CHAPTER XIV

Security and Insecurity Online: Perspectives from Girls and Young Women

Sarah Heath

Introduction

Participation in the online world is often contingent on one's ability to disclose and share personal information about one self.[1] Such disclosure can have positive implications. Critical scholars have noted that disclosure can deepen existing relationships, allow participants to express themselves, experiment with their identities, and seek auth1enticity, as well as validate themselves to others.[2] Governing discourses often draw attention to the negative consequences of this disclosure.[3] In particular, it has been noted that users may inadvertently experience a loss of privacy as a result of participating in online social networks, which may lead to the use of one's personal information for impersonation and harassment.[4] As Bailey notes,[5] the safety and security of children and youth online has been discussed in parliamentary debates in the context of child luring, sexual assault, child pornography, sexting, and cyberbullying,[6] all of which can result in physical, emotional, psychological, and/or moral harm.

Girls and young women, in particular, have been characterized by policy makers as potential victims of online security threats. In their analysis of legislative debates, Bailey and Steeves[7] note that policy solutions (i.e., increased surveillance, censorship, self-monitoring, and criminalization) portray girls and young women as all-knowing

and comfortable on the internet but naïve and vulnerable in relation to how they view their personal security and the security of their information.[8] It appears that policy makers have conceptualized insecurity primarily as a function of the risk that children and youth create themselves (i.e., their personal, intellectual, developmental, moral, and sexual traits). Although policy makers have also drawn some associations between online risks and the architecture of social networking sites (SNS; specifically the consequences of anonymity and a lack of accountability online), internet service providers, and societal messages around sexualization and objectification, the actions of children and youth remain paramount. Bailey,[9] however, suggests that girls' and young women's description of online risks in general, and the recommendations they propose to reduce those risks in particular, differ drastically from those depicted by policy makers. She instead identifies how the technical infrastructures of SNS organize girls and young women in ways that promote conflict.

What is particularly interesting are the gaps between how girls and young women, critical scholars, and policy makers have each described threats to security (or insecurity) and the kinds of responses each suggests are needed to minimize or regulate these threats. While policy makers argue that security risks are an inevitable result of online self-disclosure, such a perspective fails to recognize the presumptive controls initiated by users to protect and maintain their security online. These presumptive controls and the expectations with regards to their use were discussed by the girls and young woman who were interviewed as part of the eGirls Project.

In January and February of 2013, researchers with the eGirls Project held a series of interviews and focus groups with girls and young women between the ages of 15 and 22. All participants used interactive online media (such as social networking, blogging, and/or user-generated video sites) as a regular part of their social lives. Half of our sample resided in an urban Ontario setting and half resided in a rural Ontario setting.[10]

We interviewed six girls aged 15 to 16 and six young women aged 18 to 22. An additional twenty-two participated in four focus group discussions, as follows: (1) seven girls aged 15 to 17 living in the urban setting; (2) five girls aged 15 to 17 living in the rural setting; (3) six young women aged 18 to 22 living in the urban setting; and (4) four young women aged 18 to 22 living in the rural setting. A professional research house recruited our participants on the basis of

sex, age (either 15 to 17 or 18 to 22), and location of residence (urban or rural). Although participants were not recruited on the basis of self-identification with regard to other aspects of their identities, such as race, ethnicity, gender identity, or sexual orientation, our participant group included members of racialized, linguistic, and various religious groups.

In the interviews and the focus groups, we explored, among other things, the types of visual and textual representations the participants used online to express their identity as young women, and the benefits and pitfalls they experience on social media. We also asked for their views on the issues and policy responses focused upon by policy makers (as identified in the review of federal parliamentary debates discussed by Bailey in Chapter I of this volume). With participant permission, the interviews and focus group were audiotaped and transcribed by our research assistants for analysis. All identifying information was removed from the transcripts, and pseudonyms were used to identify participants.[11] The interview and focus group transcripts were then coded for major themes. One major theme that appeared in the data was the use of security controls by participants on SNS.

The objective of this chapter is to explore girls' and young women's perspectives regarding the threats to security (or insecurities) they encounter through their participation on SNS. This will advance the discussion about how to build an online environment that supports and encourages positive experiences for girls and young women.[12] I begin with an overview of how the eGirls participants used security controls as a way to secure their online communications and their expectations in this regard. Specifically, I explore how the presence of certain features on a SNS, including aspects that girls and young women viewed as indicators of security (e.g., control of personal content, consistency, ease of updating, and management of privacy settings), influenced how they participated on the site. For SNS perceived to be "insecure," participants managed their privacy and security by employing risk-reducing strategies through the use of security controls. These included the triage of online requests, the deployment of exclusionary techniques (blocking users, hiding profiles, creating groups, etc.), and the use of privacy settings. I then discuss these strategies, as well as the concerns expressed by participants that such strategies cannot fully ensure that they can assert control over their online interactions.

Situating (In)Securities within Broader Discussions of Online Safety and Privacy

For regulators, educators, and parents, online safety concerns generally focus on the protection of youth from sexual predation and harassment through parental supervision,[13] awareness and responsibilization[14] on the part of the child,[15] and abstinence from sharing of information.[16] In addition, policy makers rarely use the term "security" in relation to the use of online social media; instead, they discuss the issues in terms of risks and harms, especially risks to and harms associated with personal and moral safety (i.e., the corruption of an individual by exposing them to something they would not otherwise be exposed to). These kinds of harms, however, are highly unlikely to occur and the interventions adults rely on to protect youth from them are often at odds with the experiences of young people.[17] Youth tend to be more concerned about online privacy and the security of their personal information more generally.[18] Privacy refers to an individual's ability to control the sharing and dissemination of their personal information, including how it will be used and manipulated.[19] From youths' perspective, the loss of privacy is often deemed to be a loss of security and online risks to privacy create insecurities that they must navigate.[20] The loss of privacy and control over personal information may also result in safety concerns, which creates a blurring of these two concepts (i.e., security and safety).

