Hide and Seek: Surveillance of Young People on the Internet

Valerie Steeves

Disney's Club Penguin is a popular virtual community for pre-teen boys and girls, where children create their own penguins, decorate their igloos, play games, and chat with friends. The children are encouraged to be creative and share their thoughts with others. For example, they can send their stories and drawings to the site so they can be viewed by others in the community. Parents are told that they can rest assured that their children are safe, because the site constantly monitors the children's chat and keeps a permanent record of their activities. Children can also help keep the site safe by volunteering to become 'secret agents' who 'spy' on other children who use bad words, reveal personal information or treat other children rudely (Marx and Steeves 2010). Any child breaking the rules will be banned from the site for '24 hours, 72 hours or forever, depending on the offence.'[1] Various testimonials from parents congratulate the company 'for putting so much thought and care into such a wonderful and safe environment for our children.' The site claims that parents 'love the security of Club Penguin [because they] never worry about what [their] kids may happen upon while playing.' As one parent testimonial concludes, 'Your integrity as a company is inspiring.'[2]

As with other social networks, the business plan behind Club Penguin remains opaque. A careful perusal of the legal terms for the site indicates that the site collects personal and non-personal information for 'various purposes related to our business' but those purposes are not enumerated. The primary function of the site, for children to play with branded content for hours

[1] Disney.com, 2011. Club Penguin. [online] Available at: <http://www.clubpenguin.com/> [Accessed 15 January 2011].

[2] ibid

on end to encourage both direct consumption of product and to embed the brand into the social world of the child (Steeves 2006; Grimes and Shade 2005), is hidden behind the statement that, ‘We do not allow third-party companies to solicit or advertise to our users. Our intention is to keep Club Penguin free from any of this sort of direct advertising’ (Disney.com 2011).

This business of embedding brands into young people’s online interactions is part of what Montgomery (2000) calls the new ‘children’s digital media culture,’ a culture in which the blurring of the line between content and commerce is linked to a profound sense of intimacy between online marketers and the young people who play on corporate sites. Surveillance is expressly promoted on sites like Club Penguin as a way to protect children from online dangers, and parents are often co-opted into a joint surveillance project of care and control with benign corporate monitors. However, corporate surveillance also works to support the commodification of children’s online activities. Everything a child does online, from the pages they visit, the conversations they have, the pictures they post, the games they play, is analyzed so that unique individuals – whether personally identified or not – can be parsed into categories based on the preferences, attitudes and relationships they share with others.

This sorting allows companies to do more than advertise to children online; companies can manipulate the online environment around those children to change the child’s behaviour and sense of self through behavioural targeting (BT). Marketer Rob Graham explains:

> To be effective in the new world, advertisers have to stop targeting ‘us’ and start targeting 'me.’ The beauty of BT is that it allows publishers and advertisers to learn more about their customers not as group, but as individuals. Rather than sifting through mountains of data meant to encapsulate the buying patterns of groups of people … [BT

> is] a way to look into the minds of a single, potential customer. (Graham, cited in Estrin 2007: 1)

The goal of looking is to change behaviour: ‘the greatest benefit that rich media ads offer advertisers is the ability to help drive the consumer's behavior toward a specific marketing goal’ (ibid: 3). Graham sums it up: ‘There's no way to sugar coat this. In order to learn more about individual consumers, marketers have to resort to “spying”’ (1).

The complex interplay between children, parents and corporations in online spaces like Club Penguin illustrates many of the tensions found in the emerging surveillance society. Parental surveillance purports to protect the child from unknown dangers, in keeping with both moral panics related to children and technology, and with the neoliberal trend to download responsibility to individual parents and children. In this sense, online parental surveillance is a form of both care and control. Children are also co-opted as surveillance workers; they are encouraged to watch themselves as a form of self care and to watch other children who may pose dangers in and of themselves through transgressive behaviour.

However, as the following discussion demonstrates, children first turned to the internet precisely because it was beyond the parental gaze. They continue to report that the visibility they enjoy online enables them to explore an adult world that is increasingly closed to them because of the risks and dangers it entails, and to deepen the social relationships that are so meaningful to them by watching – and being watched by – their peers. Accordingly, children have a complex relationship with online surveillance. Not only do young people turn to the internet to avoid the hyper-vigilant gaze of parents in physical spaces, but the ability to watch and be watched makes the internet an attractive medium for the type of identity play that is at the core of the work of childhood and adolescence. This work is complicated by how the online environment opens it up to the gaze of the corporations that own the sites young people use. At the same time, the reflexive nature of online surveillance creates spaces where young people can resist both care and control by refocusing the surveillant gaze on the watcher.

