Summary of Research on Youth Online Privacy

Submitted to the Office of the
Privacy Commissioner of Canada
by Valerie Steeves

March 28, 2010

Research Summaries by Valerie Steeves,
Trevor Milford and Ashley Butts

Table of Contents

Executive Summary

This report seeks to inform educational initiatives to promote the protection of children's online privacy by summarizing the social science research findings regarding: how youth conceptualize and manage their personal information in an online environment; and how youth understand and experience their privacy in an online environment, including their preconceptions and attitudes. It also identifies a set of best practices for outreach and public education to help youth manage their online privacy.

General Trends in the Research

Although research continues to engage with the ways in which children's online information is collected and the effectiveness of regulatory responses that incorporate fair information practices, it is very critical of both market-driven collection and data protection responses. Privacy education must go beyond fair information practices and encourage children to critically interrogate the role of advertising, marketing, and consumerism as drivers of children's media products.

Often educational initiatives designed to support this more critical engagement with the online environment are framed in terms of safety. However, research clearly indicates that the fears that children are at risk of sexual predation and/or harassment online are over-stated at best and subject to moral panic at worst. Moreover, safety concerns are often used to legitimize increasing levels of surveillance that stigmatize youth, leading to two contradictory results: the child is a victim who must be placed under surveillance for protection; and the child is an anti-social threat who must be placed under surveillance to protect society.

Perhaps more importantly, educational initiatives that focus on teaching children not to disclose personal information because of safety risks are limited because they are out of step with what children know about and experience on the Internet. Many children rely on online media as a platform for identity play, social connectedness and self-validation, and this is the context in which they experience – or fail to experience – online privacy.

Simple rules limiting disclosure do affect behaviour, but this correlation disappears the more a child uses the Net for identity play or social interaction. Likewise, parental supervision does not eliminate but merely reduces disclosure. As such, the current regulatory model alone cannot adequately protect children who have integrated the Net most fully into their social lives. A loss of privacy affects the child's conception of self, trust and authority. Surveillance also reconstructs parenting, child care, the provision of social services, and school by embedding

discourses of risk reduction and responsibilization into the child's social world. Ultimately, a loss of privacy interferes with the child's developmental needs to manage risky situations and become resilient, consolidate a pro-social identity, develop relationships based on trust and experience democratic citizenship. Education to advance children's online privacy must therefore go beyond informational campaigns, and begin to problematize and question the real affects of surveillance on children's lives, including the crucial relationship between privacy, trust and democracy.

Managing Personal Information Online

Children frequently post information online simply because there is an entry field for the information on the site. Disclosure is also tied to perceived benefits – the more a site promises them, the more likely they are to disclose.

The information they do reveal is often highly personal. This type of disclosure is motivated by a desire to express oneself, present a positive self image and remain connected to real world friends.

Disclosure practices vary by gender. Girls are more likely than boys to post a profile but they are also more likely to try to keep that profile private. Boys who do post profiles, on the other hand, feel more comfortable than girls with disclosing their last name, city/town of residence and cell phone number. At the same time, boys are more likely to lie on their profiles, whereas girls are more likely to be truthful with the information they do post. Online parental supervision is also gendered. Parents of girls are more likely to check up on them online than parents of boys.

Nearly 80 per cent of teens report that young people are not careful enough about releasing personal information online. Many have devised strategies to protect their online privacy, including: physically shielding the screen, deleting histories; counter-surveillance of teachers; secret email accounts; giving out false information; providing incomplete information; and going to different Web sites that do not ask for personal information.

Young People's Attitudes and Experiences

Children perceive the Web to be more private because it provides them with ways to control who can overhear their conversations.

The perception that online space is private space is reinforced by the following elements: it allows them to communicate behind a screen; they can either bypass the physical constraints of face-to-face communications (such as judgments based on body type or facial features) or exercise greater control over their image and/or conversations with peers; the design of social networking sites appear to draw acquaintances together in a more or less reclusive online venue; the sites ask for email addresses and establish membership requirements; public blogs have minimal content restrictions and are relatively free of punishment for transgressive communications.

