Winter 1-7-2012

Not Just A "Place For Friends": Teenagers, Social Networks, and Identity Vulnerability

Cenate Pruitt
Georgia State University

NOT JUST A "PLACE FOR FRIENDS": TEENAGERS, SOCIAL NETWORKS, AND IDENTITY VULNERABILITY

by

CENATE CASH PRUITT

Under the direction of Lesley Reid

ABSTRACT

This study is an empirical analysis of adolescents' risk management on internet social network sites such as Facebook and MySpace. Using a survey of 935 U.S. adolescents gathered by the Pew Internet and American Life Project, I investigate the influence of offline social networks on online socialization, as well as the impact of parental and self mediation tactics on risky online information-sharing practices. Overall, the relationship between offline social network strength and online communications methods was inconclusive, with results suggesting that most teens use online communications in similar ways, regardless of offline connectedness. Some relationships were discovered between parental and individual mediation tactics and risky online information sharing, largely supporting the use of active mediation techniques by parents and informed control of shared information by individual users. User demographics had a strong effect on risky information sharing, with gender and age playing a significant role. This study also offers some suggestions for parents and policy-makers interested in the topic.

INDEX WORDS: Internet, Internet safety, Teenagers, Adolescents, Internet usage, Social network sites, Myspace.com, Facebook.com

NOT JUST A "PLACE FOR FRIENDS": TEENAGERS, SOCIAL NETWORKS, AND IDENTITY VULNERABILITY

by

CENATE CASH PRUITT

A Dissertation Submitted in Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy

in the College of Arts and Sciences

Georgia State University

2011

NOT JUST A "PLACE FOR FRIENDS": TEENAGERS, SOCIAL NETWORKS, AND IDENTITY VULNERABILITY

by

CENATE CASH PRUITT

Comm ittee Chair: Lesley Reid

Committee: Dawn Baunach

Wendy Simonds

Electric Version Approved:

Office of Graduate Studies

College of Arts and Sciences

Georgia State University

December 2011

DEDICATION

In memory of Dr. Kathryn C. Buckner: scholar, aunt, friend.

ACKNOWLEDGEMENTS

Four years. Four years of my life that I will never, ever get back. In that time I've become a husband, a father, and a gainfully employed member of society. It's been a long and difficult journey, and I never would have completed it without help from a thousand friends.

Where to begin? With my committee, I suppose. Dawn, you have been a lifesaver on more than one occasion. Whenever I was freaking out about enrollment or qualifications or the minutia of graduate school, you always have had a quick and ready response. Cheers. Wendy, you are more than an advisor or a committee member, you are a dear friend. I'm sorry I never play Scrabble anymore. (Maybe now that I'm done, we'll get back into it!) Lesley, this is entirely your fault. All the panic, all the sleepless nights, all the self-loathing, I lay at your feet. Of course, with the dark comes the light; so I have to give you all the effort, all the hard work, and all the credit as well. Thank you for everything.

There are other people I have to thank as well; Dave Van Domelen, for the "bedsheet ghost" analogy in Chapter 3. Bobbi Carothers, for technical assistance. Gabe, Charlie, Patrick, Laurie, the Robs, and all my other friends (and Friends!), for being at least a partial inspiration to do this project in the first place. K. Thor Jensen, for freelance work that kept coffee in the cup and gas in the tank. My therapist, Dr. John R. Lucy, for listening to my endless complaining. My colleagues at Georgia State University, who kept me on the right path, who shared in my misery, and who have given me a ton of emotional support. My colleagues at Gainesville State College, who have always made me feel right at home; Pamela, Diane, Jessica, John, Michallene, Sara, Chuck, Imran, and all the rest, who have probably pushed me as hard as anybody else ever did. The late, great, Rudy Ray Moore, just because I can. The staff at Dancing Goats Coffee Bar, my other, other office. Tara Stubbs-Olowoye and Kimberly Cirino, for last minute advice.

Last, but certainly not least, my family. Mom and Dad, thank you for believing in me. Thank you for bankrolling this nonsense. Thank you for essentially shaming me into staying in grad school all those times I wanted to just bail out and do anything else. Alan and Emily, your support is deeply and honestly appreciated. Thank you for having such an awesome daughter, and for being the best in-laws ever.

Wendy, I would have given up long, long ago if not for you. You literally made this happen, from the day you came home and told me about this really interesting study you heard about on NPR all the way to printing the final draft at work on your boss's dime. I love you. Finally, Felton. You are the best thing that ever happened to me. This is all for you, buddy.

Alright, let's get this over with.

Cenate Cash Pruitt

October 16, 2011

TABLE OF CONTENTS

INDEX OF TABLES

INDEX OF FIGURES

CHAPTER 1 - Introduction

The April 2009 murder/suicide on the campus of Henry Ford Community College in Dearborn, Michigan, already a sensational enough story on its own, was pushed further into the spotlight when it was revealed that the accused killer, Anthony Powell, and his victim, Asia McGowen, had both posted material to the popular Internet video-sharing site YouTube. Still frames of Powell's videos, carefully selected to show his face twisted in laughter, anger, or frustration, filled the airwaves (clickondetroit.com 2008). Similarly, within hours of the announcement that vice presidential candidate Sarah Palin's daughter was pregnant, bloggers and the news media dug up the father-to-be's Myspace page. The pronouncements that he was a "fuckin' redneck" who liked to "shoot shit" drew worldwide attention, no small feat for an otherwise unremarkable 18 year old from a small town (Goldsmith & Lisi 2008; Stirland 2008). The process has almost become commonplace now; a young person is involved in a newsworthy event and the media immediately combs their MySpace, Facebook, or Livejournal for clues. Ethical issues aside, what is it about MySpace and other social network sites that encourages young people to reveal personal and even potentially compromising information about themselves to an anonymous audience?[1]

More than half of all U.S. adolescents report using social network sites like Myspace and Facebook (Lenhart & Madden 2007:ii). For today's teens, SNS serve a role much like the shopping mall or movie theater did for past generations, being a space where teenagers can do as they please with (a perception of) limited adult oversight, with two major differences – SNS can

[1]The term "social network site" is used in lieu of the conventional "social networking site" as the majority of SNS users are replicating existing social networks, rather than using the sites to build entirely new networks (boyd 2007).

be accessed virtually anywhere; from home, school, or even via a web-capable cell phone, and SNS can be accessed by virtually anyone (boyd 2007; Kane 2008). Indeed, their popularity is so pervasive, and their perceived risk (whether to users' safety or to employers' productivity) is so great that the U.S. Congress has proposed multiple pieces of legislation that would block social network site access in schools and libraries, the U.S. military and Canadian government have prohibited employees from using social network sites, and the city of Bozeman, Montana requires all job applicants to provide usernames and account passwords for their social network profiles (Ricker 2009; boyd 2007). Thirty-two percent of teens report being contacted by a stranger online, with several factors strongly correlating to stranger contact, most notably possession of a social network profile (Lenhart 2007:ii; Wolak 2006). While many teens who have social network profiles attempt to mask their identities, 63% believe that a sufficiently thorough search could reveal their identity (Lenhart 2007:v). Despite this, some teens openly share potentially dangerous information, such as full names, phone numbers, and even street addresses. In the wrong hands, this information can be used to stalk or harass users, or even to generate false documents for identity theft. Peers, family members, and present and future employers can see this information as well, creating problems when information meant for one social network comes into the possession of an unintended audience.

Clearly, users are not blindly throwing their personal data to the wind – there is an obvious expectation of privacy among on-line users, although there seems to be a strong disconnect between users' expectations and reality (boyd 2007). A recent imbroglio on Facebook involved a third-party advertiser's unauthorized use of members' profile photos on the site, resulting in one user being invited to meet “hot singles” such as his own wife (Ostrow 2009).

The concern here was obvious – Facebook receives money from advertisers, who then use Facebook members' likenesses without express permission. The issue received national attention, eventually resulting in an official statement from Facebook, explaining that the ads were in violation of company policies (Schnitt 2009). The statement did not, however, offer any guidance as to using Facebook's "opt-out" policy for approved advertisements.

There are a myriad of benefits to Internet use for teenagers, but there are also a host of potential problems; parents identify concerns such as emotional harm or addiction or the Internet as a gateway for sexual predators and deviants of all stripes to enter the home (Internet Safety Technical Task Force 2009). Much of the existing research on teenage Internet use, whether it involves social network sites or not, focuses on these risk issues; attempting to offer policy implications or parental advice (e.g. how to keep children safe on-line). However, a more subtle problem comes in the form of identity risk; teenagers clearly use the Internet to explore the world around them and to present themselves to their peers for approval. Hazards can arise when these presentations are inappropriate in a larger social context, or when otherwise normative presentations are misappropriated for harmful purposes. My research, while interested in the safety and policy aspects of adolescent Internet use, will focus primarily on the motivations for such risky behaviors. Specifically, what are teens doing on-line in the first place and what role do social networks play in the process? This research will generally target the relatively new medium of social network sites (SNS), although references to other forms of computer-mediated communication (CMC) will be made when relevant. SNS operate as a unique vector for identity performance – users "offer themselves up for surveillance," creating a profile that may reinforce existing cultural norms, but also allows for fluidity and resistance, as the profile (and the

resulting identity being presented) can be altered at will (Westlake 2008:23). Using a data set from The Pew Internet and American Life Project (PIAL), this research will analyze the relationship between teenagers' offline and online social networks as well as the influence of these networks on teens' identity creation practices and their willingness to share personal information online. The data will also allow an exploration of teenagers' perception of the Internet as a risky environment, as well as parental efforts to mediate teens' Internet use. The end goal of this research is to provide potential explanations for a relatively new social phenomenon that is of interest to educators, parents, legislators, and private industry, hopefully while remaining true to teenagers' own motives, goals, and understandings of a complex situation.

A Typology of Aspects of Computer-Mediated Communication: Directionality, Response, Persistence

Digital identities are fascinating because they often are expressed in multiple dimensions – users interact through CMC in a variety of forms, each with its own unique attributes.[2] Early research into CMC proposed that multiple anonymous spaces (such as Multi-User Dungeons or MUDs, chat rooms, and bulletin boards) might allow a potential fracturing of the individual into a sort of postmodern collage of distinct personalities, with opportunities for a great deal of fluidity and play with sexuality, gender, and other identities (Rheingold 1995; Surratt 1998; Turkle 1995). However, research into contemporary, less-anonymous CMC venues such as personal websites, Internet dating, and SNS suggest the various profiles an individual generates are not distinct experimentations with completely new identities, but specifically-targeted

[2] Schau & Gilly (2003) use the term "digital self", while Booth (2008) uses "persona" to refer to users' online identities. I will use "profile" as it the term most commonly associated with social network sites.

representations of a singular self-identity (Schau & Gilly 2003; Yurchisin et al. 2005; Zhao et al. 2008).

Virtually all forms of CMC can be organized by three key aspects: directionality of communication (multi- versus unidirectional), response rate expectation (real-time versus displaced response), and persistence of data (persistent versus fixed). Multi-directional communication refers to those forms of contact where two or more individuals actively engage in a dialogue with each other: e-mail, chat rooms, instant messaging, message boards, and multi-player gaming all fall into this category. Unidirectional communication is one-sided; the user only interacts with the material. There is communication, but it is mediated by the format; creators post content for an audience, and the audience engages with that content, but there is no allocation for cross-communication without switching methods. The browsing and creation of traditional web sites, blog posts and single-player online gaming generally fall into this category.

Real-time response is exactly what it sounds like; the users interact with an expectation of prompt response. Chat rooms, instant messaging, and gaming generally fit this description. Conversely, displaced response is detached, as users have an expectation of time to think and generate their ideas before replying, if they choose to reply at all; e-mail, blog comments, and message boards tend to fit this category.

Finally, persistent methods are generally stored remotely and can be accessed again at a later date or from a different location – traditional websites, archived email and most message boards fit this description. The semi-permanent nature of these sites allows their creators to "present a physically absent self to others" long after the communication has been completed (Schau & Gilly 2003:394). Fluid methods are relatively transient and leave little lasting trace;

chat rooms and instant messages are gone the moment a user closes the program, unless a copy was intentionally saved. Most online games fit this category as well.[3]

In all of these categories, SNS are unusual – SNS profiles combine the unidirectional communicative aspect of a traditional website through the posting of blogs, quizzes, photos, and other created content with the multi-directionality afforded by chat areas, "wall posts" and the like; they include real-time and displaced aspects via "status updates," integrated instant messaging capabilities, and user mail; and are both fluid and permanent – status updates and wall posts disappear from the "front page" after a while, as do the various toys and quizzes, but all of these things are archived elsewhere on the profile unless actively deleted. In keeping with boyd & Ellison (2007), social network sites are defined as any web-based community that allows users to (1) generate a virtual representation of themselves (a "profile"), (2) visibly link their profiles with those of other users (via "Friending" or similar agreed-upon relationships), (3) view and explore this list of connections as well as those of others in the community (via a "Friends of Friends" list, a search engine or browsing functionality, or some other system).[4] I would add a fourth qualifier to boyd and Ellison's definition: the ability of connected users to modify or append one another's profiles in some way (most commonly via the posting of "comments"). While SNS can be used to create new relationships, users largely communicate with people who are already a part of their social network (Ellison et al. 2007; Strano 2008). The unifying theme for the site may vary – it may be an online replication of a pre-existing school or business

[3]An exception would be "persistent world" online games (such as *World of Warcraft* or *Second Life*), where the game world exists on a remote server and continues to exist even after an individual user leaves the game (James et al. 2004). Even then, an absent player generally 'disappears' from the game world and cannot be affected by other users.

[4]For clarity, the act of creating such social connections on SNS will be referred to as Friending, and the individuals engaged in such connections will be referred to as Friends, after boyd & Ellison (2007). This will hopefully prevent confusion in later chapters when discussing online Friends versus offline friendship networks.

network (Facebook for students, LinkedIn for professionals) or based in some commonality of age, location, or interest (Yelp! for local business reviews, MyChurch for Christians) (boyd & Ellison 2007; Hinduja & Patchin 2008). The data set I use in this study identifies MySpace and Facebook as the most popular SNS amongst adolescents, but many other sites fit these criteria - even Amazon.com has introduced some social network elements to its service, allowing users to Friend one another based on their reviews of products.

Historically, CMC presentations were limited entirely to the content a creator put forth; "the specific content of posting is, in itself, a definition of the poster." (Booth 2008:527). With traditional web sites, message boards, and the like, a creator's identity is defined solely by information they have complete control over, but a social network profile is not just the product of its creator – it is a shared text, as Friends or other guests can alter the profile in a variety of ways; adding messages, linking to photographs, or using features such as "poking" or the giving of "virtual gifts", which adds another layer of complication to the process of self-presentation. A carefully constructed presentation can be dismantled very quickly by an unflattering revelation. Notably, the fluid nature of SNS can extend beyond the interest, desire, or capability of the profile's creator; most strikingly in cases where profile creators die, as other users may turn such profiles into impromptu virtual memorials (Williams & Merten 2009).[5]

It is important to note that Friend networks of the type seen on SNS are not necessarily correlated 1:1 with off-line 'real world' social networks. Boyd (2009) identifies three different potential understandings of the concept of a "social network": (1) the traditional sociological sense of the various and sundry interpersonal affiliations an individual holds; (2) behavioral

[5]Intriguingly, comments left by adolescents on the profiles of deceased peers are virtually always directed at the decedent rather than other visitors to the profile, and generally written in the form of a standard comment - a first person statement addressed to the profile owner (Williams & Merten 2009).

networks, the people an individual actually encounters during their regular activity; and (3) articulated social networks, the people an individual personally and intentionally identifies as being members of a network, and it is this category that SNS fall into. Essentially, a SNS network is "not the same list of people you would say constitute your nearest and dearest" and might include "friends, acquaintances, family members, people from your past, fans, professional colleagues, familiar strangers, … people you don't particularly like but don't want to offend... and the occasional celebrity you think is interesting" (boyd 2009).[6] That is not to say there is no correlation between these networks whatsoever – as discussed in-depth below, SNS often serve as a means for users to communicate with absent friends and to announce and maintain versions of their off-line social networks; furthermore, much of the "drama" to be found amongst adolescent SNS users is related to the Friending or unFriending of various individuals, or the all-important matter of which Friends qualify for the vaunted "Top 8" spots on a MySpace profile (boyd 2006b; boyd 2007).

Risk and Mediation

Online Risks Facing Teenagers

The Internet Safety Technical Task Force (2008) identifies three main areas for concern regarding child and adolescent safety on the Internet; sexual solicitation, cyberbullying, and exposure to problematic materials. Other research identifies privacy risks and the potential physical and emotional side-effects of Internet use (lack of physical activity, Internet addiction,

[6] I currently have over 300 Friends listed on my Facebook profile, ranging from immediate family to professional colleagues to high school classmates to relatives I have not seen in over a decade.

social isolation, etc.) as areas of potential concern (Hinduja & Patchin 2008; Livingstone & Helsper 2008; Rosen et al. 2008).

Sexual solicitation or "stranger danger" seems to be the most commonly cited concern regarding online safety. 83% of parents and 35% of teens in a 2008 study said they were "very concerned" or "somewhat concerned" about sexual predators online (Rosen et al. 2008:462). More than half of adults in a 2007 survey said "online predators are a threat to the children in their households," despite the fact that only about 13% of adolescents reported being sexually solicited online (ISSTF 2008:C-17). Even then, many of the "predators" soliciting adolescents for sexual contact are 21 or younger, with almost half being minors themselves (ISSTF 2008:C-20). Furthermore, 92% of teens who report being solicited via CMC react in appropriate ways; blocking or reporting the solicitor or simply ignoring the request (Rosen et al. 2008:464, 469). This is not to downplay the existence of adult sexual predators, but they are clearly a fraction of the overall problem, and their significance has perhaps been over-hyped by media outlets. Also, stranger contact in and of itself does not appear to be inherently risky – between 45% and 79% of U.S. adolescents engage in it, and some 10%-15% of teens report inviting online friends to meet up offline (ISSTF 2008:C-39-40). Online friendships that develop an offline component are typically nonsexual, between peers of similar age, and generally occur with parental knowledge or permission (Wolak et al. 2002).

Cyber-bullying or online harassment seems to be a topic of less concern, despite it being potentially more common than sexual solicitation – depending on the study, between 4% and 46% of teens report some form of online harassment or bullying (ISSTF 2008:C-23). The broad range of reported cases is due to problems with definition – different studies offer varying

explanations of what cyber-bullying or online harassment actually consist of, and what, if anything, is the difference between the two. Indeed, given the disparate sample sizes, target populations, and definitions of terms found in the research, it is difficult to conclusively say much of anything about online harassment. What is generally accepted is that cyber-bullying is seemingly most common amongst older adolescents, the bully and the victim are generally the same age and often know each other, and there may be significant gender differences in the tactics used (ISSTF 2008).

On the other hand, much research has been done on adolescents' encounters with objectionable material, both wanted and unwanted. When teens unintentionally come across such content the most common sources are unsolicited emails, web sites that use misspelled or incorrect URLs of popular sites as traps, or web searches with unanticipated results.[7] A recent study found that 34% of 10-17 year olds were exposed to some degree of unwanted pornography, while only 13% of respondents reported actively seeking out pornographic websites (Wolak et al. 2006:54). Other material, while non-sexual, is potentially problematic; hate speech, violent/gory imagery, and content related to self-injury. A particularly common and troubling topic is the "pro-ana" community; a loose network of web sites, message boards, and blogs where users "promote, celebrate, encourage and support" other users' eating disorders (Mantella 2007:1). These sites provide tips on topics such as dieting, escaping detection, and the best ways to induce vomiting (Keller et al. 2005; Mastronardi 2003).[8]

---

[7]The practice of registering misleading domain names to entrap careless users (called "typosquatting") is illegal in the United States, but convictions are relatively rare as the perpetrators largely operate outside of the U.S. (McMillan 2007).

[8]It seems highly unlikely that an adolescent would happen upon a "pro-ana" site unwittingly; such materials are probably actively sought out by their consumers.

Many of the concerns identified by parents and policy professionals as risky are, ironically enough, precisely the kinds of activities teenagers are looking for, from a self-presentation perspective (Livingstone 2008). Consider this: stranger contact provides an opportunity for teens to experiment and explore new identities with relatively little possibility of real-world harm, as well as offering potential new friendships, while materials parents deem unsuitable or inappropriate (especially those that are sexual in nature) may be actively sought out by curious teenagers.

Identity Vulnerability

While it is not a direct hazard to teenagers' physical or emotional safety, the privacy risk more properly referred to as "identity vulnerability" is a concern on multiple levels. Identity vulnerability refers to the various personally identifiable information that can be revealed by people on the Internet (Huffaker 2006). The data most commonly identified as vulnerable includes personal data such as full name, school or business name and home address or contact information like instant messaging account, e-mail address and phone number (Hinduja & Patchin 2008; Rosen et al. 2008; Williams & Merten 2008). Of course, there are many ways a teenager's confidential information can be unintentionally compromised; a peer or family member could share personal data, antagonists could illicitly access a teen's personal computer or another computer containing their records (belonging to a school, an employer, or some other authorized possessor), or improperly secured communications could be intercepted (Milne et al.

2004).[9] However, the focus of this study is specifically on self-disclosure, i.e., the personal information that teenagers themselves choose to distribute.

In and of itself, identity vulnerability may not put teenagers directly into harm's way, but it creates multiple opportunities for short or long-term problems.[10] First and foremost, identifying data can be used by unwanted parties to stalk, harass, intimidate, or otherwise violate the privacy of individuals (Hinduja & Patchin 2008). Indeed, issues like cyber-bullying and stranger contact essentially require a degree of information vulnerability; otherwise, how would these individuals decide upon a target? Without the real-time physical cues of the offline world, predators and bullies must rely on the data that is available to them via online interactions.

Second, and closely related to the first aspect, is the issue of unintended audiences accessing vulnerable information. Profile creators post personal data, photos, or other potentially compromising materials with a specific audience in mind – their peer group. However, problems can arise when this material is accessed by individuals other than those for whom it was intended. There are two specific external audiences that want access to teenagers' data, for two very different reasons: authority figures such as parents, teachers, and law enforcement seek to protect teens while spammers, marketers and predators seek to exploit them, whether economically or sexually (boyd 2007). Teenagers' profiles can include relatively harmless but age-inappropriate material, such as profanity, discussions of alcohol and tobacco use, sexual activity, photographs in swimsuits or various stages of undress, and so forth (Hinduja & Patchin 2008; Moreno et al. 2009a; Williams & Merten 2008). This material, while problematic in the

[9] A surprising source of identity vulnerability is social organizations such as churches, which may create online membership rosters complete with names, photos, and addresses (Hoy & Phelps 2003).

[10] One argument is that since so many young people post personal information online when compared to the relatively low number of youths who are actually being harmed, identity vulnerability alone is not a valid predictor of other, more obviously harmful activity (Wolak et al. 2008).

eyes of authority figures, is most likely normative amongst teenage peer groups – discussions of drugs and sex are presumably quite similar to those that were traditionally held "under the bleachers," at the drive-in, or in some other adult-free locale, while swimsuit photos and the like would presumably have been shared privately instead.[11] Some teens have posted more directly offending content, including discussions of drug abuse and criminal activity or photographs such as "an individual urinating" and "a homemade device captioned as 'a working bomb'" (Williams & Merten 2008:264). In some cases, law enforcement agencies have actually used photographs posted on SNS to charge users with crimes including weapon possession and vandalism (Clark 2009; Perez 2007).

Beyond the inherently hazardous nature of some of these activities, the idea that the Internet is one giant repository for potentially embarrassing data, ready for mining at a moment's notice, suggests that Internet users should take greater care, as potential employers, classmates, colleagues, and romantic interests can use this archive of virtual information to create their own impression of an individual beyond that which was intended to be seen. Warranting theory (Walther & Parks 2002) argues that information about an individual is accepted with greater validity when it appears the individual had a limited influence in its creation. In other words, external statements about a person (or "testimonials") are considered more accurate or reliable than a person's own statements about themselves ("disclosures"). Walther et al. (2009; 2008) specifically cited publicly visible Facebook messages as an example of such other-generated statements. Comments left on a profile by the owner's Friends have a strong effect on a stranger's perception of the profile creator; a person who has attractive Friends is regarded as

[11]This does not include, nor does it address the legal ramifications of activities such as the creation of sexually explicit material by underage individuals for consumption by other underage individuals.

more attractive, complimentary statements about a user improved perceptions of that user, and so forth. This creates another potential hazard; an individual's online persona, created as a form of intentional identity management, can be thrown askew by a third party's addition of damaging content, whether real or falsified. Given that 83% of teens who use SNS report having added comments to a Friend's picture, and 77% posted messages to a Friend's profile, the possibility for this sort of identity harm is considerable (Lenhart 2009a). As different online communication methods require/allow different levels of personal disclosure, information from one profile (real name, birthday – commonly found on Facebook) could be matched to information on a separate profile (sexual interests, drug status – commonly found on various personal ads) via data shared across both profiles (photograph, email address, location), allowing for an unwanted level of identity disclosure (Acquisti & Gross 2006). The more personally identifiable information available, the greater the potential risk, especially if connections can be drawn between an individual and participation in some objectionable behavior or another (Moscardelli & Divine 2007).

From this perspective, it could also be argued that the sort of data that can turn up in an online search would be considered similarly vulnerable. This means there are potentially dozens, if not hundreds, of sources of information waiting to be tapped by an external observer. Any or all of this information can then be used to create a sort of virtual “rap sheet” of the target, even though the information may be inaccurate, out of date, posted against the person's will, or an outright falsification. Much has been made recently of “Googleability,” the extent to which

information about a person is revealed by searching for them online.[12] As far back as 2006, 26% of hiring managers surveyed said they had used the Internet to do background checks on potential employees, and 51% of those managers said they did not hire an applicant based on search results (CareerBuilder.com 2006).

