of cybervictimology—traditional victimology in the context of cyberactivities. The framework points to cyberbullying as being best explained by Cohen and Felson’s (1979) routine activities theory of crime. Because one of the main criteria of “traditional” corporeal bullying is repetition, the routine activities of victims in social media environments are key facilitators in the bullying process; they serve as advanced indicators of victimization in a space where anti-social behaviour is comparatively tolerated—and even celebrated—in the absence of suitable guardianship.

KEYWORDS Cyberbullying; Victimology; Routine activities theory; Law/legislation; Conversation analysis

RÉSUMÉ La recherche actuelle sur cyberintimidation a souvent négligé le role des victimes en cas de les crimes engagé en linge, et aussi les compartements de victimes comme facilitateurs et prédicteurs de predation numérique. Cet essai offre une critique interdisciplinaires de la récherche et propose un noveau cadre de cybervictimologie—le victimologie tradionnel en cas de les activités en ligne. Le cadre proposé indique que cyberintimidation est mieux expliqué par le ‘routine activities theory’ proposé par Cohen et Felson (1979). Parce que l’un des principaux critères de cyberintimidation traditionnel est repetition, les activities discret des victimes dans les environments des médias sociaux sont les principaux facilitateurs de cyberintimidation dans les environments en ligne où le compartement déviant est souvent toléré et encore célèbre en l’absence de la tutelle apprpriée.

MOTS CLÉS Cyberintimidation; Victimologie; Routine activities theory; La loi et législation; L’analyse de la conversation

Introduction
Cyberbullying has become one of the leading sources of technological, social, and policy debate in Canada and across North America over the last decade. Despite considerable attention from journalists, public figures, politicians, and lobby groups to raising aware-
ness of and combating cyberbullying, responses from the law enforcement community have proven comparatively glacial; this is in part due to the fact that there has been no substantive mechanism provided by either lawmakers or technology providers for identifying, arresting, or prosecuting cyberbullies (Arntfield, 2014). At the time of writing, a recently tabled Canadian bill proposing amendments to the Criminal Code legislating the nonconsensual trafficking of intimate images using cybertechnologies—a bill inspired in part by the high-profile suicides of Canadian teens Rehtaeh Parsons in 2013 and Amanda Todd in 2012—has recently begun its second reading in the House of Commons. While these amendments seeking to outlaw “sexting” would ostensibly expand the powers of law enforcement with respect to their interactions with Internet providers, the proposed amendments, unlike in the case of child pornography legislation where written narratives in the absence of explicit images are also criminalized, would not extend to text-based offending.

Part of the apparent lack of progress in combating and legislating cyberbullying would seem to rest in the fact that there is remarkably still no consensus on a clear and workable definition of cyberbullying in either a scholarly or a criminal context—a shortcoming aggravated by the fact that the vast majority of cyberbullying is thought to go unreported, or is at least significantly underreported (Hinduja & Patchin, 2008). Thus, the identification and classification of cyberbullying has to date relied, usually by default, on often doctrinaire and dated research on bullying in its traditional, offline, and corporeal context as first postulated by Olweus (1993). This includes its understanding as a frequently adolescent phenomenon, rooted in causing unprovoked and sadistic physical harm, based on repetition and asserting physical and social power differentials. Both cyberbullying and its derivatives (cybermobbing, flaming, trolling, etc.) and workplace bullying as increasingly topical areas of public discussion and scholarly analysis actually seem to draw on the term “bullying” somewhat liberally, without much thought as to the term’s origins and classification criteria.

Nearly two decades later, Olweus (2012) himself challenges the contemporary understanding of cyberbullying as a “new” problem, and posits that it is in fact a networked extension of his definition of bullying as it has always existed, and one that is a “low prevalence phenomenon” (p. 528). Using a meta-analytical approach, he suggests that current research has been largely knee-jerk, catering to hyperbolic news reports that overstate the prevalence of cyberbullying as compared to the still common version of traditional bullying offline. He also takes exception with the fact that researchers, in disseminating simple questionnaires among middle and secondary school students or focusing on isolated, unusually egregious incidents, have not properly accounted for how the compulsory element of repetitiveness in cyberbullying is quantified in the asynchronous world of the Internet. In this article, I propose an exploratory theory and point of departure for new research that addresses this missing link in the victimology of cyberbullying. In simultaneously looking at cyberbullying and victimology through a multi-disciplinary lens, and in synthesizing existing research on victim-offender relationships under the umbrella of what I call cybervictimology, I offer a review of how victim behaviour—versus offender behaviour—can provide a clarified un-
derstanding of cyberbullying, including how new and emerging media platforms function as instruments of victimization.