Children who know they are being watched report that they continue to participate in online communications because they feel they do not have a choice – online communication has become an essential part of their social world and one of the ways in which they connect with friends and family.

Many continue to assert a claim of privacy to online information even though it is posted on the Internet. From the child's perspective, the problem is not that they reveal but that others – unintended others – watch them. Creating regulatory mechanisms based on public accessibility is therefore problematic because the mere fact of technical accessibility does not affect young people's expectation that their conversations are private and should be treated as such.

Children do not perceive that they are giving up their privacy by posting information online; instead, they are redefining privacy to take into account the ways in which transparency enhances their personal and social experiences. They rely on new rules of etiquette to protect their privacy and are able to police privacy invasions among their own peers because, paradoxically, online invasions of privacy, particularly within social networks, take place in the public sphere.

Young teens, who are developmentally pre-disposed to participate in identity play, tend to post elaborate, stylized, comprehensive personal profiles. Older teenagers post profiles which contain more or less authentic, straightforward information which is made available to friends and acquaintances who are also known in the real world, reflecting an age-appropriate developmental interest in authenticity and genuine links to others.

Young people already engage in at least an elementary form of self-protection in virtual spaces and, even subconsciously, youth evaluate which private information is too private to make publicly available.

Best Practices for Outreach and Public Education

Although informational campaigns that tell children about fair information practices do serve a purpose, they are not sufficient in themselves to adequately meet children's needs.

Educational materials that simply tell children not to disclose their information online are likely to fail because they do not take into account the fact that online media are an integral part of many children's social world and that young people benefit from online transparency.

Similarly, safety oriented campaigns are ineffective because they focus on dangers that are both highly unlikely and at odds with young people's social experiences. They can also encourage adults, especially parents and teachers, to place children under online surveillance, in effect invading children's privacy to protect children's privacy.

Fair information practices campaigns should therefore focus on practical skills, such as how to: use privacy settings; delete an account; ask someone to remove a tag from a tagged photo; avoid filling in non-mandatory fields on registration and profile pages; provide false or misleading information when appropriate; effectively use pseudonyms; complain about unfair practices; and find alternative Web sites that do not collect their information.

At same time, educational initiatives that encourage children to critically interrogate the broader issues at play should be prioritized. These issues include:

- The role of advertising, marketing, and consumerism as drivers of children's online experiences
- The relationship between privacy and identity, trust and social relationships
- The role privacy plays in democratic relationships
- The relationship between surveillance, risk reduction and responsibilization

Privacy education needs to illustrate the ways in which surveillance and consumerism come together to constrain girls' potential for equality and manipulate their private relationships for commercial purposes, as corporations intentionally structure online spaces to embed marketing messages, encourage a certain type of consumption and entrench the legitimacy of a certain kind of body and a certain kind of girl.

It is also important to educate adults, especially parents and teachers, about the important role privacy plays in healthy child development. Parents who talk to their children about online issues and encourage them to develop their own views of the world raise more privacy-savvy children. In addition, educational initiatives that incorporate discussion with other reference groups, including peers, teacher, and parents, play an important role in positively affecting children's online privacy behaviour.

Introduction

A literature review was conducted in 2007 in order to identify major trends in academic research on children's privacy. This review indicated that researchers in a number of fields were doing work that could inform our understanding of the area, although few addressed the issue of children's privacy directly. For example, non-governmental organizations in both Canada and the United States had done research on children's use of new technologies but few had focussed solely on privacy issues. Those few studies that had done so had typically sought to measure compliance with regulatory schemes thought to protect their privacy, rather than to explore children's privacy preferences and practices.

Turow's 2001 report entitled *Privacy Policies on Children's Websites: Do They Play by the Rules?* is a good example. The research was published by the Annenberg Public Policy Centre of the University of Pennsylvania, a leading American research centre. The vast majority of the Centre's work focuses on children's use of traditional media. When children began to migrate to online media, the Centre gathered data about information collection practices on children's online playgrounds and published a single report on the issue. Given the fact that the question of privacy fit within a broader research agenda focusing on children and media, the paper focused less on children's lived experience of privacy than it did on the effectiveness of regulatory mechanisms to protect the flow of children's online information.