Finally, the sort of information that is commonly available on SNS is the same type of information used to verify an individual's identity when registering for secure websites. In theory, it would be quite easy for someone to use information from a social network profile to perform a "brute force" attack on the profile owner – recall that the personal email account of Alaska governor and Vice-Presidential candidate Sarah Palin was allegedly accessed by a college student who used publicly available information (Palin's birthday, ZIP code, and her high school) to reset Palin's Yahoo! Mail password (United States Department of Justice 2008). The disclosure of this kind of identifying data is quite normative on SNS – birthdays may be set to hidden, but are often readily shared, while much the same is true of home towns and current locations. Other potentially viable data is often revealed accidentally; posted as a seemingly-harmless bit of self disclosure, "all about me"-type quizzes generally include the sort of questions that are used to verify a secured online identity - make and model of first car, names of pets, schools attended, and so forth. In the sort of small-scale attacks described above, the opportunity for criminal identity theft or serious fraud is relatively unlikely, although

[12] A brief Google search for the author reveals academic publications and conference presentations, as well as social network profiles and several websites related to various hobbies and interests. A deeper, targeted search using the right criteria could uncover old chat logs, message board posts, and the like, some of which could be potentially embarrassing.

compromised accounts could be used to harass the owner or their contacts, held for ransom, vandalized or simply deleted outright.[13]

A more serious version of this is "phishing," the creation of a false but seemingly trustworthy identity in order to lure victims into giving up personal information (Jagatic et al. 2007; Jakobsson & Myers 2006). While phishing is traditionally done via mass e-mails to large lists of random individuals, SNS are rapidly becoming a new vector of attack; in at least two cases, men used SNS information to access women's personal email accounts, which they then scoured for nude photographs (McMillan 2011a, McMillan 2011b). SNS profiles compromised in this way are often used to further distribute the trap to a user's Friends, as a message sent from a Friend is more likely to be trusted than one from a stranger (Jagatic et al. 2007:97). Captured SNS profiles may be used to send spam, used by the phishers to post bogus reports of an emergency befalling the profile owner and requesting donations from Friends, or simply defaced for the phisher's amusement (Richmond 2009; DiSpirito 2010).

The choice of what information adolescents share is intentional, and often rather mundane amongst their peers (Livingstone 2008; Westlake 2008). Online communities, whether frequented by teens or adults, have their own norms that must not be violated; "in order to have an effective post, a poster must necessarily construct an identity that is different from the others, but similar enough to warrant being in on the same page" (Booth 2008:529). Teenagers create profiles that not only represent themselves, but also reflect their adherence to the norms and

[13] The 2007 intrusion and defacing of a California teenager's MySpace profile by individuals reportedly associated with the online group "Anonymous" led to a feverishly panicked report by a Los Angeles-area Fox affiliate which identified the group as "hackers on steroids" and "domestic terrorists" (Shuman 2007).

narratives that are considered relevant and appropriate amongst contemporary youth culture, as well as meeting the expectations of their peers; a teenager will use the same site all of her or his friends use, share content they feel friends would enjoy, and so forth (Livingstone 2008). Some of the information that older generations consider highly personal (political leaning, religious affiliation, and so forth) is considered public to contemporary adolescents, suggesting that the boundaries between public and private life might be in a state of flux for the entire cohort (Lenhart & Madden 2007:20; Westlake 2008).[14] Indeed, Mark Zuckerberg, the founder of Facebook, recently stated that privacy is no longer even a "social norm" online, claiming that the rise of social networking reflects a decrease in the importance of privacy (Johnson 2010).

As an example, one key piece of data readily revealed online is "A/S/L," or the user's age, sex, and location. A/S/L is a key component of user-to-user communication modes like chat rooms, where there is often no visual cue to a user's identity (Subrahrnanyam et al. 2006). SNS users' profiles typically contain this critical information, to the point where most contemporary research does not even bother to ask teenagers if they reveal this information – it is simply taken as assumed. Age, in particular, is a issue for concern. By default, MySpace limits its userbase to those 14 and older, and all users under the age of 16 have their profiles automatically and forcibly set to "private" status (i.e., only accessible by those they allow to see it). However, users can provide false data about their age to bypass this protection;[15] a profile nominally belonging to a 21-year-old female expressed an interest in "hot boys 11-14," implying the creator was either an adolescent girl who lied about her age to access the site or "an inept paedophile"

[14]An analysis of the social factors influencing this shift is beyond the scope of this research, but would undoubtedly prove fascinating.

[15]Hinduja & Patchin found some evidence of age falsification amongst about 8% of MySpace users under the age of 18, suggesting that the actual figure could be considerably higher (2008:134).

(Thelwall 2008:1328).[16] Similarly, location, while potentially hazardous in the wrong hands, is extremely commonplace – for adolescent users, it is a convenient way to locate peers; if you are looking for an individual, their hometown, school, etc. are conclusively identifying factors (Lenhart & Madden, 2007:22).

In this case, age, sex, and location, while definitely information that could be harmful if exposed in certain contexts, have become a mundane aspect of online communication. Photographs of the profile creator are extremely commonplace as well; between 57% and 79% of SNS users have a photograph on their profile (Hinduja & Patchin 2008; Lenhart & Madden 2007:16). Personal information is often shared as a means of proving one's identity – Friends can authenticate a user based on the photographs and other information present on a profile (Livingstone 2008). Furthermore, the Friending process itself seems to serve as a form of identity verification with the Friend population representing a network of individuals who will vouch for the user's identity (boyd & Ellison 2007; Donath & boyd 2004). Given that an individual's profile is a social performance, the number of Friends a user has attached to their profile could further represent the acceptance of that performance amongst the creator's peers (Westlake 2008).

Simply put, teens share their personal information both to be found by their off-line peers and to validate their performances to their on-line peers. Problems arise when seemingly innocuous data is accessed by individuals who use it for purposes that were never intended by the subject, whether it be a predator looking for a victim, a potential employer doing a background check, peers spreading the latest gossip, or simply Mom and Dad checking up on the

[16]It is also possible that the profile creator could have been an underaged homosexual male disguised as a female to dodge attention, but this seems unlikely – Thewall does not even suggest this as an option.

kids. For teens themselves, the issue with identity risks seems to be less that they shouldn't be sharing this information, but rather that adults shouldn't be looking at it – MySpace, to paraphrase boyd (2007), is seen as *their* space.

Despite the risks, little of the existing research suggests outright rejection of the Internet as a venue for adolescent identity work; indeed, much has been made of the positive effects online participation has for adolescents. Communication with a potentially infinitely diverse population broadens users' perspectives, and allows for interaction outside their ethnic or cultural group (Tynes 2007b; Tynes et al. 2008). The real-time text-based nature of online communication requires advanced cognitive skills (Tynes 2007a; Valkenburg & Peter 2008). The friendships generated via online networks create an extended social support structure beyond family and immediate peer groups (Tynes 2007a). Lonely teenagers can practice their social skills and use online peers as a sounding board for identity concerns (Valkenburg & Peter 2008). Blogs, podcasts, and other forms of decentralized content creation allow for organic cultural innovation, potentially free from external influence (Livingstone 2008). Targeted use of the web and new media can potentially increase teenagers' interest in political participation (Lupia & Philpot 2005; Quintelier & Vissers 2008). Teenagers can seek information on health and sexuality issues in a discreet fashion, especially regarding topics that might be awkward or uncomfortable to discuss face-to-face (Harvey et al. 2007). Even risk in and of itself is not necessarily a problem – attempting to shield teenagers from any and all harm would rob them of essential life experiences and potentially hamper their ability to deal with "real world" challenges once they reach adulthood (Staksrud & Livingstone 2009). On the other hand, it is entirely reasonable and understandable for parents and other authority figures to have an interest

in minimizing the severity of online risk, leading to the development of multiple forms of mediation.

Forms of Mediation: Parental and Self

Mediation, in this context, can be defined as "parental management of the relation between children and media... beyond simple restrictions to encompass also conventional and interpretive strategies" (Livingstone & Helsper 2008). Mediation goes beyond pure boundary setting to include a variety of potential tactics for controlling, limiting, or mitigating the risks adolescents might encounter on the Internet.

There are several sub-divisions of mediation that can be readily identified in the literature. The first level is the break between parental mediation, in which the parents attempt to moderate a teen's activities, and self-mediation, in which the teens themselves attempt to regulate or control the degree of risk. Within the realm of parental mediation, there are multiple possible vectors for control, which can be subdivided between those based on observation and those based on restriction. Of the observation-based mediation methods, *active mediation* consists of parental discussion and interaction with the child during the process of engaging with the medium (Livingstone & Helsper 2008). A similar practice is *evaluative mediation*, in which the parent observes the child's activity, but does not necessarily comment on it; this runs the risk of implicitly approving of objectionable behaviors or content (Eastin et al. 2006). *Restrictive methods* are those where a parent attempts to directly or indirectly prevent access to potentially hazardous situations. Restrictive methods take two forms: *interaction restrictions*, the setting of restrictions external to the computer itself – rules about time spent online, location of the computer, or sites/content that are not acceptable, while *technical restrictions* are those that rely

on the computer itself as a means of control; most commonly, software designed to restrict access to certain sites/content ("filters") or designed to track teenagers' Internet use so that parents may review where their child has been ("monitors") (Livingstone & Helsper 2008).

Self-mediation, the ways by which teenagers themselves control and mitigate risk while online, is a relatively under-discussed area. Teenagers are certainly savvy when it comes to their online experience, and have developed their own ways for negotiating potentially hazardous situations (Tynes 2007a). Given the relative lack of focused research on teens' self-mediation skills, it is more difficult to create a typology, but self-mediation can essentially be divided into two categories; identity control and situation management. Identity control refers to the ways that teens themselves choose which information they share and who has access to that information. There is an intentional decision on the part of most teens as to what information is to be shared, and how; often based on the mode of communication, the goal of the communication, and even the structural differences between similar methods – for instance, the degree of anonymity allowed between two SNS (Livingstone 2008; Retelas 2008). As noted above, certain aspects of identity are commonplace and readily shared, especially on SNS – age, sex, location, a photograph, etc. However, teens may also modify or alter personal information for a variety of reasons, whether to experiment with new identities, to joke with peers, because they did not bother to include it in the first place, or perhaps most importantly, to hide from unwanted attention - especially parents (boyd 2007; Lenhart & Madden 2007).17 Sixty-two percent of teens whose parents were aware of their SNS profile reported setting their profiles as "Friends only," compared to 46% of teens whose parents were unaware of their profile (Lenhart

[17]A popular website, *Oh Crap. My Parents Joined Facebook*, is dedicated to users' accounts of their parents engaging in "embarrassing" acts on the popular SNS ("Jeanne & Erika" 2009).

& Madden 2007:27). Teenagers also use false data to bypass sites that require personal information as part of the registration process (Moscardelli & Divine 2007). Fifty-six percent of teens with profiles report posting at least some false information, with eight percent claiming most or all of their profile is falsified (Lenhart & Madden 2007:23). Boys seem to be more likely to share false data, with 64% of boys reporting some degree of falsification compared to 50% of girls (Lenhart & Madden 2007:24). This could be due to the differing reasons for SNS use detailed above – boys might "puff up" their presentation to appear more interesting to the girls they flirt with, while girls may value honesty amongst their friendship networks. Age plays a role as well, with 69% of teens 12-14 reporting false information, compared to 48% of older teens (Lenhart & Madden 2007:24). This is most likely related to the age restrictions on SNS; users under the age limit of 14 must lie about their age to gain access.

Even if teenagers are entirely truthful with their online presentation, SNS often offer an extra layer of identity protection; profiles can be set to "private" or "friends only," limiting access only to those users approved by the profile creator. Thelwall (2008:1234) found that about 18% of a sample of MySpace users aged 16 and over had profiles that were set as "private," while Lenhart & Madden (2007:26) found that 59% of teens said their profiles were only visible to friends, while another 40% said their profiles were visible to everyone. While this would suggest a degree of identity protection, the act of Friending may be less about controlling access to data and more about the public display of social connections (boyd 2007; Thelwall 2008). As discussed above, some SNS users have hundreds of Friends, ranging from family members and significant others to distant relatives, casual acquaintances, and in some cases,

musical groups, celebrities, or even novelty profiles representing fictional characters (boyd 2009; Booth 2008).

Furthermore, the binary nature of Friending is rather limiting once the initial control is applied – whether the profile is "friends only" or publicly visible, it is the same information (Preibusch et al. 2007). In December 2009, Facebook massively restructured its privacy settings, but not without controversy. While the new Facebook allows users to organize their Friends into categories that can then be assigned different levels of access to a user's profile, it also changed its definition of "publicly available" information. Facebook users' names, profile picture, gender, location, school and work networks, and "fan pages" (an articulated statement of support or approval for a celebrity, company, cause, etc.) are all available for any visitor to view. This could be problematic if a user is a "fan" of a controversial issue such as drug legalization and an unwanted visitor views such information (Paul 2009). Even with the security changes, the process of assigning Friends into various categories is counter-intuitive at best and Byzantine at worst, prompting some third-party sites to set up "walk-through"-type guides (Driscoll 2009, Paul 2009). While Facebook users can now determine on a post-by-post basis which Friends get to see their status updates, SNS remain "weak by design" when it comes to identity security; a user has to reveal pertinent information in order to be found by real-world friends, as well as to prove to Friends that they are who they claim to be (Schroeder 2008, Acquisti & Gross 2006:2). This weak privacy scenario may actually benefit SNS financially; after all, nobody goes to Facebook or MySpace to be left alone. The entire point of SNS is sharing information with an audience, and too much privacy would remove the panoptic appeal of the site. The less appealing the site, the less money the site's owners stand to make. Essentially, Facebook (and by

that virtue, other SNS) need users' private information to keep the rest of the user base coming back (boyd 2010).

This raises a specific question about SNS – if the site's business model is hinged on monetizing access to users' personal information and other user-created data, then who actually owns that information?[18] Facebook's "Statement of Rights and Responsibilities" claims that Facebook has the right to use any "IP content" (photos, videos, and other materials covered under intellectual property law) as they see fit, worldwide, until that content is deleted (facebook 2009a). Facebook recently sued the creators of "Web 2.0 Suicide Machine," a site that allows users to remotely "kill" their Facebook, Myspace, LinkedIn and Twitter accounts, claiming that the program's ability to log into Facebook users' profiles on their behalf is a violation of Facebook's terms of use (Hoover 2010; McNamara 2010).

The second aspect of self-mediation, situation management, concerns the ways teens react when they are presented with a risky scenario. In the case of stranger contact, blocking the stranger from further contact, rebuffing the stranger's advance, or reporting the incident to an authority figure are all considered "appropriate" responses (Rosen et al. 2008; Staksrud & Livingstone 2009). On the other hand, the suggested appropriate response for issues of identity vulnerability is simply to remove the vulnerable data or to limit access to it (i.e., by setting a profile to "private") which, as noted above, can be a complicated process (Moreno et al. 2009b). Identity vulnerability is at its core an identity control issue, although there are potential cases where situation management might come into play, such as a teenager finding their personal data

[18]In at least one case, an online community has abandoned a site over the monetization of user-created content; in 2008, editors of a wiki dedicated to the Transformers toy robot line left their for-profit hosts and recreated the entire site on a private server following a heated and public disagreement about advertising placement (Finkelstein 2008; TFWiki.net 2008).

in an unexpected and unwanted venue, or more likely, a website requesting information the user is not willing to part with. Teenagers who perceive the sharing of personal data as risky are less likely to provide such information when prompted (Youn 2005).[19] Their management strategies in such situations reflect back to the issue of identity control – teens either falsify data, provide incomplete data, or simply leave the site altogether (Youn 2005).

Again, teenagers are certainly aware of the risks of Internet use, and clearly take steps to maintain their own safety. Teens whose profiles contain "all" or "most" false data feel they are less likely to be identified by their profile than their peers who just have "some" or "very little" false data (Lenhart & Madden 2007:26). Overall, the strongest predictors of a teenager's concern for their online privacy appear to be their own frequency of internet use and the level of parental communication (Moscardelli & Divine 2007).

Both parental and self mediation strategies have their shortcomings, however. Several studies found that less than half of parents offered any form of mediation, and the techniques used were limited in effectiveness, if not outright ineffectual (Livingstone & Helsper 2008; Rosen et al. 2008). Even in situations where parents do attempt to mediate teens' Internet experiences, the most obvious problem is the potential disconnect in awareness of limitations – attempts at interactive restrictive mediation can only be effective if the child is aware of the rules (Livingstone & Helsper 2008). Multiple studies present exactly such a disconnect; while parents reported a set of rules or limits on Internet behaviors, their children did not (Liau et al. 2005; Wang et al. 2005). Older teenagers reported far fewer restrictions on Internet use, as did teenagers who had Internet access in their bedrooms (Livingstone & Helsper 2008; Rosen et al.

[19]Conversely, if teenagers perceive some benefit to the disclosure, their willingness increases considerably (Youn 2005).

2008; Wang et al. 2005). Indeed, one study suggested that teenagers who identify as highly skilled at Internet use were more likely to engage in certain forms of risky behavior (e.g., stranger contact, viewing of inappropriate material) than their peers (Livingstone & Helsper 2008).

Self-mediation has its limitations as well; some teenagers are simply not as technically adept as their peers, and may have a hard time moving SNS profiles into a protected status, while others may lack the skills or savvy needed to deal appropriately with risky encounters (Livingstone 2008). While it is heartening to see that teenagers are handling potentially risky situations in appropriate ways, it still smacks of closing the barn door after the horses have escaped; these risky scenarios may well never have happened if the teenagers had been more judicious in their identity control strategies. On the other hand, holding teens overly responsible for receiving unwanted attention might be a case of blaming the victim, especially when the vast majority of teens handle risky situations in a thoughtful and reasonable manner. The problem with identity vulnerability comes about because, as discussed above, the boundaries for what is acceptable and unacceptable sharing of information seems to vary between contemporary youth culture and the norms of mainstream society – while teenagers may know how to handle stranger contact, cyberbullying, or the presentation of unwanted content, identity vulnerability is largely a peer-motivated problem.

Overall, the literature clearly demonstrates that there is a need to further explore what teenagers are doing online, both on SNS and in a more general sense. In the next chapter, I address some critical questions from a theoretical perspective – what is the influence of offline social networks on teens' online behavior? What social factors influence teens' decisions to use

SNS versus other forms of CMC? Why do they persist in risky identity activity, even when they seem to be aware that their information could be compromised? What, exactly, do they gain by doing all of this? What can parents do to prevent these risks, if anything? By applying a combination of symbolic interactionist, postmodern, and developmental psychological thought, I can begin my search for answers.

CHAPTER 2 - Theoretical Approach

Generally speaking, the social science literature regarding online identity formation and management tends to draw from two schools of thought; the sociological theories of Erving Goffman and developmental psychological concepts based on the work of Erik Erikson. Additional insight has come from postmodern thought, particularly interpretations of Michel Foucault. I will attempt to fuse these disparate conceptualizations into a single, holistic overview of adolescent online activity and identity risk. This model will reflect the influence of teens' offline social networks on their online activity, as well as means by which teens and their parents can mitigate potential risks.

Goffman & Self-Presentation

Erving Goffman's *dramaturgical sociology* (1959) provides an excellent framework for approaching Internet communication and online identity formation. Simply put, Goffman's thesis is that every social interaction is predicated to some degree in a process of *impression management*. When around other people, an individual will act in a manner that is designed to present an impression that is useful to that individual's interests. To this end, people tailor their appearance, actions, mannerisms, and so forth to present the best possible impression. Within this realm of impression management are a host of motives; the confidence artist hoping to swindle a widow uses the same general tricks, tactics, and techniques as a teenaged boy hoping to impress his date; the con artist is perhaps less altruistic in his motives, but the staging is nonetheless similar. While Goffman died in 1982, well before the popularization of CMC, his theory still resonates; perhaps even more so now.

The business of impression management can be thought of in terms of two types of expressions – those that are "given" or deliberately manipulated, and those that are "given off" or (at least seemingly) unintentional (Goffman 1959:7). "Given" expressions are largely under the control of the performer; the spoken or written word, the style of dress, the manner of bearing, and so forth, while "given off" expressions are generally uncontrolled and often unconsidered; a nervous stutter, an accent, a shaky hand, all the various and sundry "tells" that gamblers use to their advantage - they can be feigned, but are more often taken for granted. These unintentional expressions are critical to face-to-face interaction for Goffman, as they provide an audience with some means of potentially discerning the validity of a given performance. Given that so much of Internet communication is directly controlled by the user, the opportunity to observe "given off" expressions in online communication is extremely limited, even accounting for the availability of web-conferencing software. This intense control over one's own expressive activity also means that identity management on the Internet is almost fully in the hands of the performer; an audience can only see the expressions that are selected for them. Indeed, Internet users have gone to some lengths to generate stand-ins for non-verbal cues such as vocal tone; consider the "emoticon," a symbolic tool to represent humor, displeasure, etc. in text-based conversation (Derk et al. 2008; Lo 2008).

Traditional websites, while relatively one-sided, are an excellent example of this aspect of Goffman's theory. Walker (2000) divides web pages into two categories - "extrinsic" pages, used by creators to support off-line activities or networks (keeping in touch with friends, sharing links with peers) and "intrinsic" pages, those that are used by creators to address the Internet at-large. Extrinsic sites are targeted towards people the creator already knows, while intrinsic sites

are “overtures aimed at unknown audiences” (Walker 2000:107). In either case, the essential presentation found on traditional websites is similar – some personal information, some images, some links to other websites, and some means for delivering feedback – a guestbook or e-mail account (Dominick 1999; Walker 2000). Images, links, and other visual effects allow website creators to generate visual cues to replace the lost non-verbal ones; they are calculated displays of the creator's intended self-presentation (Papacharissi 2002). Flashing lights, wildly colored text in odd fonts, and the like all display a certain creativity, while a simple and understated website in muted tones might reflect a more professional attitude. A serious website might be identified as a “web page” or “personal site” while a more casual one is dubbed a “forbidden zone,” “lair” or “crap” (Dominick 1999:654). All of these visual and textual cues allow a creator to display specifically targeted aspects of their personality, as well as serving to lure in visitors who share the creator's interests (Dominick 1999; Papacharissi 2002; Walker 2000). Furthermore, the displaced nature of websites means that it is quite easy for a creator to make statements about their identity, and relatively difficult for audiences to refute or disprove such statements (Walker 2000). Even in a situation where an audience member does not accept the creator's self-presentation, the visitor can simply ignore it and move on, while the creator can similarly ignore negative feedback (Dominick 1999). Essentially, websites allow their creators a “carefully controlled performance... under optimal conditions” (Papacharissi 2002:644).

Goffman identified the social realm in which acts of impression management take place as a “front region”; traditionally this might be a classroom, office, or other place of business (1959:107). Similarly, a “back region” would be the areas where performers prepare, rehearse, and manage their self-presentations before utilizing them in the front region; this might be a

teachers' lounge, the kitchen area of a restaurant, or other areas where audiences are generally not allowed to intrude (Goffman 1959). These regions do not directly correlate with the common notion of "public" or "private" areas; a family's living room would be considered a private space in the traditional sense, but when that family entertains guests it would be a front region in Goffman's terms. In such a case, the family are a team of actors portraying the role of "happy family," the guests are the audience, and the living room is the stage on which the performance takes place. This distinction is crucial to understanding how self-presentation works on the Internet.

Persistent forms of CMC, like the web sites discussed above, serve as a sort of fixed performance in a permanent front region; while the performer may be absent, the website/profile/post serves as a continual and consistent presentation of the self. This performance can reach any audience, anywhere, anytime, as long as there is Internet access. This is a great load off the creator, as traditionally impression management is a careful task requiring much effort, but the nature of CMC allows for far greater levels of image control than previously possible. This is not to say that all on-line spaces are front regions – any form of CMC where the users identify as part of the same team or cohort and subsequently discard or minimize their self-presentation in favor of self-disclosure could be considered a back region. Walker (2000) found that creators of extrinsic sites, those web pages that were meant to be used only by the creator and/or a closely chosen group of people, were surprised to imagine that anyone else might be interested in their presentation. The creators of extrinsic sites in Walker's study viewed their sites as part of a back region, meant for consumption only by those who were part of the shared performance team of "family" or "friend network," despite the fact that such sites could

be theoretically visited by anyone with Internet access (Walker 2000). Clearly, the lines between "front" and "back" regions (and subsequently, between "public" and "private") can quickly become blurred on the Internet, as the case of blogging demonstrates.

Papacharissi (2004) argues that blogs are designed for self-disclosure rather than self-presentation, allowing the viewer access to the more mundane (yet simultaneously more intimate) details of the creator's day-to-day life. For teenagers, blogs offer "an outlet for personal expression and reflection, as well as a way to communicate and connect with others" (Huffaker 2006:1). As such, blogs seem to function as a Goffmanesque "back space," a "behind the scenes" realm where the creator is more vulnerable and discusses the process of content creation (Trammell & Keshelashvili 2005:972). However, while a blog may let "the performer... drop his front... and step out of character" (Goffman 1959:112), there is still an element of the front space inherent in the existence of the blog – while it is a demystifying of the blogger's virtual identity, the blogger is still making calculated decisions as to which aspects of her or his personal life to put on display. Indeed, Trammell & Keshelashvili (2005) extensively discussed the means by which "A-list" bloggers (i.e., the most popular/most widely read creators) attempt to present their identity to their audiences, often via considerable self-disclosure. These top bloggers readily reveal information such as full names, location, and even phone numbers; by doing so, they create a degree of (perhaps feigned) intimacy with their audience.[20] In these cases it would seem that the blog is a front space manipulated to appear as a back space and this level of self-disclosure is simply part of the performance of blogger identity, at least amongst "celebrity" bloggers, although the same may not be true of the remainder of the blogging

[20] An application of this study to Twitter, the popular "micro-blogging" site used by many celebrities as a promotional vehicle, might prove fascinating.

community. Huffaker's study of teen bloggers found that the majority reveal information such as first name (70%), age (67%), city/state location (59%) and some form of contact information (61%) (2006: 6). These teens do not create pretend or fictitious identities; their blogs are "realistic" depictions of their creators (Huffaker 2006:9). As such, blogs straddle the line between front and back areas, a situation that is critical to understanding the nature of self-disclosure on SNS.

The individual SNS profile is very much a front region in Goffman's terms, or at least an aspect of one – it is the calculated presentation of the self the creator wishes to express. But for teenagers as an aggregate population, SNS services are often treated as a back region - a place for teens to "hang out," ostensibly far from the prying eyes of parents, teachers, and other authority figures (boyd 2007). Teens' expectation of privacy on SNS is drawn from the site's perceived status as safe for self-disclosure, behind-the-scenes chatter, and displays of vulnerability amongst a team – the Friend network.[21] Some SNS openly tout this status; MySpace's slogan is "A place for friends." The relationship between individual profile and the larger social network is thus complicated; teenagers use their SNS profiles to generate identities that are peer-appropriate and intended exclusively for the peer network. In effect, the team and the audience are one and the same.