In keeping with the understanding of victimology as the study of the relationship between victims and offenders, victims and other victims, and victims and institutions such as the police, courts, and the media (Karmen, 2007; Turvey, 2013), cybervictimology examines these same relationships as they exist in a computer-mediated context. This includes the role of certain computing behaviours that lead to victim proneness and victim facilitation, based on the routine activities model first proposed by Cohen and Felson (1979). The routine activities model, once exported to a digital environment, would in theory enable researchers to populate a corpus of specific keywords, screen names, and websites used as a matter of routine by victims of cyberbullying to better quantify and forecast risk. It would also help identify correlates among victims with respect to specific methods of Web connectivity and Web-enabled devices, and establish a nexus between online and offline risk tolerance among victims. These behaviours, all of which constitute routines by definition, might then assist us in determining why certain victims are selected for cyberbullying and why victim responses vary so drastically, ranging from indifference in cases where victims are also bullied offline (Olweus, 2012), to extreme responses, such as circuitous victimization, self-harm, emotional despair, and even suicide in some cases.

**Review of the literature**

Some of the more relevant studies (Hinduja & Patchin, 2008; 2009; Holt, Burress & Bossler, 2010; Mason, 2008; Pelfrey & Weber, 2013; Strom & Strom, 2005; Williams & Guerra, 2007) have consistently used Olweus’s paradigm of traditional bullying—which dates to the 1970s—as a point of departure for a revised etiology of cyberbullying. These studies and others also typically fuse dependent and independent variables gleaned from studies of select identifiable groups—typically adolescent, full-time students in metropolitan areas—most of which tend to point towards causative factors in relation to offenders only. Some of these studies have yielded results that, while certainly provocative, actually reflect a number of known correlates with respect to traditional forms of schoolyard bullying, including identified links between bullying and other co-morbid behaviours, such as smoking, alcohol abuse, truancy, and bringing weapons to school (Hinduja & Patchin, 2009; Mason, 2008; McGuinness, 2007).

Conversely, studies focusing on the salient technological underpinnings of cyberbullying have deferred to existing research on what can be classified as cyberdeviance in a discursive context, lumping cyberbullying in with other forms of computer-mediated misconduct, such as digital piracy, password hacking and phishing, Internet luring, malware authorship, online auction fraud, and the downloading and distribution of child pornography (Higgins, 2006; Higgins & Makin, 2004; Higgins & Wilson, 2006; Holt et al., 2010). In these cases, some comprehensive studies indicate that operant conditioning from peers and parents, teachers, and guardians is the driving force behind cyberbullying. In brief, a review of the literature reflects research on cyberbullying that has thus far proven disproportionately offender-centric. This article conversely argues that the principal distinction between traditional offline bullying and online cyberbullying—aside from the obvious technological differences—and in part the reason for
the reluctance by experts to commit to a coherent definition of cyberbullying, is the overlooked role of victims and their user-based relationship to the victimizing media.

The risk of being a victim of cyberbullying clearly increases proportionally with the time spent not only online, but also in digital environments that pose identified risks. These locales are places that, like offline, remove physical and social barriers and bring victim and offender into close proximity (Bossler & Holt, 2009; Mustaine & Tewksbury, 1998; 1999; 2002; Pratt, Holtfreter & Reisig 2012; Yar, 2005). These online places include environments susceptible to external surveillance and thus ripe for predatory behaviour, such as message boards, chat rooms, and in open access discourses subject to public view (Holt & Bossler, 2009).

Routine activities theory: Online
Cohen and Felson’s (1979) routine activities theory, as an adjunct of the model of cultural criminology that emerged from the Chicago school tradition in the 1930s, initially examined the spike in all areas of crime in the United States, following World War II. In particular, the theory sought to explain how changes in work, travel, and family during the social restructuring of the late 1940s impacted changes in national crime patterns. The routine activities model, supported in their initial 1974 data collection by overwhelming empirical evidence, was subsequently based on the idea that where a motivated offender and a suitable victim converge in a place in the absence of a suitable and capable guardian (police, security guards, Neighborhood Watch, responsible adults, surveillance cameras, etc.), offending will almost inevitably occur. The routine activities of daily life, including work, school, shopping, driving an automobile, using public transit, walking through public places, and attending community events, all enable opportunities for motivated and criminally inclined predators to identify and prey on suitable victims or their property. Over time, the routines of specific victims, or a pool of potential victims, can be forecasted by offenders and crimes planned or premeditated based on predictors as simple as the design of the eight-hour work day, where targets will leave their homes and cars unoccupied, will be leaving a location alone and after dark using predictable routes, and so forth. This model has since been used to explain why, in offline contexts, persons occupying certain perceptively low risk occupations find themselves grossly overrepresented as victims of violent crime, including females working as nurses, models, and servers—three of the most over-represented occupations in “targeted stranger” offences—all of which required interactions with unknown persons, working unusual and often nocturnal hours, and having their names and other personal data either visible or openly discussed in public (Hickey, 2010).

