

# Journal of Adolescent Research

<http://jar.sagepub.com/>

---

## **Risky Disclosures on *Facebook*: The Effect of Having a Bad Experience on Online Behavior**

Emily Christofides, Amy Muise and Serge Desmarais

*Journal of Adolescent Research* published online 17 January 2012

DOI: 10.1177/0743558411432635

The online version of this article can be found at:

<http://jar.sagepub.com/content/early/2012/01/12/0743558411432635>

---

Published by:



<http://www.sagepublications.com>

**Additional services and information for *Journal of Adolescent Research* can be found at:**

**Email Alerts:** <http://jar.sagepub.com/cgi/alerts>

**Subscriptions:** <http://jar.sagepub.com/subscriptions>

**Reprints:** <http://www.sagepub.com/journalsReprints.nav>

**Permissions:** <http://www.sagepub.com/journalsPermissions.nav>

>> [OnlineFirst Version of Record](#) - Jan 17, 2012

[What is This?](#)

---

# Risky Disclosures on Facebook: The Effect of Having a Bad Experience on Online Behavior

Journal of Adolescent Research

XX(X) 1–18

© The Author(s) 2012

Reprints and permission:

[sagepub.com/journalsPermissions.nav](http://sagepub.com/journalsPermissions.nav)

DOI: 10.1177/0743558411432635

<http://jar.sagepub.com>



Emily Christofides<sup>1</sup>, Amy Muise<sup>2</sup>,  
and Serge Desmarais<sup>1</sup>

## Abstract

Social network websites are widely used by adolescents, but disclosing in this environment has inherent risks, as does connecting with others online. In a sample of 256 adolescent *Facebook* users, the authors explore the relationship between having a negative experience, privacy knowledge, and behavior. Their reports of bad experiences on *Facebook* are categorized as bullying/meanness, unwanted contact, exposure/unintentional disclosure, and misunderstandings. Adolescents who report having a bad experience are more likely to protect their privacy, and this relationship is mediated by knowledge of the privacy settings. Participants who experience negative consequences are more aware of the risks of online disclosure and how to protect themselves, which results in greater information control. Implications for educating adolescents about privacy and disclosure online are discussed.

## Keywords

emerging adulthood, media, positive youth development, risk behavior

---

<sup>1</sup>Department of Psychology, University of Guelph, Guelph, Ontario, Canada

<sup>2</sup>Department of Psychology, University of Toronto, Mississauga, Ontario, Canada

## Corresponding Author:

Emily Christofides, MSc, University of Guelph, 50 Stone Road East, Guelph, N1G 2W1, Ontario, Canada

Email: [echristo@uoguelph.ca](mailto:echristo@uoguelph.ca)

The news is filled with stories of the dangers that exist for adolescents today. To the risks of drugs, alcohol, delinquency, and risky sexual behavior, we can now add the dangers that the internet brings: predators, lurkers, access to inappropriate information, identity theft, and the like. Not only does danger exist from strangers on the internet, but there can also be risks associated with disclosure to friends and acquaintances. Research shows that there are risks to sharing information that current and future employers may see (CareerBuilder, 2009) as well as the potential for bullies and stalkers to use the information they find online (Juvonen & Gross, 2008). Given the alarming nature of these findings, it is perhaps not surprising that adults are concerned with the potential negative consequences of what adolescents share online. Indeed, numerous organizations around the world have been formed to protect youth in this new and potentially dangerous online world (e.g., National Cyber Security Network<sup>1</sup> in the United States and U.K. Council for Child and Internet Safety<sup>2</sup> in the United Kingdom).

Despite the dangers, online communication is extremely popular. The internet as a whole has 2.1 billion users worldwide (Central Intelligence Agency, 2011) and use of social media websites such as *Facebook*, *YouTube*, and *Wikipedia*, where the content is contributed by users, accounts for 22% of the time that internet users spend online (Nielsen, 2010). *Facebook* is one of the most popular social media sites with more than 750 million users worldwide (*Facebook*, 2011a), with users spending on average 6 hr per week on the site (Nielsen, 2010). Although people of all age groups use the internet and social media, users of social networking sites in the United States are more likely to be adolescents than any other age group (Blackshaw, 2009). Adolescents experience benefits from their use of social media, and researchers have shown that perceiving more potential benefits from online disclosure is associated with a greater likelihood of sharing information online, but greater perception is associated with less disclosure (Youn, 2005). Although the media allege that youth share extensively without heed to the warnings of the dangers of doing so, research suggests that perception of risk does influence adolescents' disclosure behavior. If adolescents are sharing information so extensively, what effect does experiencing negative consequences have on their privacy behavior?