Since the early 2000s, researchers from a number of disciplines have begun to examine the meaning of children's online practices, and the body of knowledge on children's online behaviours and experiences has grown considerably. At the same time, an international consensus has emerged to prioritize educational initiatives to promote the protection of children's online privacy[1].

This report seeks to inform those initiatives by summarizing the social science research findings regarding:

(a) How youth conceptualize and manage their personal information in an online environment; and

(b) How youth understand and experience their privacy in an online environment, including their preconceptions and attitudes.

and identifying a set of best practices for outreach and public education to help youth manage their online privacy.

Method

Much of the early research regarding children and online media was conducted by non-governmental organizations. The research protocol was therefore designed to identify both research reports published by NGOs and academic literature dealing with children's online privacy.

First, Web sites of NGOs known to be leaders in research regarding young people's use of new technologies and media were identified. These NGOs include the Media Awareness Network, the Canadian Teacher's Federation, the Kaiser Foundation, the PEW Centre's Internet and American Life Project, the Vanier Institute of the Family, UK Kids Go Online, EU Kids Go Online, UNICEF and the Annenberg Public Policy Centre. A detailed review of all research published on these sites was conducted to identify those reports that either deal with privacy directly or provide insight into young people's online privacy behaviours. Links to partner organizations or cited studies found on these sites were followed, to identify other research in the field. In addition, a general Web search was conducted. A list of all relevant NGO reports was created.

Second, a comprehensive search of the academic literature was conducted to identify relevant research in the disciplines of political science, sociology, communication, law, psychology, geography, criminology, business studies, social work, and education. Because of the multi-disciplinary nature of the search, a number of academic search engines were used, including:

- ACM
- Blackwell Synergy
- Cambridge University Press
- EBSCO
- Emerald Library
- JSTOR
- Project Muse
- PsychINFO
- Sage Journals
- Scholar's Portal
- Springer
- Web of Science (Web of Knowledge)
- Wilson Web (Humanities parameter and Social Sciences parameter)

Search terms were designed to identify a broad range of research about children and online media in general, so we could select specific articles that dealt with privacy (expressly or implicitly) for annotation after reviewing abstracts. The terms therefore included the following parameters:

- [child* OR youth OR young person OR teen* OR adolescent*] AND:
    - priv*
    - technolog*
    - internet
    - world wide web
    - www
    - social networking
    - Facebook
    - MySpace

Search results were reviewed on a page-by-page basis until we reached 5 pages with no relevant results. Articles with relevant abstracts were selected and a running list of citations was created.

The lists of relevant research reports/articles from the NGO search and the academic search were merged. Each report/article was then read to determine whether or not the research findings helped inform our understanding of the two primary research questions. Discarded reports/articles were removed from the list.

A summary was then drafted for each of the 113 reports/articles left on the list. The summaries were read through a number of times to identify key themes. In order to facilitate document retrieval and analysis, a list of key words was developed and relevant key words were added to each summary.

The full list of reports and articles summarized, list of keywords, and research summaries are available online at www.techlaw.uottawa.ca.

Analysis

General Trends in the Research

Earlier research on children's online privacy was mostly limited to: (1) identifying the ways in which children's personal information was collected online; and (2) evaluating regulatory responses that incorporated fair information practices (Montgomery, 1996; Turow, 2001; Cai & Gantz, 2000; Hertzel, 2000; Lewandowski, 2003). Although more recent research continues to engage with these issues, it is far more critical of both market-driven collection and data protection responses.