A handful of studies (Miethe & Meier, 1994; Wilcox, Land & Hunt, 2003) have sought to expand on this theory by espousing integrated models of victimology that examine the interplay between not only occupation, but also the home life and pastimes of victims in the context of specific spatial environments. While a good deal of Chicago school criminology has focused on the convergence of crime, time, and place (Eck & Weisburd, 1995; Shaw & McKay, 1942), few courses of research have heretofore considered the role of victim lifestyle and the discernible patterns in their activities online—an environment where there is neither direct contact between offender and
victim, nor any discernible “place” as understood in traditional scholarship of criminology and victimology (Reyns, Burek, Henson, & Fisher, 2011). Eck and Clarke (2003) were arguably the first to identify this shortcoming in the traditional routine activities approach when seeking to explain crime and victimization in a fluid space like the Internet, an environment where both time and space are relative. The shortcoming, they argued, could be accounted for in the way that networks as integrated locations might be conceived as a composite place—a space in at least a symbolic sense—where offender and victim meet by proxy, but with sufficient depth of contact to invoke the routine activities model. More recent research (Holt & Bossler, 2009; Reynolds et al., 2011) has pointed out that the Internet’s modularity makes the process of capturing crime data all the more problematic, in that establishing a specific time of offence—requisite Uniform Crime Reporting (UCR) data throughout the Western world—is largely impossible. It might be prudent for future studies to address this issue by distinguishing between electronic communications like email or similar “inbox” messaging systems and instant messaging that requires a live, real-time exchange and therefore a more tangible temporal marker for offender-victim contact.

Since Cohen and Felson first postulated their theory, the global reach, diffusion of space and time, and asynchronous access to information and people afforded by the Internet has enabled new forms of criminality, creating motivated offenders who have unprecedented access to victims as compared to in their offline life. As adolescents—the most studied group with respect to cyberbullying in empirical research—additionally find themselves outcast or ushered away from traditional places of social congregation, such as shopping malls and public greenspaces, the Internet has become the main conduit of social connectivity, and by extension, the de facto locale where bullies can troll for suitable victims in the absence of more traditional offline locations (Berson, Berson & Ferron, 2002; Kirchen, 2008; Ito, 2013; Pelfrey & Weber, 2013).

That said, the problem with applying any criminological model to cyberbullying is its legislative handicap; that is, that cyberbullying (unlike other forms of cyberdeviance) is in most regions not a codified crime per se. In Canada, for instance, child luring, unlawfully recording and distributing copyrighted motion pictures, causing mischief to data, and electronic voyeurism are all legislated offences whose statutory wordings in the Criminal Code reflect their being computer-mediated crimes in earnest. Conversely, cyberbullying, like cyberstalking, has thus far tended to most commonly defer to a charge of criminal harassment under Criminal Code Section 264 when circumstances merit it, which is legislatively defined as unwanted and continuous contact, either direct or indirect, and that is known or likely to be known to cause fear or distress. Cyberbullying as a digital rendering of repetitious harassment and “pursuit ... by electronic means” (Reyns et al., 2011, p. 1153; see also D’Ovidio & Doyle, 2003; Finn, 2004; Finn & Banach 2000, Marcum, Higgins, & Ricketts, 2010; Sheridan & Grant, 2007) certainly fits the legislative definition of “harassment,” but carries with it other individuating factors in terms of victim experience—factors thus far overlooked by lawmakers and analysts. Similarly, in the United States, the 2009 federal case of United States v. Lori Drew for offences alleged to have been committed under the Computer Law and Abuse Act (CLAA) confirmed that violating a private website’s terms of use,
no matter how egregious, does not in itself constitute criminal culpability or merit prosecution (Arntfield, 2014; Zetter, 2009).

Whether the lack of a consistent or predictable physical consequence, as in the case of offline bullying, is a factor in inhibiting more aggressive legislation to combat cyberbullying is yet another area of research to be negotiated by the model of cyber-victimology proposed here. In brief, it is time to establish new and critical methodologies of studying the risk-tolerant behaviours of victims, as well as the concomitant role of specific media in both enabling and normalizing risk. Cybervictimology must therefore begin by addressing what is perhaps the most perilous of online routine activities, and the one variable that most significantly distinguishes cyberbullying from traditional iterations of offline bullying: social media.