## Adolescents and Social Media

Within the context of adolescents' use of social media, environments such as *Facebook* normalize disclosure (Christofides, Muise, & Desmarais, 2009). Livingstone (2008), in her exploration of 13- to 16-year-olds' use of social network sites, found that information such as age, religion, politics, and

sexual preference are not viewed as private matters by these young users of social network sites. This demographic and psychographic information is standard on sites such as *Facebook*—to be completed as part of the sign-up process—and participants in her study are more concerned about being able to control their information than they are with the nature or type of information being shared. Teens perceive that this element of control allows them to share only information or activities they have chosen to share, which reflects no violation of privacy. However, as Livingstone pointed out, these websites may undermine adolescents' ability to control their disclosure in two important ways. First, social networking websites do not provide settings that allow sufficiently subtle control over who has access to what information. Second, privacy controls available in social networking websites tend to be difficult to find and understand, not only for adolescents but also for adults. Although *Facebook* provides numerous privacy controls, they are accessed through different pages on the site and are not always intuitively labeled. In addition, research shows that the factors that lead users of social network sites to disclose information are not the same as those that lead them to protect their information (Christofides et al., 2009).

Clearer instructions about privacy options along with better privacy controls would allow adolescent users to gain better control over the information they post. In this way, specific others, such as parents, are only able to access the information that teens wish to share with them, which would enable them to share and explore more freely and openly within their chosen group. At the time this study was conducted, users could choose whether their pictures and profile were made public but could not choose to differentiate who saw what individual pieces of information. Some of these privacy controls have changed in response to public concerns, and *Facebook* now provides more detailed information about privacy on the site. There are also some additional safeguards for teens that are not available to adults. Default settings are such that if users under the age of 18 choose not to restrict their profiles, their information will be shared with friends of their direct contacts as well as anyone in networks they have joined, rather than with everyone on *Facebook* (*Facebook*, 2011b). In addition, profiles for underage users are not searchable throughout the internet, though they are searchable on *Facebook*, and *Facebook* accounts are freely available.

## Risks of Online Disclosure

There are many documented benefits to sharing online, such as the ability to explore different identities (boyd, 2007), create an identity that is shared with

friends (Christofides et al., 2009), and increase one's social capital (Ellison, Steinfield, & Lampe, 2007), but there are also numerous potential and actual risks. Hasebrink and colleagues (Hasebrink, Livingstone, Haddon, & Olafsson, 2009) researched the various risks to children, and their categorization of these risks provides a useful framework for understanding them. They divide risks into content risks (where the child receives unwanted or inappropriate content), contact risks (where they receive unwanted contact), and conduct risks (where they engage in inappropriate behavior).

Although the news media generally focuses on contact risks, numerous conduct risks also exist. Peluchette and Karl (2008) found that the availability of information on *Facebook* can make it easier for one's own postings to be incriminating, as, for example, when adolescents post stories about their drinking and drug experiences or other illegal activities. These stories can lead to consequences such as school suspensions and criminal charges. Although these consequences are indeed negative, some of the other negative consequences that can be experienced may never be known. When someone applies for a job, 45% of employers in the United States check social networking sites to screen job applicants and a further 11% plan to do so in the future (CareerBuilder, 2009). The two most common reasons for ruling out a candidate involve the sharing of personal information such as provocative or inappropriate photos or information and posting content about drinking or drug use. If an employer chooses not to hire someone based on the information they find online, the job applicant is unlikely to know that this is the reason they were not hired.

Postings on *Facebook* may also lead to feelings of regret if negative consequences such as loss of opportunity or punishment are experienced. Youn (2005) found that the content of young people's postings sometimes resulted in social risks, such as conflicts with parents, or in psychological risks, such as feeling anxious or regretful about the information they have shared. In a study of online bullying, 72% of adolescents respondents had experienced at least one incident in the past year (Juvonen & Gross, 2008). Online disclosures may also result in negative consequences for romantic relationships. Recent research with young adults (aged 17-24) shows that those who spend more time on *Facebook* are more likely to experience jealousy in response to ambiguous information that they see on the site, which may have consequences for their intimate relationships (Muise, Christofides, & Desmarais, 2009). Information on *Facebook* tends to be ambiguous because people may only see one side of a conversation and pieces of information are often viewed without such contextual information as the relationship between two conversants, which person initiated the conversation, and what response was given.

As a result, someone may see a posting on their boyfriend or girlfriend's page and jump to conclusions about the significance of that comment.

## Mitigating the Risks

Unfortunately, the risks of online disclosure are inextricably linked with the benefits (Livingstone, 2010). In order for people to participate in these online social environments they must open themselves up to others to the extent that they must provide enough information for others to find them. Conversely, sharing no information with others inevitably results in decreased online interactions, an outcome that is particularly upsetting to those who value popularity. Recent research has shown that adolescents, emerging adults, and even adults who highly value popularity are more likely to disclose online (Christofides et al., 2009, 2012). In addition, the *Facebook* environment itself may intensify the importance of popularity since it provides a steady stream of information that others have shared as well as evidence of a person's connections and interactions with others (Christofides et al., 2009). Hence, advising adolescents to restrict their use of social network sites as a way to mitigate the risk of online disclosure may not be reasonable or even advisable.