Adults and other unwanted guests are a form of what Goffman would term "outsiders," they are not performers, and they are not the intended audience (Goffman 1959:144). The presence of outsiders can severely derail a given performance, as the actors and audience must both scramble to maintain their assumed roles in the presence of unwelcome individuals who do not understand what they are witnessing. However, as these outsiders often have an interest in

[21]The same is presumably true of adult users.

the performance for a variety of reasons, they may set up observation. The nature of this observation can be thought of in terms of intrusiveness (i.e. how deep the observation goes) and obtrusiveness (i.e. how overt the observation happens to be). A parent who creates an SNS profile and attempts to Friend their child to monitor their activity would be intrusive and obtrusive, while a marketing firm data-mining user profiles for research purposes without notification would be intrusive, but not obtrusive. The "serial adder," a user who Friends as many people as possible regardless of any actual connection, but never leaves comments or otherwise interacts with the resultant massive Friend network, would be obtrusive but not intrusive. Much of the problem with adolescent identity risk on-line arises through teens' back region activity, intended only for their close peers, being observed by outsiders.

The SNS user's profile is a form of self-presentation; it serves as a stand-in for the creator in the particular digital world it inhabits (Booth 2008; Hinduja & Patchin 2008). SNS users have multiple ways of maintaining their desired identity; the sharing of pictures, both of the user and of their Friends, allows users to make implicit statements about themselves and their peer networks beyond mere physical appearance – a user who wishes to appear as popular will post pictures that show their social side, while an introvert might post more solitary images, and barring an (intentional and calculated!) display of cheekiness, users will post the most flattering pictures possible (Sessions 2009; Zhao et al. 2008).[22] By listing their interests and hobbies, users can present themselves in terms of their consumption habits, with many SNS profiles offering extensive lists of the owner's favorite musicians, books, television shows, and so forth (Zhao et

[22]The preponderance of SNS user self-portraits taken at a high exposure with the camera overhead and at arm's-length has earned such photos the waggish nickname "MySpace Angles." Such photos are considered to accentuate a female's breasts and facial features while obscuring the rest of the body, a practice that some male users consider highly deceptive (Sessions 2009).

al. 2008). This allows for self-presentation as part of a larger consumer culture; users who wish to identify with a particular "scene" can deliver an appropriate performance of taste, whether that taste runs towards "Gossip Girl" and pop music or towards NASCAR and country music. Finally, profile creators can directly describe themselves; most SNS profiles include an "About Me"-type category where users can provide as much or as little information as they see fit (Zhao et al. 2008). By posting various information to an SNS profile, a creator can develop and maintain a rather thorough self-presentation; photographs identify the creator and her or his role in various social networks, a list of taste preferences locate the creator within a culture/sub-culture, and self-disclosure statements allow the creator to have an ultimate say over how the entire presentation should be viewed. Each profile is a representation of the creator as he or she wants to be seen by an audience – not exactly the creator's real-world personality, but not quite the sort of limitless "true self" promised by more anonymous communication methods; instead, the online profile represents a "hoped-for possible self" (Turkle 1995; Yurchisin et al. 2005:737).

Profiles are carefully designed and targeted for specific sites – a professional profile on a job-search site, a romanticized profile on a dating site, a casual profile on a social network site, and so forth (Booth 2008; Schau & Gilly 2003; Yurchisin et al. 2005). Goffman calls this "audience segregation;" a form of situational control that allows a creator to know which role to perform at any given time – the process by which a performer "segregate(s) his audience(s) so that the individuals who witness him in one of his roles will not be the individuals who witness him in another of his roles" (Goffman 1959:137). The failure of Friendster, one of the earliest SNS, was blamed in part on audience segregation gone awry, as "users had to face their bosses and former classmates alongside their close friends" (boyd & Ellison 2007). Friendster was

nominally set up as a dating site, operating under a sort of "strength of weak ties" concept – users could add their real-life friends, and then could browse those friends' real-life friends and so forth, with the assumption that people who had friends in common likely had interests in common, and would be more romantically compatible than a total stranger. However, the sort of self-presentation an individual might use when seeking a romantic (or sexual) partner can often differ quite vastly from the self-presentation an individual might use around family, co-workers, or even close friends, and it was this failure of audience segregation that led to the site's eventual abandonment. As another example, consider the case of Melinda England, an elementary school teacher from Tennessee. England posted topless photographs of herself on one of her profiles; while England's breasts were covered, and the profile was only accessible to users 18 and over, well beyond the age of the students she worked with, the photos were reported to the school administration, causing an uproar that reached the national level (Nauert 2007; WVLT-TV 2008). In this case, England's attempt at audience segregation failed – the pictures were in a venue for making personal connections, and were intended to be seen by potential suitors, not by her employers or the parents of her students. This created a situation of disconnect, as the parents' impression of how a teacher should behave was at odds with the impressions put forth by England's photographs.

Perhaps because of the potential risks of failed audience segregation, most users present fairly mundane versions of themselves. For instance, Facebook profiles often include the creator's name, location, and likeness, and the Facebook user's audience consists of friends, classmates, relatives, and other acquaintances; there is no logical reason to present oneself in a way that is not socially acceptable when such a varied group of peers are privy to that display

(Westlake 2008). Indeed, Goffman (1959) claimed that public presentations often highlight the existing norms of a society, and most online presentations would then be similarly normative. Even a presentation that untrained observers might find shockingly deviant is likely normative for a given social network: the MySpace profile of Jacob Robida, the Massachusetts teenager who attacked several men in a Massachusetts gay bar with a hatchet, then shot and killed a police officer, a female companion, and himself during the ensuing manhunt, featured Neo-Nazi signifiers as well as potentially violent images, but also hosted more mundane information such as "What kind of kisser are you?" and "what type of car are you?" quizzes (Levenson 2006; Robida 2006). Aside from the Neo-Nazi material, much of the information on Robida's MySpace, while disturbing to the uninitiated, is par for the course amongst fans of the rap group Insane Clown Posse (who use the term "Juggalos" as a self-identifier); a cartoon figure wielding a meat cleaver is the logo of Insane Clown Posse's record label, while an ominous image of a bouncing axe with the caption "PASS THE AXE" encouraging readers to "get your hands bloody baby!" is a reference to song by a related artist, meant to be shared amongst fans as a statement of belonging to the Juggalo subculture (Dark Lotus 2004).[23] While Robida's MySpace certainly had problematic content, made all the more troubling by his eventual actions, virtually all of the non-Neo-Nazi material might be found on the profile of any other member of the Juggalo subculture or any other user with "dark" or "gothic" leanings. While the Juggalo signifiers might appear deviant to the eyes of society at large, they are simply a statement of in-group identification and as such, rather normative amongst that subculture. Here I see further support

[23]Shortly after the incidents discussed above, Insane Clown Posse's label released a statement assuring the media that Robida was "out of his mind" and "anyone that knows anything about Juggalos knows that in no way... would we ever approve of this type of bullshit behavior" (Boyd 2006a). These statements define an acceptable performance of Juggalo identity – strange, profane, and perhaps a little scary, but not murderous.

for Goffman's theory – even members of a deviant subculture will create performances that are normative within that subculture.

The Influence of Foucault

Westlake (2008) fuses the Goffmanesque focus on identity management with the Foucauldian concept of surveillance. In this context, SNS are a panoptic system – users are under constant observation, both by themselves in an identity management context as well as by the visitors to their profile who serve as an audience. Where SNS differ from traditional surveillance systems is in their performative aspect; users have many ways to control and mediate their presentation – profiles can be changed, compromising materials can be altered, access limited, and so forth. A certain degree of surveillance is expected, and perhaps even desired; why bother engaging in an identity performance if nobody is around to see it? The desire for surveillance implies a degree of resistance as well; while adolescents want to be seen and known based on the identities presented on SNS profiles, they also want to have control over how those same identities are managed and constructed. Livingstone mentions several such cases of resistance on SNS profiles – users who falsify profile data for comedic effect (a 13-year-old boy claiming to be "36, married, living in Africa") or who use pictures of their pets in lieu of an image of themselves (2008:399). While these acts are also potentially viable as forms of identity management (as discussed above), the humorous exaggeration of the false statements also suggests an intentional subversion of SNS performance expectations.

There is also a complicating element of Foucauldian self-monitoring in the process – the profile is a representation of the creator, but it is mitigated and influenced by a perceived "imagined audience" consisting of both real peer expectations and a desire to be seen by

unknown potential parties as "well-rounded, sociable and fun-loving" (boyd 2007:14; Zhao et al. 2008:1828). Any deviation from these panoptic peer expectations could potentially result in negative feedback via comments or the dreaded unFriending. In essence, while there is the potential for the SNS profile to be a transformative and fluid work, the processes of impression management and audience segregation mean the profile is not a completely honest assessment; the profile is altered to be socially acceptable, the creator intentionally limiting and constraining her or his identity in an attempt to appeal to the omnipresent peer network. What could be (and was proposed by early Internet scholarship *to* be) a radical and liberatory opportunity for writing the self into existence is more likely to be just another form of internalized social control.

The Developmental Psychological Approach

The other major social science perspective on adolescent Internet use approaches the topic from a developmental psychological framework. One of the primary goals of adolescent development is to experiment with different behaviors and different possibilities to discover (or create) a "true" personality that "is simultaneously autonomous and socially valued... that balances critical judgment and trust, inner unity and acceptance of societal expectations" (Erikson 1963; Nurmi 2004; Livingstone 2008:397). The Internet is one of many vectors for adolescent emotional and psychological development; by generating a virtual identity, adolescents also generate a real-world one as well. The "hoped-for possible self" discussed above is an actual potential future identity for the creator; it is literally the self the individual wishes to become as an adult. Teenagers can experiment with multiple potential identities in relative safety via the anonymity of the Internet, using online communities as sounding boards for their identity explorations (Valkenburg & Peter 2008). These online spaces not only allow

for experimentation with new individuals, they allow for intimacy between peers in a shared (and presumed safe) space, a different form of identity exploration (Livingstone 2008).

In addition to providing a solid rationale for why teenagers use CMC in a general sense (i.e., identity formation and exploration), the developmental psychological literature also offers some interesting perspectives as to why specific types of teenager are more or less likely to engage with the internet in a given way, particularly as relates to a teenager's feelings of social connectedness. The "rich-get-richer" (RGR) hypothesis suggests that adolescents who already have strong social skills and a dense network of off-line friends use the Internet to strengthen those existing friendships. For these users, the Internet is just one of many ways to stay in touch with peers, with SNS in particular allowing teens to maintain a large network of friends (Steinfield et al. 2008). The "social compensation" (SC) hypothesis suggests that teenagers who lack friends, especially those who are lonely or who have trouble communicating in person, turn to the Internet to make new friends. The aforementioned lack of physical cues might also make it easier for these adolescents to communicate online (Valkenburg & Peter 2007; Valkenburg & Peter 2008; van den Eijnden et al. 2008). These online friendships are, much like offline friendships, based primarily on some shared social status between peers, and while online relationships are sometimes perceived as weaker than offline ones, research suggests that they are not necessarily inferior, but simply different (Mesch & Talmud 2007).

The developmental psychological literature to date tends to support the RGR over SC model, however, I would argue that the two are not necessarily mutually exclusive. While one study found that usage of instant messaging software was inversely proportional to loneliness (van den Eijnden et al. 2008), this simply suggests that well-connected adolescents use IM as one

form of contact with their peers, whereas less-connected teens might turn to message boards, chat rooms, or other forms of online communication. Indeed, another study found that both hypotheses were supported; the rich-get-richer hypothesis was applicable to adolescents who primarily used the Internet to communicate with existing friends, while the social compensation hypothesis was applicable for those who explicitly used the Internet as a means of safe self-disclosure (Valkenburg & Peter 2007). Furthermore, "lonely" teenagers were more likely to use online communication to experiment with alternate identities (Valkenburg & Peter 2008; Valkenburg & Peter 2009). Offline, these lonely teens were less socially engaged and had fewer close friends than their non-lonely peers, but online communication presented new opportunities to experiment with identities and practice their social skills. This experimentation and exploration brought those teens into contact with a wide variety of people, which had a positive effect on their offline social competence – essentially, communicating with lots of different people online gave these teens the skills or the confidence needed to be more capable when communicating offline. Among a sample of college students, Facebook use was shown to have a positive effect on the level of "bridging" social capital, suggesting that SNS usage in general will lead to increased social connections for the user, even (or especially) if that user had a low level of connectedness beforehand (Steinfield et al. 2008). These connections will be relatively superficial, and could best be described as "weak ties," but users will put forth considerable effort in their care and maintenance, suggesting support for both the RGR and SC models. Some socially anxious adolescents avoid online communication altogether, suggesting the social compensation hypothesis is not completely supported, but even those teens are still interacting

with someone, somehow, online even if they are simply reading websites or playing single-player games.

The developmental psychological literature can be dovetailed nicely into both Foucault and Goffman; the performances teenagers carry out as presentations of a hoped-for possible self are also part of the process of psychological identity formation. Successful performances are validated by peers (and internally validated by the actor), kept, and added to the repertoire while performances that fail are rejected, modified and attempted again at a later date. Acceptable performances will fit within a culture's (or subculture's) normative expectations as the actor will often self-police, constraining her or his true desires to meet the expectations of the perceived audience. The tactics and targets of online experimentation may vary depending on the adolescent's off-line network strength; teenagers with strong friendship networks engage in performances which reflect and reify their position amongst their peers, while teens with weaker friendship networks engage in more expressive performances to improve their communication skills and perhaps generate alternative social networks. In both cases the "hoped-for possible self" that teens perform online is honed and refined, as the process of experimentation is part of the socialization into adulthood, as teens learn which roles and performances society will accept, and which ones society will reject. Identity risks arise when teens' perception of SNS as a private area for communication and exploration amongst peers is compromised by external actors who are not the intended audience for these performances.

Theoretical Model

This research examines the influence of teenagers' off-line social network strength on their on-line behaviors, most especially as relates to risk perception and identity vulnerability,

using a framework based on Goffman's concept of self-presentation and the developmental psychological literature on loneliness and Internet communication. Working from Goffman, teens' online profiles serve as a form of self-presentation, an idealized representation of who teens claim to be. Personal data is shared to reinforce this process of impression management. Furthermore, while individual teens use these profiles to engage with one another in a "front region" of calculated social action, teenagers as a group tend to view these venues as a "back region," limited in scope only to their peer network, i.e., other teenagers they know; parents, authority figures, and unknown strangers are outsiders and implicitly, if not explicitly, unwelcome. The developmental psychology literature suggests that teenagers' relative feelings of loneliness affect their online usage. Non-lonely teens use the Internet to interact with their friend networks and reinforce those relationships, while lonely teens use the internet to explore their own identities and perhaps to generate new social networks. Sociologically speaking, it would then make sense that teenagers' social networks would have a similar effect; well-connected teens might use the Internet to reinforce existing offline friendships, while less-connected teens might use the Internet to create new connections or relationships; the degree of anonymity provided by online communications as well as the relative ease of finding other users of similar social status makes it an ideal venue for exploratory contact (Mesch & Talmud 2007). I can then classify online social activity into two categories - "reinforcing" activities are exactly what the name implies; behaviors that reinforce existing friendships, while "exploratory" activities are those where the user is seeking new social connections.[24] From there, I can classify different online social activities by their function – reinforcement or exploration.

[24]Another type of Internet activity would be "information-seeking" - again, the name is self-explanatory; teens using the Internet for academic study or personal edification. While this may have a social aspect (e.g. a chat room

Given that much existing research suggests that the primary purpose of adolescent SNS and IM usage is reinforcing in nature, I would expect to see higher levels of SNS and/or IM usage amongst well-connected adolescents (Ellison et al. 2007; Livingstone 2008; Steinfield et al. 2008). Similarly, existing research suggests that adolescents who interact with strangers online are more likely to visit chat rooms, suggesting that these teens are potentially looking to make new social connections (Liau et al. 2005; Mitchell et al. 2008). As such, I would expect to see higher levels of chat usage amongst less-connected adolescents. I can also look at what I have broadly dubbed "content creation" usage, Internet activity forms in which the user creates original content to be shared with the Internet at large (as opposed to SNS, where the profile content is intended to stay within the confines of the SNS site and the creator's chosen Friends). These forms would include blogging, non-SNS website creation, uploading of photos and videos to non-SNS sites, and other forms of sharing something the adolescent has created with the Internet at large.[25] By creating websites, videos, and blogs, less-connected youth can extend their exploratory activity – posting content dedicated to a topic is an attempt to contact other people who share the creator's interest, regardless of the actual topic (Papacharissi 2002; Schau & Gilly 2003). Given that these forms of communication are inherently expressive, and their usage often serves to focus on one specific aspect of an individual's personality or interests, I believe that content creation will be more common amongst less-connected adolescents.

In either case, reinforcing and content creation usage has a great deal of potential for identity vulnerability risks. SNS ask users to share their personal data as part of the membership process. Chat room users may use personal data as a way to "break the ice" in conversation,

---

about health concerns), the primary goal of this activity is research.

[25]This would not include the sharing/downloading of commercial music/films/software/etc., as the materials being transferred in those cases are not the original creations of the adolescent.

while blogs and personal websites might share vulnerable information as a way of displaying individuality and the creator's identity. In any case, malefactors could gain access to personally identifying information, whether it is freely given, or obtained through social engineering methods like phishing. Seemigly innocuous information can become deeply damaging in the wrong hands.

Working from the assumption that the strength of a teen's social network has an effect on how she or he communicates online, it is possible that how a teenager moderates their identity vulnerability is also influenced by their reasons for using the Internet. Combining the varied perspectives on adolescent self-presentation on the Internet gives us a general explanation for potentially risky behaviors: teenagers' profiles are self-presentation testing grounds – they present themselves as they want to be seen by their peers, with a careful eye for detail. The photographs must be as flattering as possible, the data given out must be appropriate, and the entire goal of the enterprise is to provide a sort of "highlight reel" of who the creator is; an idealized representation targeted for consumption by his or her peers. Well-connected teens can use the profile to reinforce existing friendship connections, while less-connected teens can use their profile to explore their own identity and search for like-minded peers. This profile is a performance of the hoped-for possible self; any falsification is done for the sake of creating a more acceptable image, not out of an attempt to maliciously deceive. The system is panoptic as well – the teens create their profiles for others to see, and spend countless hours updating, modifying, and playing with their own profiles, as well as those of their Friends – the profile is a relatively fluid performance that can be changed with ease, a text that can be written and rewritten as the creator's identity shifts. The primary limitation on a user's performance are the

expectations of their peers, whether represented externally via deFriending, negative comments, or other 'drama' or internally through the creator's own self-policing as part of the process of audience segregation. The entire process helps the creator further refine their own self-image, both by choosing aspects of their own lives to display or conceal as well as by allowing others to modify those presentations in order to represent or reify their own relationship to the creator. Unflattering photos, damaging information and the like can quickly be excised and the profile can be altered into something more appealing to the target audience. The process of identity creation and impression management becomes both an individual gesture and a collaborative action.

These performances, while seemingly transgressive to adult audiences, are generally normative within the parameters of youth culture. Teens' desires to present themselves in a manner acceptable to their peers leads to potentially compromising situations at least partially because teenagers view SNS as a secure venue for identity experimentation, with an expectation of privacy comparable to traditional communication methods. In other worlds, teens are not acting in malevolence or ignorance, but plain old peer pressure; simply put, everybody else *is* doing it. However, these sites are often far from secure; even via the Friending process, the ability to delineate clear levels of access is still complicated at best. Identity risks arise from unwanted individuals' obtaining data that was meant to be shared with a specific group, of which the outsider is not a member. When this content spreads beyond its intended audience, the consequences can be emotionally, socially, or even physically damaging to the creator, as discussed earlier.

That being said, teenagers do actively attempt to control and manage the amount of identifiable material they release on-line. The sharing of data is an important part of the self-presentation process, as this personal information serves to verify the user's identity – posting a photograph, real name, address, etc. allows a user to back up their claims about who they really are off-line. For reinforcing users, personal information is an immediate and effective form of verification – your offline friends can find you online by searching for your name. Photos of yourself and your friends then further confirm that you are indeed who you say you are, and that the relationships you claim with other users are in fact real (Livingstone 2008). Vulnerable data is posted to show inclusion in a peer group, as a way of proving that the poster belongs in that particular realm. Conversely, for exploratory users, personally identifying data serves as a form of self-disclosure amongst peers, a show of trust. By sharing your name and photo with a relative stranger online, you reaffirm and strengthen your connection, and give added weight and credence to your statements.

In either case, a teen's degree of social connection should influence their level of identity vulnerability; well-connected teens should theoretically post more information than their less-connected peers, as maximizing the amount of data available makes it easier for offline peers to confirm their identities. Less-connected teens might share less personal data, as that knowledge is reserved for those who have earned their confidence or trust; they let their online profiles speak for them otherwise.

It is also possible that the communication methods themselves play an influence in the degree of self-mediation – SNS profiles are practically expected to have a name, photograph, and location, for instance, while chat or message boards can remain relatively anonymous. Even

within the different SNS communities, there are varied expectations of self-disclosure, as discussed above. Another factor to consider when discussing self-mediation would be risk perception – teens who perceive the Internet as more dangerous or hazardous than their peers will likely have higher levels of self-mediation. The effect of self-mediation on identity vulnerability seems obvious; teens with higher levels of self-mediation will have lower levels of identity vulnerability, and vice versa. The final factor to consider when discussing teens' identity vulnerability is the influence of parental mediation factors – while parental mediation seems to have a relatively limited effect on teens' online behaviors, it must be included in any model, if nothing else, for the sake of thoroughness.[26] In this model, parental mediation is introduced as an separate intervening variable, roughly contemporary with self-mediation. By placing parental mediation at the same stage in the model as self-mediation, I can test the relative effectiveness of one against the other.

FIGURE ONE: Theoretical Model

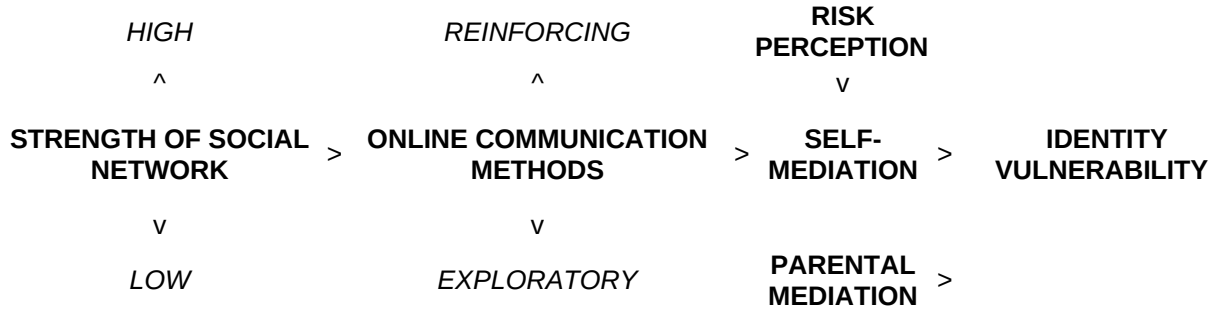


Figure One is a visual representation of my theoretical model: Teenagers' relative levels of network strength will directly affect their choice of on-line communication methods. Teens with high levels of network strength will primarily use SNS or instant messaging, methods that

[26]While the influence of parents' perception of the Internet as a risk-filled environment would be interesting to use as an independent variable for parental mediation, the lack of variables testing parental risk perception in the data set precludes such an investigation.

reflect their desire to reinforce existing social networks. Conversely, teens with low levels of network strength will tend to utilize content creation-based methods in order to expand their social networks further. This is not to say that there will be no overlap – isolated teens use SNS as well, and there is no reason that highly connected teens could not engage in content creation. The choice of online communication methods also influences to some degree how teens mediate their behavior online, as different methods call for or allow differing levels of identity disclosure (Livingstone 2008). Various forms of CMC have different normative expectations of identity disclosure; SNS generally want at least a first name, photograph and location, while chat rooms and message boards can be completely anonymous outside of the user's IP address. These expectations would logically influence a given user's level of self-mediation. Behavior mediation is also affected by teens' perceptions of the Internet as a potentially risky environment. This self-mediation has a direct effect on teens' level of identity vulnerability, which is also affected by the parents' attempts at mediating teens' Internet usage. This model potentially explains many of the questions raised in Chapter 1. In the next chapter, I will apply the Pew Internet and American Life Project data set to my model.

CHAPTER 3 - Data, Measurements and Hypotheses

The overall question of my research is deceptively simple: why do teens engage in risky identity displays online? Actually getting an answer, however, is a much more complicated task. Chapter 1 dissected the problem, looking at the ways teenagers use the Internet and the potential for risk. While teenagers may not see any problems with posting compromising information on the Internet, seemingly harmless information can become quite dangerous when in the wrong hands. In Chapter 2, I constructed a theoretical model of teenage Internet use, risk management, and identity vulnerability. These risky behaviors are part of a process of self-presentation and identity formation, and the ways teens present themselves are strongly connected to the ways they want to be seen by their peers, whether online or off. By measuring teenagers' offline social network strength, I can determine if there is any effect on their online activities, and from there, their dealings with risk on the Internet.

Data Set

In this chapter, I plan to create a testable version of the theoretical model, using data from the Parents and Teens 2006 Survey carried out by the Pew Internet & American Life Project. The dataset consists of interviews with 935 12-17 year olds living in the continental United States, as well as a parent of each teen. Interviews were done in English by Princeton Data Source, LLC between October 23 and November 19, 2006 (Pew Internet and American Life Project 2006). The sample was designed to represent teens living in the continental U.S. in households with telephones. The sample is also designed to be representative of parents living with teenaged children. The margin of sampling error for the complete data set is ±3.7% (Pew

Internet and American Life Project 2006:25). This means that in 95 out of any 100 samples drawn using methodology identical to PIAL's, proportions estimated from such a sample will be no more than 3.7 percentage points away from the true value in the population. As an example, 93% of the teenagers in the sample said they used the Internet (Pew Internet and American Life Project 2006:6). If this study was replicated 100 times using the same sampling methods, in 95 out of the 100 samples the percentage of teens who report using the Internet would be between 89.3% and 96.7% of the samples in question.