**Digital predation, victim facilitation and social media**

Explicating the reasons for the link between victimization and risk tolerance with respect to social media usage has traditionally involved researchers quantifying risk according to demographic factors alone, and with sample groups demarcated by age and/or educational setting (middle school, secondary school, or college/university students). Yet, only a handful of studies, mostly in the field of communications and new media, rather than criminology or victimology (Bouvier, 2012; Lewis & West, 2009; Livingstone, 2008), have examined how risk can be measured more longitudinally beyond standardized schooling and into early adulthood, where daily routines and cyberactivities can vary greatly among respondents. Cybervictimology as an alloy of traditional victimology, criminology, and digital humanities might then go on to examine how the architecture of a given media platform or digital environment is itself an aggravating factor in victimization at different points in the life course; this would include the creation, activation, or re-activation of a social media profile as in itself constituting a routine activity that serves as a predictor of victimization. With respect to proposing cybervictimology as an extension of the routine activities theory, and routine activities theory as the leading explanation for cyberbullying, we must then critically examine the criminal ecology of the Internet itself, including social media as an inherently risk-tolerant and criminogenic environment that is well suited—even customized—for predation.

While social media has come under increasing scrutiny as of late, with countless and well-publicized arrests, prosecutions, public shamings, firings, and even murders, serious assaults, and the counseling and abetting of terrorist activities all stemming from nefarious posts and correspondences published to public view, few if any scholars have directly addressed the inherently criminogenic and anti-social constitution of specific social media sites. The nexus between social media and what is known as the Dark Triad of personality (that is, the convergence of psychopathy, Machiavellianism, and narcissism) has already been identified by Sumner, Byers, Boochever, and Park (2012) as has the link between offline bullying and psychopathy (Fanti & Kimonis, 2012; Sutton, Smith, & Swettenham, 1999), with the cyberbullying-psychopathy correlation remaining a fertile area for future interdisciplinary research. This includes an analysis of the use of specific platforms to lure victims, as well as the concerning normalization of certain paraphilias and deviant fantasies that exceed the scope of this
article, but that demand more focused attention from both academics and clinicians. In terms of a routine activities approach to cybervictimology in particular, social media as an inherently risk-tolerant activity should therefore be understood as a key mechanism in bringing victims and offenders together with an expediency and efficiency not commonly found in offline environments.

While certain risk-tolerant online activities have been associated with increased risk of victimization, including an identified correlation between the habitual viewership of hardcore pornography and being the subject of a malware attack (Szor, 2005), the illegal downloading of copyrighted material and being the victim of hacking or phishing (Holt, 2007), and the predisposition of being victimized when otherwise engaged in what could be broadly classified as cyberdeviance (Holt & Bossler, 2009), there is a dearth of research on what constitutes risk tolerance with respect to social media, an accepted and comparatively—or perceptively—innocuous cyberactivity. Scholarship on cyberbullying and cybervictimology must therefore initiate a critical re-assessment of social media as a routine activity in earnest, including assessing risk on a graduated scale of exposure. Victims might then be classified according to a system of gradation, ranging from infrequent users or dormant account holders to frequent users whose communications tend to occur in real-time or near real-time. This latter group—frequent users—will naturally have a social media experience defined by negligible lapses between the delivery and reception of aggressive or harassing communication (victim-offender contact by definition) versus less frequent users. There is little doubt that frequent users experience an immediacy of victimization through the increased speed of communicative transaction that, drawing on McLuhan (1964), will necessarily shape the content of the message itself, including any harm inflicted. In this context, the duration and frequency of use—or more accurately, the inability or unwillingness to disengage from these environments—might be understood as an increased tolerance of risk among cybervictims. Bossler and Holt (2009) have previously identified connectivity itself as a major factor in one’s routine; specifically, the costs associated with certain connectivity options as being lifestyle indicators and peer group determinants in the context of routine activities theory. It therefore stands to reason that opting into a routine and justifying the costs of a lifestyle where social media pervades everyday functioning, such as allowing all digital communications to push to a ubiquitous mobile device, creates a disproportionate risk based on frequency and duration of exposure.

The culture of proactive disclosure and information promiscuity endemic to social media also enables predators to summarily identify, and to some extent customize, their existing victim preferences. The public dissemination of personal details, photographs, and audio-visual material on social media sites—information that would seldom if ever be proactively released on consent in an offline context—naturally assists offenders in acquiring suitable victims for any number of offences, including criminal harassment vis-à-vis cyberbullying. With Felson (2002) having classified “suitable” in the context of the routine activities theory as any indicator that a person is subject to interpersonal control with minimal risk of consequence, social media sites are able to expedite and streamline this identification and victimization process; they allow cy-
berbullies to effectively window shop for victims based on searchable markers of suitability and vulnerability. This same victim selection process and has been previously identified in offline victim-offender contacts, specifically targeted stranger attacks, and where conventional scholarship on victimology has identified what is known as the “reassurance-oriented victim,” a typology classified by individuals who inadvertently expose themselves to at-risk situations by disclosing excessive personal information in good faith and in an attempt to make meaningful connections and seek validation (Petherick & Sinnammon, 2009).