Scholarship addressing young people's perspective of online security suggests that even though children disclose personal information online, they generally think about and are concerned with the protection of their privacy.[21] Moreover, Burkell, Steeves, and Micheti report that the children they interviewed did not necessarily disclose personal information online willingly, but often saw disclosure as a compromise that was required in order to participate in social activities online.[22] Youn found that the promise of additional benefits from an online forum correlated with greater disclosure by youth, even when the information was not required in order to participate on the site.[23] But young people still identify a variety of perceived insecurities, including the inability to limit information to "just friends" or to change default settings that maximize exposure, and the ability of corporations, education institutions, and law enforcement officers to access information marked as private.[24]

In response to these insecurities, children have developed risk reduction strategies. For example, a 2013 survey conducted by MediaSmarts on the social media use and privacy practices of Canadian children revealed that 90 percent of grade 4 students refrained from posting their contact information online.[25] Many teenagers reported altering their behaviour to protect their privacy, by "falsifying information, providing incomplete information, or going to different websites that do not ask for personal information."[26] Forty-seven percent of Canadian students aged 9 to 17 also indicated that they had represented themselves as someone else to protect their privacy online.[27] Children noted other strategies, such as deleting comments and photos where they were tagged (which 97 percent of students reported doing).[28] Youth, in addition, reported using privacy settings to restrict the disclosure of their information.[29] These self-help strategies are particularly noteworthy, given the fact that privacy policies are often incredibly difficult to interpret and the privacy options offered by SNS are often limited, both of which combine to constrain the flexibility youth need to handle privacy dilemmas online.[30]

Moreover, some youth believe the ability to access information does not necessarily mean it should be accessed by corporations, educational institutions, parents, and law enforcement, as youth may still deem this material "private" (regardless of its accessibility in a public place).[31] This flies in the face of privacy regulations that typically assume individuals will protect their privacy by limiting what they disclose online.

These research findings have focused on the online experiences of youth as a whole. However, girls' online experiences, as described by Bailey and Bailey and Steeves, suggest that girls' and young women's experiences on SNS are highly gendered.[32] Regan and Steeves have also highlighted "gendered differences in patterns of online communication among children and youth, especially with regard to privacy protective behaviours," where girls are less likely to disclose characteristics because they are girls.[33] This is further complicated because the structure of the online environment reinforces "media stereotypes and the commodification of girls' sexuality."[34] Marketing messages embedded within SNS encourage a certain type of consumption, especially by girls, and legitimate a certain kind of sharing.[35] Coercive marketing techniques built into the architecture of the site also persuade youth to disclose

information, which is collected for marketing purposes, often without their knowledge.[36]

This means that girls are in a unique situation. On the one hand, they are attracted to SNS because of their desire to control the presentation of their online self and to be seen positively in the online world.[37] On the other hand, the gendered nature of their visibility "creates a sense of fear among policy makers precisely because it allows girls to step beyond the constraints they experience in real space."[38] Girls are therefore seen as in need of regulation, both to protect them from harms and to ensure they perform a particular type of femininity.

However, as the eGirls data demonstrates, the nature of those harms remains highly contested, especially because safety and security are typically understood as two separate concepts. Safety addresses the risk of harm to oneself, as opposed to security, which focuses on the risk of harm to one's personal information. The distinction between the two blurs in relation to the online world, where one's personal information is easily accessible and risks to the protection of one's personal information can be associated with risks to one's safety. For example, in the case of cyberbullying, one's profile picture, which is personal information, can be accessed by anyone due to the technical architecture of the SNS, and can expose the poster to various forms of harassment, potentially resulting in a variety of harms (e.g., physical, emotional, psychological, and/or moral harm).

SNS Insecurities and Security Controls from the Perspectives of Girls and Young Women

Just as the term "security" was rarely used by policy makers, the girls and young women who participated in the eGirls Project rarely used the term "security" in relation to the use of online social media. Instead, they talked about risks and harms. However, whereas policy makers focus on risks that implicate personal and moral safety (i.e., the corruption of an individual by exposing them to something they would not otherwise be exposed to), the eGirls participants talked more about technical risks to their information and possible implications for their physical safety. Nonetheless, the former concerns were paramount. Although the girls discussed stranger danger,[39] particularly in the context of unsafe things they may have done in

the past, they were primarily concerned about the security of their personal information because of its permanency online. They complained when pictures of them were shared because a friend or family member uploaded them online without their consent. They were also concerned that information posted about them could possibly be retrieved by others (potentially undesirable others) and used to inhibit their opportunities in the future, such as career prospects.