A brief history of online surveillance of children

Qualitative research on children's use of online media has created an interesting window into their lived experience with surveillance, and demonstrates how that experience has changed over time. While digital divide issues remain, a large proportion of children in developed countries have access to the net – moreso than children in the global south. Moreover, children's access reflects their socio-economic status, although there are indications that children in lower income families in both developed and developing countries are increasingly getting access to the net through cell phones and other mobile devices.

One of the earliest research initiatives was conducted in 1999 by the Canadian non-governmental organization, the Media Awareness Network (2000), which held a series of focus group interviews with parents and children to explore children's use of the internet. Canada is an interesting exemplar because Canadian children were among the first to go online, and the vast majority enjoy relatively inexpensive high speed access at home and school.

In the parents' groups, the mood was optimistic. The internet, it was believed, would expand children's educational opportunities and help them prepare to be the knowledge workers of tomorrow. Although there was some concern about children 'wasting time' playing games online, things were pretty well under control. As with other forms of media, such as the television, parents kept a watchful, benign eye on their children's online actions, checking in on them from time to time. Almost all agreed that children needed their privacy. Although guidelines were important, rules were there to ensure that their children could learn from their mistakes, and more invasive forms of surveillance were thought to abrogate the trust that was essential to the parent-child relationship.

For their part, children in 1999 reported that not only were their online activities wholly unsupervised by their parents; parents could *not* watch them even if they wanted to because the internet was ‘uncontrollable.’ Children celebrated this new online space precisely because their real world environments were subjected to hyper-vigilant surveillance on the part of their parents. The internet was one place they could explore the adult world, try on new identities and connect with friends without being monitored. As such, a lack of parental surveillance was a defining element of both the space and the opportunities that children found there.

The one point of agreement between children and parents in 1999 was the need for children to be careful about releasing personal information to the strangers they would encounter in this new space. However children felt that online corporations were not strangers and could be trusted to provide age-appropriate content that would filter out some of the unwanted surprises children often found online. Accordingly, they reported a high level of comfort about providing personal information to corporations to win a prize, join a club or play a game.

A second set of qualitative interviews in 2004 told a very different story (Media Awareness Network 2004; see also Livingstone and Bober 2003). Parents expressed a deep frustration over the role of the internet in their children’s lives. From their perspective, their children were merely wasting time playing and chatting endlessly; however, that playing and chatting exposed their children to multiplying risks and parents accordingly needed *more* control to protect them from the evils to which they were exposed online. Surveillance was seen as the solution. Monitoring would provide parents with a way to either find out exactly what their children were doing so they could intervene when needed, or to pre-emptively control their children's behaviour in real time as they surfed so problems could be avoided. In this sense, surveillance would provide both care *and* control. Concerns about invading children's privacy and stunting their developmental need to develop resiliency by encountering and resolving difficult situations were no longer at the forefront.

Children in 2004 reported that this online surveillance was both patronizing and overly invasive. They argued that they were exposed to offensive content continuously across all forms of media, including the films, music videos and advertising they saw with their parents. From their perspective, pornography in particular was 'everywhere' and they could not understand why their parents thought online pornography was any different (Media Awareness Network 2005b: 11). Monitoring was especially problematic for them because the internet was where they achieved privacy *from* their parents. It was this ability to communicate outside of parental control that attracted children to the internet in the first place (ibid: 12). Moreover, online surveillance put children into a difficult position. They felt that if monitoring software reported a pop-up ad with offensive content, for example, they would be unable to convince their parents or teachers that they did not seek out the material. This was particularly troublesome because they could lose access to the internet which would in turn cut them off from their circle of friends (ibid: 11). Instead of surveillance, they called for more education so they could make their own informed choices about the sites they were comfortable visiting.

Interestingly, the one thing children and parents agreed on in 2004 was that branded online content was 'safe'; a large company with a recognizable brand was 'a friend, not a stranger' (Media Awareness Network 2004) and children could visit those sites safely. Both groups reported that corporations would not want to hurt them and could be trusted to act responsibly. The blurring line between content and advertising was largely unnoticed. Over three-quarters of children surveyed in a follow up quantitative study who played games with branded content said that they were ‘just games,’ not ‘mainly advertisements.’ Younger children were particularly prone to believe this: the percentage varied with age, from 18 per cent of eight- and nine-year olds, to 31 per cent of 15- and 16-year olds (Media Awareness Network, 2005b).