For adolescents, perception of the outcomes of a risky behavior has been shown to affect the likelihood of engaging in that behavior (Moore & Gullone, 1996). If adolescents believe that the outcomes of a particular behavior will be negative and unpleasant they are less likely to engage in it. Similarly, adolescents and adults who are more aware of the consequences of disclosing online are less likely to share information and more likely to protect their privacy (Christofides et al., 2012). However, Moore and Gullone have suggested that although adolescents can identify possible negative outcomes, they are less skilled at identifying their likelihood, perhaps because they have not yet experienced them and, therefore, cannot predict their potential occurrence. As a result, behavior change may rely on personally experiencing a negative outcome rather than simply being aware that such outcomes are possible.

This argument has already received much support in the coping literature. The experience-behavior hypothesis (Norris, Smith, & Kaniasty, 1999) predicts that adults who experience a negative event increase their risk reduction behaviors and preparedness for future similar events. This hypothesis has been used extensively to explain the coping behaviors of victims of natural disasters, but we argue that it will apply equally well to online risks since some of their characteristics, such as the random and unpredictable nature of

online risks, can be mitigated by taking specific precautionary measures. In a review of theories of self-protective behaviors, Weinstein (1993) found that personally experiencing a negative event is necessary but not sufficient to inspire risk reduction behaviors; it is also important that the risk be viewed as controllable in order to result in a change in behavior.

## Goals of the Present Study

Previous research, as well as media coverage about risks of online disclosure, gives us some clues about the negative events that adolescents are experiencing on *Facebook*. However, what is not yet known is how adolescents themselves describe negative events on *Facebook* and whether bad experiences influence their privacy and disclosure behaviors online. For the current study we chose to explore the effects of having a bad experience on *Facebook* privacy behavior since research has shown that adolescents are willing to change their behavior if they anticipate or experience negative consequences (Christofides et al., 2012; Moore & Gullone, 1996; Norris et al., 1999). Any change in disclosure behavior is likely to be affected by knowledge of the mechanisms for protecting privacy. Users are unlikely to change their online behavior if they do not know what measures to take to protect their privacy. However, knowledge of privacy settings alone does not appear to be sufficient for behavior change to occur in online disclosure (Aquisti & Gross, 2006). Hence, we hypothesize that the relationship between having a bad experience and using the privacy settings will be mediated by knowledge of those privacy settings. We also explore qualitatively the nature and types of negative experiences that adolescents have had on *Facebook*. This element of the research design provided us with a better understanding of the way that adolescents describe their experiences and the impact of those experiences on their behavior.

## Method

### Participants

Our sample consisted of 256 young *Facebook* users (aged<sup>3</sup> 12-18,  $M = 14.83$ ,  $SD = 1.84$ ), with a mix of boys and girls (boys,  $n = 96$ ; girls,  $n = 156$ ; 4 participants did not report their gender). Participants were distributed across junior high and high school grades: Grades 7 and 8 (26.9%), Grade 9 (20.3%), Grade 10 (9.4%), Grade 11 (21.9%), Grade 12 (17.2%), and other (4.3%). The *other* category most likely represents those students

who were enrolled in high school to finish or upgrade courses after their 12th year, which is the final year of school in the province of Ontario, Canada. Participants identified primarily as White or Caucasian (68.0%), which is less diverse than Toronto's makeup of 53% White/Caucasians (City of Toronto, 2011), but more diverse than that of Canada as a whole (Canadian Council on Social Development, 2004). Visible minority groups included Asian (12.2%), Hispanic (5.9%), Black or African American/Canadian (3.5%), Middle Eastern (1.7%), Native (2.1%), and the remaining 6.6% of participants selected "Other," which sometimes indicated multiple ethnic identities.

## Procedures

In order to provide insight into the nature of behavior change as a result of a negative experience on *Facebook*, we administered a survey over several weekends to a sample of adolescents who were visiting a Science Center with their parents in Toronto, Ontario, Canada. Science Center visitors who met the inclusion criteria for this study (adolescents who used *Facebook*) were informed about the study and invited to participate by a research assistant. Signage posted at various areas in the Science Center and a presentation given by the primary researchers also alerted visitors to the study. Adolescents who agreed to participate (and whose parents provided consent) were taken to one of the computer terminals and the study was described to them before they completed their own consent form and survey online. The survey took approximately 15 min to complete and had a series of questions about disclosure and privacy behavior on *Facebook*, knowledge about the privacy settings, open-ended questions about their experiences on *Facebook*, and additional questions that were used in another research study. This study received ethical clearance from the University Research Ethics Board as well as approval from the Ontario Science Centre.