The girls and young women also described their concerns regarding the requirement that they must provide personal information in order to participate on most SNS. Specifically, they were worried that unknown individuals would obtain their information and use it to impersonate them online, or to contact them, or to do other things that would harm or violate them (psychologically or physically). They also noted how the design and structure of the SNS meant they shared more information. For example, when asked if there is any information participants do not include in their profile, Amelia (18) noted, "I used to have my cellphone number in there. I took that off though, umm, cause people were texting me who, you know, I was like, I don't really want you to have my number type thing." And when asked about privacy and the various platforms, she continued to say,

> Twitter, I think you, you don't post a lot of personal information. Like you don't post, um, really very much cause if you go to someone's profile, [it] just gives you the layout and it just gives you the picture and your name. Um, and then it'll have, you can write a little blurb about yourself type of thing but, like, in that you don't, you don't have to put anything like, you don't even have to put anything in that so you could just have your picture, your name and just all your tweets. So you could really be whoever you wanted to be. You would, could keep stuff out of it that you didn't want people to know really easily. Um whereas in Facebook, I think because you go on Facebook and then you can edit your file and it will give you all these options that you can add to, right, like you can add your name and your number and your address and like where you're from and there's apps like, um, I went to high school with you type thing. Like it's going to connect you back to who you are and you might get connected to things that you didn't want to be connected to. So I think more so with Twitter, you're free to be absolutely like,

> who like, whoever you wanted to be, whether that's a negative or a positive thing because you could really like, somebody else could be pretending to be someone who they're totally not. Um, so, I mean I don't know, it's a positive and a negative, right, just depends on how they're using it … But I think Facebook definitely more so. There, you feel more obligated to include like, all your information, because they put it there and they label it, right, whereas Twitter, they don't.

Some participants likewise acknowledged that they were unaware that SNS collected their information or knew what those companies did with that information; further, most of the participants were disgruntled by the fact that their information was being used for other nefarious purposes (e.g., data mining, marketing, advertising, business planning, etc.) than what they intended, which was limited to their own social participation. For example, when asked if they had a sense of what Facebook and other sites did with their information, focus group participants responded as follows:

> Donna (19): Yeah. I know that they use some of your information to post, like, advertisements that are directly related to you, which I find kind of creepy. Like, I was actually kind of—not worried, but more just surprised to find that out, that they can just go through my stuff and find their way around and find a way to post something they think I'll find interesting.
> Ashley (18): Yeah, I hate that.
> Researcher: And you said that's creepy?
> Donna (19): I don't know if creepy's the right word.
> Andrea (22): I'd say creepy.
> Donna (19): The fact that they're going through all of my information and can specifically—Like, I'll have advertisements for university, advertisements for gym memberships, like, stuff that's directly related to, like, my age group of people. I don't know, I was really surprised when I found that out. I thought they just post stuff … And they don't tell you what they're accessing. They just say, "Can I access your information?"
> Andrea (22): At any time. Any day. I'm like, "What?"

The primary source of these kinds of security risks was rooted in the pressure girls and young women felt to participate in networked

communications. Indeed, in responding to the risks posed by participation online, some girls and young women suggested that the best approach to remove such risks was to abstain from participating altogether: to "not connect with the outside world" (Brianne, 20), or "if you're really worried about something being on the internet or if you don't, if you're so afraid of someone else seeing it, don't post it, don't sign up, don't put your name on it" (Cindy, 20).

However, abstaining from connection with the outside world (as suggested by Brianne) was described as impossible by other girls and young women. They noted that they felt pressure from friends, community groups, and family members both to actively participate on SNS and to include friends, community group members, and family members in their online communities. Clare (16) suggested that even girls who experience online harassment might find it hard to disconnect: "[Bullying is] harder to stop unless the person deletes their account and for some reason a lot of kids don't like to do that even if they are being bullied. So I guess, I don't know, they don't really take responsibility for it. They don't realize it can escalate into bigger things. But also it's harder to do I guess."

Along with this social pressure to participate in SNS comes the need to share personal details with numerous people as a result of having a plethora of friends or followers on various SNS. However, several girls and young women explained that the greater number of people associated with your various profiles, the more likely it is that the security of your information will be reduced. For example, Jill (20) reported,

> I feel like, as people grow up, they do, like, cleanups of their friends on Facebook. It drops by, like, 200 people, because they realize as they're getting older that, like, they're more mature and it's less about having so many friends on Facebook. And they're realizing that their security is more at risk. I feel like I dropped [pause] I was at, like, almost 600 friends, then I went down to, like, 350. And I couldn't even [pause] It's just so difficult to delete friends on Facebook, as it is now … 'cause, when I got my Facebook, I was a lot more young, younger. And I'd comment on a lot more people's photos, who I'm not really friends with now, and I felt, like, I don't really need that comment there. Or, like, a conversation I had with a friend once on Facebook, I didn't find it necessary. So instead of going to delete, like, all

> my comments that I'd made, I just figured I would delete my Facebook; deactivate it. And then I think it was the entire summer, I didn't have Facebook. Then when I went back to school in the fall, I got it again. 'Cause you really feel, like, shunned out sometimes, because everything happens on Facebook. Like, party updates, or events.

The participants also alluded to the complexity of privacy policies and privacy settings on several of the SNS. This complexity was deemed to be the cause of some of the insecurity they experienced online. Indeed, the complexity of privacy settings, and the requirement to enter significant amounts of personal information on particular platforms online, was seen as a direct threat to their ability to control the disclosure of their information and, subsequently, their security. Participants noted that they did not trust Facebook's privacy settings as they made it hard to keep personal information private. Even if they set their settings to "private" (meaning that their information was only available to their "friends"), the settings were often changed without them knowing, and the complexity of the settings made it hard to see how they could restrict their information to a smaller audience. Some participants felt that this increased the likelihood that their information would be collected and used for unintended purposes by unknown users, institutions, and corporations. For example, Catlin (19) said,

> Like, Facebook privacy settings, they change all the time, and you have to keep on, like, updating your privacy settings and a whole bunch of other stuff. But Google, like, it just stays, it stays the same. And they have way more security. Like, no one can search me on my Google account. It's just for pictures, so absolutely no one can. But Facebook, they'd be able to.