The PIAL sample was obtained using random digit dialing (RDD). There are known liabilities when using RDD, from both a sampling and a response perspective. The most obvious sampling concern is non-representation; households without telephones are by default not going to be sampled. Current estimates suggest that about 2% of U.S. households have no telephone service whatsoever (Blumberg & Luke 2009:3). Cell phones provide another series of problems: approximately 20% of U.S. households have no landline and use a cell phone as their only method of telephone service (Blumberg & Luke 2009:2). Sixty percent of households consisting of adults living with unrelated roommates were wireless-only, as well as 39% of adults renting their homes, 41% of adults between 25-29, and 30% of adults living in poverty (Blumberg & Luke 2009:3). These individuals may be missed in RDD research, as federal law prohibits the use of automatic dialing systems when calling cell phones, so any survey including cell phone users must be dialed by hand, a much more time consuming process (Pew Research Center for People & the Press 2006). Furthermore, some cell phone numbers may have been ported over from an existing land-line, and would appear in a block of phone numbers assumed to consist solely of land-lines, creating further problems (Battaglia et al. 2005; Kulp 2004). As such, many

RDD designs limit their sample to households with land-lines, treating cell phones as invalid (Battaglia et al. 2005). Even when households with cell phones are sampled, households with more than one voice line (such as for a teenager or a home office) have a higher chance of being sampled than those with a single line, which could result in a skewing of the sample (Merkle & Langer 2008). As of December 2008, 59.6% of U.S. households have both landlines and wireless telephones, which creates serious concerns for sampling bias (Blumberg & Luke 2009:5).

The sampling frame for this data set was drawn from previous Pew projects in 2004, 2005, and 2006; households that reported having children under 18 in previous studies were called back and screened for 12-17 year olds. The original sampling frame was obtained from Survey Sampling International and gathered according to Princeton Survey Research Associates International specification (Pew Internet and American Life Project 2006). In this case, the PIAL sample used physical dialers, and as such includes households with cell phones. While this does create problems with multi-line households having a higher likelihood of being sampled, as discussed above, it also avoids the problem of entirely missing wireless-only households. As many as ten attempts were made to contact each sampled telephone number. Calls were staggered through various times of day and days of the week to maximize the potential of making contact. Each number received at least one daytime call. Respondents were first screened to determine if a 12-17 year old lived in the household. Households without children were marked as ineligible. In eligible households, interviewers first spoke with a parent or guardian, then interviewed the target child. In households with more than one child, the child

was chosen at random. The response rate is 46% according to American Association for Public Opinion Research standards (PIAL 2006:25).[27]

To control for nonresponse bias, PIAL used sample balancing, also commonly known as raking, to weight the data set. Sample balancing is commonly used when working with telephone surveys, as it is a generally accepted means of dealing with nonresponse bias (Battaglia et al. 2004a). In the sample balancing process, known parameters of the population are used as controls and the sample is repeatedly weighted until the sample's parameters match those of the population, which is known as convergence (Battaglia et al. 2004b). In most cases, socioeconomic and demographic data are used as the population control standards, with the goal being that the demographic makeup of the weighted sample should closely approximate that of the target population (Battaglia et al. 2004b). One known issue with sample balancing comes about when two closely correlated variables are used as controls, for instance, eligibility for food stamps and poverty status (Battaglia et al. 2004b). In such cases, convergence may never be reached as the weighting process simply continues ad infinitum (Montaquila et al. 2003). Given that the PIAL data set weighted parents on sex, age, education, race, Hispanic origin, marital status and U.S. Census region, while children were weighted on gender and age, this was not an issue. The control parameters came from 2005 U.S. Census Bureau data covering all continental U.S. households with a telephone.[28] A complete list of the sample demographics, their weighted versions, and the population control totals is available in Appendix A.

---

[27]While there has been a significant decrease in response rates for RDD phone surveys over the last fifteen years, research suggests that RDD data is still generally representative of the population, and that studies with response rates around 30 percent are functionally similar to studies with response rates around 60 percent (Fowler 2009). Previous Pew surveys have had response rates as low as 22 percent (Keeter, et al. 2006).

[28]The exclusion of non-telephone households from the population is obviously problematic, for reasons discussed above.

Perhaps the biggest difficulty when using a pre-existing data set is they are gathered to answer a particular set of questions, which may not necessarily be the same questions the secondary analyst is interested in (Friedman 2007). Even if a survey is nationally representative, properly designed, and rigorously coded, survey items still may not precisely measure the concepts a secondary analyst has in mind, and an existing data set rarely covers all the variables a researcher is interested in (Kiecolt & Nathan 1985:13). Another issue is the quality of the data set itself; while PIAL extensively documents its recruitment process, interview method, response rate and margins of error, other existing data sets are sometimes not as thorough in their descriptions, leading researchers to put too much faith into their data (Sales et al. 2006).

Analysis of existing data has its advantages as well. One admittedly crass but nonetheless valid rationale for using existing data is the very low cost and effort involved in gathering the data, making it ideal for testing new hypotheses or alternate methods of analysis (National Institute of Health 2003; Sales et al. 2006). An exploratory analysis such as this one is better served by initially using existing data to quickly test a theoretical model, rather than going to the time and effort of generating a completely new research instrument, gathering an equally representative sample, carrying out the data gathering process, and so forth. For an individual researcher working on a limited budget, producing a data set with the depth, breadth, and representative value of the PIAL data is highly unlikely (Kiecolt & Nathan 1985; Sales et al. 2006). Future applications of this research could certainly move forward with the testing and development of specialized scales and the like, but for now budget and time considerations preclude such advanced design work. Indeed, given the rapid pace of development in CMC, by the time a more carefully-targeted instrument was ready for implementation, the population of

interest may well have already moved on to whatever the next communicative method happens to be. Another advantage is the potential for future research; the 2006 Parents and Teens data set is a modification and replication of a survey carried out in both 2004 and 2000. If PIAL were to replicate the study again in the future, it would be quite easy to modify this research for a longitudinal analysis of teens' online behaviors.

Applied Model

Connecting the theoretical model from Chapter 2 with the PIAL data set requires some element of finesse in the measurements used. As discussed above, an existing data set will rarely cover all the topics a researcher has in mind. However, with some creative application of theory and the use of specific analytical techniques, the variables in the PIAL data approximate the model. Measuring a degree of parental mediation is rather straightforward – count up the different ways a parent attempts to mediate a child's online experience, and the higher the score, the greater the degree of mediation; much the same is true of "identity vulnerability." However, several of the variables in the theoretical model, such as "risk perception" and "reasons for using the Internet" are quite abstract. Risk perception, in and of itself, is an unobservable construct – it does not "exist" per se in the real world in the way that "parental mediation" or "online communication methods" does. Constructs of this type are referred to as latent variables in the literature, and the process of analyzing one requires determining a statistical relationship between a set of observable variables that are taken to represent the presence or the influence of the latent variable (Borsboom, et al. 2003).

A latent variable is an unseen (and unmeasurable) force manipulating a set of observed variables; the problem is to find the appropriate observed variables to deduce the presence and

strength of the latent variable. As an analogy, consider an individual who dresses as a "ghost" by covering herself with a bedsheet. While the "ghost" is free to roam, it is not the bedsheet that is truly ambulatory – the person underneath is doing the work. As the bedsheet covers the wearer's body, certain points where the body and the sheet make contact can be observed and measured – the top of the head, the ends of the fingers, the tip of the nose, and so forth. By appropriately analyzing these points, I can then deduce who is under the bedsheet.

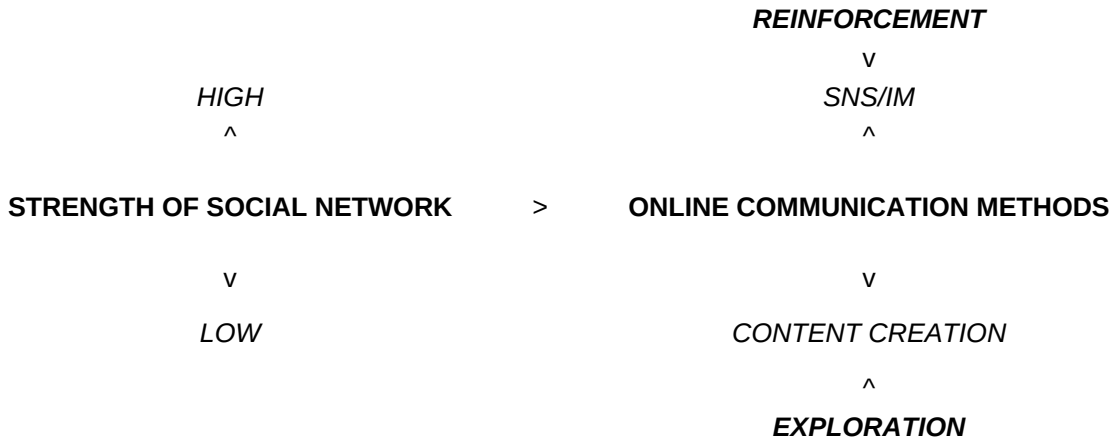
The process of analyzing these latent variables is a bit more complex than throwing a sheet over the data and poking away. Measurable variables from the data set will be chosen as indicators based on their use in prior research on the topic and theoretical assumptions about their validity to generate *reflexive models* for the latent variables. Reflexive models suppose the indicators are independent beyond the influence of the latent variable (Borsboom, et. al 2002; Edwards & Bagozzi 2000). When I choose measurable variables to serve as indicators, I am making assumptions about the nature of my latent variable. To stretch the "ghost" metaphor a bit further; I am measuring my bed sheet under the presumption that it is a person in disguise while it could in fact be a robot, a stack of highly acrobatic hamsters, or an actual supernatural entity.

As discussed above, using a pre-existing data set has its limitations, and a primary flaw of this set is that the questions pertaining to identity vulnerability were only asked of adolescents who have SNS profiles, excluding non-participatory teens. As such, it is necessary to cut the applied model into two pieces, one focusing on offline network strength and its effects on online activities, using the sample of all teen Internet users; while the second focuses on risk perception, mediation, and identity vulnerability among teens with SNS profiles. Both models still test the theoretical model, while working within the limitations created by the data set. The result is a

shift in scope, first looking at a broader population of all online teens, then narrowing my focus to the realm of SNS and its users.

The first model is shown in Figure Two. A sociological adaptation of the developmental psychological literature would suggest that teenagers who have strong off-line social networks will tend to use the Internet to reinforce said networks. Conversely, teenagers with limited off-line social networks will largely use the Internet for exploratory purposes, whether to experiment with their own identity or to generate on-line social networks based on some shared interest.

FIGURE TWO: Influence of Social Network



H1a: Respondents who are highly connected to off-line social networks will have a greater likelihood of using reinforcing communications methods.

H1b: Respondents who are weakly connected to off-line social networks will have a greater likelihood of using exploratory communications methods.

Theoretically, the choice of on-line communications methods has an influence on a user's level of self-mediation. Here I strike a roadblock – the questions in the PIAL data set regarding self-mediation were only asked of teenagers with SNS profiles. As such, my model testing the

effects of risk perception and mediation on identity vulnerability must be limited to those respondents. Reinforcing methods seem to require a sharing of personal data as a form of identity verification, with SNS users expected to provide a variety of information simply to have a normative performance.

Figure Three depicts my second model. Identity vulnerability itself is a direct result of a teenager's attempts at self-mediation. Teens who maintain a careful control over their online presence will presumably have lower levels of identity vulnerability than their peers. It is logical to assume that teenagers who view the Internet as a risky environment are most likely to self-mediate, as they likely feel they are in more danger than their less-worried peers. Furthermore, attempts at mediating the online experience by parents may also have some effect on identity vulnerability.

FIGURE THREE: Risk Perception, Mediation, Vulnerability

H2: Respondents who perceive the Internet with high levels of potential risk will have a higher level of self-mediation.

H3a: Respondents who report a high level of self-mediation will have a low level of identity vulnerability.

H3b: Respondents who report a high level of parental mediation will have a low level of identity vulnerability.

H3c: Self-mediation will have a stronger effect on respondents' degree of identity vulnerability than parental mediation.

Once the models are run on the data, I expect to see the following results: respondents with high social network strength will tend towards reinforcing online methods such as SNS and IM, while respondents with lower network strength will tend towards exploratory methods like blogging, website creation, and so forth. Risk perception will have a positive, but minor influence on self-mediation. Finally, both self-mediation and parental mediation will have a negative influence on identity vulnerability, but self-mediation will have the stronger influence of the two. In my theoretical model, the connection between choice of online communication method and self-mediation is more strongly articulated. If both models produce promising results, it would be possible to retest with only the SNS-using respondents.

Measurements

Given the use of a preexisting data set and the inherent suppositions required as part of the process, there will be an element of finesse involved in the identification of latent variables in this research; however, given the exploratory nature of the study and the theoretical strength of the model itself, I feel the indicators chosen are those which will provide the best possible fit. Where applicable, I plan to engage in exploratory factor analysis to refine my latent variables. The variables I am looking at, and the survey questions I intend to use as indicators are as follows:

Strength of Social Network: Table One displays the two sets of questions that potentially offer insight into the respondents' social networks. The first series serve to measure the respondent's participation in organized activities, which would expose the participant to a large

network of potential off-line friends. The second series attempts to more directly measure off-line peer-to-peer contact, focusing on the respondents' frequency of social interaction, whether in person or over the phone. Neither series actively attempts to count the number of friends a respondent has, or the relative feelings of closeness between friends, but I would argue that a combination of exposure to many people via participation in group activities and frequent contact with peers in a variety of methods would suggest a strong social network. In this case, higher frequencies of time spent with friends and positive acknowledgements of social activities participated in would indicate a higher degree of offline social network strength.

Online Communication Methods: Multiple sets of questions in the PIAL data address the sorts of activities teenagers engage in online. For my model, I plan to use a mix of questions that concern communication methods and content creation methods, as seen in Table Two. These questions cover SNS and IM, the two methods most commonly identified as being used for reinforcement, as well as content creation methods, which I believe will be more popular amongst exploratory users. In addition, I included questions about chat rooms and gaming, largely for exploratory purposes. I discarded questions related to information seeking and content consumption, preferring to focus strictly on forms of communication. In this case, these questions serve a dual purpose – they are measurements in and of themselves of the sorts of activities teens engage in online, as well as acting as manifest indicators for the latent variable "Reasons for Internet Use." Effectively, by identifying specific methods as exploratory or reinforcing, I can then extrapolate that teens who participate in those methods do so for exploratory or reinforcing reasons.

Risk Perception: Table Three covers questions which address teens' perception of the Internet as a risky environment. The first question is limited only to those teens with SNS profiles, and regards their perceived risk of discovery via information on their profile, while the other two questions are more general and concern non-identity related risks. However, it would follow that teens who identify any part of the Internet as a greater potential risk than the real world would likely identify other parts of the Internet as risky. In this case, "risk perception" would be a latent variable with the identified questions serving as indicators.

Self-Mediation: The questions in Table Four measure some degree of adolescent users' attempts at self-mediation. These questions were only asked of respondents who reported having SNS profiles, creating an obvious limitation – I am in the dark, so to speak, as pertains to self-mediation amongst other users. Regardless, users who report controlling access to their profiles or creations would be considered to have higher levels of self-mediation than respondents who did not limit access.

Parental Mediation: The PIAL data set asked both teenagers and parents to discussion the level of parental mediation in the respondent's household. Research suggests that teens' awareness of parental mediation is a more significant predictor of effectiveness than parental statements about mediation (Liau et al. 2005; Livingstone & Helsper 2008; Wang et al. 2005). As such, I primarily use questions asked of the child, supplemented by some questions asked by the parent, as shown in Table Five. All of the questions discuss in some fashion parental rules about computer use, whether explicitly stated orders not to do something, the use of software barriers, or the more indirect issue of computer location. As such, all of these questions are considered to address restrictive forms of parental mediation. This is a limitation of the data; as

there is a lack of questions concerning parents' use of active or evaluative forms of mediation. Regardless, the higher the number of positive responses regarding mediation techniques, the higher the level of perceived parental mediation. For the question on computer location, having the home computer in an open family area is considered a positive response.

Identity Vulnerability: Finally, the data set contains a series of questions concerning the types of information teenagers post to their social network profiles, as listed in Table Six. These questions were only asked of teens who have SNS profiles, limiting their effectiveness when discussing all online teens. The questions include such common information as a personal photograph and first and last name, as well as more inherently problematic data such as home address and phone number. As discussed earlier, while much of this information is normative in SNS culture, any or all of these pieces of data can potentially be risky when accessed by unwanted viewers. The higher the number of "yes" responses, the higher the respondent's level of identity vulnerability.

Implications

The implications of my research are theoretically striking; if there is a connection between offline network strength and online communication, this will give Internet youth safety advocates a clearer picture of the potential risks at hand. For example, attempts at building safety awareness could be specifically targeted by communication method, based on the relative network strength of the average user. Determining the influence of teenagers' perception of the Internet as a risky venue on their attempts to control their behavior is a similarly promising proposal, and confirmation that teens' self-mediation methods are more effective than parental mediation techniques could encourage parents to find new, more effective ways to mediate their

teens' online experiences, while further awareness of how, why, and when teens self-mediate could encourage concerted attempts to strengthen those self-mediation processes, encouraging a stronger control on potentially damaging information.

Conversely, a rejection of any or all of my hypotheses is still valuable information: if all on-line teens use the same communications methods, regardless of social network strength, then that would challenge much of the existing literature and potentially present new questions about how and why teens use the internet to communicate. Furthermore, if parental mediation methods are more effective than teens' self-mediation, or if neither method was particularly effective, it would still suggest a need to reinforce both teens' and parents attempts at creating safe spaces on the Internet – that improved mediation methods are even more necessary than initially believed.

TABLE 1. Strength of Social Network

"Do you currently participate in any of the following..."
(YES/ NO/ DON'T KNOW-REFUSED)
"A school club like a drama or language club?"
"A school sports program?"
"Some other extracurricular activity, like band?"
"A club or sports program that is NOT affiliated with your school, like a church youth group,rec league or volunteer organization in your community?"

"Thinking about all the different ways you socialize or communicate with friends..."
(EVERYDAY/ SEVERAL TIMES A WEEK/ AT LEAST ONCE A WEEK/ LESS THAN ONCE A WEEK/ NEVER/ DON'T KNOW-REFUSED)
"Spend time with friends IN PERSON, doing social activities outside of school?"
"Talk to friends on a landline or home telephone?"
"Send text messages to each other?"

TABLE 2. Online Communication Methods

Reinforcing Methods

"We're interested in the kinds of things you do when you use the Internet. Not everyone has done these things. Please just tell me whether you ever do each one, or not..."
(YES, DO THIS/ NO, DO NOT/ DON'T KNOW-REFUSED)
"Send or receive 'instant messages'?"
"Use an online social networking site like MySpace or Facebook?"

Exploratory Methods

"I'm going to read another short list of activities people sometimes do online. Please tell me whether you ever do each one, or not..."
(YES/ NO/ DON'T KNOW-REFUSED)
"Create or work on your own online journal or blog?"
"Create or work on your own webpage?"
"Create or work on webpages for others, including friends, groups you belong to, or for school assignments?"
"Share something online that you created yourself, such as your own artwork, photos, stories or videos?"
"Take material that you find online – like songs, text or images – and remix it into your own artistic creation?"

"Have you ever uploaded photos online where others can see them?"
(YES/ NO/ DON'T KNOW-REFUSED)

"Have you ever uploaded a video file online where others can watch it?"
(YES/ NO/ DON'T KNOW-REFUSED)

Miscellaneous Methods

"Do you ever visit an online chat room?"
(YES/ NO/ DON'T KNOW-REFUSED)

"Do you ever play games online?"
(YES/ NO/ DON'T KNOW-REFUSED)

TABLE 3. Risk Perception

"How easy do you think it would be for someone to find out who you are from your profile? Do you think..."

(It would be pretty easy/ They would have to work at it but they could figure it out eventually

It would be very difficult for someone to find out who you are/ Don't know-Refused)

"Where do you, personally, think someone your age is more likely to be bullied or harassed? Do you think that's more likely to happen ONLINE, or more likely to happen OFFLINE, in your daily life?"

(Happens more ONLINE/ Happens more often OFFLINE/ Both equally/ Don't know-Refused)

"Where do you, personally, think someone your age is more likely to be approached by someone who is a complete stranger to them? Do you think that's more likely to happen ONLINE, or more likely to happen OFFLINE, in your daily life?"

TABLE 4. Self-Mediation

"Is your profile currently visible?"

(YES/ NO/ DON'T KNOW-REFUSED)

"Is your profile visible to anyone, or visible only to your friends?"

(VISIBLE TO ANYONE/ VISIBLE ONLY TO FRIENDS/ DON'T KNOW-REFUSED)

"Some people don't like to use real information in their profile so they use fake information instead... How much of the information in your profile is fake – all, most, some, very little, or is none of the information in your profile fake?"

(ALL/ MOST/ SOME/ VERY LITTLE/ NONE)

TABLE 5. Parental Mediation

In your household, do you happen to have rules about any of the following things? Do you have any rules about..."
(YES/ NO/ DOESN'T APPLY/ DON'T KNOW-REFUSED)
"Internet sites your child can or cannot visit?"
"The kinds of personal information your child can share with people they talk to on the Internet?"
"How much time your child can spend online?"

"Is the computer you use at home in a private area like your own, bedroom, or in an open family area, like a living room, den, or study?"
(PRIVATE AREA/ OPEN FAMILY AREA/ LAPTOP/ DON'T KNOW-REFUSED)

After you go online, do your parents ever check to see what web sites you went to, or don't they ever do that?"
(YES/ NO/ DOESN'T APPLY/ DON'T KNOW/ REFUSED)

"As far as you know, does the computer you use at home have a filter that keeps people from going to some types of Internet web sites, or does it not have this?"
(YES, HAS FILTERING SOFTWARE/ NO, DOES NOT/ RESTRICTED OR FILTERED ACCOUNT/ NO HOME COMPUTER/ DON'T KNOW/ REFUSED)

"And does the computer you use at home have monitoring software that records what a person does online, or does it not have this?"
(YES, HAS MONITORING SOFTWARE/ NO, DOES NOT/ NO HOME COMPUTER/ DON'T KNOW/ REFUSED)

TABLE 6. Identity Vulnerability

"We'd like to know if the following kinds of information are posted to your profile, or not. You can just tell me yes or no. If something doesn't apply to you just say so and I'll move on to the next item."

(YES/ NO/ DOESN'T APPLY/ DON'T KNOW-REFUSED)

"A photo of yourself."
"Photos of your friends."
"Your first name."
"Your last name."
"Your school name."
"Your cell phone number."
"Your IM screen name."
"Your email address."
"Your blog or a link to your blog."
"The city or town where you live."

CHAPTER 4 – Popularity Model

Thus far I have discussed the theoretical and practical implications of studying teenagers' online activity using a data set collected by the Pew Internet and American Life Project (PIAL). In this chapter I will actually apply the data to the model outlined in Chapter 3. First, a refresher: the overall model is broken into two segments. One, which will be covered below, tests the influence of respondents' offline social networks on their online communication methods. The second, which is the focus of Chapter 5, investigates the relationship between respondents' perception of the Internet as a risky environment with their attempts at self mediation, as well as any attempts at parental mediation and personally identifying material being posted to a SNS profile. Again, remember that I am working with two different models, due to the PIAL data set only asking respondents about IV sharing behavior on SNS, as opposed to across multiple forms of CMC.

In this chapter, I have two hypotheses (as depicted in Figure Two in Chapter 3). First, hypothesis 1a, which suggests that respondents who are highly connected to offline social networks will have a greater likelihood of using reinforcing communications methods. Second, hypothesis 1b, which suggests that respondents who have weak or limited connections to offline social networks will have a greater likelihood of using exploratory communications methods.

Method

Sample

Using the PIAL data set of 935 teens, I cut the sample down to 735 respondents who self-identified as using the Internet from home.[29] Respondents were between the ages of 12-17 (M = 14.82, SD = 1.685), 49.0% male and 51.0% female. The teens were not directly asked about their racial or ethnic identity, however, 87.2% of respondents' parents identified as white and non-Hispanic, 5.5% identified as Black and non-Hispanic, 4.1% identified as Hispanic, and 2.9% identified as some other racial group. Geographically, 21.5% of respondents lived in the Northeastern U.S., 28.3% lived in the Midwest, 30.2% lived in the South, and 20.0% lived in the West. 53.9% of respondents lived in suburban areas, while 21.9% were rural and 24.2% were urban.

Dependent Variable

Communication Methods: I selected eleven variables to represent various online communication methods. A principal components analysis loaded the items onto three factors roughly comparable to my proposed reinforcing/exploratory breakdown: the use of instant messaging and SNS loaded together on a factor, along with uploading photographs where others can see (which is logical, as photographs of the self and Friends are an important part of the SNS experience). These variables all reflect a "reinforcing" use of the internet. The creation of a personal webpage, a webpage for others, sharing something the user created and remixing something found online all loaded together, reflecting a "exploratory" paradigm. Online gaming

[29]Excluding users without home Internet access becomes relevant in the next chapter, in which parental regulation of home Internet access is a significant part of the model.

and the use of chat rooms loaded onto a third factor. This result was striking, but perhaps unsurprising; the way PIAL defined online gaming encompasses everything from highly-competitive action games like *Call of Duty 4* and *Team Fortress 2* to casual cooperative games like *Farmville* and *NeoPets*, as well as single-player games that feature no interaction whatsoever outside of a "top scores" list. It also includes dedicated gaming consoles such as the X-Box 360 and Playstation 3 alongside traditional computer games. Similarly, chat room functionality is available through multiple vectors; instant messaging services offer chat functionality, chat rooms can be implemented into personal websites, and many online gaming services offer chat as well. Uploading videos and blogging did not load, perhaps because at the time the PIAL data was collected, the most popular video sharing sites were in their embryonic stages, and the concept of uploading videos was still relatively novel. As for blogging, it can be implemented into both reinforcing and exploratory practices; many SNS offer some blogging capabilities, for instance. Regardless, this allows me to create a more nuanced model, specifically testing reinforcing vs. exploratory usage.

Dropping gaming, blogging, uploading videos, and chat gives me two solid latent variables reflecting exploratory and reinforcing methods. Given these results, I created two count variables and ran two separate regression analyses, testing my seven measurements of network strength against each activity variable. The "reinforcing behaviors" scale has three indicators; use of instant messaging programs, use of social network sites, and the uploading of photographs where others can see. This variable then ranges from 0 (none of these activities) to 3 (all of these activities). The "exploratory behaviors" scale has four indicators; creation of a personal webpage, creation of a webpage for others, sharing something created online, and

remixing something found online. This scale ranges from 0 (none of these activities) to 4 (all of these activities). Details of both scales are in Table Seven.