## Measures

*Information control on Facebook.* We assessed the extent to which participants controlled the information they posted on *Facebook* and used the privacy setting using a 7-item scale (Christofides et al., 2009). The items include: "How likely are you to change who can see your profile (e.g., only your friends)?" and "How likely are you to say no to a friend request?" The items were rated on a 7-point scale, with responses ranging from *very unlikely* to *very likely*. The scale was found to be reliable ( $\alpha = .81$ ) in this sample.



*Knowledge of privacy settings.* Participants were asked about their knowledge of the privacy settings on *Facebook* using a 6-item scale. The questions were based on an audit of the privacy settings that the first and second authors conducted and included items such as “Do you know how to block people from searching for you?” and “Do you know how to change what information you share through your newsfeed?” The items were rated on a 7-point scale with response options ranging from *very unlikely* to *very likely*. The scale was found to be reliable ( $\alpha = .80$ ) in this sample.

*Bad experience.* Participants were given an open-ended question where they could comment on any bad experiences they may have had on *Facebook*. They were asked, “If you have ever had a bad experience on *Facebook*, please tell us about it.” The responses were coded for having had a bad experience (“yes” or “no”), and this dichotomous variable was then used in the regression analysis. Coding was conducted by the first author and verified by the second author. Any disagreements were discussed, resulting in a clearer definition of bad experience. We included any experiences that the participants reported, regardless of the importance they attributed to that experience since participants sometimes reported an experience but either minimized its impact or explained how they coped with the situation (e.g., “No sometimes random people try adding me but I just reject them”). We also included experiences that the participant reported happening to others but that affected them directly (e.g., “She came over to my house crying late at night because of it”) or comments that were ambiguous as to the recipient of the bad experience (e.g., “Sometimes things on the internet can hurt people more than real life”). We excluded issues that were purely technical in nature such as “My internet wouldn’t let me log in.” The comments were used in a thematic analysis to better understand the nature of those bad experiences.

## Results

### *Qualitative Findings*

About one quarter (26.7 %) of the participants in our sample reported having a bad experience on *Facebook*. Adolescents who reported having a bad experience on *Facebook* included qualitative information about the nature of this experience. Thematic analysis (Braun & Clarke, 2006) was used to identify the main themes in adolescents’ description of their bad experiences on *Facebook*. The first author read the participants’ comments about their bad experiences and categorized them into different types of experiences. This process resulted in six identified themes, where individual comments could

be attributed to more than one theme. The second author then coded the data using these themes, and the interrater agreement was very high (Cohen's  $\kappa = .94, p < .001$ ). Following Braun and Clark's phases of thematic analysis, the authors reviewed the themes and decided that two sets of themes could be collapsed. We merged codes that had many comments in common and that seemed to relate to similar issues. For example, the initial set of codes included "Taking advantage of anonymity," but it was determined that these situations were generally instances of bullying or meanness and the anonymity of the medium merely facilitated this behavior. The analysis resulted in four main themes: bullying/meanness, unwanted contact, exposure/unintentional disclosure, and misunderstandings. Descriptions of the themes and exemplary quotes are included below.

*Bullying/meanness.* The most common bad experience (reported by 52% of participants who had had a bad experience on *Facebook*) was related to bullying, meanness, and harassment from peers. In some cases participants made reference to the fact that people made comments online that they would not have done in other contexts because of the physical and psychological distance provided by this medium. One 18-year-old female said, "There has been a lot of people who start stuff on *Facebook* because they can't do it in person." One commonly cited example was the use of the honesty box, an application that users can add to *Facebook*, which allows them to provide and receive anonymous comments.

I added the application Honesty Box on *Facebook* when I first signed up. Usually I don't get many comments, but I did get one nasty one about how I need an attitude adjustment and need to lose some weight. I blocked the user though I don't know who they are and haven't had any comments of the sort since. (female, age 16)

Other features of *Facebook*, such as the ability to create groups that other users can join (e.g., groups related to interests, causes, organization, or other topics), were also used to facilitate bullying. An appalling example of this involved a 13-year-old female participant:

Once I was bullied by a boy. He created a group on *Facebook* called "Vote for Jenna Simpson to die"<sup>4</sup> where he would get people to say if they wanted me to commit suicide or not. Of course everyone stood up for me and people got really mad at him. Me and him used to be really good friends, but he just started to hate me and created so many mean things on *Facebook*. He has since apologized, but we are not friends because I do not want to be.