Other participants similarly noted that the technical platforms of SNS combined with other technologies in their life made keeping their personal information private even more difficult, as they experience a loss of control over how (and if) their information is shared. Catlin (19) continued,

> But, like, the only thing bad about the Google account I have is that every time I take a picture on my phone, it automatically

> uploads it to my Google account. Automatically. It doesn't matter how many times I try to delete it, because I can't even delete it off my phone. It's so hooked up to my Google account. 'Cause when you first get an Android, you have to get a Google account. So now everything gets uploaded to my Google account.
> Researcher: And what bothers you about that?
> Catlin (19): Well, just, like, I don't want all of my pictures on my Google account. Like, I should be able to decide what pictures I want. But it automatically uploads it. Like, if I go to take, like – I had to take a picture of … I work at [a retail store] and I took a picture in the break room of my schedule. And it uploads it to Google. And I don't want that on my Google account.

This need to post more personal information (rather than less) and accumulate more friends (rather than fewer) was attributed to the profit-seeking focus of these SNS. Some participants discussed their distaste for the use of their personal information for marketing purposes or for the generation of corporate profits, but felt that it was inevitable and not unexpected since they were using a "corporate tool," such as Facebook.

This visibility was complicated by the perceived anonymity of other users who could peruse their profiles; and some participants saw this as a key cause of the various insecurities they experience online. Many identified the anonymity of online participation as posing a risk for interactions as people can say and do things that that they may not be accountable for, making online communication more dangerous and "unsafe":

> Brianne (20): It's like, I don't really care. They'll use, like, language that you've never used in front of your parents, or they'll say something they'd never say … so I don't know, I find it's almost like you have a split personality disorder. You have a Facebook person and you have a human person.
> Laura (18): It makes it more open, on Facebook.
> Brianne (20): Because you can hide behind the screen, you can say whatever you want.
> Researcher: So what tends to be … what tend to be the differences between your Facebook … if the person's behaving differently, the difference between the Facebook …

> Catlin (19): On Facebook, I find, you're more willing to state what you're actually thinking.
> Laura (18): Yeah.
> Catlin (19): Like, my friend, she is the worst person on Facebook. She'll be so mean to you on Facebook, but the second she sees you face-to-face, everything's perfect; everything's fine. Yeah.

Participants spoke about several strategies to reduce risks associated with this insecurity, including deleting content, blocking people, or limiting real information (e.g., posing as a boy). This discussion was typical:

> Researcher: Okay. And so, have you ever had a friend request from somebody you didn't know?
> Josie (16): Yeah. You just delete the comment, kind of thing.
> Paula (17): Yeah. My Instagram is blocked, because I post a lot of pictures of my house and stuff, that I don't want people to see. But my Twitter isn't blocked; I think I should lock that.
> Beth (16): Yeah, I block mine. I don't want other people to see my stuff.
> Researcher: Alright.
> Chelsea (17): Well, I don't have anything blocked. 'Cause I don't post … like, I don't have my real name on, like, any site. I normally just use "First Name, Last Name," because that's my mother's maiden name.
> Researcher: Do you ever think about using a name that doesn't identify you as a girl?
> Courtney (17): [jokingly] Yeah. Fred.
> Chelsea (17): Fred. [Laughter]

Other strategies involved talking to one's parents, exiting areas where they were more likely to encounter a stranger (e.g., chat rooms), or ignoring "friend" requests. But the principle strategy discussed by the participants was the use of a triage process. This process involved thinking about how a certain profile could harm them or reflect poorly on their associated friends and family. Monica described it this way:

> Researcher: What did you think you knew? What would you tell the thirteen-year-old self?

> Monica (16): Uh, just be careful what you post. Anyone could get your information. If you're not careful with it, just be conscious of what you're posting, what you're doing, how you wanna be portrayed on the internet.

Participants also spoke about investigating the profile of someone who was unknown to them, but who had sent a request to become an online "friend."

Although the participants outlined a variety of instances that led to feelings of insecurity online, each instance involved the use of their personal information by an unknown person for an unintended purpose. For example, some girls and young women spoke about receiving a "friend" request from someone they did not know. They also referred to incidents where they were contacted by someone with whom they did not have a previously established relationship. They typically considered these online requests to be "creepy," "inappropriate," or "wrong," so they would ignore, delete, or block the person:

> Andrea (22): I have a story, when I first got Facebook I was moving to Ottawa; I was on the Ottawa group because you used to have the location if you were part of a group. And I was like, "Oh, I'm moving to Ottawa," and some guy is asking me where I work and what my age is, so he could pick me up from the airport. And I'm like, "I'm pretty sure I'm coming with my family." [Laughter] He's asking what school I'm going to go to, I'm like, "Fuck."
>
> Jill (20): Yeah, I've had, like, random people just message me and be like, "Hey, nice picture," like via inbox, like, private messages or whatever. Just "Nice picture; add me on Facebook." No.
>
> Jill (20): Yeah. Somebody sent me such a weird message once. Like, the picture was, like, me and my friend and we were both wearing, like, the same outfit and doing, like, the same post, like, mirror images of each other. So he sent me a message, and it was so creepy, because, like, he was commenting on how our smiles were different. He was like, "You and the other girl, the only thing different is your smile." That was his comment.
>
> Researcher: This was someone, like, a perfect stranger?
>
> Jill (20): Yeah. And I was like, "Thank you for this. Go away." [Laughter]