Part of this is fine-tuning. For example, a number of studies have reported that privacy policies are extremely difficult for children to understand (Media Awareness Network, 2001-2005) and some have looked for ways to encourage corporations to create comprehensible policies that can better support informed decision-making on the part of children and parents (Burkell, Steeves & Micheti, 2007; Montgomery, 2009). However, most research that touches upon this topic[2] is highly critical of data protection and calls for solutions that go beyond mere informational control. Data protection is not insignificant; rather, it is insufficient on its own to deal with the problems of behavioural advertising and its impact on child development (Chung and Grimes, 2005; Steeves, 2006; Meyers, 2009; Steeves 2009a; United Kingdom, 2009). Calvert (2008) sums it up: stealth marketing techniques such as hiding advertising/commercial content within games, video clips, or other online media [are] particularly problematic to children younger than 8, since they lack the cognitive abilities to perceive the persuasive nature of online or television advertisements. Even older children are susceptible to online marketing strategies, which blur the lines between commercial and social content and prey upon children's faith in the reliability of certain virtual spaces. As such, youth may disclose personal information for marketing or advertising purposes and not know they are in fact doing so. Although some government regulations are currently in place to protect children's privacy, it is suggested that these sanctions be expanded in order to fully ensure that youth are protected from coercive marketing online.

To a large extent, the call for regulation beyond data protection has been driven by a body of research that places online marketing practices in a larger context, one that critically interrogates the role of advertising, marketing, and consumerism as drivers of children's media products. In this sense, online privacy questions are *also* questions about the appropriate role of media in children's lives and the affect of hyper-consumption on their personal and social development. Key to this approach is the finding that children do not willingly trade away their privacy for the pleasures of participating in the online world; rather, their release of personal information reflects either a belief that the medium is in

fact private (Barnes, 2006; Berson & Berson, 2006; Read, 2006; Timm & Duven, 2008) or a sense that they have no power to demand that their privacy be respected (Calvert, 2009; Burkell, Steeves & Micheti, 2007). There is evidence that when marketing intrudes on their social relationships *and* they are given a voice, they use privacy settings to erect boundaries around their online information (National Centre for Technology in Education, 2008) and come together to demand change (Steeves, 2009).

Often educational initiatives designed to support this more critical engagement with their online environment are framed in terms of safety (Adams, 2007; Livingstone & Haddon, 2009). However, research clearly indicates that the fears that children are at risk of sexual predation and/ or harassment online are over-stated at best (Di Gennaro & Simun, 2008) and subject to moral panic at worst (Lawson & Comber, 2000; Giroux, 2003). Moreover, safety concerns are often used to legitimize increasing levels of surveillance that stigmatize youth (Giroux, 2003). Ironically, the focus on safety has led to two contradictory results: the child is a victim who must be placed under surveillance for protection; and the child is an anti-social threat who must be placed under surveillance to protect society.

Perhaps more importantly, educational initiatives that focus on teaching children not to disclose personal information because of safety risks are limited because they are out of step with what children know about and experience on the Internet. The vast majority of recent research studies indicate that young people rely on networked communications to help them develop a sense of identity (including experimenting with various identities) and deepen their connection to the people they know in the real world. It is noteworthy that, although 17 of the articles[3] summarized herein discuss the kinds of relationships that form in virtual spaces, only five discuss this phenomenon as something separate and apart from the real world; and 29 articles[4] report that children use online media to communicate with and feel connected to their real world friends and family.

Accordingly, many children rely on online media as a platform for identity play, social connectedness and self-validation (Shade, 2008), and this is the context in which they experience – or fail to experience – online privacy. Simple rules limiting disclosure do affect behaviour, but this correlation disappears the more a child uses the Net for identity play or social interaction. Likewise, parental supervision does not eliminate but merely reduces disclosure (Steeves & Webster, 2008). As such, the current regulatory model alone cannot adequately protect children who have integrated the Net most fully into their social lives.

Literature that approaches the issues under the rubric of surveillance studies provides an interesting window into the ways in which a loss of privacy affects the child's conception of self, trust and authority. To date, surveillance scholars have not focused extensively on children; however, *Surveillance & Society,* the leading surveillance studies journal, put out a call for papers in January 2009 and in April 2010 a special issue on surveillance and children will be published[5].