Another way by which participants had experienced meanness or bullying on *Facebook* was when friends guessed or knew their password and entered their account without permission. Sometimes the friends read their private messages and at other times they posted things on behalf of the participant that he or she would not have posted, as illustrated in the following quote:

One of my friends guessed my password and told one of my other friends who I did not trust as much . . . he sent a few messages to my friends with the intent to embarrass me. I changed my password to something much more secure and was more cautious about what I posted online. (male, age 13)

*Unwanted contact.* The second most frequently reported type of bad experiences related to unwanted contact on *Facebook* (23%). Typically unwanted contact involved friend requests or messages from strangers. One 12-year-old female said, “A guy kept trying to add me and I didn’t even know him and I kept declining his request but he kept adding me so I blocked him.” Another 12-year-old female reported a similar experience:

Well, a couple months ago this guy whom I’ve never heard of before wanted to become my friend on *Facebook*. Of course I declined the request and a couple weeks later he asked again so I sent him a message saying, “I’m sorry but since I don’t know you I’m not going to become your friend.” His response was, “F\*\*\* you too dear, I don’t think your a nice person.” After I read that I immediately told my dad and showed him the message and we reported him.

At times, participants received inappropriate messages from people who were unknown to them and at other times they reported feeling uncomfortable simply because it was a stranger who was contacting them. One example from a 14-year-old female reads: “Some random dude from Nigeria sent me a note saying I was pretty and that I should send him a note sometime. It was very scary for me.”

At times the unwanted contact was not from a stranger, but from an acquaintance or a friend with whom the youth had reconnected. One 14 year-old female said, “Once I accepted a friend request from someone I hadn’t seen in like 5 years and he ended up being creepy and I had to delete him.” A 17-year-old female said, “I had some weird creepy people that I have only meet once add me and try talking to me on my inbox.”

**Exposure/unintentional disclosure.** Exposure or unintentional disclosure occurred when either the participant or one of his or her friends posted information or pictures that the person would have rather not shared. Seventeen percent of the bad experiences reported by sample participants fit into this category. In many instances, this involved other people posting pictures that the youth did not want on *Facebook*. One 17-year-old female reported, "I've had people post really embarrassing pictures of me." A 16-year-old female described, "I had posted a picture of me doing something that I didn't want anyone to see. I reported the picture and it got taken off."

Participants also reported unintentionally disclosing information or sharing pictures that they later regretted and as a result exposing themselves to negative consequences. Sometimes the participant did this accidentally and other times they simply did not anticipate the consequences of what they posted or who would see their posts.

I once posted a picture that I was ashamed of without noticing I checked it when uploading pictures and I didn't know that I did so people saw it. So they teased me about it for a couple months. (male, age 14)

Another male, age 17, reported an embarrassing experience, "I typed something on someone's wall instead of their inbox."

At times, information shared on *Facebook* created embarrassment, made youth feel regretful, or led to problems with other people in their lives (e.g., with parents). One participant reported, "I had my mom read my *Facebook* once which was a bad experience for me personally" (female, age 16). Another participant stated, "Sometimes things on the internet can hurt people more than in real life" (female, age 13).

**Misunderstandings.** The final category of bad experiences reported by people in this sample was related to misunderstandings caused by information posted on *Facebook* (7% of bad experiences). Generally, these were situations where information posted online lead to issues with friends or a boss. One 14-year-old female reported that information she saw on *Facebook* "ruined a friendship. . . . I saw pictures and I jumped to conclusions." A 16-year-old female experienced an issue at work as the result of a *Facebook* post: "My boss thought I was skipping work once when I told my friend on *Facebook* that I was relieved to take a break from work." A 14-year-old male reported, "I've had random people add me . . . and it causes a lot of drama with different girls in school."

In a few cases, participants reported not only their experience but also their actions in response to that experience. Responses included blocking the

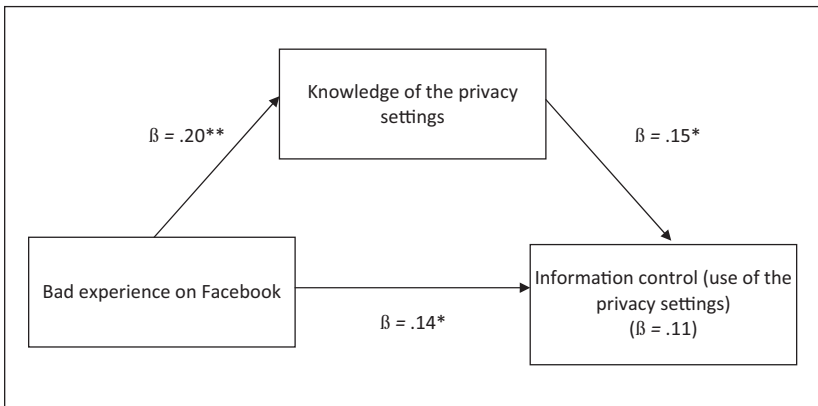
offending party, deleting them as a friend, untagging themselves in a photo, telling parents, and reporting the offender. The actions tended to follow logically from the type of issue they had experienced. For example, participants who received friend requests from strangers reported declining them. Those who received unwelcome comments reported blocking the offender, and those who had pictures posted that they did not like untagged themselves or reported the pictures.