The participants also discussed the importance of having someone to talk to if they needed advice about what to do in a particular situation, such as receiving a request that made them feel uncomfortable. It was in these instances that access to friends, family, teachers, community members, and non-governmental organizations (NGOs), such as the Kids Help Phone[40] and MediaSmarts,[41] became important. They did not expect these parties to preach or to scold the person going through the incident, or to force them into pursing a formal legal action. Instead, the participants felt that these parties should provide youth with opportunities to discuss any threats to their safety or security online and provide online tools to help girls better control the collection of their personal information. They additionally expressed a desire to have someone to converse with if they were unsure about whether something was appropriate or inappropriate or what the consequences of a particular action might be.

When asked about existing and proposed legislation regarding criminalized perpetrators of luring, assault, and pornography (including sexting), the majority of the participants favoured the use of criminal offences to discourage future events; however, in the discussion of texting legislation, which may criminalize victims as well as perpetrators, some participants were concerned with the further trauma the victim and the perpetrator would experience as a result of criminal justice involvement:

> Amelia (18): I don't think … [charging girls who sext with child pornography is a good idea] because well, I don't know, it depends on circumstances. I think, if she's getting pressured into it, I don't think having that charge of child pornography is a good thing because that's going to make her feel even worse if she actually had you know a charge for it type thing. Um, whereas if she's doing it for her own, like, if she's doing it cause she wants to, I think maybe yeah you should like, it doesn't really have as much as an effect type thing, so it, I, it depends on the circumstances.

Many participants felt that such actions would not address the underlying issues (i.e., mainstream stereotypes, architectural constraints, etc.). For example, Lauryn (17) explains,

> I [think] having a law against it is kinda like, I don't know, it's kinda like, like, as long as, like, got the awareness out to girls our age, saying, like, look, if you put this picture up here this is what can happen, and like, people, like, your picture can be sent to anybody, you don't know who's going to see it, maybe you put something on technology you can't get rid of it, maybe you can delete it off your phone but you can't delete it off of everyone else's phone, I think that would be a lot more helpful 'cause, like getting the awareness out, and then if they still chose to do it like, they chose to do it but like it's different then. I don't know. I think like more awareness about what could happen about it would be more beneficial than just saying you can't do it cause it it's get people a better idea of what can actually happen.

In addition to using various online tools to selectively share information, participants also actively removed undesirable pictures or sought to control the emailing or texting of particular pictures to certain others. For example, in a discussion on sexting, Andrea (22) noted the difficulty in controlling the distribution of one's personal pictures online, even if the original intention was not to disclose them to a wider public audience:

> "But I think the moment the picture is out there, it's, like, everyone's picture now, on the internet …. It should be your picture. Model pictures, porn, that's one thing. But our own pictures distributed like that is so unfair. But I think, I talked to somebody about this, and they said it would be hard to charge, find, and charge everybody who distributed those pictures."

Discussion: Comprehending SNS Insecurities and Controls

Although the participants frequently spoke about the loss of privacy and the collection and use of personal information by SNS, they had strategies to help them obtain control over their information and to minimize insecurities. They expressed concerns primarily about the permanency of the information they shared online, and particularly how that could pose a challenge to them in the future (i.e., when applying for jobs). Similarly, the girls and young women took issue with the collection of personal information online, which resulted

in a loss of their anonymity and their ability to distance themselves from the offline world.[42]

In contrast to policy makers who attributed these insecurities to be a result of the actions of children and youth,[43] the girls and young women we spoke to commonly assessed security risks when they were interacting online and attempted to keep control of their information. In particular, they frequently made judgments about whether something they either did or encountered on SNS was right or wrong, appropriate or inappropriate, and creepy/strange or familiar. Because of the potential consequences of their actions, they then acted accordingly by blocking or deleting users, censoring themselves, or disengaging from conversations. Although girls and young women were portrayed in policy as being unaware, or not considering the consequences of their actions online, the participants clearly expressed discomfort regarding the need to share (so much of) their personal information and were concerned with what corporations sought to do with that information. This finding is consistent with previous research that determined that girls and boys were uncomfortable with the amount of personal information corporations collected from them, and, as a result, likened such corporations to stalkers.[44] This concern for privacy also extended to family members, as children are careful to guard their activities from family members.[45] In particular, control over image and self-presentation was important to girls and young women.[46]

The eGirls participants instead attributed the insecurities they experienced online to the online environment, as opposed to their own specific actions (i.e., those within their control). The large number of people they interacted with online, and the complexity of privacy settings and online forum structures, were viewed as increasing the sharing of (permanent) information in ways that the user could not control and could not reasonably understand or predict. Control appears to be a significant issue as protection of one's privacy is dependent on one's ability to reduce or minimize the likelihood that that information is used in unknown ways.[47] It is, therefore, understandable that the participants noted feeling like they had to be a "defensive user" in today's online environment, as they were expected to understand and foresee potential incidents in a complex and ever-changing environment.