The *Surveillance & Society* papers[6] are drawn largely from child studies, social work and education, and bring a new body of academic knowledge into dialogue with privacy concerns. As a set, they problematize the purported need to "protect" children by placing them under surveillance, and demonstrate the ways in which surveillance is experienced differentially by children, based on their gender and their socio-economic status. They also document the ways in which surveillance is reconstructing parenting, child care, the provision of social services, and school by embedding discourses of risk reduction and responsibilization into the child's social world. Ultimately, this interferes with the child's developmental needs to manage risky situations and become resilient, consolidate a pro-social identity and develop relationships based on trust. Earlier work (David, 2001) also argues that surveillance interferes with the child's ability to learn because she is never given the private space in which she can struggle with and integrate new concepts.

Lastly, a number of articles examine the ways in which a loss of privacy affects a young person's understanding of citizenship and democratic governance[7]. Too often, commercial interests, the state and schools combine to create information infrastructures that make a lack of privacy the default – whether for profit, risk reduction, efficiency or convenience. Education to advance children's online privacy must therefore go beyond informational campaigns, and begin to problematize and question the real affects of surveillance on children's lives, including the crucial relationship between privacy and democracy.

Managing Personal Information Online

Children and young people release personal information on social networking sites and blogs, and in order to register for online services and obtain benefits (e.g. prizes, game points, quizzes). Much of this disclosure is non-reflexive; in one study, children reported that they frequently post information online simply because there is an entry field for the information on the site (De Souza, 2009). However, disclosure is also tied to perceived benefits – the more a site promises them, the more likely they are to disclose (Chung & Grimes, 2005; Youn, 2005).

The information they do reveal is often highly personal. Williams & Merten (2008) report that 83 percent of their random sample of profiles posted by teens between the ages of 16 and 18 included discussion or references to substances (81 percent referenced alcohol, and 27 percent discussed illegal drugs). Nearly half contained some form of sexual content, with 44 percent using explicit or graphic language and 16 percent referencing the teen's own sexual activity. Thirty-seven percent included positive comments about parents and 22 percent contained positive comments about siblings; 16 percent made negative comments about parents and two percent included negative comments about siblings. Forty-three percent included the teen's full name, 10 percent their phone number, 11 percent their place of employment, and 20 percent their email address. Most blogs (71%) also included information about the teen's interests (such as favourite movies, music, books, and hobbies), and 40 percent disclosed information about prior social gatherings.

This type of disclosure is motivated by a desire to express oneself, present a positive self image and remain connected to real world friends (Stern, 2004; Shade, 2008; De Souza, 2009). However, disclosure practices vary by gender. To a certain extent, this reflects differential patterns of online use in general; whereas boys are more likely to play games, girls typically prefer social networking and communication over other uses (Media Awareness Network, 2005; Mendoza, 2007). Accordingly, digital content that contains personal information – the profiles, websites and online videos that populate the post-Web 2.0 world – is far more likely to be created by girls than boys. Not only are girls more likely than boys to use social networking sites (SNS), they also use them for different reasons. Whereas girls rely on SNS to maintain and deepen their existing social relationships, boys are more likely to look for new friends and flirt with strangers (Adams, 2007). Teen girls who write blogs perceive their blogs to be vehicles for both interpersonal and mass communication and accordingly write for two audiences, friends and a larger public audience (mostly seen as composed of other teens they do not know) (Bortree, 2005).

Accordingly, girls are more likely than boys to post a profile but they are also more likely to try to keep that profile private. Boys who do post profiles, on the other hand, feel more comfortable than girls with disclosing their last name, city/town of residence and cell phone number. At the same time, boys are more likely to lie on their profiles, whereas girls are more likely to be truthful with the information they do post (Lenhart & Madden, 2007).

Although girls are prolific online writers, research indicates that they are particularly concerned about disclosing information that could be linked to their real world location because they are girls. In the words of one middle school girl:

> If they can access you, like person to person or in any way other than [the internet], it's not okay...Like if they can...talk to you, if they can find out where you live, that's not okay. If you're putting anyone in danger, it's not all right (p. 17).