Independent Variables

Offline Network Strength: I initially selected six variables to serve as indicators of offline network strength. Four of these variables were yes/no questions regarding participation in various activities; school clubs, school sports, other school activities, and non-school activities. Two were scaled measurements of time spent engaging in specific forms of communication: talking to friends in person outside of school and talking to friends on a landline telephone. A factor analysis showed that the six variables loaded onto three factors. Individually, none of these factors had an acceptable alpha score to be used as scales (and a scale consisting of only two indicators is hardly worth considering in the first place). As such, I decided to use all six variables in the model independently of each other. While this may not be as theoretically satisfying as a single scale, data limitations are what they are. Furthermore, testing many different measurements of "offline network strength" gives me a chance to check different patterns of behavior against each other. Each one represents an alternate concept of "popularity" as well; students who participate in school clubs likely have different social networks than students who participate in school sports (eg. "jocks" versus "preps" or what-have-you), and theoretically any student with a social network would use the telephone to contact that network, regardless of activity participation.

Demographic variables: I also included some demographic data as control factors. Gender and age were chosen for their theoretical significance; previous literature has shown a clear relationship between age and gender and internet activity (Moscardelli & Divine, 2007;

Valkenburg & Peter, 2008). Parental race was used as an admittedly questionable stand-in for respondent's race/ethnicity.[30] Respondent's community type (urban/suburban/rural) and census region were included as well, primarily to test for any potential relationships; for instance, between urbanicity/rurality and Internet use (i.e., might users in rural areas use the Internet to connect with friends more than users in more densely-packed urban areas?). Household income was reported by the parent and coded by PIAL into one of eight categories (less than $10,000/$10,000 to less than $20,000/$20,000 to less than $30,000/$30,000 to less than $40,000/$40,000 to less than $50,000/$50,000 to less than $75,000/$75,000 to less than $100,000/$100,000 or more). In the initial data set, 73 cases (9.9% of the sample) were missing (i.e., "don't know/no answer"). I attempted to restore the missing variables in SPSS both by adding the series mean and by using linear interpolation. Both attempts yielded roughly similar results, so I chose to use the series mean cases. In all cases except age and household income, the variables were recoded as dummy variables. The reference categories for each variable were "male" for sex, "white" for parental race, "South" for Census region, and "suburban" for community type.

Analytical Technique

In this data set, my dependent variables are straight counts of behaviors engaged in. A respondent cannot "half" use SNS or "seventy five percent" create a website. Either the activity is engaged in, or it is not. This means my dependent variable is polychotomous and ordinal. As such, the appropriate analytical technique is ordered logistic regression (OLR) (Long 1997).

[30]Obviously, parental race does not correlate 1:1 with a child's racial identity.

To examine the effects of offline network strength on online activity, I estimated two OLR models. The first model regresses content creation behaviors on all the variables discussed above, including demographic indicators for the child and one parent, as well as the measurements of offline network strength. The second model regresses reinforcing behaviors on the same variables. The results of these analyses are presented in Table Nine.

Results

Exploratory Methods Model

Table Nine provides the results of the regression analysis for the exploratory methods model ($M = 1.25$, $SD = 1.267$). The aim of this model is to assess the relationship between various measurements of teenagers' offline network strength and their use of exploratory methods. By including the various control variables, I am able to determine whether there were any differences based on parental or respondents' demographics. In this model, only three variables exhibit significant effects on exploratory behavior: household income, participation in school clubs, and time spent in person with friends. Because this model is an ordered logistic regression, I must use the y*-standardized coefficients to interpret its meaning (Long 1997). The y*-standardized coefficient indicates the effect on the dependent variable, in standard deviations, of a one-unit change in a given independent variable when all other variables are held constant. For example, participation in school clubs (a dichotomous variable) increases exploratory behavior by .194 standard deviations when all other variables are held constant. For each bracket increase in household income, assuming all other variables are controlled, exploratory behavior decreases by .056 standard deviations. Finally, for each reported increase in frequency

of time spent in person with friends, respondents' exploratory behaviors increase by .146 standard deviations, when all other variables are controlled.

There are two indicators of fit for this model. Ordered logistic regression inherently assumes that the slopes of coefficients are parallel at the threshold – in other words, that a model measures the likelihood of a respondent engaging in zero exploratory behaviors exactly as well as it measures the likelihood of a respondent engaging in all four exploratory behaviors. This is called the "proportional odds assumption," and it is tested using the Brant chi-square (Long 1997). A significant chi-square means that the model fails to meet the proportional odds assumption, and should be rejected. The Brant chi-square for the first model is 79.12, well outside of significance. As such, I can assume that this model accurately portrays the relationship it is purported to. By looking at McFadden's R-squared, I can say that the model explains about 2% of the variance in exploratory behavior (R2 = 0.025) for the sample. This is an admittedly small amount, and suggests that further research in the area is called for.

Reinforcing Methods Model

Moving to the second model, five variables have significant effects on reinforcing behavior: respondent's sex, respondent's age, participation in school clubs, participation in non-club, non-sport school activities, and time spent in-person with friends. Looking at the y*-standardized coefficients, female respondents' participation is .301 standard deviations higher than males, when all other variables are held constant. For each year of age, reinforcing behavior increases by .175 standard deviations, when all other variables are held constant. Participation in school clubs increases reinforcing behaviors by .167 standard deviations when all other variables are held constant. Participation in non-club, non-sport school activities (e.g.

band, student government) decreases reinforcing behaviors by .190 standard deviations when all variables are held constant. Finally, for each unit increase in time spent with friends in person outside of school, reinforcing behavior increases by .184 standard deviations.

The Brant chi-square for this model is 12.48, meaning that the proportional odds assumption is met and the model represents what it purports to. The McFadden's R-squared is .075, suggesting that this model explains about seven percent of the sample variation in reinforcing behavior.

Overall, these models are significant, but do not explain a great deal of the variance in the population. What they do suggest about adolescents' online activities and the influences of offline networks is fascinating, nonetheless.

Discussion

Exploratory Behavior

Parental Demographic Indicators

For this model, the parental demographic indicators were relatively minor. Household income has a negative influence on respondents' exploratory behavior. I am not sure exactly what would cause this relationship, although my initial hypothesis is that respondents whose households have more money might have different levels of access to creative expression for their children, i.e., children from higher SES backgrounds may participate in art classes or other means by which they can self-express without going online. Alternately, higher-SES households

may have more barriers in place to online exploratory behavior (software filters, restrictions, etc.). Further research is needed in this area.[31]

Respondent Demographic Indicators

None of the respondents' demographic indicators were significant to exploratory behaviors. This is actually interesting by its absence, as it suggests that regardless of age and gender, adolescents engage roughly equally in exploratory behavior. This is essentially what I was expecting to see.

Offline Network Strength

I initally thought that lower levels of offline network strength would correlate with higher levels of exploratory behavior, as the respondents would go online and create unique material to seek out new friends with shared interests. However, only two of the offline indicators were significant; participation in school clubs and time spent in person with friends. Participation in school clubs increases a respondent's exploratory behavior by .194 standard deviations when all other variables are held constant. Much of the behavior included in the exploratory activity count is likely to be engaged in by club members – the creation of a website for other people, for instance. Certain clubs, particularly those connected to the arts or culture, might attract respondents who are already creative and as such prone to engaging in exploratory behaviors. Furthermore, the original variable is a simple yes/no participation dichotomy; examining the frequency or depth of club participation might help explain this outcome further.

---

[31] Defining "high" and "low" SES when discussing households that own at least one computer seems a bit arbitrary. For this purpose, I would suggest that households with a median income over $50,000 would constitute "higher-SES", as the PIAL set uses $10,000 increments until $50,000, then goes to $25,000 increments.

More interestingly, the more time a respondent reports spending in person with friends, the higher their predicted exploratory behavior count. It is possible that some friendship networks could use time spent in person to engage in exploratory activities; collaborating on websites or other materials to be displayed online. Alternately, respondents who spend lots of time with their friends may just use exploratory methods to expand their friendship networks. On the other hand, time spent in person with friends has a stronger effect on respondents' reinforcing behaviors (each unit of time spent in person with friends increases exploratory behavior by .274 standard deviations, but increases reinforcing behavior by .370 standard deviations). As such, I would hesitantly accept hypothesis 1b. Low levels of offline network strength do not necessarily result in higher levels of exploratory behavior than reinforcing behavior, but reinforcing behavior is more strongly affected by offline network strength.

Reinforcement Model

Parental Demographic Indicators

Similar to the exploratory model, parental demographics seem to play no role in respondents' reinforcing behavior. This is somewhat surprising, as I had initially assumed rural residents might be more likely to use reinforcing methods to keep in touch with distant peers (and conversely, that urban residents would not use reinforcing methods, as their peer networks were more densely packed). The big surprise here is that, regardless of parental residence, race, or income, adolescents use reinforcing behaviors roughly equally.

Respondent Demographic Indicators

Respondents' sex and age were both significant in the reinforcing behavior model. When it comes to gender, females are much more likely to use reinforcing methods, an increase of .301 standard deviations relative to male users when all other variables are held constant. This finding strongly supports the existing literature; females use the internet primarily to speak with Friends and recreate/represent existing social networks, i.e., for reinforcement purposes (Lenhart & Madden 2007).

Age is also very important; as respondents grow older, their use of reinforcing methods increases fairly dramatically – with all other variables held constant, the difference in predicted outcome between a 12 year old and a 17 year old is (.1745*5= .8725) almost a full standard deviation. This increase can be theoretically linked to teens' increasing access to the internet as they age; both due to their own demands for relative independence and presumably increased parental trust (Youn 2005, Livingstone & Helsper 2008). There is a serious implication here for internet safety advocates, then: safety education needs to begin as early as possible, because the use of reinforcing behaviors like social network sites, instant messenger software, and many of the other vectors by which teens encounter online risks increase dramatically with age.

Offline Network Strength

Three of the network strength indicators are significant in the reinforcing model. Participation in school clubs and time spent in person with friends both increase reinforcing activity, whereas participation in non-club, non-athletic school activities actually decreases reinforcing activity. The relationship between time spent in person and reinforcing behavior is logical; online activity is simply another vector for connecting between friends. Friends who

spend a lot of time together offline would likely spend a lot of time together online as well. School club participation also influences reinforcing behavior; perhaps the online communication allows members of clubs to communicate with one another outside of school – or possibly vice versa; members of school clubs use the internet to organize and communicate. The relationship between non-club activities such as band and online communication is more interesting. In practice, this could reflect several possibilities. First, teenagers who engage in such activities are busier than their peers (practice, etc.) and as such less likely to spend time using the Internet at all. Alternately, these activities might represent a different sort of "popularity" relative to club participation; respondents in clubs may represent one clique who are actively engaged with reinforcing methods, while participants who are active in non-school activities are part of different cliques or networks that do not value reinforcing methods as strongly ("preps" versus "band geeks" or what-have-you).

Hypotheses

Comparing the results between the two models provides some interesting results. Hypothesis 1a suggested that respondents who have higher levels of offline network strength are more likely to engage in reinforcing activity, while hypothesis 1b claimed respondents with lower levels of offline network strength will be more likely to use exploratory methods. The most obvious signifier in my results is the difference in r^2 for reinforcing activity relative to exploratory activity (.075 or 7.5% of variance explained for reinforcing activity versus .025 or 2.5% of variance explained for exploratory activity). This would initially seem to support both hypotheses, as respondents with higher levels of offline network strength are more likely to participate in reinforcing methods. On the other hand, participation in clubs and frequency of in-

person communication increased reinforcing *and* exploratory methods of Internet communication, and at almost identical levels (with all other variables held constant, school club participation increased exploratory activity by .194 standard deviations and reinforcing activity by .167 standard deviations, for example), which suggests at best a tenuous connection between low offline network strength and higher exploratory activity; indeed, club participation actually has a stronger effect on exploratory behaviors than on reinforcing behaviors. By plugging equal and arbitrary data into either model, I can compare the influence of offline network strength on a fictitious respondent. My imaginary subject is a 15 year old female who is active in school clubs but not non-school activities, lives in a rural area, and spends time in-person with friends outside of school every day (a score of 4 in the coding). Her family's household income was between $40,000 and $50,000 (a score of 5 in the coding). This gives me the following sample models:

Exploratory = -.0593*5 + .1940 + .1456*4 = .4799

Reinforcing = .3009 + .1745*15 + .1665 + .1837*4 = 3.8197

In these examples, the effects of age and gender actually determine much of the influence on reinforcing activities relative to exploratory activities, especially relative to the influence of time spent with friends outside of school. As such, I need to find another way to measure the actual influence of offline network strength, such as comparing the standardized coefficients for the offline network strength indicators. In the exploratory behavior model, school club participation and time spent in person with friends are both significant, with y*-standardized coefficients of .194 and .146, respectively. In the reinforcement model, the y*-standardized coefficients for those indicators are .167 and .184. This comparison is a bit of a mixed bag; while school club participation is more influential to exploratory behavior, time spent in person with friends is

more influential to reinforcing behavior. Given that club participation is a simple yes/no variable, while time spent in person has four levels, it would seem that time spent in person with friends has a stronger effect overall, and with reinforcement having a (slightly) higher coefficient, reinforcing behavior may be more influenced by offline network strength than exploratory behavior.

This somewhat confirms hypothesis 1a (respondents who are highly connected to off-line social networks will have a greater likelihood of using reinforcing communications methods), at least insofar as time spent with friends is more influential on reinforcing behavior than exploratory. On the other hand, the difference between the exploratory and reinforcing models is so small as to be almost negligible, and most of the actual difference between the two is largely driven by the influence of age and gender on reinforcing behavior. As such, I would suggest that the result for hypothesis 1a is tentatively confirmed, while hypothesis 1b (respondents who are weakly connected to off-line social networks will have a greater likelihood of using exploratory methods) is inconclusive at best.

There are some interesting implications for parents and safety advocates here – first and foremost, it does not seem that a teen's level of off-line social engagement plays a significant effect on their online activities, especially as compared to age and, in the case of reinforcing behaviors, gender. As such, any sort of online safety program needs to start as early as possible, while potentially offering different focuses on boys and girls' online risks.

In the next chapter, I will investigate the effects of risk perception, parental mediation, and self-mediation on the sharing of vulnerable personal information via SNS profile.

TABLE 7. Measures of Online Activity (n = 735)

	Mean or %
Exploratory characteristics	
Work on own webpage (%)	27.20
Work on webpage for others (%)	29.80
Share something found online (%)	41.50
Remix things found online (%)	26.40
Exploratory scale characteristics	
Zero behaviors reported (%)	25.30
One behavior reported (%)	25.60
Two behaviors reported (%)	20.20
Three behaviors reported (%)	18.10
Four behaviors reported (%)	10.70
Reinforcing characteristics	
Upload photos (%)	52.90
Send instant messages (%)	75.50
Use social network sites (%)	58.90
Reinforcing scale characteristics	
Zero behaviors reported (%)	2.60
One behavior reported (%)	5.80
Two behaviors reported (%)	21.40
Three behaviors reported (%)	70.20

TABLE 8. Exogenous Variable Characteristics (n = 735)

	Mean or %
Region	
Northeast (%)	21.50
Midwest (%)	28.30
South (%)	30.20
West (%)	20.00
Community	
Rural (%)	21.90
Suburban (%)	53.90
Urban (%)	24.20
Parent's race	
Black (%)	5.40
Hispanic (%)	4.10
White (%)	87.60
Other (%)	2.90
Household Income	
Child's sex	
Female (%)	51.00
Male (%)	49.00
Child's age	14.82
Offline Network Strength	
School Club Participation (%)	39.60
School Sports Participation (%)	53.70
Other School Activities (%)	44.00
Non-school Activity Participation (%)	62.60
Time spent in person	
Time spent on landline	

Table 9. Ordered Logit Regression of Online Activities on Exogenous Variables (n = 735)

	Exploratory		Reinforcing	
	β	β^{Sy*}	β	β^{Sy*}
Region				
Northeast	-.28503	-.15150	-.09954	-0.0495
Midwest	.08380	.04450	-.31053	-0.1543
West	-.09989	-.05310	.02521	0.0125
Community				
Rural	-.06364	-.03380	-.28774	-0.1430
Urban	-.08064	-.04280	-.23852	-0.1185
Parent's race				
Black	.49699	.26410	-.19406	-0.0964
Hispanic	.43614	.23180	.36458	0.1812
Other	.19964	.10610	-.43488	-0.2161
Household Income	-0.11154*	-.05930	-.02515	-0.0125
Child's sex	.21057	.11190	0.60542***	0.3009
Child's age	.04676	.02480	0.35116***	0.1745
Offline Network Strength				
School Club Participation	0.36514**	.19400	0.33504**	0.1665
School Sports Participation	-.08124	-.04320	.11390	0.0566
Other School Activities	-.03997	-.02120	-0.38265**	-0.1902
Non-school Activity Participation	.17627	.09370	-.00774	-0.0038
Time spent in person	0.27393***	.14560	0.36968***	0.1837
Time spent on landline	.06280	.03340	.02163	0.0107
Log likelihood	-1046.846		-889.716	
McFadden's R^2	.025		.075	
Brant chi-square	79.120		12.480	

$p < .05$. ** $p < .01$. *** $p < .001$.

CHAPTER 5 – Identity Vulnerability

In the previous chapter, I began my investigation by studying the effects of offline network strength on adolescents' online communication methods. In this chapter, I will focus specifically on adolescent usage of social network sites (SNS) and their sharing of vulnerable identity data, those materials that an unwanted individual could theoretically use to identify or track the owner of a given SNS profile.

Method

Participants

From Chapter 4's data set of 735 teens, I cut the sample down further to the 430 teens who reported creating a profile on a social network site like Myspace or Facebook, due to PIAL only asking identity vulnerability questions of respondents who had SNS profiles. Respondents were between the ages of 12-17 (M = 15.17, SD = 1.495). 45.8% were male and 54.2% female. The teens were not directly asked about their racial or ethnic identity, however, 86.5% of respondents' parents identified as white and non-Hispanic, 5.8% identified as Black and non-Hispanic, 4.7% identified as Hispanic, and 3.0% identified as some other racial group. By region, 20.0% lived in the Northeastern U.S., 26.0% in the Midwest, 31.9% in the South, and 22.1% in the West. 55.1% of respondents lived in suburban areas, while 21.6% were rural and 23.3% were urban.

Dependent Variable

Identity Vulnerability: In the initial factor analysis, nine variables were chosen to represent various potentially compromising pieces of information that could be shared on a

respondent's profile; photos of self, photos of Friends, first and last name, school name, hometown, instant messaging user name, email address, and a blog link. These variables loaded onto three core factors; one consisting of respondents' last name, school name, and hometown (physical identity data), photos of self and Friends (visual identity data), and IM name/email address (digital identity data). In this case, theoretically the physical identity data is the most problematic, as it can be used for the most nefarious purposes (e.g. by a predator to locate potential victims or by bullies to confirm the online presence of an offline target). As such, I decided to use a combined scale of the physical identifier variables, giving us a range from 0 (no physical identifiers posted) to 3 (all physical identifiers posted). I also tested the visual and digital identity data simply for the sake of thoroughness. Details of this scheme are presented in Table 10.

Independent Variables

Risk Perception: For this concept, I chose two questions concerning whether strangers and bullies were more likely to use the internet or the real world to approach people. As a "scale" consisting of two variables is relatively pointless, I simply used each indicator individually in my regression.

Self-Mediation: I chose three variables to represent degrees of self mediation; whether or not a profile was visible to all users, whether or not the respondent was Friends with any total strangers (i.e., individuals they had no online or offline connections to), and the level of reported honesty in a respondent's profile. The first two variables were coded bivariate (i.e., a profile was visible to everybody or was not visible to everybody, and a respondent was Friends with a total

stranger or was not Friends with a total stranger), while the third was scaled with levels running from “Profile is completely honest” to “Profile is completely false”.

Parental Mediation: The nine variables related to parental mediation in my model fall into two groups; one related to parents' responses about rule-setting behavior, and the other related to responses about external forms of mediation (monitoring/filtering software, parents actively checking what respondents do online). It appears there are two different interpretations of parental mediation; rule-setting behavior by parents and then hands-on mediation techniques. I decided to investigate both separately, creating two distinct stages in my model, one using three indicators regarding parents' statements about rule-setting (i.e. whether or not the parents said there were rules about what sites their children could visit) and the other using children's awareness of parental mediation techniques (i.e., does the child believe the computer they use at home has monitoring or filtering software). I chose the variables measuring children's perception of mediation rather than the ones using the parents' statements as, theoretically, it is more important for the child to believe that their behavior is being monitored or moderated (whether it actually is or not) than it is for the parents to have mediation systems in play without the child's awareness; after all, the child will only alter their behavior if they are actively aware of any mediation practices – they cannot react to what they do not know exists.

Demographic Variables: As with the models in the previous chapter, I used a mix of demographic variables as well; gender and age were chosen for theoretical interest. Parental race was used as an admittedly questionable stand-in for respondent's race/ethnicity, and respondent's community type (urban/suburban/rural) and census region were included as well. In all cases except age, the variables were recoded as dummy variables. The reference categories for each

variable were “male” for sex, “white” for parental race, “South” for Census region, and “suburban” for community type. Details of all exogenous varaibles are presented in Table 11.

Analytical Technique

To examine the effects of risk perception, parental mediation and self-mediation on identity vulnerability, I estimated three ordered logistic regression models. The first model regresses physical identity vulnerability indicators on the variables discussed above, including demographic indicators for the child and one parent. The second model regresses visual identity vulnerability indicators on the same variables. Finally, the third model regresses digital identity vulnerability indicators on the same independent variables. Results of these analyses are found in Table 13.

Results

Physical Identity Vulnerability Model

In the first model, six variables exhibit significant effects on respondents' levels of physical identity vulnerability: having a parent who identifies as black, gender, age, child reporting that their parents check to see where they have been online, child reporting that their parents use filtering software, and level of respondent's profile honesty. Looking first at the control variables, having a parent who identifies as black increases a respondent's level of physical vulnerability by .430 standard deviations when all other variables are held constant. Female respondents have a .457 standard deviations higher level of physical vulnerability than males, while each year increase in a respondent's age increases the level of physical vulnerability by .091 standard deviations. Looking at parental mediation methods, children who report that

their parents check to see where they have been online have a .267 standard deviations lower level of physical vulnerability than their peers, while children who report that their parents use filtering software see a decrease in physical vulnerability of .197 standard deviations. Finally, each increasing level of falsehood in a respondent's profile decreases their physical vulnerability by .144 standard deviations.

The McFadden's r-squared for this model is .075, meaning that this model explains 7.5% of the variance in the sample, and the Brant chi-squared is 53.08, meaning that the model accurately depicts the relationship between variables.

Visual Identity Vulnerability Model

In the second model, four variables exhibit significant effects on respondents' levels of visual identity vulnerability: household income, sex, age, and parents reporting rules about the types of sites children can visit. Each level increase in household income raises a respondent's level of visual vulnerability by .082 standard deviations, when all other variables are held constant. Females have a .318 standard deviations higher level of visual vulnerability, while each year of age increases visual vulnerability by .138 standard deviations. Finally, parents who report having rules about the types of sites their children can visit decrease the respondent's visual vulnerability by .542 standard deviations.

The Mcfadden's r-squared for this model is .083, suggesting that it explains 8.3% of the variation in visual vulnerability in the sample. The Brant chi-square is 10.64, so I can accept this model as accurate.

Digital Identity Vulnerability Model

The third model has only two variables that display significant effects on digital identity vulnerability: living in an urban community and whether or not a respondent was Friends with a stranger. Urban respondents have a .276 standard deviations lower level of digital vulnerability than suburban dwellers, while being Friends with a stranger increases the level of digital vulnerability by .282 standard deviations when all other variables are held constant. The McFadden's r-squared for the model is .027, meaning that the model explains 2.7% of the variance in the sample. The Brant chi-squared is 21.79, meaning the model is acceptably accurate.

Discussion

General Observations

It would appear that respondents' perception of the Internet as a potentially risky environment has absolutely no influence on their sharing of personally identifying material. This actually seems to conflict somewhat with earlier research, which found that the more comfortable a teenager reportedly felt with the Internet, the more likely they were to engage in risky behavior (Youn 2005, Livingstone and Helper 2008). I see two potential explanations here. The more likely of the two is data-related - the questions in the PIAL data set simply do not measure risk perception as accurately I would have hoped. Simply asking teenagers if they are more worried about stalkers and bullies online does not really measure whether or not they consider the internet as a whole to be unsafe. Alternately, SNS users as an aggregate are more comfortable online (or at least *believe* they are more capable) and as such are less worried about

online risk. In either case, this seems to be an area where further research is definitely called for. Also, across all three IV models, Census region had absolutely no effect. This is interesting by its absence, as it suggests that across the United States, teenagers share personal information in roughly similar ways.

Physical Identity Vulnerability

Looking at the physical identity vulnerability results, it is interesting to see that having a Black parent has an effect on PIV relative to having a white parent, but not having a Hispanic or other non-white parent. I am not sure exactly what could be causing this effect. It is not due to mediation techniques, as those are already tested for. However, only 5.3% of responding parents identified as Black, relative to about 13% of the total U.S. population.

When it comes to respondents' own demographic data, PIV is influenced by both sex and age. Girls are considerably less likely to post PIV than boys. This seems reasonable, given that much of the media coverage about online risks focus on girls as the primary victims. On the other hand, given that girls are supposedly more likely to use SNS to bolster offline friendship netowrks, it seems odd that girls are less likely to post PIV than boys. However, if the friendship networks are pre-existing, perhaps posting too much information is not necessary – if a teenager already knows how to find her offline friends online, why would she need to post more information than is absolutely necessary? Indeed, data falsification could be an intentional part of the process, using specific alterations as a code. This ties in well with the significance of profile falsification as it relates to the sharing of PIV – a fake hometown, last name, or school might act as a sort of shibboleth – Sarah Jones from Anytown Middle School is being careful and dubs herself “Sarah Sparkles” from “Lazytown Middle School.” While previous research

suggests that boys are more likely to falsify information than girls, it seems the falsification may not be in the areas immediately pertinent to PIV (Lenhart & Madden 2007). This logically ties in with boys' reported use of SNS to meet and flirt with girls; physical location would be highly useful in such a scenario – users might be more willing to engage with flirtatious chat with a Friend on the other side of the country, under the assumption that the long distance involved diminishes any chance of offline awkwardness. Alternately, users might explicitly look for Friends in their immediate area with hopes of meeting in person.