Digital predation targeting reassurance-oriented victims, and the exploitation of social media sites as conduits for predatory behaviour, and target selection in a more general sense, allows cyberbullies access to victims who would normally elude direct face-to-face contact with offenders in the traditional routine activities approach. As Hayward (2012) has noted, the Internet—and by extension digital culture—has diffused traditional barriers between life stages and led to generational and demographic confusion that enables these types of unprecedented intersections. Similarly, barriers between identifiable groups that might normally inhibit access to certain victims in offline environments have proven equally permeable in the realm of social media, with certain environments presenting as “soft targets” and thus the easiest point of access for predators and motivated offenders. In brief, the evolutionary design of social media from its earliest versions (ICQ, MSN Messenger, MySpace, etc.) to the current menu of customizable and multi-platform networks necessitates a certain degree of risk-taking by all users that elevates a baseline assumed risk.

A critical analysis of cybervictimology and assumed risk

In this context, I qualify “risk” as any activity that draws on Kaplan and Garrick’s (1981) model, which, citing Baye’s theorem of probability, they argue involves choosing between, rather than avoiding, known hazards based on the availability of certain safeguards. Phrased differently, risk is a relative concept and one that can be measured according to individual tolerance levels. Distinct from uncertainty, risk requires awareness of a hazard, and is either mitigated or aggravated according to the safeguards applied to a given environment. Decisions with respect to enacting safeguards are equally subjective, and are typically based on the frequency of an expected or predicted outcome. This subjective calculus is what we might call assumed risk.

With Bossler and Holt’s (2009) assessment of computing activities that might be described as hazardous, or “illegitimate” as they describe them (p. 412), suggesting a correlation between routine activities that are inherently self-serving and therefore pose an increased acceptance of assumed risk, the exercise of safeguards decreases as potential rewards of attending certain digital spaces are thought to increase. As with any risk-taking behaviour that occurs offline, disproportionately increasing one’s likelihood of victimization, so too would it seem that victims willingly opt-in to online activities whose possible rewards are seen as outweighing the probable hazards. With respect to decisions about accessing specific social media sites in particular, so too would it seem that exposing oneself to cyberbullies is interpreted as an acceptable degree of risk based on expected or frequent reward for the same activity.
Routine activities theory online—perhaps even more than offline—shifts partial responsibility for the occurrence of crime to its victims. Not surprisingly, the theory is often considered polemical and is not without its detractors who decry it as victim blaming. In fact, beyond the annals of criminology and traditional victimology, such postulates have actually proven wholly unpopular, frequently misunderstood as an attempt implicate victims as active participants in their own victimization. That said, some of the most recent and cogent research (Agnew, 2011; Copes, 1999; Hickey, 2010; Reyns, Henson, & Fisher, 2011; Reyns, Burek, Henson, & Fisher, 2013; Robinson, 1999) that stems from von Hentig’s (1948) seminal treatise, *The Criminal and His Victim*, clearly points to the role of victims in at least enabling crimes of opportunity where one’s “routine” becomes a hazard that can be easily deduced or extrapolated by motivated offenders, and where focusing solely on “the outcome of a criminal event sometimes presents a distorted image” (Doerner & Lab, 2012, p. 4) of a crime’s genesis. Thus, an understanding of victim facilitation is less about espousing the idea of victim blaming as much as it is about recognizing the role of predictive routines as “crime-provocative” (p. 4) behaviours by default.

Cybervictimology as a theory and method that transcends traditional victimology and criminology is no doubt just as polemical, yet it needs to be understood as a missing link in the existing discourse on cyberdeviance. This includes an understanding of cyberbullying as arguably the least understood but most topical form of cyberdeviance. Given that nearly all of the documented cases of cyberbullying—and certainly the most publicized in terms of associated violence, including suicide—involve social media as the main activity that connects cybervictims and cyberbullies, the construct of a cybervictimology is really not a radical departure from the existing criminological or victimological literature, with only the medium of interaction having changed. Further, bearing in mind the correlation between social media and cyberdeviance, social media sites may very well conform to what Durkin (2009), followed by Roberts and Hunt (2012) have classified as “deviant cybercommunities” (p. 757), or subcultural networks defined by what would be considered delinquent and definitively anti-social behaviour in an offline context. Deviant cybercommunities can be identified by their paradoxical architecture, ostensibly serving a “social” purpose but actually intensifying the most deviant, sadistic, and anti-social of impulses among its users (Durkin, 2007; Quayle & Taylor, 2002; Quinn & Forsyth 2005). While obviously not populated exclusively by deviants, deviant cybercommunities nonetheless exhibit collective norms and customs that are by definition anti-social, including: callousness, consistent recklessness, an incapacity for real or meaningful relationships, persistent aggression, and need to lay blame and find fault with everything (American Psychiatric Association, 2013). Given that anti-sociality is implicit in a classification of psychopathy, and that the link between some social media activity and psychopathic traits has already been confirmed through empirical studies (Arntfield, 2014; Sumner et al., 2012), the construct of a social spaces as having an inherently deviant component can no longer really be disputed.