### Quantitative Findings

Having a bad experience was significantly correlated with privacy knowledge ( $r = .21, p < .01$ ) and information control (e.g., use of the privacy settings;  $r = .19, p < .01$ ). Privacy knowledge and information control were also significantly correlated ( $r = .25, p < .001$ ). Since girls ( $M = 4.81, SD = 1.89$ ) were significantly more likely to control their information than boys were ( $M = 3.92, SD = 1.29$ ),  $t(246) = -5.31, p < .001$ , gender was controlled for in the regression analyses. Controlling for gender, we found that having had a bad experience on *Facebook* significantly predicted greater knowledge of privacy settings,  $\beta = .20, t(253) = 2.73, p < .01$ , and a greater likelihood of controlling information (e.g., using the privacy settings) on *Facebook*,  $\beta = .14, t(253) = 2.00, p < .05$ . In order to better understand the nature of these relationships, we tested a mediation model, whereby knowledge of the privacy settings mediated the relationship between having had a bad experience and information control. Privacy knowledge was also a significant predictor of information control on *Facebook*,  $\beta = .15, t(252) = 2.20, p < .05$ , and when privacy knowledge was entered into the model, the relationship between having had a bad experience and being willing to control information on *Facebook* became nonsignificant,  $\beta = .11, t(252) = 1.52, p = ns$ , indicating full mediation (Baron & Kenny, 1986; see Figure 1). To formally test whether mediation occurred, Sobel's test was used (MacKinnon, Warsi, & Dwyer, 1995). Sobel's test was significant ( $z = 2.52, p < .01$ ), confirming that privacy knowledge significantly mediates the relationship between having a bad experience on *Facebook* and use of the privacy settings (information control).

### Discussion

The current study aimed to explore the effects of having a bad experience on the use of the privacy settings on *Facebook*. We predicted that having a bad experience on *Facebook* would lead to increased use of the privacy settings



**Figure 1.** Knowledge of the privacy settings as a mediator of the relationship between having a bad experience and information control on *Facebook*

Note: Gender is controlled in these analyses; numbers in parentheses are the  $\beta$  values from the mediation analysis.

\* $p < .05$ . \*\* $p < .01$ .

and that this behavior would be mediated by knowledge of the privacy settings. Consistent with the experience-behavior hypothesis, having a bad experience predicts precautionary behaviors against future bad experiences. Specifically, participants who had a negative experience on *Facebook* were more likely to know about and use the privacy settings. Using the privacy settings constitutes a controllable element of the risks involved in sharing online, which is consistent with [Weinstein's \(1993\)](#) suggestion that the ability to control a negative outcome is necessary for a bad experience to effect behavior change.

In a recent study, [Derlega, Winstead, Mathews, and Braitman \(2008\)](#) found that their college-aged participants most often reported disclosing because of a close and trusting relationship. However, a generalized lack of trust motivates adolescents and emerging adults to maintain their privacy ([Christofides et al., 2009, 2012](#)). In the present study, once adolescents had experienced something negative personally, they were more likely to seek out information about the privacy settings and use those settings to protect their information. This finding indicates that participants may have become less trusting as a result of their experiences. These bad experiences may have also affected their trust in their relationships as some participants reported that

they deleted, blocked, or reported *Facebook* friends following such an experience.

Our analysis of the bad *Facebook*-related experiences reported by adolescents in our sample showed great similarity to those reported in other studies of online risks. We found that most of the risks that adolescents reported on *Facebook* fell into what Hasebrink and colleagues' (2009) define as contact or conduct categories. Although participants may not have had a bad experience as a result of being exposed to unwanted or inappropriate material, the *Facebook* environment is rife with opportunities for unwanted contacts from acquaintances and strangers, which may at times also contain inappropriate material. It also provides people with the opportunities to engage in inappropriate conduct such as bullying behavior and meanness as well as the problems that may go along with inappropriate or inadvertent disclosures. *Facebook* has updated its privacy settings in response to these sorts of issues and has provided safety guidelines for users, parents, and educators. However, because some participants reported lying about their age on *Facebook*, they may actually bypass one of the safeguards that *Facebook* has put in place for adolescent users. Default settings for users under the age of 18 are more restrictive than for those who are older (*Facebook*, 2011b) and so lying about one's age may increase the likelihood of receiving unwanted contacts from strangers.

Participants' behavior may well depend on what they are exposed to online. It is possible that those who do not receive unwanted comments or requests have no need to employ the privacy settings. Perhaps those who have fewer requests actually crave more contact and so are less likely to use the privacy settings. Although this is possible, we expect that these behaviors would depend on personality as much as the situation. Indeed, research shows that adolescents with higher self-esteem are more likely to use the privacy settings to protect themselves from unwanted contact (Christofides et al., 2012).