Age also proves to be a siginficant indicator of a respondent's likelihood of engaging in PIV sharing. For each year's increase in age, PIV increases by .0912 standard deviations. Given that the range of ages runs from 12 to 17, age has the potential to be extremely significant. This makes sense, as not only do parents give more responsibility to older children (both as pertains to the Internet and in general), but older children are probably more likely to be online in the first place. Furthermore, while SNS usage is technically restricted to children over the age of 13 for Facebook and 14 for Myspace[32], it is well documented that younger children lie about their age in order to bypass SNS blocks (Thewall 2008; Lenhart & Madden 2007). Older teens may also be more competent in their ability to bypass various restrictions imposed on their online behavior.

It is extremely interesting to see that parental rule-setting behavior has absolutely no effect whatsoever on PIV sharing. It is significant that the questions about rule-setting were only asked of parents and not of the teenaged respondents. As such, while the parents may feel there are clear rules in place about online activities, the respondents themselves may not be as aware of those rules as parents might think. It is also possible that children might be aware of the rules,

[32]When the data set was collected, the age minimum for both sites was 16.

but simply ignore them. In either case, it appears that attempts to control PIV behavior via simple rule-setting is completely and totally ineffectual. Similarly, monitoring software proved equally insignificant as a means of PIV prevention. The use of filters to actively restrict usage, as well as parents checking a child's online activity (and perhaps more importantly, telling a child they check the online activity) both proved significant, however. This is unusual, as it seems that more technologically-savvy teens could find workarounds (deleting a browser history, using SNS from an unrestricted location, etc.) to circumvent these mediation tactics. On the other hand, it is possible that parents who use such active mediation techniques are simply more involved in all aspects of their children's lives, and this heightened involvement is the significant factor, rather than the software or the checking.

Finally, and perhaps unsurprisingly, the amount of false material a respondent posts to their profile decreases their level of PIV. This seems obvious on first glance, but upon further consideration there are some interesting implications. PIV factors might not necessarily be the ones a user would falsify on an SNS profile, as they are amongst the most critical (other than a photograph) in allowing offline friends to find an online profile. That is not to say there is no reason to falsify such information, as discussed above. While profile falsification may not be done for security purposes, it seems that respondents who falsify some data are more likely to falsify critical PIV data as well.

Intriguingly, the other self-mediation indicators in the PIV model were not significant – suggesting that a respondent's level of PIV is unconnected to Friendship with strangers or the overall visibility of their profile. A teen whose profile is visible to the entire Internet is just as likely to share PIV data as a teen who secures everything behind a “Friends only” shield, and a

teen who Friends total strangers is just as risk-prone as a teen who carefully monitors her Friend network.

It is also worth pointing out that this model only explains 7.5% of the total variance in PIV behavior in the population. While that is certainly worthy of attention, it still means that over 90% of PIV behavior is going unexplained.

Visual Identity Vulnerability

When it comes to VIV, location indicators play no significant role – across the U.S., regardless of population density, teenagers have similar VIV sharing patterns. As far as parental demographics go, race did not prove significant, but household income does play a role. I would surmise that the positive relationship between household income and VIV data is most likely due to children from higher-SES households having greater access to digital cameras and other devices that allow for VIV sharing.[33] As with PIV, age and gender are both significant to respondents' PIV behaviors. The most significant difference is that girls are more likely to post VIV data than boys. One potential explanation is that girls may believe that their apperance is valued more than boys', and as such are more likely to share images of themselves for peer approval. Alternately, as discussed earlier, girls use SNS to reinforce existing offline networks, and posting photographs of themselves with their offline friends would be a strong component of such behaviors. As far as age is concerned, I imagine much the same factors are in play as with PIV – older teens are more likely to use SNS in the first place, they are more likely to believe

[33]Recall again this is 2006 data – even though 80% of respondents in this sample claimed to have a cell phone, it is unclear how many of those phones had camera capabilities compared to today, when a camera is practically standard equipment.

they are competent online, and they are more likely to have their parents' trust with the technology that generates VIV data (cameras, etc.).

Only one of the parental mediation indicators proved significant – respondents whose parents report setting rules about which sites can and cannot be visited have a lower VIV level than their peers. This finding is somewhat peculiar – none of the active mediation methods were significant, and none of the other parental rules were significant. Interestingly, none of the self-mediation tactics were significant either. I believe this speaks to the ubiquitousness of images on SNS profiles – if a respondent has a profile, they likely have a photograph attached to it. It is simply part of the normative culture of SNS. Perhaps this explains the rule-setting behavior's significance as well – if a child is forbidden from using the SNS sites (in which case they access it furtively), posting VIV data might be seen as too risky – not in the sense of predators, strangers, or other malefactors finding their profile, but simply to keep their parents (or their Friends' parents) at bay.

Digital Identity Vulnerability

Living in an urban area has a significant effect on respondents' digital identity vulnerability. Urban dwellers are less likely to post DIV data than their suburban counterparts. I would suggest this may have something to do with population density – respondents in urban areas can more readily get in touch with their peers, and do not need to share connecting information online. Suburban respondents may have friends who live a significant distance away. On the other hand, if this was the case, I might expect rural dwellers to have a higher level of DIV data – so density may not be the only answer.

None of the parental or respondent demographic data has any significance on DIV activity. This in and of itself is interesting – it would seem that all teenagers with SNS profiles share this data in roughly the same ways. Furthermore, none of the parental mediation methods are significant. The only other indicator significant to DIV activity is a respondent's reporting a Friendship with a stranger. Perhaps teens who are Friends with total strangers are using SNS in ways that other teens do not – to build broader social networks based on shared interests (i.e. for exploratory purposes). By sharing this information, they are allowing their distant Friends to stay in contact outside of the SNS sphere.

Going back to Table 11, only about half of all SNS-using respondents engage in either of the two DIV-sharing activities. Perhaps this is part of the issue; so few respondents even bother sharing a blog link (most likely because they do not have one[34]) that those who share DIV are largely a self-selecting crowd. To share blog links or email addresses, the respondents have to care about sharing those things – both of which are significantly less relevant to the overall SNS experience than PIV or VIV data.

Hypotheses

Returning now to my hypotheses, I feel the results for hypothesis 2 (Respondents who perceive the Internet with high levels of potental risk will have a higher level of self-mediation) are inconclusive. Mostly, I feel this is due to the indicators available in the PIAL data set simply being insufficient to measure risk perception. As such, I would recommend further targeted research in this area.

[34]Only 41.5% of the sample reported having an online journal or blog.

I strongly accept hypothesis 3a (respondents who report a high level of self-mediation will have a low level of identity vulnerability). Looking at both the PIV and DIV models, a respondent with higher levels of mediation (e.g., increased profile falsification or not being Friends with strangers) will have a decreasing level of identity vulnerability. Looking at the PIV model, each level of increased profile falsification increases a respondent's overall PIV score by .1435 standard deviations when all other variables are held constant. This is as significant as a year of age, and a fully false profile has as significant an effect on a respondent's PIV score as gender or parental race (-.1435*5= -.7175 versus -.4565 or .4303). Simply put, self-mediation does have a direct effect on profile vulnerability.

Regarding hypothesis 3b (respondents who report a high level of parental mediation will have a low level of identity vulnerability), I would accept it with some qualifications – only respondents who report *specific* types of parental mediation have lower levels of physical identity vulnerability. Parental rules and technological mediation do not seem to effect PIV, whereas more active forms of parental mediation (i.e., parents checking to see where their children have been online or outright blocking problematic sites) do decrease PIV.

Finally, hypothesis 3c (self-mediation will have a stronger effect on respondents' degree of identity vulnerability than parental mediation) can be accepted, again with qualifications. The y-sub Beta score for level of profile falsification is -.144, meaning that for *each level* of falsification (out of five possible) a respondent's physical identity vulnerability score decreases by .144 standard deviations with all other variables held constant. Conversely, a respondent's awareness that their parent checks where they have been online has a y-sub Beta of -.267, meaning that with all other variables held constant, parental checkups only decrease identity

vulnerability by .267 standard deviations. The use of filtering software to block teenagers from using specific sites has a y-sub Beta of -.197, only decreasing PIV by .197 standard deviations. As such, it seems that two levels of profile falsification is equivalent in effect to a parental checkup, while one level of falsification is almost as effective as filtering software. Therefore, I can accept hypothesis 3c with the aforementioned qualifications.

Overall, these results have some very important implications for parents, safety advocates, and others who are interested in teens' safety online. First and foremost, age matters. Any intervention protocol that hopes for a real chance of success has to strike early, before kids get deeply involved in SNS activity. Teens are going to use these sites, even if it requires lying about their age during the registration process (and falsifying one's age is as simple as picking the wrong year of birth while signing up for the site). As such, parents and safety advocates need to warn teens early on about the potential risks involved. Second, parents *must* take a more active role in their child's online activities. Simply setting rules is not enough, and while filters and monitors might keep adolescents away from sexual or violent materials, they appear to have very little effect on risky SNS behavior. Monitors, at least in the context of SNS, appear to be completely ineffectual, possibly because teens do not think they are doing anything wrong (and in the context of adolescent SNS protocol, they are not). Filters are essentially either/or – a site is either blocked or it is not, which might simply encourage the child to access the forbidden site through some other means. As noted above, the most effective parental mediation tactic was when respondents were actively aware that their parents check online activity after the fact. While it was only a minor effect relative to age and gender, it was still significant enough to make a difference. Parents must take an active role in their child's experience, rather than

passively declaring rules and hoping technological controls will prevent risky behavior. Any systematic attempt to prevent risky behavior on SNS then must involve the parents and the children.

Complete Model

As a final attempt to evaluate my theoretical model, I ran the SNS-users' data through a complete model, combining the offline network strength indicators from Chapter 4 with the identity vulnerability indicators from earlier in this chapter. Results of this analysis are found in Table Thirteen. I specifically chose to only run the data through a model using physical identity vulnerability as the dependent variable, primarily because PIV is the greatest cause for social concern (as it is directly connected to stalking, bullying, stranger contact, and many other risks).

In this model, seven indicators display significant effects on respondents' sharing of PIV data. Having a black parent, respondent's sex, respondent's age, frequency of talking to offline friends on a landline telephone, respondents' knowing their parents check their online activity, respondents knowing their parents use filtering software, and the degree of a respondent's profile honesty all are significant. Having a black parent increases a respondent's degree of PIV by .412 standard deviations when all other variables are held constant. Females have a .389 standard deviations lower level of PIV than boys when all other variables are held constant. For each year of respondent's age, PIV increases by .072 standard deviations when all other variables are held constant. For every reported increase in time spent talking to friends on a landline telephone, PIV decreases by .122 standard deviations when all other variables are held constant. Respondents who know their parents check online activity have a PIV score .262 standard deviations lower than their peers when all other variables are held constant. Respondents whose

parents use filtering software see a .214 standard deviation decrease in PIV level when all other variables are held constant. Finally, for each increased level of profile honesty, respondents' PIV level decreases by .144 standard deviations when all other variables are held constant. The McFadden's r-squared for the model is .096, meaning that this model explains almost 10% of the total variance in the sample. The Brant chi-squared is 14.69, meaning I can accept the model as accurate.

Discussion

There are some very interesting results here. Most significantly, a respondent's levels of exploratory and reinforcing behavior have no effect on PIV when using SNS. It would seem that regardless of how teens use the internet, they are equally likely to share personal information on their profiles. Of course, this particular data set is specifically limited to those respondents who have created an SNS profile, and only measures PIV on those profiles. It does not, and cannot, say anything about PIV sharing via other vectors such as chat rooms or message boards.

Of the offline network strength measurements, as respondents' reported frequency spent speaking with friends via landline telephone increases, the level of PIV sharing decreases. This is somewhat surprising, as it would seem that those teens who spend much of their time on the phone would also use SNS to connect with friends, and would share PIV information as a means of furthering that connection. Perhaps some teens prefer the telephone to SNS, and simply spend less time on SNS overall, relative to their peers. Alternately, frequent telephone communication simply reflects a different type of social connectedness – the phone calls are with a romantic interest, while SNS is used to connect with friends (or vice versa). Possibly, respondents who frequently use landline telephones to communicate with friends are still using dial-up internet

(remember, this is data from 2006) and can only either speak or be online at a given time. Regardless, this is an interesting finding, and warrants further investigation. Also significant is the fact that none of the "participation" indicators had any effect on PIV sharing. Regardless of participation or non-participation in sports, clubs, or other activities, respondents share information in roughly the same ways and at the same levels.

Two of the parental mediation methods have a significant effect on PIV sharing. Respondents who know their parents check their online activity and respondents whose parents use filtering software on the home computer both see a decrease in PIV sharing. As was the case in earlier models, parental rule-setting has absolutely no effect. This would suggest that parental rule-setting is only viable as part of a holistic safety system; checking where teens go, actively filtering out dangerous content, and remaining engaged with what teens are actually doing online.

Of the self-mediation tactics, only profile falsification affects a respondent's level of PIV sharing, which again, seems obvious. By putting false information, a respondent is logically excluding honest information. It also suggests that the profile information that is most frequently falsified falls under the aegis of PIV information – first name, last name, hometown, school, etc. The reasons for falsifying this information are varied. As discussed earlier, false information might serve as a gatekeeper for safety-conscious users (a false last name or hometown could winnow out users who aren't "true" Friends) or it might simply be for comic effect. Either way, this result is largely unsurprising. What is surprising is that Friendship with strangers and visible profiles do not have an effect on PIV sharing. This is definitely cause for some concern; a visible profile is just that. While a visible profile might aid offline friends in creating online

connections, it also opens up the user to all the risks discussed earlier; phishing, stalking and harassment, stranger contact and so forth. All of these rely on exactly the sort of PIV data being shared. Stranger Friendship is perhaps a slightly smaller concern, as some of the Friending behavior teens engage in online certainly counts as "being Friends with a person you do not personally know" but is actually relatively innocuous, such as following a musician, athlete, or other celebrity. Furthermore, most cyber-bullying appears to be perpetrated by individuals the victim knows offline, which means stranger Friendship is likely a limited risk in that case. On the other hand, malefactors using phishing techniques may use a false account to Friend a potential victim. Similarly, much has been made of cases where bullies, etc., have used fake profiles to trap their victims, and PIV sharing simply makes it easier for these would-be bullies to connect with their targets.

Once again, risk perception seems to have no effect on PIV sharing. As discussed earlier, I believe this is largely due to the variables I chose poorly reflecting the reality of teens' understanding of internet risk. Residential demographics (Census region and community type) also have no effect. This is again consistent with the previous models, and reinforces the idea that across the United States, in big cities and small towns, North, South, East, or West, teens are equally likely to share PIV data. The same holds true for household income.

The only parental demographic that mattered was having a black parent. Again, I am not sure exactly how to interpret this result. It is not due to household income or use of mediation tactics, as both of those are already controlled for. Perhaps black parents are less aware of SNS, or less concerned about the risks involved. It is possible that there may be other mediation

techniques in play that the data set does not cover. This is an area that definitely needs further, targeted, research.

Respondents' sex and age both were very important to the level of PIV sharing. As discussed earlier, it is interesting that girls share less information than boys do, but there are a host of potential explanations. The activities that girls engage in may not necessarily require much PIV sharing, especially if some profile information is falsified. Conversely, boys may share more information as part of their desire to use SNS to flirt and meet girls. The significance of age is also logical. Older children are more likely to be allowed online in the first place, and may share more information on their profile to seem "mature." It may also be the case that having a SNS profile (and sharing PIV data) is part of the normative culture of teenagers, and past a certain age, those who do not share this information are seen as pariahs or weirdoes.

Table 10. Measures of Identity Vulnerability (n = 458)

	Mean or
Physical Identity Vulnerability characteristics	
Last name (%)	27.3
School name (%)	52.9
Hometown (%)	60.1
PIV scale characteristics	
Zero behaviors reported (%)	25.8
One behavior reported (%)	25.5
Two behaviors reported (%)	31.6
Three behaviors reported (%)	17.1
Visual Identity Vulnerability characteristics	
Photos of self (%)	81.6
Photos of Friends (%)	65.6
VIV scale characteristics	
Zero behaviors reported (%)	14.7
One behavior reported (%)	23.5
Two behaviors reported (%)	61.9
Online Identity Vulnerability characteristics	
IM handle on profile (%)	40.8
Email address on profile (%)	28.2
OIV scale characteristics	
Zero behaviors reported (%)	48.4
One behavior reported (%)	34.1
Two behaviors reported (%)	17.5

Table 11. Exogenous Variable Characteristics (n = 458)

	Mean or %
Region	
Northeast (%)	20.0
Midwest (%)	26.0
South (%)	31.9
West (%)	22.1
Community	
Rural (%)	21.6
Suburban (%)	55.1
Urban (%)	23.3
Parent's race	
Black (%)	5.8
Hispanic (%)	4.7
White (%)	86.5
Other (%)	3.0
Household Income	
Child's sex	
Female (%)	54.2
Male (%)	45.8
Child's age	15.2
Parent: Rules about sites (%)	84.7
Parent: Rules about sharing (%)	88.3
Parent: Rules about time (%)	63.2
Child: Parent checks activity (%)	38.8
Child: Filtering software (%)	48.8
Child: Monitoring software (%)	33.5
More likely to be bullied online (%)	34.4
More likely to be approached online (%)	80.0
Profile visible to everyone (%)	29.3
Friends with strangers (%)	30.7
Level of profile honesty	

Table 12. Ordered Logit Regression of Identity Vulnerability on Exogenous Variables (n = 458)

	Physical		Visual		Digital	
	β	β^{Sy*}	β	β^{Sy*}	β	β^{Sy*}
Region						
Northeast	-.15195	-0.0753	0.1944	0.0779	0.39306	0.20970
Midwest	-.20488	-0.1015	0.0867	0.0430	0.20207	0.10780
West	-.26959	-0.1336	0.2025	0.1005	0.27372	0.14610
Community						
Rural	.34008	0.1685	-0.0910	-0.0452	0.22445	0.11980
Urban	.35202	0.1745	0.0297	0.0148	-0.51632*	-0.27550
Parent's race						
Black	0.86819*	0.4303	0.5908	0.2932	0.21884	0.11680
Hispanic	.73115	0.3624	0.2334	0.1163	-0.12166	-0.06490
Other	.62903	0.3118	0.0955	0.0459	-0.12964	-0.06920
Household Income	-.00382	0.0912	.16539*	0.0821	0.05153	0.02750
Child's sex	-0.92116***	-0.4565	.64170**	0.3184	0.06312	0.03370
Child's age	0.18408**	0.0912	.27857***	0.1382	-0.08278	-0.04420
Parental Mediation						
Rules about sites	-.10156	-0.0503	-1.09226**	-0.5420	-0.08407	-0.04490
Rules about sharing info	-.12210	-0.0605	0.0152	0.0756	-0.16121	-0.08600
Rules about time	.03669	0.0182	0.2347	0.1165	0.03749	0.02000
Parent checks activity	-0.53878**	-0.2670	-0.1673	-0.0830	-0.15800	-0.08430
Filtering software	-0.39749*	-0.1970	-0.1987	-0.0986	-0.00190	-0.00100
Monitoring software	-.10865	-0.0538	0.2012	0.0998	0.28822	0.15380
Risk Perception						
More likely to be bullied online	-.04017	-0.0199	0.0867	0.0430	0.08484	0.04530
More likely to be approached online	.06236	0.0309	-0.1306	-0.0648	-0.05371	-0.02870
Self-Mediation						
Profile visible to everyone	0.16945	0.0840	-0.2025	-0.1005	0.16441	0.08770
Friends with strangers	0.12342	0.0612	0.3790	0.1881	0.52834*	0.28190
Level of profile honesty	-0.28955**	-0.1435	-0.1764	-0.0867	-0.10591	-0.05650
Log likelihood	-538.503		-362.4380		-425.87025	
McFadden's R^2	0.075		0.0830		0.028	
Brant chi-square	53.08		10.6400		21.79	

* $p < .05$. ** $p < .01$. *** $p < .001$.

Table 13. Ordered Logit Regression of Final Model on Exogenous Variables (n = 427)

	Physical Identity Vulnerability	
	β	$_R^{Sy*}$
Region		
Northeast	-.26140	-.12540
Midwest	-.27709	-.13290
West	-.41756	-.20030
Community		
Rural	.31810	.15260
Urban	.35303	.16940
Parent's race		
Black	0.85914*	.41220
Hispanic	.80459	.38600
Other	.78052	.37450
Household Income	-.04899	-.02350
Child's sex	-0.81041***	-.38880
Child's age	0.14919*	.07160
Offline Network Strength		
School Club Participation	-.08896	-.04270
School Sports Participation	.27640	.13260
Other School Activities	.36328	.17430
Non-school Activity Participation	.10796	.05270
Time spent in person	.02982	.01430
Time spent on landline	-0.25485***	-.12230
Level of exploratory behavior	-.11916	-.05720
Level of reinforcing behavior	.11896	.05710
Parental Mediation		
Rules about sites	-.09191	-.04410
Rules about sharing info	-.14234	-.06830
Rules about time	.04096	.01970
Parent checks activity	-0.54625**	-.26210
Filtering software	-0.44681*	-.21440
Monitoring software	-.08635	-.04140
Risk Perception		
More likely to be bullied online	-.05343	-.02560
More likely to be approached online	.05874	.02820
Self-Mediation		
Profile visible to everyone	.16905	.08110
Friends with strangers	.20843	.10000
Level of profile honesty	-0.2999**	-.14390
Log likelihood	-526.36900	
McFadden's R^2	0.096	
Brant chi-square	14.69	

* $p < .05$. ** $p < .01$. *** $p < .001$.

CHAPTER 6 - Conclusions

This study began with a simple question: what would possess someone to post photographs to the internet which could get them suspended, expelled, or even arrested? It is quite possibly the oldest social research question: "what is wrong with kids these days?" I had an initial idea that teens share every minute detail of their personal lives with total strangers because they live in a world where shows like *Big Brother* and *The Real World* turn the mundane doings of "ordinary" people into celebrity culture. Teens see that, and they want to be the stars of their own "reality show", both figuratively and literally.[35] There has to be more to it than that, though – blaming it all on celebrity culture is too easy an explanation.

The problem of risky behavior by teenagers on the internet comes back again and again to the issue of information sharing. The posting of problematic material like profanity or suggestive photographs can cause immediate friction with parents and other authority figures and could potentially lead to long-term problems for teens as they continue into adulthood in a world where colleges and employers routinely run background checks. Sexual solicitation and cyber-bullying require at least an initial sharing of information; for an offline bully to locate someone online, the target must share enough pertinent information to allow the bully to track them down. Even in a case where an online miscreant is seeking a random victim, there has to be an initial release of information suitable to draw the malefactor's attention. The kinds of data commonly shared on social network sites (first and last name, hometown, school, photographs) are ideal for online confirmation of offline identities, as well as for gaining unauthorized access to email hosts and other web services which use that sort of data as a security check.

---

[35] Consider "Tila Tequila," the model who turned her Myspace popularity into a reality show, a book deal, and a recording contract.

The existing literature on adolescent usage of social network sites suggested several potential answers to the problem of risky information sharing. The dramaturgical models argue that teens use SNS as a vector for identity performance; adolescents create profiles as a way of maintaining their image to their peer network. A MySpace or Facebook profile is an idealized self, the version of reality that teenagers want their friends (and Friends) to believe. Photos, links, and comments are all tactically deployed to display a specific aspect of the creator's personality, whether serious, silly, or downright strange. The specific choices may vary, but overall the SNS is seen as a "backspace" area where teenagers can engage with their peers in relative privacy, free from the overprotective adult world. Authority figures and other unwelcome individuals are seen as outsiders and SNS profiles as a performance they were not invited to witness. It does not matter if the interlopers are bullies seeking a target, parents seeking the truth about what their children are up to, or sexual deviants seeking victims, the contents of the SNS profile were never meant for outside consumption. From this perspective, the risk to teenagers is not in the sharing *per se*, but in unwanted audiences gaining access to these private displays, whether through accidental interception or through intentional intrusion.

The postmodern perspective claims that SNS are a panoptic observation device, a 24-hour social control mechanism that teens willingly submit to. The reflexive design of SNS means that users are constantly on display for their Friends. The Friend network polices user behavior; appropriate performances receive "likes" and positive comments, inappropriate performances are penalized with negative comments or the dreaded "unfriending." While users have the potential for play and transgression in their SNS profiles, the vast majority remain constrained by the norms of the Friend network. From this perspective, risky behavior is largely

part of the normative performance, as in the dramaturgical model. Teens who engage in risky information sharing are just doing what is expected by their peer network; what one shares, all the rest have to confirm and share in kind. Again, the risk is less in the actual sharing of information, and more in who has access to the shared information.

The developmental psychology model suggests that for teenagers, SNS are one way to experiment with who they are, or more accurately, who they are going to become. Online communication allows these teens to develop their adult selves. The ways teenagers use the internet reflect their feelings of belonging and social connectedness as well. Teens may use the internet to engage with their offline friends and strengthen those existing social connections, or they may seek out new friends online, based on shared interests or a common sense of outsiderness. Here, risky sharing is part of the experimentation process, teens share potentially compromising materials as part of the exploring process – telling strangers who they are is part of telling the world (and by extension, telling themselves) who they are. The real risk is in sharing the wrong information with the wrong individuals.

My theoretical model offers a synthesis of these three disparate approaches. Dramaturgical impression management is the psychologists' self-identity construction. The postmodernist panopticon is the dramaturgist's front-space performance area. The three naturally and logically blend into a single flowing narrative. Teenagers' offline social connectedness will influence their choice of online communication methods, with better connected teens favoring instant messaging and SNS to reinforce their offline networks, and less connected teens preferring chat rooms, blogs, and other creative forms to express themselves and seek out kindred spirits. The types of risk teenagers face, as well as the mediation practices they

use to mitigate that risk, are largely based on the normative culture of different internet communications methods. SNS expect users to share names, photographs, and personal information, whereas chat rooms and message boards offer a greater degree of anonymity. Between these community expectations of privacy and the influence of parental restrictions of online activity, teenagers decide which information to share with the internet and which information to keep private. The risk is in choosing the wrong information to share, and in allowing otherwise harmless information to fall into the wrong hands.