These insecurities were also linked to the pressure on girls and young women to participate with friends, family members, schools

(e.g., teachers), and community organizations (e.g., Girl Guides, sports activities, community groups, etc.) online. Through all of these offline interactions, girls and young women were also expected to create and maintain mutual and respectful online interactions. This contrasts with policy makers' attribution of risks to the extensive use girls make of social media, since people within the individual's offline world are expecting and demanding that use and, in some cases, participating in online social media on their behalf (e.g., parents' pictures and videos of their children).

Moreover, the commercial nature of digital spaces and the profit associated with the trade in personal information not only promote but also require insecurity, in many cases. The emphasis to include more friends, messages, notes, posts, personal information, and pictures, rather than less, is consistent with a business model that encourages the disclosure and sharing of information on the part of many users who are visibly linked to each other through "tagging" each other in comments and pictures.[48] The sharing of personal information that results from these SNS features often occurs without the express consent and knowledge of the user until after the fact. Deleting and removing oneself from these comments and photographs is often difficult and time consuming. Accordingly, even when one intends to limit the disclosure of one's information and reduce insecurities, these insecurities still result.[49]

Girls and young women both attributed the cause of some insecurity to the nature of the online environment due, in large part, to the perceived anonymity of other users and the resulting lowering of inhibitions. This is in sharp contrast to policy makers, who tend to privilege the actions of these companies, while requiring children and youth to act in certain proscribed ways to avoid risks that have been created by the design of the environment itself.[50] Current policies accordingly constrain the privacy of youth and children and their ability to use technology for exploration, self-expression, relationship building, and social validation. In some cases, these constraints have resulted in the criminalization of those who such laws were originally designed to protect. As Bailey and Steeves note, "corporate and policy practices often simultaneously ignore and constrain girls' online agency." [51]

In terms of responding to online insecurities, although girls and young women were generally in agreement with the response of policy makers to criminalize perpetrators, they also noted the

potential impact the criminal justice system would have on girls as victims. As a result, the participants were focused on responses that included providing advice and assistance to girls and young women who were inexperienced in using social media. They were also focused on providing them with opportunities to learn about social media and the importance of certain (defensive) practices and strategies online, in order to develop resiliency with respect to threats to security.[52]

These practices included the use of false information to ensure anonymity.[53] Other strategies included the use of a triage process to provide an opportunity to think about the potential consequences of how their information appeared, whether it could be used by unknown others, and how that use may reflect on or be seen by their friends and family. This demonstrates what Karaian refers to as a broadening of the scope of responsibilization where girls and young women are "often understood as both victim and perpetrator" of their own and others' demise.[54] As Karaian notes in her examination of sexting campaigns, "girls are responsibilized for managing not only their own risks but also the risks, such as criminalization, faced by their peers"; that is, "by abstaining from sexting these girls can prevent the criminalization of their peers who, presumably, would not have re-posted or further disturbed their images had the girls not created them in the first place."[55] And since one's ability to secure one's information is constrained by the architecture of SNS themselves, the ability of girls and young women to prevent these instances is likely an illusion. The constraints placed on girls ironically force them to "lose the calculating subjectivity that is necessary for governing oneself"[56] in an online environment shaped by privacy laws that seek to commodify the information they post there.

Conclusion

As Bailey notes, policymakers are implicitly asking and expecting children and youth to respond to infrastructural challenges that they themselves have no control over. As a result, refraining from participation in SNS appears to be the most effective response to these challenges.[57] However, because SNS are so essential to the social interactions of children and youth, such action is not possible. We need to make available safer ways to participate in SNS that do not threaten the security of one's personal information.[58] For example,

more control over one's privacy settings in a clear and understandable manner appears to be one way to improve the experiences of girls and young women online.[59] In addition, alternatives to the law, such as the promotion of societal values and mechanisms that reshape social media into an encouraging and learning environment for girls, may also assist in the creation of positive online experiences.

Notes

1 Jane Bailey & Valerie Steeves, "Will the Real Digital Girl Please Stand Up?: Examining the Gap Between Policy Dialogue and Girls' Accounts of their Digital Existence," in *New Visualities New Technologies: The New Ecstasy of Communication*, eds. Hille Koskela & Macgregor Wise (London: Ashgate, 2013), 1–36; D. Buhrmester & K. Prager, "Patterns and Functions of Self-Disclosure during Childhood and Adolescence," in *Disclosure Processes in Children and Adolescents*, ed. K. Rotenberg (New York: Cambridge University Press, 1995), 10–56; Patti M. Valkenburg & Jochen Peter, "Social Consequences for the Internet for Adolescents," *Current Directions in Psychological Science*, 18 (2009): 1, doi:10.1111/j.1467.