This perception is reinforced by the fact that online parental supervision is also gendered. Parents of girls are more likely to check up on them online than parents of boys (Lenhart & Madden, 2007; Shin, Schriner & Cho, 2009). In the words of two high school boys:

> Girls are more vulnerable than guys are... I have two older sisters and my parents tell me that all the time. They let me get away with stuff that they never got away with. (Lenhart & Madden, 2007, p. 18)

> I have an older sister and a younger sister, and I watch over my little sister. They are kind of like are more lenient when she's with me. But if she's not, she's in at 10:00. If she's with me, she can come home at like three, four in the morning (*ibid*).

Interestingly, navigating the line between the private and the public sphere both online and off is still problematized for girls in ways that it is not for boys. Perhaps the best illustration of this is the way that girls manage their online pictures.

When boys and girls are young, they tend to post pictures of themselves or friends at an equal rate. By 12-14 years of age, girls begin to pull ahead a bit, and by 15-17, girls are significantly more likely than boys to post pictures of themselves or friends. Paradoxically, girls, particularly older girls, are more likely to restrict access "most of the time" to the photos they post (Lenhart & Madden, 2007; National Centre for Technology in Education, 2008).

If you keep in mind what girls like about online media, this apparent contradiction begins to make sense. Research indicates girls use the Internet to escape the kinds of things that constrain their movement in the real world, to try on different identities, to maintain their real world social connections, including connections with family, and to create a sense of authenticity by forming real friendships and enjoying a sense of community. Accordingly, it is important for girls to be seen in the online world, but at the same time, it is important that they not be seen "badly".

In spite of what looks like rampant disclosure to adult eyes, nearly 80 per cent of teens report that young people are not careful enough about releasing personal information online (Barnes, 2006), and many have devised strategies to protect their online privacy. For example, Hope (2005) reports that students hide their online activities from teachers by physically shielding the screen and deleting histories; they also use the computer to put the teacher under surveillance[8]. Young people use similar strategies with parents; as early as 2001 many had secret email accounts and more than one third were deleting their Internet search histories so their parents could not track them (Media Awareness Network, 2001). They also seek to avoid surveillance on Web sites by giving out false information (Media Awareness Network, 2004; Youn, 2005), and providing incomplete information and going to different Web sites that do not ask for personal information (Young, 2005, 2009).

Young People's Attitudes and Experiences

Interestingly, many children report that using online communication is, in and of itself, a strategy to protect their privacy. The Web is perceived by them to be more private because it provides them with ways to control who can overhear their conversations (Livingstone, 2005a, 2005b; Media Awareness Network, 2005; Steeves, 2005). In like vein, they actively search out private physical spaces so they can go online to search for sensitive or personal information (e.g. sexual health) without the burden of being judged or identified (Skinner, Biscope & Poland, 2003).

The perception that online space is private space is reinforced by a number of elements. The technology allows for a form of pseudo-anonymity that children exploit in the context of identity play. Online communication is empowering precisely because it allows them to communicate

behind a screen; they can either bypass the physical constraints of face-to-face communications (such as judgments based on body type or facial features) (Berson & Berson, 2005) or exercise greater control over their image and/or conversations with peers (Livingstone & Bober, 2003; Media Awareness Network, 2004; Ito, 2008).

The design of social networking sites in particular also contributes to this sense of being in a private space. SNS appear to draw acquaintances together in a more or less reclusive online venue; the fact the sites also ask for email addresses and establish membership requirements leads children to believe that their discussions are in fact private (Barnes, 2006). Even public blogs are seen by children as relatively anonymous since they have minimal content restrictions and are relatively free of punishment for transgressive communications; this creates a sense of trust, encouraging children to express themselves more freely than they would otherwise and to post content which would otherwise considered inappropriate in a public medium (Berson & Berson, 2006).

Although many children may not be aware of the ways in which their online activities are watched by others, those who are frequently report that they continue to participate in online communications because they feel they do not have a choice – online communication has become an essential part of their social world and one of the ways in which they connect with friends and family (Burkell, Steeves & Micheti, 2007; Di Gennaro, Corinna, and Miriam Simun, 2008).