My research model was designed to test the relationships in my theoretical model by applying it to a set of nationally representative data. Respondents with higher levels of offline connectedness would be more likely to use instant messaging and SNS, which are tailor-made for reinforcing offline relationships, while respondents with lower levels of connectedness would be more likely to use chat rooms, blogs, and other creative forms of communication which allow users to seek out online relationships with other users who share their interests.

The Pew Internet and American Life Project data set I utilized for this research only measures respondents' information sharing over SNS, which limited my results somewhat. Within this framework, respondents' self mediation when using SNS would be limited by default to controlling who has access to a profile and the falsification of profile data. Higher levels of self-mediation would lead to lower levels of risky information-sharing on the actual profile. Parental attempts at mediation and respondents' own perceptions of the internet as a risky venue would also serve to lower the sharing of personal data.

After performing an ordered logistic regression on the data, the results were not precisely what I anticipated finding. As far as the relationship between offline network strength and online

communications activity, the most striking result is that respondents, regardless of their offline connections, use the internet in similar ways. This conflicts somewhat with my model, as I suggested that less-connected teens would do more exploration and less reinforcing, while the more connected teens would do less exploring and more reinforcing. While teens that have more offline social connections clearly use the internet to communicate with friends more frequently, they also use the internet to explore their personalities and express themselves online; respondents who were members of school clubs and who reported higher levels of time spent in person with friends had increased likelihoods of using both reinforcing and exploratory communication methods. There was not, as I anticipated, a negative relationship between offline social connections and online exploratory activity. While exploratory communication is not as strongly influenced by offline network strength as reinforcing communication, there is still a positive relationship between the two. Indeed, it seems the more connected teens are offline, the more teens communicate online, period. This is a significant finding in and of itself.

Some of the biggest impacts on online activity were not related to network strength, but user demographics. Indeed, in some cases the demographic variables were actually a stronger predictor of online activities than the network strength variables. Older teens and females were more likely to use reinforcing methods, which tracks well with the existing literature; older teens are given more freedom to use the internet, and females specifically report using the internet to communicate with their offline friends (Lenhart & Madden 2007). Increased levels of household income result in higher levels of exploratory usage, presumably as these respondents have more access or more encouragement to engage in creative endeavors offline as well as online.

Looking at the effects of risk perception and mediation tactics on identity sharing behavior, risk perception appeared to have no real effect on respondents' information sharing, although I believe this is more due to limitations in the data set. Respondents' risk management strategies had only a limited effect on sharing personal information, with profile falsification being more effective than controlling profile access. This follows my theoretical model after a fashion; the nature of the communication method (in this case, SNS) directly influenced the means by which respondents mediate their own experience, with data falsification easier to engage in as opposed to navigating the sometimes complex privacy settings of the major SNS. Respondents whose parents used filtering software to block prohibited websites had lower levels of risky information sharing, as well as those respondents whose parents actively checked their online activities. This is also in keeping with my theoretical model. It also has some major implications for parents and safety advocates, as discussed below.

Finally, the overall relationship between network strength, online communications methods, risk perception, parental and individual mediation techniques on personal information posting behaviors is relatively inconclusive. Demographic factors like parental race, respondent's age, and respondent's sex have as strong a, and in some cases stronger, effect on information sharing than any of the indicators I chose to test for. While this is not what I expected, it is certainly significant. Teenagers with a black parent, boys, and older teens are all at a higher risk for sharing personally identifying information online. The amount of time a respondent spends on a landline telephone speaking with friends actually decreases information sharing. This was the only one of the network strength indicators to test significant against information sharing, and the negative nature of the relationship bears further investigation.

Interestingly, a respondent's level of exploratory or reinforcing behavior has no significant effect on information sharing behavior. Again, not something I expected, but definitely worth investigating further – it would seem risky information sharing via SNS is the same for teens, regardless of their engagement with other communication methods. Parental mediation has a significant effect, specifically in cases where parents check teens' online activity or use filtering software to limit access to unacceptable sites. I would suggest this is due more to parents' active engagement with their children than the actual filters; if a parent filtered an SNS site entirely, a child would have to create and maintain their profile from some other location (or circumvent the filter). Within the options available to respondents to mediate their own experience, respondents who report higher levels of profile falsification have lower levels of risky information sharing. This is perfectly reasonable; if the risky information is fake, it is not truly being shared, is it?

Overall, the final analysis fits my theoretical model reasonably well; offline network strength clearly has an effect on what teens do online. When it comes to SNS, the options available to users have an effect on how they mediate their online risks, and parental mediation methods further influence teens' risk mediation strategies.

Limitations

While my findings are certainly interesting, I have some personal concerns about the effectiveness of my study. Secondary data analysis is never perfect, and this project was no exception. First and foremost, the data set I am using is five years old, and rapid changes in online communication opportunities for teenagers might mean that my research is in some ways already outdated. Indeed, since I started the project Facebook and MySpace both dramatically revamped their security settings (several times, in Facebook's case). When this sample was

gathered, YouTube was barely a year old, and Twitter, now seemingly ubiquitous, did not even exist.[36] By mid-2008, 71% of teens reported owning a cell phone and 58% used text messaging to contact friends – an increase from the 2006 data set I am using (Lenhart 2009). Furthermore, the fastest growing section of Facebook's user base is adults over 35 (Facebook 2009), which does not specifically mean that teenagers are abandoning SNS by any stretch of the imagination, but, if these sites really are seen by adolescents as a private space, the increasing incursion of unwelcome older people may alter younger audiences' use of the sites in as-yet unforeseen ways.

While I am pleased with my findings regarding offline network strength and online activity, I am disappointed that my results did not show more of an influence of teens' perception of the internet as a risk-laden environment, or of teens' own ability to mediate their online experiences. I suspect this is largely due to limitations of the data set. The questions I used to measure risk perception were probably not as effective as I would have liked, while the questions about self mediation only covered identity control techniques – profile falsification, etc. as opposed to situation management – how teens actually deal with stranger contact, bullying, and so forth. Of equal significance, while the data asks extensive questions about time spent on social network sites, reasons for using social network sites, and features used on social network sites, it has considerably less information about other online communication methods. Specifically, the data on identity vulnerability is explicitly limited to those teens with social network profiles, preventing us from doing more than speculating on what forms of identity vulnerability the average teenager might face via instant messaging, chat rooms, personal websites, or other forms of online communication. Despite the shortcomings of the Pew data, it

[36]Recent research suggests that teenagers are less engaged with Twitter than with other communication methods – the Twitter userbase is largely 25-54 with 12-17 year olds a distinct minority (Lenhart 2009).

was the only logical choice for this study. It is nationally representative and broad in scope, including over a thousand U.S. high school students. There is essentially no way I, as a solitary researcher, could have implemented such a study by myself without significant financial and logistical assistance. Working with what I had, however, I feel I came up with some worthwhile results.

Implications for Existing Theory

This project draws from three disparate theoretical traditions, and I believe my results serve as a solid synthesis of all three schools. First, my research strongly reinforces the Goffman-based dramaturgical interpretations of online identity work. SNS are obviously powerful agents for impression management; users have massive amounts of control over what aspects of their lives are put on display, and with improved security settings, extensive control over who has access to that display. The respondents in the Pew study clearly use SNS in this way – their choices over whether or not to share personal information reflect their desires to control their online presence.

Once again, unwanted viewers serve as 'outsiders' in Goffman's terminology, and teenage SNS users use multiple methods to prevent such outsiders from accessing their profiles, which are a performance they were not meant to witness. Profile falsifications, as well as setting a profile to “Friends Only” both serve to restrict access to a designated subset of the SNS population. In essence, SNS security settings and their use are a means of separating a Goffmanesque back space (the profile itself) from the front space (the school or work environment). Friends who are granted access, meanwhile, are privy to the carefully constructed performance that is a SNS profile. Every choice about what appears on a user’s profile is a

calculated step in the process of impression management. Even the risky information that is shared serves to support this performance; as a real name or photograph can serve as verification of a performance, so can selectively falsified information. For SNS users, the risk is simply part of the protocol: how can you prove you are who you claim to be without the pertinent data?

My results also strongly support and inform the postmodern theory that SNS serve as a form of surveillance. SNS, especially in the early stages depicted in the Pew data, are open spaces for observation. By generating a profile, users offer themselves up for observation by a network of peers, colleagues, and even strangers. Information sharing here, as with the dramaturgical model, is a necessary part of the SNS activity. The vast majority of profiles/performances are normative: users post real names, photographs, and other identifying information as a simple matter of protocol. Profiles that lack identifying data will be policed by the peer group, and users bombarded with requests to add the pertinent material. Friend-setting and other controls seem to simply reinforce the panoptic relationship; limiting access means that only the chosen can participate, but those that do have essentially free reign. A user sees what all their Friends are up to, and can freely comment on, post to, and police their Friend networks. The catch is that the Friend network can comment, post, and police the user's performance in kind. This opens the user up to bullying, stranger contact, and all the other risks that come with internet communication.

As for the developmental psychological literature, there are two key models of online activity. In the "rich get richer" model, teenagers who are popular or socially well-connected benefit from using the internet to enhance and reinforce their offline relationships. The "social compensation" model suggests that teenagers who are less popular or socially awkward turn to

online communication to find new friends or experiment with social connections that they lack offline. My research effectively supports the rich get richer model; respondents with high levels of offline social activity have higher levels of reinforcing usage. On the other hand, the results for the social compensation model are much more inconclusive – the higher a respondent's level of offline social activity, the higher their level of exploratory behavior. This suggests that even the "popular" or "non-lonely" teens use exploratory methods. However, there is an obvious limitation of the data set at work here; we only know that the respondents are using these communication methods; we do not know *why*. It is also reasonable to point out that measuring participation in offline social activity does not necessarily measure an individual's feelings of loneliness.

Implications for Policy Makers

This study clearly demonstrates how the potential for identity risk is indeed there on teens' SNS profiles, and presumably in other vectors for identity work. Teens regularly post personally identifying information, photographs of themselves, and contact information that could be accessed by stalkers, scammers, or bullies. The recent media attention towards the suicides of gay teens that were harassed by classmates both in person and online demonstrates just one potential problem; when physical violence isn't an option, Facebook is. As this is being written, several states are considering laws that would criminalize certain acts of bullying, including online harassment, and New Jersey recently instituted a set of anti-bullying statutes that have been alternately lionized and criticized as too draconian. (Bazelon 2011; Allen 2011) These laws raise serious legal concerns – at what point does Facebook bullying become criminal activity? What rights do the targets of online harassment have? What is the responsibility of the

communications service to inhibit these now-criminal activities? These questions are beyond the scope of my research, but declaring being hateful on the Internet to be an actual crime could set some very disturbing First Amendment precedents.

That being said, online content providers cannot be trusted to self-regulate. The entire business model of SNS is to gather as much information on their users as possible, with an eye towards using that information to lure in more users, who will then share their own information, and so on in a sort of "information snowball." All of those users can then be bombarded with advertisements specifically targeted to their likes, dislikes, hobbies, and interests. Besides serving as a draw for advertising space, users' personal information can itself be monetized – a typical SNS profile contains valuable demographic information that advertisers and marketers would pay significant amounts of money for. While Facebook, MySpace, and other SNS have made great strides in improving their privacy policies, at the end of the day the questions of what to share and how to share it remain up to the individual user, and much of the truly risky information is part of the normative SNS experience. Removing last names, photographs, and hometowns from profiles effectively removes the entire point of SNS. As such, simply attempting to regulate information sharing on SNS through legal channels seems less-than-feasible. The most reasonable means of preventing teens from engaging in risky online behaviors would be to educate teens directly. Here we strike the same wall that parents face; how do we convince teenagers that any group of adults are worth listening to? One potential vector for this sort of engagement would be working in concert with SNS themselves to publicize the availability of privacy and security settings. As discussed above, SNS have a vested interest in keeping information free-flowing, as it is a primary source of advertising

revenue. Essentially, bad publicity may be the most likely way to encourage SNS to enact more rigorous privacy protocols; the companies probably will have to be badgered by parents, teachers, law enforcement, and (most significantly) the media into making any dramatic changes.

Even with the popularity of shock-and-horror programming like "To Catch a Predator," campaigns using similar scenarios are probably not the best approach to educating teens about online risks. Encouraging teens to be careful when solicited by strangers does little to prevent solicitation by peers (or "near-peers" such as 18-25 year olds), given that the majority of online sexual solicitation appears to come from other teenagers and young adults (Wolak Mitchell & Finkelhor 2006). Much of this online solicitation is simply a digital version of the coercion that would normally take place in other "back-space" areas of teenage life; bedrooms, back seats of cars, and so forth. As such, trying to frame the problem as "creepy old men" stalking hapless young teens is both short-sighted and a disservice to the very audience we are trying to protect. Any advertising campaign targeted at informing teenagers about the risks of online activity would have to be realistic about the hazards teens face, and take into account their own rationales for being online in the first place.

Another vector for creating positive changes in teenagers' risky internet behaviors could come through the educational system. Many middle and high school students in the U.S. now have the opportunity to take various computer-related courses, and basic internet/SNS safety could readily become a component of those programs. In 2007, Virginia became the first state in the U.S. to require internet safety classes in public schools, and starting in 2011, internet safety became a mandatory part of the UK primary school curriculum (Hochberg 2007, Fildes 2009). Groups like the National Center for Missing and Exploited Children, WebWiseKids, and the U.S.

Attorney General's Office all provide a variety of resources for teachers to use in the classroom, and some even offer full curricula suitable for students in primary, middle, or high school. Adapting these for use on a system-wide level would not be a particularly difficult task. Even then, the fundamental problem with any safety education, whether it be driving safety or safe sex or drug abuse education, is that the materials often consist of a great many cautions and platitudes that some teenagers follow faithfully, some half-heartedly accept, and others reject outright. Clearly, the educational system has a role to play in internet safety education, but they cannot be expected to carry the majority of the burden.

Implications for Parents

On one level, parents need to trust their teenagers. The vast majority seem to know what they are doing, and are navigating SNS just fine. When they are contacted inappropriately, they block the stranger or report it to the appropriate authorities. Most of the images and comments they post are relatively harmless adolescent nonsense. Essentially, the negative actions of a minority are driving much of the moral outrage surrounding teenage internet use. It is entirely possible that as the Facebook generation comes of age and moves into positions of responsibility and power in society, the behaviors that terrify today's parents will be seen as "youthful indiscretions" in essentially the same way that those parents look back on their own equally irresponsible teenage experimentation.

That does not mean that parents do not need to be concerned. While these behaviors may be normal (or at least normative), parents and other authority figures still have a vested interest in protecting teenaged internet users, especially when SNS themselves have little financial reason to do so. Personal information, after all, is essentially their product. My results suggest

that parental mediation can be an effective deterrent to some forms of teenage internet risk, but the mediation must be active. Simply telling teens where they can and cannot go online is largely useless. It is important to note that parents' rule-setting behavior had almost no effect on what respondents posted to their profiles. The most effective techniques are those where a parent is directly involved in the mediation process – checking a teenager's usage habits to see what they have been up to, or using filtering software to block certain sites entirely. While I personally believe the latter to be untenable, as teens will simply find other ways to access forbidden information (e.g. from school, a friend's house, or a smartphone), the broader message is clear – internet safety education needs to begin as soon as children are exposed to the internet.

Parents must become internet-savvy if they are to have any hope of mediating their teens' online activities. Parents need to familiarize themselves with the various means of communication and their unique characteristics, and become as comfortable with the internet as their teens are. If rule-setting behaviors are used, teens must be made aware of the rules, and the rules must be enforced. If a parent tells a child certain sites or activities are forbidden, the parent must have some way to back that claim, whether by actively checking where the child has been or by using software to block those sites/activities whole cloth.[37] You cannot simply tell teenagers not to do something – they are teenagers!

Areas for Future Study

Overall, I am happy with the results of my research, but I feel there is still room for improvement. Going forward, investigations into this topic need to use specifically gathered

[37]A waggish suggestion would be for parents to join the SNS their child uses and Friend their teenager. While it is certainly possible for teens to block their parents from viewing their shared information, at the very least that would require the teenager to actively engage with their SNS's safety and privacy settings. It also might drive the child from the service entirely.

data, rather than adapting an existing survey. Were I gathering such a data set, there are quite a few things I would do differently. A more in-depth survey instrument, with specific questions about risky activities – not just "have you ever posted photographs to your profile" but "have you ever posted pictures of something illegal or unsafe to your profile" or "have you ever posted photographs of yourself or your friends in a swimsuit or underwear to your profile?" I would focus on the ways teens mediate their online experiences, focusing on sexual contact, posting of personal data, and bullying. How do teens deal with these situations when they come up online? How do they avoid them in the first place? I would ask more questions about the relationships teens have online – how many SNS Friends do they have? How many people are on their instant messaging contact lists? Who are these Friends and how often do they interact? I would also ask about risky communication via other CMC vectors – chat rooms, instant messaging, chat rooms, and so forth.

Broader research into adolescent internet activity can go in multiple directions. I would like to investigate both parents' and teens' perceptions of internet risk – if they see the internet as risky, where did those concepts come from? The media, peer groups, or safety advocates? Do existing prevention methods actually help teens negotiate the internet? A focused study of teenagers' awareness and deployment of online safety features would be worthwhile – do teens know what privacy settings are available on SNS, and do they actually utilize them? How is knowledge of privacy options transmitted – through announcements by the SNS themselves or via the all-too-common panicked chain forward of the "hackers broke into facebook/facebook is going to start charging users/selling user data to the chinese" variety?[38] I am also interested in

[38] These generally end up being hoaxes, although occasionally useful information can be disseminated in this manner (Mikkelson & Mikkelson 2011)

the particular finding that respondents with Black parents have a higher likelihood of risky information sharing over SNS. A targeted study of Black teens, their parents, and internet usage would help understand why this audience is particularly at risk.

I would also be interested in studying the reasons and ways in which teens use other online communication methods, particularly online video. In addition to further exploration of why teens use SNS, an investigation of teenagers who do not use SNS and their motives for staying disconnected would be fascinating. I would also be interested in studying teens' immersion in other media; time spent watching television, time spent listening to music, etc. as a way of returning to the line of questioning that led to this research in the first place.

In closing, a story that I hope displays the challenges of SNS; in early 2011 an Indiana woman created a Facebook account claiming to be a 17-year-old girl in hopes of gaining incriminating information about her ex-husband. The ex-husband proceeded to tell the presumed teenager that he was planning to kill his ex-wife and their children, and expressed interest in hiring an assassin. When the ex-wife handed transcripts of the conversations over to the FBI looking to have him arrested, the man provided a notarized statement, signed before he accepted the false account's Friend request, that he suspected the fake account was his ex-wife, and that he had lied to her in order to incriminate *her* in their ongoing child custody case. All charges against the man were dropped. (thesmokinggun.com 2011) Perhaps instead of being concerned with children acting too much like adults, our real problem is adults acting too much like children.

A Chili Recipe, Just To See If Anyone Ever Reads This:

- 1.5 lbs ground meat of choice
- 1-2 cans tomato sauce
- 1 can diced tomatoes (with or without peppers)
- 2 cans beans, your choice
- 1/2 onion, chopped
- 1/2 bell pepper, chopped
- 3 cloves garlic, minced
- 1 can corn niblets (optional)
- Pinch of brown sugar
- Splash of beer
- CHILI SEASONING:
- 1 tsp dried basil
- 2 tsp white sugar
- 2 tsp cumin
- 4 tsp chili powder
- 1 tbsp onion powder
- 1 tbsp red pepper (or to taste)
- 1 tbsp garlic powder
- 2 tbsp flour
- Salt

Brown beef in a skillet. Drain corn and beans, combine all canned ingredients in dutch oven or crock pot. Drain fat from beef, add to pot. Saute all vegetables in oil, add to pot. Add seasoning mix to pot. Add brown sugar and beer. Bring to a boil. Let simmer until you are too hungry to continue simmering.

REFERENCES

Acquisti, Alessandro and Ralph Gross. 2006. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook." Presented at the Privacy Enhancing Technologies Workshop, June 28-30, Cambridge, United Kingdom.

------. 2009. "Predicting Social Security Numbers from Public Data." *Proceedings of the National Academy of Sciences of the United States of America,* 106(27):10975-10980.

Allen, Jonathan. 2011. "Bill to crack down on cyber-bullies introduced in New York." Reuters, September 26. Retrieved October 7, (http://www.reuters.com/article/2011/09/26/us-newyork-cyberbully-idUSTRE78P6F820110926).

Barker, Rachel. 2008. "Presentation of the Virtual Beyond-Self on Cyber Stage: Real, Constructed, Staged and/or Masked?" *Communicatio: South African Journal for Communication Theory & Research,* 34(2):189-210.

Barnes, Susan B. 2006. "A Privacy Paradox: Social Networking in the United States." *First Monday,* 11(9).

Battaglia, Michael, David Izrael, David Hoaglin, and Martin Frankel. 2004a. "Tips and Tricks for Raking Survey Data (A.K.A. Sample Balancing)." Presented at the Annual Meeting of the American Association for Public Opinion Research, May 13, Phoenix, Arizona.

-----. 2004b. "Practical Considerations in Raking Survey Data." Presented at the Annual Meeting of the American Association of Public Opinion Research, May 13, Phoenix, Arizona.

Battaglia, Michael, Meg Ryan, and Marcie Cynamon. 2005. "Purging out-of-Scope and Cellular Telephone Numbers from RDD Samples." Presented at the Annual Conference of the American Association for Public Opinion Research, May 12-15, Miami Beach, Florida.

Bazelon, Emily. 2011. "Anti-Bullying Laws Get Tough With Schools." *Weekend Edition*, National Public Radio, September 17. Retrieved October 7, (http://www.npr.org/2011/09/17/140557573/anti-bullying-laws-get-tough-with-schools).

Blumberg, Stephen and Julian Luke. 2009. "Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, July-December 2008." National Center for Health Statistics, May 6. Retrieved August 3, 2009, (www.cdc.gov/nchs/data/nhis/earlyrelease/wireless200905.htm).

Booth, Paul. 2008. "Rereading Fandom: MySpace Character Personas and Narrative Identification." *Critical Studies in Media Communication,* 25(5):514-536.

Borsboom, Denny, Gideon J. Mellenbergh, and Jaap van Heerden. 2003. "The Theoretical Status of Latent Variables." *Psychological Review,* 110(2):203-219.

Boyd, Brian. 2006a. "Insane Clown Posse Separates Music, Violence" *SouthCoastToday.com*, February 9. Retrieved August 10, 2009, (www.southcoasttoday.com/apps/pbcs.dll/article?AID=/20060209/NEWS/70302026/-1/SPECIAL06).

boyd, danah. 2006b. "Friends, Friendsters, and Top 8: Writing Community into Being on Social Network Sites." *First Monday,* 11(12).

------. 2007. "Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life." in *Macarthur Foundation Series on Digital Learning - Youth, Identity, and Digital Media Volume*, edited by David Buckingham. Cambridge, MA: MIT Press.

------. 2008. "Facebook's Privacy Trainwreck." *Convergence: The Journal of Research into New Media Technologies,* 14(1):13-20.

------. 2009, "Would the Real Social Network Please Stand Up?" *apophenia*, July 28. Retrieved August 11, 2009 (www.zephoria.org/thoughts/archives/2009/07/28/would_the_real.html).

------. 2010, "Facebook's Move Ain't About Changes in Privacy Norms" *apophenia,* January 16. Retrieved January 20, 2010 (http://www.zephoria.org/thoughts/archives/2010/01/16/facebooks_move.html).

boyd, danah and Nicole B. Ellison. 2007. "Social Network Sites: Definition, History and Scholarship." *Journal of Computer-Mediated Communication,* 13(1):11.

CareerBuilder.com. 2006. "One-in-Four Hiring Managers Have Used Internet Search Engines to Screen Job Candidates; One-in-Ten Have Used Social

Networking Sites, Careerbuilder.com Survey Finds" *CareerBuilder.com*, October 26. Retrieved June 22, 2009, (www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr331&sd=10/26/2006&ed=12/31/2006&siteid=cbpr331&sc_cmp1=cb_pr331_).

Clark, Sarah. 2009. "Police Use Facebook to Identify Weapon Carriers" *The Journal (Edinburgh)*, February 11. Retrieved June 22, 2009 (www.journal-online.co.uk/article/5410-police-use-facebook-to-identify-weapon-carriers).

clickondetroit.com. 2008. "Campus Killer Speaks out on YouTube" *clickondetroit.com*, April 13. Retrieved June 14, 2009, (www.clickondetroit.com/news/19165557/detail.html).

Dark Lotus [musical group]. 2004. "Pass the Ax." On *Black Rain* [CD]. Royal Oak, MI: Psychopathic Records, 4024.

Derk, Daantje, Arjan E. R. Bos, and Jasper von Grumbkow. 2008. "Emoticons in Computer-Mediated Communication: Social Motives and Social Context." *CyberPsychology & Behavior,* 11(1):99-102.

DiSpirito, Lauren. 2010. "Macon Chef Victim of Internet Scam" *13WMAZ.com,* February 24. Retrieved February 25, 2010 (http://www.13wmaz.com/news/local/story.aspx?storyid=75444&catid=153).

Dominick, Joseph R. 1999. "Who Do You Think You Are? Personal Home Pages and Self-Presentation on the World Wide Web." *Journalism & Mass Communication Quarterly,* 76(4):646-669.

Donath, Judith and danah boyd. 2004. "Public Displays of Connection." *BT Technology Journal,* 22(4):71-82.

Driscoll, Alison. 2009, "Facebook Fail: How to Use Facebook Privacy Settings and Avoid Disaster" *Mashable.com*, April 28. Retrieved August 20, 2009, (http://mashable.com/2009/04/28/facebook-privacy-settings/).

Eastin, Matthew S., Bradley S. Greenberg, and Linda Hofschire. 2006. "Parenting the Internet." *Journal of Communication,* 56(3):486-504.

Edwards, Jeffrey and Richard Bagozzi. 2000. "On the Nature and Direction of Relationships between Constructs and Measures." *Psychological Methods,* 5(2):155-174.

Ellison, Nicole B., Charles Steinfield, and Cliff Lampe. 2007. "The Benefits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network Sites." *Journal of Computer-Mediated Communication,* 12(4):1143-1168.