In addition to the dangers that participants reported, situations such as bullying, meanness, and unwanted contact, participants also experienced challenges within their relationships as a result of their disclosures. Participants experienced misunderstandings with peers and other contacts as a result of their posts. Often the misunderstandings that participants reported were a result of the lack of context provided by the *Facebook* environment. As such, information posted on *Facebook* may be more easily misinterpreted. Although only 7% of the bad experiences reported by this sample related to this theme, we saw many similarities with our previous work on *Facebook* and the experience of relational jealousy (Muise et al., 2009).

Taken together, the findings from this study have many useful implications for designing interventions to combat the challenges that adolescents may face

online, and particularly within social network sites. Programs aimed at educating adolescents about privacy and the consequences of information disclosure on *Facebook* will need to incorporate strategies that help them to avoid such situations before they occur. Clues as to how to approach this problem come from our research with emerging adults on popularity and disclosure (Christofides et al., 2009), where we found that undergraduate students are willing to forgo their privacy for the sake of participating more fully in their social environment, which suggests that the benefits of using social media may outweigh the risks when deciding to share information on *Facebook*. However, our recent research on the impact of having a future orientation shows that when adolescents do think about the future consequences of their disclosures, as they might when they have a bad experience, they are more careful with their personal information and may take greater steps to protect their privacy (Christofides et al., 2012). As a result, increasing awareness of the potential negative consequences may be a helpful strategy when educating adolescents about privacy and disclosure on *Facebook*.

Although negative experiences have the most impact on behavior change when they have been personally experienced, research shows that negative experiences within a community also have a large impact on precautionary behavior (Norris et al., 1999). Therefore, being educated about the occurrence of these events within their peer group may lead adolescents to be more protective of their privacy. This may be particularly important for more covert consequences, such as being declined a job or admission to a school program. In these ways, adolescents may be negatively affected by information shared on *Facebook* without being aware of this fact.

One limitation of the current study is that we have only explored the negative consequences that the adolescents in our sample identified. There may be other consequences of *Facebook* disclosure that are not captured in this research. Today, many employers use *Facebook* and other social network sites to learn about potential candidates (CareerBuilder, 2009). However, we do not know how this is perceived by adolescents and emerging adults who will be entering the job market. Future research could explore young people's awareness of these risks and whether privacy behavior changes as a result. The current study is also limited by its cross-sectional design. The findings suggest that having a bad experience on *Facebook* increases privacy knowledge and information control; however, we do not know whether this effect is sustained over a longer period of time. After a natural disaster, behavior change is sustained as much as 2 years later, but negative events on *Facebook* may not have such a strong and lasting impact. Since *Facebook* and other social network sites are environments where high levels of disclosure are



normalized (boyd & Ellison, 2007), it will be important to learn about privacy knowledge and behavior over time and across various age groups.

### Declaration of Conflicting Interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

### Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: The authors would like to thank the Office of the Privacy Commissioner of Canada for their support through the Research Contributions program.

### Notes

1. <http://www.staysafeonline.org/>
2. <http://www.dcsf.gov.uk/ukccis/>
3. Note that the minimum age requirement for *Facebook* use is 13 years, but participants under 13 years reported lying about their age in order to use the site. In the case of our research participants, their parents were aware of this behavior as they gave their consent for participation in our study.
4. Name is a pseudonym.

### References

- Baron, R. M., & Kenny, D. A. (1986). The moderator-mediator variable distinction in social psychological research: Conceptual, strategic and statistical considerations. *Journal of Personality and Social Psychology, 51*, 1173-1182.
- Blackshaw, P. (2009). *A pocket guide to social media and kids*. Retrieved July 31, 2011, from <http://blog.nielsen.com/nielsenwire/consumer/a-pocket-guide-to-social-media-and-kids/>
- boyd, d. m. (2007). Why youth (heart) social network sites: The role of networked publics in teenage social life. In D. Buckingham (Ed.), *McArthur Foundation series on digital learning—youth, identity, and digital media volume*. Cambridge: MIT Press.
- boyd, d. m., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication, 13*(1), 210-230.
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*, 77-101.
- Canadian Council on Social Development. (2004). *Stats & facts: Demographics of the Canadian population*. Retrieved July 30, 2011, from <http://www.ccsd.ca/factsheets/demographics/>