However, that does not mean that they no longer value or experience privacy. Many continue to assert a claim of privacy to online information even though it is posted on the Internet (Barnes, 2006; Livingstone & Bober, 2003; Steeves, 2005). And there is a growing concern among young people regarding who *should* have access to their online journals and profiles (Barnes, 2006; Tim & Duven, 2008). For example, some argue that parents who read their children's online journals are participating in acts which are equivalent to eavesdropping (Barnes, 2006). In this sense, the problem is not that they reveal but that others – unintended others – watch. Similarly, students report that they do not think that their school administrators are watching them and if they are, they *should* not be[9]. Creating regulatory mechanisms based on public accessibility is therefore problematic because the accessibility does not affect their expectation that their conversations are private and should be treated as such (Steeves, 2008).

Moenk (2007) accordingly argues that children are not giving up their privacy – they are redefining it to take into account the ways in which transparency enhances their personal and social experiences. He cites new rules of etiquette that enforce their privacy expectations, and suggests that they are able to police privacy invasions among their own peers because, paradoxically, online invasions of privacy, particularly within social networks, actually take place in the public sphere.

Young people's privacy behaviours are also effected by their developmental needs. Livingstone reports that young teens tend to post elaborate, stylized, comprehensive personal profiles, which is consistent with the high levels of identity play that is part of those developmental years. Older teenagers post

profiles which contain more or less authentic, straightforward information which is made available to friends and acquaintances who are also known in the real world, reflecting the developmental interest in authenticity and genuine links to others that is common at that age. Online privacy is also affected by social networking systems' binary classifications of friends, where friends may be prioritized and certain information may be released only to certain high-priority friends. In this way, young people already engage in at least an elementary form of self-protection in virtual spaces and, even subconsciously, youth evaluate which private information is too private to make publicly available (Livingstone, 2008). There is also evidence that young people are aware of the public/private nature of the medium, and have used this to collectively challenge institutional control over their information when they are given the tools to do so. In this sense, the technology itself is what provides them with a channel to resist surveillance and reassert privacy boundaries (Regan & Steeves, forthcoming).

Best Practices for Outreach and Public Education

Although informational campaigns that tell children about fair information practices do serve a purpose, they are not sufficient in themselves to adequately meet children's needs because data protection is limited in its ability to fully address children's online privacy concerns.

Educational materials that simply tell children not to disclose their information online are likely to fail because they do not take into account the fact that online media are an integral part of many children's social world and that young people benefit from online transparency. Moreover, these types of campaigns legitimize commercial and state surveillance without addressing young people's desire to protect their privacy from others who "should not be looking".

Similarly, safety oriented campaigns are ineffective because they focus on dangers that are both highly unlikely and at odds with young people's social experiences. They can also encourage adults, especially parents and teachers, to place children under online surveillance, in effect invading children's privacy to protect children's privacy. This may be counter-productive. For example, children who participated in the Young Canadians in a Wired World, Phase II focus groups reported a bemusement that adults were concerned with their exposure to online pornography because it was merely part of a broader social mediascape that is highly sexualized. They felt that safety measures constrained their online activities by placing them under surveillance but failed to protect them from pornographic pop-ups and other irritations. Most importantly, such measures were patronizing and demonstrated adults' lack of trust in them. They indicated a preference for educational initiatives that would give them the tools they need to critically evaluate online information and make informed choices about what they wanted to see (Media Awareness Network, 2005).

Interestingly, teachers mirror the same concerns. Rather than imposing content controls on children in school, they prefer to give them the critical thinking skills they need to both navigate through the online world and better understand the media images they encounter (and create) there (Hope, 2005).

There is evidence that children will use privacy controls if they are available to them. Fair information practices campaigns should therefore focus on practical skills, such as how to: use privacy settings; delete an account; ask someone to remove a tag from a tagged photo; avoid filling in non-mandatory fields on registration and profile pages; provide false or misleading information when appropriate; effectively use pseudonyms; complain about unfair practices; and find alternative Web sites that do not collect their information. This could be facilitated by creating a Facebook group that provides instructions and gives young people a place to talk about their privacy experiences and concerns.