Erikson, Erik. 1963. *Childhood and Society*. New York: W.W. Norton & Company.

facebook.com. 2009a. "Press Room: Statistics". Retrieved September 2, 2009 (http://www.facebook.com/press/info.php?statistics).

------. 2009b. "Statement of Rights and Responsibilities", August 28. Retrieved January 20, 2010 (http://www.facebook.com/terms.php?ref=pf).

Fildes, Jonathan. 2009. "Internet Safety for Children Targeted." *BBC News*, December 8. Retrieved November 3, 2011, (http://news.bbc.co.uk/2/hi/technology/8398763.stm).

Finkelstein, Seth. 2008, "How Will Wikia Cope When the Workers All Quit the Plantation?" *Read me first,* July 31. Retrieved January 20, 2010 (http://www.guardian.co.uk/technology/2008/jul/31/wikipedia).

Fowler, Floyd J. 2009. *Survey Research Methods*. 4th Edition. Thousand Oaks, CA: SAGE Publications, Inc.

Friedman, Sarah L. 2007. "Finding Treasure: Data Sharing and Secondary Analysis in Developmental Science." *Journal of Applied Developmental Psychology,* 28(5-6):384-389.

Gibbs, Jennifer L., Nicole B. Ellison, and Rebecca D. Heino. 2006. "Self-Presentation in Online Personals: The Role of Anticipated Future Interaction, Self-Disclosure, and Perceived Success in Internet Dating." *Communication Research,* 33(2):152-178.

Goffman, Erving. 1959. *The Presentation of Self in Everyday Life*. New York: Doubleday.

Goldsmith, Samuel and Clemente Lisi. 2008. "Palin Admits Her 17-Year-Old Daughter Is Pregnant" *New York Post,* September 1. Retrieved June 14, 2009, (www.nypost.com/seven/09012008/news/nationalnews/palin_admits_her_17_year_old_daughter_is_127025.htm).

Harvey, Kevin James, Brian Brown, Paul Crawford, Aidan Macfarlane, and Ann McPherson. 2007. "'Am I Normal?' Teenagers, Sexual Health and the Internet." *Social Science & Medicine,* 65(4):771-781.

Hinduja, Sameer and Justin W. Patchin. 2008. "Personal Information of Adolescents on the Internet: A Quantitative Content Analysis of MySpace." *Journal of Adolescence,* 31(1):125-146.

Hochberg, Adam. 2007. "Back to School: Reading, Writing, and Internet Safety." *Morning Edition*, National Public Radio, September 17. Retrieved November 3, 2011. (http://www.npr.org/templates/story/story.php?storyId=14427020).

Hoy, Mariea G. and Joseph Phelps. 2003. "Consumer Privacy and Security Protection on Church Websites: Reasons for Concern." *Journal of Public Policy and Marketing,* 22(1):58-70.

Huffaker, David. 2006. "Teen Blogs Exposed: The Private Lives of Teens Made Public." Presented at the Annual Meeting of the American Association for the Advancement of Science, February 16-19, St. Louis, MO.

Internet Safety Technical Task Force. 2008. "Enhancing Child Safety & Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States." Boston: The Berkman Center for Internet & Society at Harvard University, December 31. Retrieved May 10, 2009, (cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf).

Jagatic, Tom N., Nathaniel A. Johnson, Markus Jakobsson, and Filippo Menczer. 2007. "Social Phishing." *Communications of the ACM,* 50(10):94-100.

Jakobsson, Markus and Steven Myers. 2006. *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*. Hoboken, NJ: Wiley-Interscience.

James, Daniel, Gordon Walton, David Kennerly, Nova Barlow, George Dolbier, and Justin Quimby. 2004. "2004 Persistent Worlds Whitepaper." International Game Developers Association. Retrieved July 30, 2009, (www.igda.org/online/IGDA_PSW_Whitepaper_2004.pdf).

"Jeanne & Erika". 2009. *Oh Crap. My Parents Joined Facebook*, September 3. Retrieved August 30, 2009, (www.myparentsjoinedfacebook.com).

Johnson, Bobbie. 2010. "Privacy No Longer a Social Norm, Says Facebook Founder" *The Guardian,* January 11, 2010. Retrieved January 17, 2010 (http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy).

Jones, Steve, Sarah Millermaier, Mariana Goya-Martinez, and Jessica Schuler. 2008. "Whose Space Is MySpace? A Content Analysis of MySpace Profiles." *First Monday,* 13(9).

Kane, Carolyn M. 2008. "I'll See You on MySpace: Self-Presentation in a Social Network Website." M.A. Thesis, College of Liberal Arts and Social Sciences, Cleveland State University, Cleveland, OH.

Keeter, Scott, Courtney Kennedy, Michael Dimock, Jonathan Best, and Peyton Craighill. 2006. "Gauging the Impact of Growing Nonresponse on Estimates from a National RDD Telephone Survey." *Public Opinion Quarterly,* 70(5):759-779.

Keller, Sarah, Lori Rosenthal, and Paul Rosenthal. 2005. "A Comparison of Pro-Anorexia and Treatment Web Sites: A Look at the Health Believe and Stages of Change Models Online." Presented at the Annual Meeting of the International Communication Association, May 26-30, New York.

Kiecolt, K. Jill and Laura E. Nathan. 1985. *Secondary Analysis of Survey Data*. Newbury Park, CA: SAGE.

Kinkaid, Jason. 2009, "Spammers Running Wild in Latest MySpace Phishing Attack" *TechCrunch*, July 20. Retrieved August 1, 2009, (www.techcrunch.com/2009/07/20/spammers-running-wild-in-latest-myspace-hack/).

Kleck, Christine, Christen Reese, Dawn Ziegerer-Behnken, and S. Shyam Sundar. 2007. "The Company You Keep and the Image You Project: Putting Your Best Face Forward in Online Social Networks." Presented at the Annual Meeting of the International Communication Assocation, May 23, San Fransisco, CA.

Kulp, Dale. 2004. "Meeting the Challenges of the TCPA and the FCC Telecommunications Act: Development of a Process to Identify Landlines Ported to Cellular Service." Presented at the the Joint Statistical Meeting, August 8-12, Toronto, Canada.

Lenhart, Amanda. 2009a. "It's Personal: Similarities and Differences in Online Social Network Use between Teens and Adults." Washington DC: Pew Internet & American Life Project, May 23. Retrieved June 15, 2009,

(www.pewInternet.org/Presentations/2009/19-Similarities-and-Differences-in-Online-Social-Network-Use.aspx).

------. 2009b. "Teens and Social Media: An Overview." Washington DC: Pew Internet & American Life Project, April 10. Retrieved June 22, 2009, (www.pewinternet.org/Presentations/2009/17-Teens-and-Social-Media-An-Overview.aspx).

Lenhart, Amanda and Mary Madden. 2007. "Teens, Privacy & Online Social Networks: How Teens Manage Their Online Identities and Personal Information in the Age of MySpace." Washington DC: Pew Internet & American Life Project, April 18. Retrieved August 10, 2009, (pewinternet.org/~/media//Files/Reports/2007/PIP_Teens_Privacy_SNS_Report_Final.pdf.pdf).

Levenson, Michael. 2006. "Manhunt for Teen Ends in Mayhem" *The Boston Globe*, February 5. Retrieved August 10, 2009, (www.boston.com/news/nation/articles/2006/02/05/manhunt_for_teen_ends_in_mayhem/).

Liau, Albert Kienfie, Angeline Khoo, and Ang Peng Hwa. 2005. "Factors Influencing Adolescents' Engagement in Risky Internet Behavior." *CyberPsychology & Behavior,* 8(6):513-520.

Livingstone, Sonia. 2008. "Taking Risky Opportunities in Youthful Content Creation: Teenagers' Use of Social Networking Sites for Intimacy, Privacy and Self-Expression." *New Media & Society,* 10(3):393-411.

Livingstone, Sonia and Ellen J. Helsper. 2008. "Parental Mediation of Children's Internet Use." *Journal of Broadcasting & Electronic Media,* 52(4):581-599.

Lo, Shao-Kang. 2008. "The Nonverbal Communication Functions of Emoticons in Computer-Mediated Communication." *CyberPsychology & Behavior,* 11(5):595-598.

Long, J. Scott. 1997. *Regression Models for Categorical and Limited Dependent Variables*. Thousand Oaks, CA: SAGE Publications, Inc.

Lupia, Arthur and Tasha S. Philpot. 2005. "Views from inside the Net: How Websites Affect Young Adults' Political Interest." *Journal of Politics,* 67(4):1122-1142.

Mantella, Dana. 2007. ""Pro-Ana" Web-Log Uses and Gratifications: Towards Understanding the Pro-Anorexia Paradox." M.A. Thesis, College of Arts and Sciences, Georgia State University, Atlanta, GA.

Mastronardi, Maria. 2003. "Policing Dis-Order: Moral Panic and Pro-Ana Citizenship." Presented at the Annual Meeting of the International Communication Association, May 23-27, San Diego, CA.

McMillan, Robert. 2007. "Typosquatter Fined Again by FTC" *Networkworld.com*, October 16. Retrieved June 23, 2009 (www.networkworld.com/news/2007/101607-porn-typosquatter-fined-again-by.html).

McMillan, Robert. 2011. "Man Stole Nude Photos from Women's E-Mail Accounts", January 13. Retrieved June 22, 2011 (http://www.pcworld.com/businesscenter/article/216734/man_stole_nude_photos_from_womens_email_accounts.html#tk.mod_rel).

McMillan, Robert. 2011. "Police: Man Stole Nude Photos from Hacked E-Mail Accounts" IDG News Service, June 4. Retrieved June 22, 2011 (http://www.pcworld.com/businesscenter/article/229414/police_man_stole_nude_photos_from_hacked_email_accounts.html).

Merkle, Daniel and Gary Langer. 2008. "How Too Little Can Give You Too Much: Determining the Number of Household Phone Lines in RDD Surveys." *Public Opinion Quarterly,* 72(1):114-124.

Mesch, Gustavo S. and Ilan Talmud. 2007. "Similarity and the Quality of Online and Offline Social Relationships among Adolescents in Israel." *Journal of Research on Adolescence (Blackwell Publishing Limited),* 17(2):455-465.

Mikkelson, Barbara and David P. Mikkelson. 2011. “Facebook” *Snopes.com Urban Legends Reference Pages*. Retrieved November 5, 2011 (http://www.snopes.com/computer/facebook/facebook.asp)

Milne, George R., Andrew J. Rohm, and Shalini Bahl. 2004. "Consumers' Protection of Online Privacy and Identity." *Journal of Consumer Affairs,* 38(2):217-232.

Mitchell, Kimberly J., Janis Wolak, and David Finkelhor. 2008. "Are Blogs Putting Youth at Risk for Online Sexual Solicitation or Harassment?" *Child Abuse & Neglect,* 32(2):277-294.

Montaquila, Jill, John Michael Brick, and Shelley Brock Roth. 2003. "Identifying Problems with Raking Estimators." Presented at the Annual Meeting of the American Statistical Association, July 31-June 7, Alexandria, Virginia.

Moreno, Megan A., Malcolm R. Parks, Frederick J. Zimmerman, Tara E. Brito, and Dimitri A. Christakis. 2009a. "Display of Health Risk Behaviors on MySpace by Adolescents: Prevalence and Associations." *Archives of Pediatrics & Adolescent Medicine,* 163(1):27-34.

Moreno, Megan A., Ann VanderStoep, Malcolm R. Parks, Fredrick K. Zimmerman, Ann Kurth, and Dimitri A. Christakis. 2009b. "Reducing at-Risk Adolescents' Display of Risk Behavior on a Social Networking Web Site: A Randomized Controlled Pilot Intervention Trial." *Archives of Pediatrics & Adolescent Medicine,* 163(1):35-41.

Moscardelli, Deborah M. and Richard Divine. 2007. "Adolescents' Concern for Privacy When Using the Internet: An Empirical Analysis of Predictors and Relationships with Privacy-Protecting Behaviors." *Family & Consumer Sciences Research Journal,* 35(2):232-252.

National Institute of Health. 2003. "NIH Data Sharing Policy and Implementation Guidance." Washington DC: National Institute of Health, March 5. Retrieved September 2, 2009, (grants.nih.gov/grants/policy/data_sharing/data_sharing_guidance.htm).

Nauert, Heather. 2007. "Teachers Need to Practice Good Judgment" *Fox News*, October 9. Retrieved May 20, 2009, (www.foxnews.com/story/0,2933,300417,00.html).

Nurmi, Jari-Erik. 2004. "Socialization and Self-Development: Channeling, Selection, Adjustment and Reflection." Pp. 85-124 in *Handbook of Adolescent Psychology, 2nd Ed.*, edited by R.M. Lerner & L. Steinberg. Hoboken, NJ: John Wiley & Sons.

Ostrow, Adam. 2009. "Facebook Dating Ad Hooks up Married Man... With His Wife" *Mashable.com,* July 17. Retrieved August 20, 2009, (mashable.com/2009/07/17/facebook-dating-ads-2/).

Papacharissi, Zizi. 2002. "The Presentation of Self in Virtual Life: Characteristics of Personal Home Pages." *Journalism & Mass Communication Quarterly,* 79(3):643-660.

------. 2004. "The Blogger Revolution? Audiences as Media Producers." Presented at the the Annual Meeting of the International Communication Association, May 27-31, New Orleans, LA.

Paul, Ian. 2009. "5 Things to Know About Facebook's New Settings" *MSNBC.com,* December 10. Retrieved December 31, 2009, (http://www.msnbc.msn.com/id/34365455/ns/technology_and_science-tech_and_gadgets/).

Perez, Erica. 2007. "Getting Booked by Facebook" *The Milwaukee-Wisconsin Journal Sentinel*, October 3. Retrieved July 30, 2009, (www.jsonline.com/news/milwaukee/29260684.html).

Peter, Jochen, Patti M. Valkenburg, and Alexander P. Schouten. 2005. "Characteristics and Motives of Adolescents Talking with Strangers on the Internet and Its Consequences." Presented at the Annual Meeting of the International Communication Association, May 26, New York.

Pew Internet and American Life Project. 2006. "November 2006 - Parents & Teens." Washington DC: Pew Internet and American Life Project, November 19. Retrieved December 20, 2008, (pewinternet.org/Shared-Content/Data-Sets/2006/November-2006—Parents-and-Teens.aspx).

Pew Research Center for People & the Press. 2006. "The Cell Phone Challenge to Survey Research." Washington DC: Pew Research Center for People & the Press, May 15. Retrieved August 2, 2009, (people-press.org/report/276/).

Preibusch, Sören, Bettina Hoser, Seda Gürses, and Bettina Berendt. 2007. "Ubiquitous Social Networks - Opportunities and Challenges for Privacy-Aware User Modelling." Presented at the Data Mining for User Modelling Workshop at the the 11th International Conference on User Modeling, June 25-29, Corfu, Greece.

Quintelier, Ellen and Sara Vissers. 2008. "The Effect of Internet Use on Political Participation: An Analysis of Survey Results for 16-Year-Olds in Belgium." *Social Science Computer Review,* 26(4):411-427.

Retelas, George. 2008. "Anonymity and Self-Disclosure on MySpace." M.S. Thesis, School of Journalism & Mass Communications, San Jose State University, San Jose, CA.

Rheingold, Howard. 1995. *The Virtual Community: Finding Connection in a Computerized World*. London: Secker & Wargurg.

Richmond, Riva. 2009, "More Facebook Phishing Trouble" *Gadgetwise,* May 14. Retrieved August 1, 2009, (gadgetwise.blogs.nytimes.com/2009/05/14/more-facebook-phishing-trouble/).

Ricker, Amanda. 2009. "City Requires Facebook Passwords from Job Applicants" *The Bozeman Daily Chronicle,* June 18. Retrieved August 18, 2009, (bozemandailychronicle.com/articles/2009/06/19/news/10socialnetworking.txt).

Robida, Jacob. 2006. "www.myspace.com/jakejekyll" *MySpace.com*, February 1. Retrieved August 10, 2009, (photos.imageevent.com/revolution/myspace/www_myspace_com-jakejekyll.htm (archived version)).

Rosen, Larry D., Nancy A. Cheever, and L. Mark Carrier. 2008. "The Association of Parenting Style and Child Age with Parental Limit Setting and Adolescent MySpace Behavior." *Journal of Applied Developmental Psychology,* 29(6):459-471.

Sales, Esther, Sara Lichtenwalter, and Antonio Fevola. 2006. "Secondary Analysis in Social Work Research Education: Past, Present, and Future Promise." *Journal of Social Work Education,* 42(3):543-558.

Schau, Hope Jensen and Mary C. Gilly. 2003. "We Are What We Post? Self-Presentation in Personal Web Space." *Journal of Consumer Research,* 30(3):385-404.

Schnitt, Barry. 2009, "Debunking Rumors About Advertising and Photos" *The Facebook Blog,* July 24. Retrieved August 20, 2009, (blog.facebook.com/blog.php?post=110636457130).

Schouten, Alexander P., Patti M. Valkenburg, and Jochen Peter. 2007. "Precursors and Underlying Processes of Adolescents' Online Self-Disclosure: Developing and Testing An "Internet-Attribute-Perception" Model." *Media Psychology,* 10(2):292-315.

Schroeder, Stan. 2008, "MySpace Launches Profile 2.0. No, You Don't Have to Switch" *Mashable.com*, November 10. Retrieved August 20, 2009, (http://mashable.com/2008/11/10/myspace-profile-2o/).

Sessions, Lauren. 2009. ""You Looked Better on MySpace": Deception and Authenticity on the Web 2.0." *First Monday,* 14(7).

Shuman, Phil. 2007. "Fox 11 Investigates: 'Anonymous'." *FOX News at 11* (Television broadcast). July 26, Los Angeles, KTTV-TV.

Staksrud, Elisabeth and Sonia Livingstone. 2009. "Children and Online Risk." *Information, Communication & Society,* 12(3):364-387.

Steinfield, Charles, Nicole B. Ellison, and Cliff Lampe. 2008. "Social Capital, Self-Esteem, and Use of Online Social Network Sites: A Longitudinal Analysis." *Journal of Applied Developmental Psychology,* 29(6):434-445.

Stern, Susannah. 2003. "Gender Differences in the Style and Substance of Adolescents' Personal Home Pages." Presented at the Annual Meeting of the International Communication Association, May 23-27, San Diego, CA.

Stirland, Sarah Lai. 2008. "MySpace Page Provides Tabloids a Peek at Palin Daughter's Beau" *Wired*, September 2. Retrieved June 14, 2009, (www.wired.com/threatlevel/2008/09/myspace-page-pr/).

Strano, Michele M. 2008. "User Descriptions and Interpretations of Self-Presentation through Facebook Profile Images." *Cyberpsychology: Journal of Psychosocial Research on Cyberspace,* 2(2):article 5.

Subrahmanyam, Kaveri and Gloria Lin. 2007. "Adolescents on the Net: Internet Use and Well-Being." *Adolescence,* 42(168):659-677.

Subrahrnanyam, Kaveri, David Smahel, and Patricia Greenfield. 2006. "Connecting Developmental Constructions to the Internet: Identity Presentation and Sexual Exploration in Online Teen Chat Rooms." *Developmental Psychology,* 42(3):395-406.

Surratt, Carla G. 1998. *Netlife: Internet Citizens and Their Communities*. New York: Nova Science.

TFWiki.net. 2008. "Teletraan-1 Wikia Moves to TFWiki.net", September 15. Retrieved January 20, 2010 (http://tfwiki.net/wiki/Press_Release:_Teletraan-1_Wikia_moves_to_TFWiki.net).

Thelwall, Mike. 2008. "Social Networks, Gender, and Friending: An Analysis of MySpace Member Profiles." *Journal of the American Society for Information Science & Technology,* 59(8):1321-1330.

thesmokinggun.com. 2011. "Charges Dropped in Facebook Spy Vs. Spy Case", June 9. Retrieved June 22, 2011 (http://www.thesmokinggun.com/documents/funny/facebook-spy-vs-spy-case-126493).

Tong, Stephanie Tom, Brandon Van Der Heide, Lindsey Langwell, and Joseph B. Walther. 2008. "Too Much of a Good Thing? The Relationship between Number of Friends and Interpersonal Impressions on Facebook." *Journal of Computer-Mediated Communication,* 13(3):531-549.

Trammell, Kaye D. and Ana Keshelashvili. 2005. "Examining the New Influencers: A Self-Presentation Study of a-List Blogs." *Journalism & Mass Communication Quarterly,* 82(4):968-982.

Turkle, Shelly. 1995. *Life on the Screen: Identity in the Age of the Internet*. New York: Simon & Schuster.

Tynes, Brendesha M. 2007a. "Internet Safety Gone Wild? Sacrificing the Educational and Psychosocial Benefits of Online Social Environments." *Journal of Adolescent Research,* 22(6):575-584.

------. 2007b. "Role Taking in Online "Classrooms": What Adolescents Are Learning About Race and Ethnicity." *Developmental Psychology,* 43(6):1312-1320.

Tynes, Brendesha M., Michael T. Giang, and Geneene N. Thompson. 2008. "Ethnic Identity, Intergroup Contact, and Outgroup Orientation among Diverse Groups of Adolescents on the Internet." *CyberPsychology & Behavior,* 11(4):459-465.

United States Department of Justice. 2008. "Tennessee Man Indicted for Alleged Hack of Governor Sarah Palin's E-Mail Account." Washington DC: United States Department of Justice, October 8. Retrieved June 22, 2009, (http://www.usdoj.gov/opa/pr/2008/October/08-crm-910.html).

Valkenburg, Patti M. and Jochen Peter. 2007a. "Internet Communication and Its Relation to Well-Being: Identifying Some Underlying Mechanisms." *Media Psychology,* 9(1):43-58.

------. 2007b. "Online Communication and Adolescent Well-Being: Testing the Stimulation Versus the Displacement Hypothesis." *Journal of Computer-Mediated Communication,* 12(4):1169-1182.

------. 2007c. "Preadolescents' and Adolescents' Online Communication and Their Closeness to Friends." *Developmental Psychology,* 43(2):267-277.

------. 2008. "Adolescents' Identity Experiments on the Internet: Consequences for Social Competence and Self-Concept Unity." *Communication Research,* 35(2):208-231.

------. 2009. "Social Consequences of the Internet for Adolescents: A Decade of Research." *Current Directions in Psychological Science,* 18(1):1-5.

van den Eijnden, Regina J. J. M., Gert-Jan Meerkerk, Ad A. Vermulst, Renske Spijkerman, and Rutger C. M. E. Engels. 2008. "Online Communication, Compulsive Internet Use, and Psychosocial Well-Being among Adolescents: A Longitudinal Study." *Developmental Psychology,* 44(3):655-665.

Vanden Boogart, Matthew R. 2006. "Uncovering the Social Impacts of Facebook on a College Campus." M.S. Thesis, Department of Counseling and Educational Psychology, Kansas State University, Manhattan, KS.

Walker, Katherine. 2000. ""It's Difficult to Hide It": The Presentation of Self on Internet Home Pages." *Qualitative Sociology,* 23(1):99-121.

Walther, Joseph B. 2006. "Nonverbal Dynamics in Computer-Mediated Communication, Or :(and the Net :('s with You, :) and You :) Alone." Pp. 461-479 in *Handbook of Nonverbal Communication*. Thousand Oaks, CA: Sage.

Walther, Joseph B. and M. Parks. 2002. "Cues Filtered out, Cues Filtered In: Computer Mediated Communication and Relationships." Pp. 529-563 in *The Handbook of Interpersonal Communication*, edited by M. L. Knapp, J. A. Daly, and G. R. Miller. Thousand Oaks, CA: Sage.

Walther, Joseph B., Brandon Van Der Heide, Lauren M. Hamel, and Hillary C. Shulman. 2009. "Self-Generated Versus Other-Generated Statements and Impressions in Computer-Mediated Communication: A Test of Warranting Theory Using Facebook." *Communication Research,* 36(2):229-253.

Walther, Joseph B., Brandon Van Der Heide, Sang-Yeon Kim, David Westerman, and Stephanie Tom Tong. 2008. "The Role of Friends' Appearance and Behavior on Evaluations of Individuals on Facebook: Are We Known by the Company We Keep?" *Human Communication Research,* 34(1):28-49.

Wang, Rong, Suzanne M. Bianchi, and Sara B. Raley. 2005. "Teenagers' Internet Use and Family Rules: A Research Note." *Journal of Marriage & Family,* 67(5):1249-1258.

Westlake, E. J. 2008. "Friend Me If You Facebook: Generation Y and Performative Surveillance." *The Drama Review,* 52(4):21-41.

Williams, Amanda L. and Michael J. Merten. 2008. "A Review of Online Social Networking Profiles by Adolescents: Implications for Future Research and Intervention." *Adolescence,* 43(170):253-274.

------. 2009. "Adolescents' Online Social Networking Following the Death of a Peer." *Journal of Adolescent Research,* 24(1):67-90.

Wolak, Janis, Kimberly J. Mitchell, and David Finkelhor. 2002. "Close Online Relationships in a National Sample of Adolescents." *Adolescence,* 37(147):441.

------. 2006. "Online Victimization of Youth: Five Years Later." Alexandria, VA: National Center for Missing & Exploited Children. Retrieved June 22, 2009, (www.unh.edu/ccrc/pdf/CV138.pdf).

WVLT-TV. 2008. "Teacher Cleared of Any Wrongdoing" *volunteerTV.com*, September 8. Retrieved May 12, 2009, (www.volunteertv.com/home/headlines/10506317.html).

Youn, Seounmi. 2005. "Teenagers' Perceptions of Online Privacy and Coping Behaviors: A Risk–Benefit Appraisal Approach." *Journal of Broadcasting & Electronic Media,* 49(1):86-110.

------. 2008. "Parental Influence and Teens' Attitude Towards Online Privacy Protection." *Journal of Consumer Affairs,* 42(3):362-389.

Yurchisin, Jennifer, Kittichai Watchravesringkan, and Deborah Brown McCabe. 2005. "An Exploration of Identity Re-Creation in the Context of Internet Dating." *Social Behavior & Personality: An International Journal,* 33(8):735-750.

Zhao, Shanyang, Sherri Grasmuck, and Jason Martin. 2008. "Identity Construction on Facebook: Digital Empowerment in Anchored Relationships." *Computers in Human Behavior,* 24(5):1816-1836.