2 Bailey & Steeves, *supra* note 1; Helen Adams, "Social Networking and Privacy: A Law Enforcement Perspective," *School Library Media Activities Monthly* 23 (2007): 33, as cited in Priscilla Regan & Valerie Steeves, "Kids R Us: Online Social Networking and the Potential for Empowerment," *Surveillance & Society* 8:2 (2012), <http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3483/3437>; Ilene R. Berson & Michael J. Berson, "Challenging Online Behaviors of Youth," *Social Science Computer Review* 23:1 (2005), 29–38, <http://www.abusewatch.net/Challenging%20Online%20Behaviors%20of%20Youth%20Berson%20and%20Berson.pdf>; Sonia Livingston & Magdalena Bober, *UK Children Go Online: Surveying the Experiences of Young People and Their Parents* (London: Economic and Social Research Council, 2004); Kelly Mendoza, "'WATZ UR NAME?' Adolescent Girls, Chat Rooms, and Interpersonal Authenticity," Working Paper No. 403, (Media Education Lab, 2007), <http://mediaeducationlab.com/sites/mediaeducationlab.com/files/403_WorkingPapers_Mendoza.pdf>; Leslie Regan Shade, "Internet Social Networking in Young Women's Everyday Lives: Some Insights from Focus Groups," *Our Schools/Ourselves* (Summer 2008): 65–78, <http://www.policyalternatives.ca/sites/default/files/uploads/publications/Our_Schools_Ourselve/8_Shade_internet_social_networking.pdf>.

3 Bailey & Steeves, *supra* note 1.

4 Sandra Petronio, *Boundaries of Privacy: Dialectics of Disclosure* (New York: State University of New York Press, 2002).

5 Bailey, Chapter I.
6 For a list of the relevant bills being debated at the time of discussion, see Hannah Draper, "Canadian Policy Process Review 1994–2011," 5 March 2012, The eGirls Project, <http://egirlsproject.ca/research/research-memos-backgrounders/2013-policy-discourses-jurisdictions/>.
7 Bailey & Steeves, *supra* note 1.
8 *Ibid*.
9 Bailey, Chapter I.
10 For a rural/urban comparative analysis, see Burkell & Saginur, Chapter V.
11 Our rural adult focus group included Catlin (19), Laura (18), Trish (18), and Brianne (20). Our rural minor focus group included Courtney (17), Chelsea (17), Paula (17), Beth (16), and Josie (16). Our urban adult focus group included Keira (21), Donna (19), Jill (20), Andrea (22), Ashley (18), and Kathleen (20). Our urban minor focus group included Vicky (17), Eve (16), Abby (17), Jacquelyn (17), Lauryn (17), Monique (16), and Jane (16). Our rural adult interviewees were Cassandra (19), Becky (19), and Amelia (18). Our rural minor interviewees were Monica (16), Lynda (17), and Nicole (16). Our urban adult interviewees were Alessandra (21), Mackenzie (20), and Cindy (20). Our urban minor interviewees were Alicia (17), Clare (16), and Josée (15).
12 See also Bailey, Chapter I.
13 Valerie Steeves & Cheryl Webster, "Closing the Barn Door: The Effect of Parental Supervision on Canadian Children's Online Privacy," *Bulletin of Science, Technology & Society* 28:1 (2008), doi:10.1177/0270467607311488.
14 The notion of "responsibilization" derives from the work of O'Malley. The concept refers to the process whereby government agencies provide individuals with tools to govern themselves by modifying their behaviour and taking precautions in order to decrease the likelihood that they become victimized through decreased exposure to crime. P. O'Malley, "Responsibilization," in *The SAGE Dictionary of Policing*, eds. A. Wakefield & J. Fleming (London: SAGE, 2009), 277–279. In her analysis of the Respect Yourself campaign, Lara Karaian argues that slut shaming is used to responsibilize teenage girls in order to prevent sexting harms to themselves and potential perpetrators. Lara Karaian, "Policing 'Sexting': Responsibilization, Respectability and Sexual Subjectivity in Child Protection/Crime Prevention Responses to Teenagers' Digital Sexual Expression," Theoretical Criminology 18:3 (2014): 284.
15 Karaian, *supra* note 14 at 284.
16 Valerie Steeves, Trevor Milford & Ashley Butts, *Summary of Research on Youth Online Privacy* (Ottawa: The Office of the Privacy Commissioner of Canada, 2010), <https://www.priv.gc.ca/information/research-recherche/2010/yp_201003_e.pdf>.

17 *Ibid.*
18 Sonia Livingstone, "Taking Risky Opportunities in Youthful Content Creation: Teenagers' Use of Social Networking Sites for Intimacy, Privacy and Self-Expression," *New Media and Society* 10 (2008): 393–411, <http://eprints.lse.ac.uk/27072/1/Taking_risky_opportunities_in_youthful_content_creation_(LSERO).pdf>.
19 Susan Barnes, "A Privacy Paradox: Social Networking in the United States," *First Monday* 11 (2006), <http://firstmonday.org/article/view/1394/1312>.
20 Esther Dyson, "Reflections On Privacy 2.0," *Scientific American* 299 (2008): 50–55, <http://libserver.wlsh.tyc.edu.tw/sa/pdf.file/en/e080/e080p042.pdf>.
21 Valerie Steeves, *Young Canadians in a Wired World, Phase II: Trends and Recommendations* (Ottawa: MediaSmarts, 2005), 17, <http://mediasmarts.ca/sites/mediasmarts/files/pdfs/publication-report/full/YCWWII-trends-recomm.pdf>.
22 Jacquelyn Burkell, Valerie Steeves & Anca Micheti, *Broken Doors: Strategies for Drafting Privacy Policies Kids Can Understand* (Ottawa: Office of the Privacy Commissioner of Canada, 2007): 2, <http://www.idtrail.org/files/broken_doors_final_report.pdf>.
23 Seounmi Youn, "Teenagers' Perceptions of Online Privacy and Coping Behaviors: A Risk-Benefit Appraisal Approach," *Journal of Broadcasting & Electronic Media* 49 (2005): 86, <http://beta.orionshoulders.com/Resources/articles/26_22338_%20().pdf>.
24 Priscilla Regan & Valerie Steeves, "eKids R Us: Online Social Networking and the Potential for Empowerment," *Surveillance & Society* 8 (2012), <http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3483/3437>; Youn, *supra* note 23; Kate Raynes-Goldie, "Aliases, Creeping and Wall Cleaning: Understanding Privacy in the Age of Facebook," *First Monday* 15 (2010), <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2775/2432>.
25 Valerie Steeves, *Young Canadians in A Wired World, Phase III: Online Privacy, Online Publicity* (Ottawa: Media Awareness Network, 2014): 2, <http://mediasmarts.ca/sites/mediasmarts/files/pdfs/publication-report/full/YCWWIII_Online_Privacy_Online_Publicity_FullReport.pdf>
26 Regan & Steeves, *supra* note 24 at 156.
27 *Ibid.*
28 *Ibid.*
29 Matthew J. Hodge, "Comment: The Fourth Amendment and Privacy Issues on the 'New' Internet: Facebook.com and Myspace.com," *Southern Illinois University Law School Journal* 31 (2006): 111–112, <http://pdf.aminer.org/000/244/151/privacy_issues_on_the_internet.pdf>; Regan & Steeves, *supra* note 24.