Of the broad array of social media sites that currently exist online, the cybercommunity that has rightfully received the greatest attention in respect of cyberbullying—
finding itself at the centre of nearly every well-publicized case—and the one that is arguably the most emblematic of an anti-social and deviant cybercommunity, is Facebook. Currently boasting over one billion active users (Fowler, 2012), Facebook, in spite of recent figures suggesting that membership is slowly declining (Edwards, 2014) remains unrivalled in terms of its cultural prominence and global dominance as a social media platform; however, confirming the number of bona fide, legitimate users is difficult given that conservative estimates put the number of counterfeit profiles in excess of 83 million (Sweney, 2012). Recent research suggests that Facebook membership is in fact still “mandatory” for inclusion in most adolescent social circles (Robards, 2012), a theory supported by the Media Technology Monitor—a survey and research focus group—which indicates that in Canada alone, as many as 63 percent of Internet users and over 90 percent of social media users have a Facebook account, over twice the number on any competing social media network (Oliveira, 2013).

Focusing specifically on Facebook as a deviant cybercommunity, Lim, Vadrevu, Chan, and Basnyat (2012) have equally noted the compulsory role of Facebook, ahead of other competing social media networks, as the preferred global platform used to self-manage the delinquent public images and reputations of at risk youth, gang members, and known offenders—even while incarcerated. Given its obvious appeal to overtly anti-social groups and individuals, one can theorize Facebook is an inherently risk-prone and criminogenic environment to navigate. While attendance in analogous offline environments would normally be dismissed by many as an unreasonable risk given similar identified hazards, indicators of collective delinquency, and proneness to victimization—biker bars, raves, violent demonstrations or other unruly assemblies, et cetera—Facebook’s perceived redeeming qualities apparently make it an acceptable risk among suitable targets as defined in the routine activities model. Given its expansive virtual real estate and simultaneous penetration into most offline social interactions, one can also come to rationalize the network as a discernible “place” in the context of routine activities theory, and thus a point of argumentation for future scholarship in cybervictimology.

Facebook and victim facilitation

Facebook as the most relevant of social media sites since the emergence of Web 2.0 and the Semantic Web (Ellison, Steinfield, & Lampe, 2007), and an environment that has the additional distinction of using informal social controls that are invariably negative in nature, will no doubt define the thrust of early scholarship on cybervictimology, especially as cyberbullying fast becomes the priority of government focus groups and experimental policing initiatives. For instance, the Government of Canada’s forthcoming report on cyberbullying, coupled with the recent enactment of the Province of Nova Scotia’s aggressive Cyber-Safety Bill, will cultivate unprecedented opportunities for research into the actual versus perceived incidence of cyberbullying, and also help moderate future debates about risk versus privacy in the context of cyberactivities.

Collectively, this research will also offer the opportunity to generate a database of known cases of cyberbullying from which text samples can be extracted, analyzed, and used to contour a better understanding of cybervictimology as linguistically and culturally relativistic. Facebook will no doubt be at the forefront of these and other early
enforcement initiatives, all of which mark attempts to police an environment that, despite its purported commercial and even intellectual applications, remains very much a lifestyle-oriented and optional routine activity. Despite the number of innocuous profiles held by no doubt well-intentioned users, the reality is that Facebook remains a place defined almost exclusively by gossip, ridicule, narcissism, exhibitionism, voyeurism, hyper-competitiveness, and a number of behaviours that straddle both anti-social and other psychopathological classifications that fall within the Dark Triad of personality previously discussed. These are the nodes of connectivity among all users—both victims and bullies alike—that govern its collective norms and online culture. To understand cyberbullying is therefore to understand how victims, rather than offenders, navigate and rationalize their presence in such a perilous and anti-social environment.

By way of comparison, Instagram and Twitter—arguably the closest rivals to Facebook in terms of cultural relevance—remain comparatively understudied in the areas of both cyberbullying and cyberdeviance. Reasons for this might include the fact that Twitter in particular necessitates the truncating of narrative text, limiting the detail of written content and naturally restraining the harmful lexicon of cyberbullies. One of the principal objectives of cybervictimology will therefore be to disaggregate victimization and victim experience within competing social media platforms, some of which by their very design may prove more anti-social and criminogenic than others. This disaggregation will additionally require identifying the decision-making processes of victims to opt for certain online environments over others in spite of the elevated and accepted risks posed by certain networks like Facebook. Incipient research on cybervictimology also needs to address why victims keep social media profiles active during the cyberbullying process, and whether victims who maintain multiple, contemporaneous social media accounts (Facebook, Twitter, Instagram, Pintrest, Google+, LinkedIn, etc.) are at increased risk of victimization, or decreased risk by virtue of being able to dilute their online presence across multiple environments. This type of social media diversification and diminished personal investment in any single platform might also be revealed to be a safeguard by definition, buffering a cyberbully's ability to identify suitable targets as a result of their routines being diffused across multiple networks and thus difficult to anticipate or extrapolate. It may in effect be the online equivalent of varying one's routine, a strategy often used to mitigate the risk of being targeted or pursued offline (Karmen, 2007).