At same time, educational initiatives that encourage children to critically interrogate the broader issues at play should be prioritized. These issues include:

- The role of advertising, marketing, and consumerism as drivers of children's online experiences
- The relationship between privacy and identity, trust and social relationships
- The role privacy plays in democratic relationships
- The relationship between surveillance, risk reduction and responsibilization

This is especially important because, although young people have devised a number of strategies to protect their online privacy from people in the real world, many are often naïve about commercial surveillance which intentionally plays upon their developmental needs to encourage them to disclose information (Media Awareness Network, 2005; Steeves, 2005; Shade, Porter & Sanchez, 2005).

And since online privacy is a gendered phenomenon, girls in particular need to learn how to manage the relationship between their online privacy and their sense of identity. Girls are attracted to the Net because it gives them control over their self-presentation. However, the identities available to these girls are constrained by both the business model behind these sites that seeks to commodify their social interactions, and the prevalence of mainstream media images in the offline and online world that privilege a certain type of identity, one that is physically thin and hyper-sexualized.

Privacy education needs to illustrate the ways in which surveillance and consumerism come together to constrain girls' potential for equality and manipulate their private relationships for commercial purposes, as corporations intentionally structure online spaces to embed marketing messages, encourage a certain type of consumption and entrench the legitimacy of a certain kind of body and a certain kind of girl[10].

It is also important to educate adults, especially parents and teachers, about the important role privacy plays in healthy child development. Kerr and Stattin (2000) report that monitoring children will not encourage prosocial behaviour; rather, better adolescent behaviours correlate with

children's willing disclosure of information to parents based on pre-existing relationships of trust. Moreover, children's feelings of being controlled were linked to poor behaviours, suggesting that adult surveillance and tracking may be detrimental to children's adjustment.

Parents who talk to their children about online issues and encourage them to develop their own views of the world raise more privacy-savvy children (Youn, 2008) and family discussions about risky online activities diminish the occurrence of undesirable virtual behaviour in youth, such as meeting strangers face-to-face (Berson & Berson, 2005). Sangmi, et. al. (2009) report that educational initiatives that incorporate discussion with other reference groups, including peers, teacher, and parents, play an important role in positively affecting children's online privacy behaviour.

References

1   See 30th International Conference of Data Protection and Privacy Commissioners *Resolution on Children's Online Privacy*, Strasbourg, 17 October 2008 and Canada's Privacy Commissioners and Privacy Oversight Officials *Resolution on Children's Online Privacy*, Regina, Saskatchewan, 4 June 2008.

2   Indexed under key word "Consumer Choice".

3   Indexed under key word "Social Relationships (Virtual)".

4   Indexed under key word "Social Relationships Real World)".

5   The special issue is co-edited by Valerie Steeves and Owain Jones.

6   Indexed under key word "Surveillance/Monitoring".

7   Indexed under key word "Democratic Participation".

8   See also Livingstone, 2005a and 2005b.

9   This correlates with socio-economic status. For example, although all participants of a study conducted in the United Kingdom reported that surveillance was used to police behaviour and discipline students, girls in private schools felt themselves to be immune because they perceived that the surveillance was targeted at "criminals" and "drunks" rather than at them. In contrast, the girls who attended a working class public school were subjected to surveillance when they participated in a variety of working-class leisure activities such as loitering and public drinking, or because they dressed in a way that was likely to lead to monitoring (McCahill & Rachel Finn, 2010).

10 Montreal-based Do I Look Good encourages young people to post pictures so others can vote on how hot they are. Toronto-based Nexopia asks members to disclose their height, weight, sexual orientation and dating status on their profiles; teens like 14 year old Faith create polls that ask visitors Am I pretty? Ugly? Gorgeous? Alright? and advertise their relationship with their "amazing" boyfriends. These aren't exceptional cases. As noted above, Williams and Merten (2008) report that half of teen profiles contain some form of sexual content, 44 percent use sexually explicit or graphic language, and 16 percent talk about their own sexual adventures.