- CareerBuilder. (2009). *Forty five percent of employers use social networking sites to research job candidates, CareerBuilder survey finds*. Retrieved July 31, 2011, from [http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr519&sd=8%2f19%2f2009&ed=12%2f31%2f2009&siteid=cbpr&sc\\_cmp1=cb\\_pr519\\_&cbRecursionCnt=2&cbsid=d7ecf4ae7d1e457aa0d4f3aefbe5a8f6-332435109-RS-4](http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr519&sd=8%2f19%2f2009&ed=12%2f31%2f2009&siteid=cbpr&sc_cmp1=cb_pr519_&cbRecursionCnt=2&cbsid=d7ecf4ae7d1e457aa0d4f3aefbe5a8f6-332435109-RS-4)
- Central Intelligence Agency. (2011). *The world factbook: Communications*. Retrieved July 31, 2011, from <https://www.cia.gov/library/publications/the-world-factbook/geos/xx.html>
- Christofides, E., Muise, A., & Desmarais, S. (2009). Information disclosure and control on Facebook: Are they two sides of the same coin or two different processes? *CyberPsychology & Behavior, 12*(3), 341-345.
- Christofides, E., Muise, A., & Desmarais, S. (2012). Hey mom, what's on your Facebook? Facebook disclosure and privacy in youth and adults. *Social Psychological and Personality Science, 3*(1), 48-54.
- City of Toronto, (2011). *Toronto's racial diversity*. Retrieved July 30, 2011, from [http://www.toronto.ca/toronto\\_facts/diversity.htm](http://www.toronto.ca/toronto_facts/diversity.htm)
- Derlega, V. J., Winstead, B. A., Mathews, A., & Braitman, A. L. (2008). Why does someone reveal highly personal information? Attributions for and against self-disclosure in close relationships. *Communication Research Reports, 25*(2), 115-130.
- Ellison, N. B., Steinfield, C., & Lampe, C. (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.
- Facebook. (2011a). *Company statistics*. Retrieved July 31, 2011, from <http://www.facebook.com/press/info.php?statistics>
- Facebook. (2011b). *Help your teens play it safe*. Retrieved July 31, 2011, from <http://www.facebook.com/help/?safety=parents>
- Hasebrink, U., Livingstone, S., Haddon, L., & Olafsson, K. (2009). *Comparing children's online opportunities and risks across Europe: Cross-national comparisons for EU Kids Online*. London: LSE, EU Kids Online.
- Juvonen, J., & Gross, E. F. (2008). Extending the school grounds? Bullying experiences in cyberspace. *Journal of School Health, 79*(9), 496-505.
- Livingstone, S. (2008). Taking risky opportunities in youthful content creation: Teenager's use of social networking sites for intimacy, privacy and self-expression. *New Media & Society, 10*(3), 393-411.
- Livingstone, S. (2010). Internet, children, and youth. In M. Consalvo & C. Ess (Eds.), *The handbook of Internet studies* (pp. 348-368). Oxford, UK: Blackwell.
- MacKinnon, D. P., Warsi, G., & Dwyer, J. H. (1995). A simulation study of mediated effect measures. *Multivariate Behavioral Research, 30*(1), 41-62.

- Moore, S., & Gullone, E. (1996). Predicting adolescent risk behavior using a personalized cost-benefit analysis. *Journal of Adolescence, 25*(3), 343-359.
- Muise, A., Christofides, E., & Desmarais, S. (2009). More information than you ever wanted to know—Does Facebook bring out the green-eyed monster of jealousy? *CyberPsychology & Behavior, 12*(4), 441-444.
- Nielsen. (2010). *Social networks/blogs now account for one in every four and a half minutes spent online*. Retrieved July 31, 2011, from <http://blog.nielsen.com/nielsenwire/global/social-media-accounts-for-22-percent-of-time-online/>
- Norris, F. H., Smith, T., & Kaniasty, K. (1999). Revisiting the experience-behavior hypothesis: The effects of hurricane Hugo on hazard preparedness and other self-protective acts. *Basic and Applied Social Psychology, 21*(1), 37-47.
- Peluchette, J., & Karl, K. (2008). Social networking profiles: An examination of student attitudes regarding use and appropriateness of content. *CyberPsychology & Behavior, 11*(1), 95-97.
- Weinstein, N. (1993). Four competing theories of health-protective behavior. *Health Psychology, 12*, 324-333.
- Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviours: A risk-benefit appraisal approach. *Journal of Broadcasting & Electronic Media, 49*(1), 86-110.

## Bios

**Emily Christofides** is a doctoral candidate in psychology at the University of Guelph. Her research focuses on the psychology of privacy and information disclosure as well as the social consequences of using new media, such as loss of privacy, relationship issues, gender differences, and gender stereotyping.

**Amy Muise** is a postdoctoral fellow at the University of Toronto, Mississauga. The focus of her research has been on interpersonal relationships, especially as mediated by new technology such as *Facebook*. Her research has contributed to the understanding of relational consequences of disclosing information on *Facebook*.

**Serge Desmarais** is professor of psychology and the associate vice-president (Academic) at the University of Guelph. Over the past few years, he has been involved in a program of research that explores the social and relational consequences of online disclosure. He also studies close relationships, social justice, gender issues, pay entitlement, and sexuality.