In seeking to satisfactorily explain how assumed risks can be collectively and willingly undertaken by such a large online population, we then have to choose one of two hypotheses. We have to either side with Olweus's position that cyberbullying as a social problem is overstated and that the actual frequency of this hazard is low enough to justify the risks of using Facebook and other social media, or we need to believe that the hazards are real, the risk of victimization is high and the safeguards low, and yet account for why there remains some other incentive to commit to Facebook as a routine activity in spite of the known risks. In opting for the latter, and in espousing a transdisciplinary model of cybervictimology to better understand the online victim experience, I am drawn to Clifford Geertz's (1973) seminal analysis of risk, reward, and social meaning.
In this context I am focusing specifically on Geertz’s ethnography of the Balinese cockfight as a ritualistic and symbolic social network that lacks formal controls and yet, at the same time, dictates daily reality. It is a network that by its very nature is reflexively delinquent, not unlike how opting into (or remaining committed) to the similarly unregulated Facebook environment becomes a routine activity that requires significant assumed risk. Facebook as a social network and online society steeped in structured symbolism, and an analogue of the same high-stakes social network and observed by Geertz in Balinese society, can therefore be interpreted as a digital rendering of what Geertz, drawing on Jeremy Bentham, calls “deep play” (p. 412).

Geertz rightfully recognized that deep play was the most logical explanation for the role of cockfighting in male Balinese culture, as on the surface it would seem that any theoretical payoff for wagering on the matches could never outweigh the almost certain losses (death of the animal, impossible odds, financial ruin, risk of arrest given the illegality of the contests, etc.). Deep play online and in the context of Facebook today can thus be defined as any cyberactivity whose risks are so great and known hazards so high they are purely irrational, and such that no reasonable person would agree to participate. Geertz recognized that, in an offline environment, it was not so much extrinsic rewards of financial gain that motivated participants engaged in deep play, but rather, the intrinsic rewards that were not directly tied to winning as much as they were to the fantasies of power, celebrity, sexuality, and elevated social status that came with merely participating, win or lose. This same structure might explain in part why cybervictimology would seem to defy conventional approaches to the study of victims. It might also explain why cybervictimology yields a number of variables that cannot be quantified by using surveys, statistics, or the conventional “hard” measurables that have defined much of the modern criminological literature, but instead requires a structured and semiotic approach through online fieldwork.

Some studies that have focused on the collection of field samples from actual Facebook interactions, including Ellison et al. (2007) as probably the first and most enduringly relevant, have examined—drawing loosely on Bourdieu (1986)—the prevalence of low self-control and risk tolerance on Facebook as trade-offs rationalized by users in search of social capital. As users endeavour to accumulate “friends” as commodities, endlessly and competitively searching for evidence of acceptance among peers to build self-esteem and self-identity—hallmarks of the reassurance-oriented victim—social capital can be defined as the tangible resources and rewards reaped through investment in specific alliances (Bourdieu, 1986; Coleman, 1988). The social capital gleaned from these alliances is itself divisible into one of three categories: bridging capital (weak, ephemeral, or situational relationships); bonding capital (enhancing existing relationships with friends, family, and immediate peers); and maintained capital (hoarded contacts and casual acquaintances stockpiled over the life course) (Ellison et al., 2007; Johnston, Tanner, Lalla, & Kawalski 2013). In an environment like Facebook, where the ability to maintain any three of these relationship types is largely contingent on conforming to the frequently delinquent social ecology of that same environment, social capital may in fact be a leading facilitator of cyberbullying victimization in a space that, while apparently innocuous, is still one defined by anti-sociality.
Recent research (Ellison et al., 2007; Ito, 2013; Pelfrey & Weber, 2013) suggests that adolescents as the most frequently documented victims of cyberbullying seldom use Facebook to initiate new friendships or reciprocate unsolicited or random friend requests from strangers (bridging social capital), preferring instead to digitally replicate the dynamics of their existing offline cliques (bonding social capital). The question then emerges as to why cyberbullies choose Facebook as a preferred victimization environment in lieu of more discreet offline locations. One possible explanation rests in a fourth and hypothetical division of social capital that Johnston et al. (2013), building on Portes (1998), call negative social capital.