30 Jim Rapoza, "'Privacy Policy' as Oxymoron: Current United States (US) Law Prevents Real Progress in the On-Line Privacy Push," *eWeek*, 20 October 2008, 48, cited in James P. Lawler & John C. Molluzzo, "A Study of the Perceptions of Students on Privacy and Security on Social Networking Sites (SNS) on the Internet," *Journal of Information Systems Applied Research* 3:12 (2010), <http://proc.conisar.org/2009/3732/CONISAR.2009.Lawler.pdf>; Sören Preibusch, Bettina Hoser, Seda Gürses & Bettina Berendt, "Ubiquitous Social Networks: Opportunities and Challenges for Privacy-Aware User Modelling," (Berlin: Impressum, 2007), <http://www.diw.de/documents/publikationen/73/diw_01.c.59994.de/dp698.pdf>.
31 Barnes, *supra* note 19; Steeves, *supra* note 25; Steeves at al, *supra* note 16.
32 Bailey, Chapter I; Bailey & Steeves, *supra* note 1.
33 Regan & Steeves, *supra* note 24 at 152.
34 Bailey & Steeves, *supra* note 1 at 4.
35 Steeves et al, *supra* note 16 at 7.
36 Clay Clavert, "Sex, Cell Phones, and the First Amendment," *The Catholic University of America CommLaw Conspectus* 18 (2009), <http://firstamendment.jou.ufl.edu/pubs/SexCellPhonesPrivacyArticle.pdf>.
37 Steeves et al, *supra* note 16 ; Bailey & Steeves, *supra* note 1; Shade, *supra* note 2.
38 Bailey & Steeves, *supra* note 1 at 25.
39 Bailey, Chapter I.
40 Kids Help Phone is a free, anonymous, and confidential phone and online professional counselling service for youth. For more information, please visit:http://org.kidshelpphone.ca/en.
41 MediaSmarts is an educational website containing a wide range of copyright-cleared resources to help teachers integrate media literacy and web literacy. For more information, please visit:<http://mediasmarts.ca/>.
42 Amy Dobson, "Performative Shamelessness on Young Women's Social Network Sites: Shielding the Self and Resisting Gender Melancholia," *Feminism & Psychology* (2013): 411, doi:0959353513510651.
43 Bailey & Steeves, *supra* note 1. Also see Bailey, Chapter I, for further discussion.
44 Bailey & Steeves, *supra* note 1 at 4; Burkell et al, *supra* note 22; Amanda Lenhart & Mary Madden, *Teens, Privacy and Online Social Networks* (Washington, D.C.: Pew Internet & American Life Project, 2007).
45 Livingstone & Bober, *supra* note 2; Steeves, *supra* note 21.
46 Bailey & Steeves, *supra* note 1 at 1.
47 *Ibid*., at 26.
48 Burkell et al, *supra* note 22; Regan & Steeves, *supra* note 24.
49 Bailey & Steeves, *supra* note 1 at 2.
50 *Ibid*., at 25.

51 Bailey & Steeves, *supra* note 1.
52 Valerie Steeves, "Young People on the Internet," in *The Routledge Handbook of Surveillance Studies,* eds. David Lyon, Kevin Haggerty & Kirstie Ball (New York: Routledge, 2012).
53 Regan & Steeves, *supra* note 24.
54 Karaian, *supra* note 14 at 289.
55 *Ibid.*
56 Dawn Moore & Mariana Valverde, "Maidens at Risk: 'Date Rape Drugs' and the Formation of Hybrid Knowledges," *Economy and Society* 29 (2000): 526, cited in Karaian, *supra* note 14.
57 Bailey, Chapter I.
58 Jacquelyn A. Burkell, Alexandre Fortier, Lorraine Wong & Jennifer Lynn Simpson, "The View From Here: User-Centered Perspectives on Social Network Privacy," *FIMS Library and Information Science Publications,* Paper 25 (2013), <http://ir.lib.uwo.ca/cgi/viewcontent.cgi?article=1027&context=fimspub>.
59 See Bailey, Chapter I, for further discussion and a detailed description of the ways in which technical infrastructures set girls up for conflict online.

Page left blank intentionally