In brief, negative social capital can be defined as the engineered dislike and distrust of a person or group by another person or group; it is, by definition, the antithesis of social capital and actually results in the willful destruction of social bonds (Wacquant, 1998). Cybervictimology is in effect the study of negative social capital in an applied, digital context. It is the study of why certain environments facilitate collective hostility rather than community and collective efficacy, and how the anti-social architecture of platforms like Facebook don’t just facilitate victimization, but actually promote the cultivation of negative social capital. In other words, for the same reasons that victims engage in deep play by rationalizing remaining on Facebook and in comparable digital spaces in spite of advanced warning of trouble, so too do delinquents know that they can find like-minded predators—ad hoc collaborators in group-cause cyberbullying activities like cybermobbing—operating in a deviant cybercommunity that actually enables the sabotaging of social capital by its design.

While Facebook purports to diligently follow-up on reported misuses of the platform and investigate these sorts of violations of its terms of use, these measures are apparently insufficient in terms of deterring predators, as both certainty and severity of punishment are fundamentally lacking. Another research question emerging from this confluence of negative social capital and cybervictimology is whether victims of cyberbullying are predisposed to being not only contemporaneous victims of traditional bullying offline, but also to other forms of crime and deviance.

In what is arguably the most enduring and penetrating study of victimization on record, drawing on Canter and Youngs (2009), Hickey (2010) examines the role of routine activities and other “journey-to-crime” (p. 406) models that suggest victims exhibit either low-facilitation (minimal risk-proneness) or high-facilitation (maximum risk-proneness and involvement in their own victimization). In cases of high-facilitation, drawing on numerous empirical case studies dating to the 1950s, Hickey (2010) notes that victims whose lifestyles serve as key contributors to their victimization tend to be continuously pre-disposed to a specific type of crime, rather than general victimization to a variety of crimes. While Hickey’s work is limited to victims of multiple murder—specifically serial homicide—the data collected examines a disparity of crimes and is probative to understanding how cyberbullies select victims, and what routine activities might be considered facilitators of serialized bullying and bullying alone—not bullying in concert with other offences. Studies such as those by Vieraitis, Kovandzic, and Britto (2008) have to some extent mirrored the work of Hickey (2010) and others by conducting victim profiling experiments that approximate the
Hollingshead Four-Factor Index of Socioeconomic Status as a proxy of risk, examining variables such as age, occupational prestige, and marital status as facilitators of victimization. Nonetheless, cybervictimology instead requires a longitudinal analysis of “offences” that—like cyberbullying—do not necessarily have a firm definition or punishment. It also requires uncovering whether victims of cyberbullying have a history victimization of other offences based on their routine activities, whether online or offline, and how these routines translate into equally risk-tolerant cyberactivities.

**Conclusion**

In the wake of well-publicized, and in some cases sensationalized, tragedies involving cyberbullying, policymakers and law enforcement officials have had to grapple with understanding how, unlike apparent advances in preventing traditional bullying offline, anti-social behaviour is not only tolerated but to some extent also condoned through inaction online.

The well-publicized suicides of Ryan Halligan (cyberbullied on AOL Instant Messenger), Megan Meier (cyberbullied on MySpace), the near consecutive suicides of Canadian teens Amanda Todd and Rehtaeh Parsons (both cyberbullied on Facebook), as well as countless other incidents of humiliation and torment are not, however, a matter of theory—they expose the harsh realities of cyberbullying as perhaps the least understood area of victimization in the digital age, and one of the most socially topical and divisive issues of our time. By extension, these cases and the existing, pending, and proposed changes to legislation substantiate the need for victimology as a discipline to expand—like “new” media studies and the “digital” humanities as extensions of existing disciplines—towards an updated model of cybervictimology that accounts for the role of technology in victim-offender contacts.

From a purely practical perspective, the proposed designation of cyberbullying enforcement agencies—whether police or civilian—will in the long-term assist us in understanding how cyberbullying is both defined and criminalized, as well as how both bullies and their victims are classified, free of media sensationalism and emotive reportage. From a theoretical perspective, cyberbullying additionally represents a paradigm shift with respect to understanding how digital environments constitute places with their own spatial and temporal considerations, as well as the factors that determine victim selection and facilitation by predators who—as compared to offline environments—can operate with relative anonymity. It is not only anonymity, but also membership in a deviant community where anti-social (and by extension negative social capital) is an accepted form of informal control, that facilitates the victim-offender encounters at the core of cyberbullying and acts of cyberdeviance targeting discrete individuals or groups. It is cybervictimology that is in turn the locus through which such encounters need to be studied on a carry forward basis.

**Acknowledgments**

The author would like to acknowledge the support of the Social Sciences and Humanities Research Council of Canada (SSHRC) and Western University in the completion of this research.
References