However, by 2007, this trust in corporations on the part of children was beginning to wane. Burkell, Steeves and Micheti (2007) report that many of the children they interviewed were uncomfortable with the amount of personal information corporations sought to collect from them. Young people likened corporate web sites to ‘stalkers’ who were out to take advantage of them (ibid: 15). As one 17 year old boy put it, ‘Well, they’re taking advantage of you, that your friends have a hotmail account, they’re on Messenger, like you have to have Messenger … It’s another way to control you’ (ibid). To protect themselves, many lied about their names when asked, but they were also concerned that corporations collected a great deal of information about them surreptitiously, such as their geographic location and their preferences. However, they felt that there was little they could do about this precisely because the internet was so central to their social interactions. And that centrality was rooted in the watching and being watched enabled by the space itself, which allowed them to try on new identities and deepen their social connections through their mediated communications.

Watching you watching me – The internet and the performance of identity

The emphasis on identity play is consistent with the developmental need to pursue what Livingstone calls ‘the social psychological task of adolescence – to construct, experiment with and present a reflexive project of the self in a social context’ (Livingstone 2008: 396). From a

Meadian perspective, this is an inherently social process: children perform various identities through their social interactions with others and their behaviour is then mirrored back to them through intersubjective communication (Regan and Steeves 2010). In Livingstone's words, 'the adolescent must develop and gain confidence in an ego identity that is simultaneously autonomous and socially valued, and that balances critical judgment and trust, inner unity and acceptance of societal expectations' (Livingstone 2008: 397). From this perspective, the ability to watch others, and be watched by them in turn, is an essential part of ego formation. It enables children to acquire the cultural capital they use to construct an identity, and then evaluate the authenticity of that identity by monitoring the reactions of peers to their own performance of it.

The internet is attractive to young people then at least in part because of its surveillant properties. Young people report that it is a relatively safe space to experiment with adult identities and try out social behaviours that they would not otherwise encounter. They can 'lurk' on adult sites, 'stalk' peers on Facebook and 'flirt' in chat rooms, all while minimizing the social risk that face-to-face interaction entails (Livingstone and Bober, 2003). They can also privately seek out information they might not want to ask their parents about. Ironically, what adults see as risks of online interaction children often embrace as opportunities (Livingstone 2008: 396).

Adults often also mistakenly assume that this desire to perform what was previously considered private behaviour in a public space (ibid: 404) means that children no longer value their privacy. Corporations in particular assert that this de-problematizes surveillance because being seen is an integral part of a narcissistic youth celebrity culture. Media headlines like, 'Generation shock finds liberty online: the children of the internet age are ready to bare their bodies and souls in a way their parents never could' and 'Kids today. They have no sense of shame. They have no sense of privacy' (cited in Livingstone 2008: 395) fail to appreciate the subtle ways in which young people negotiate whom to trust, and what to disclose, online (397).

One of Livingstone's most interesting insights is the distinction between the types of identities that children perform as they mature. Younger children typically construct an 'elaborate, highly stylized statement of identity as display' (402) that appropriates highly coded cultural symbols, such as pink hearts for girls and fast cars for boys. The online projection of these identities provides an opportunity for children to be accepted and affirmed by their peers. However, as children grow older, they abandon this stylized presentation of the self in favour of a performance that privileges social connection with others. Hearts and cars are replaced by links to friends and photographs of social interactions with peers (ibid). Both of these kinds of identities benefit from visibility: not only must they be seen, but the ability to see others provides an opportunity to learn about social conventions and ways of being, and to examine other people's location in their broader social network.

Negotiating self in this space necessitates careful and deliberate judgments about who sees what, as well as a familiarity with both the technical and social tools at one's disposal. And the process is highly gendered. For example, boys tend to make social networking profiles public, and girls tend to use privacy settings to restrict who can access what they post on their profiles. However, girls are much more likely to tell the truth about themselves, in contrast with boys who tend to lie and exaggerate. Girls also tend to use coded language to communicate with 'insiders,' posting song lyrics, for example, to tell intimate friends how they may be feeling about a relationship.

This skilful manipulation of public and private reflects the fact that young people seek both publicity and privacy online, in particular publicity with peers and privacy from parents. One research participant puts it this way:

> You don't mind [other] people reading it, but it's your parents, you don't really want your parents seeing it, because I don't really like my parents sort of looking through my room and stuff, because that's, like, my private space. (quoted in Livingstone 2008: 405)

This language resonates strongly with the views of parents expressed in 1999. Similar to those parents, children liken online parental surveillance to 'having your pockets picked' (Livingstone and Bober 2003) and argue strongly that it is a breach of trust (Media Awareness Network 2004). However, this language is at odds with parental claims in 2004 that protection necessitates knowledge and control that can only be acquired through surveillance.

Surveillance as loving and responsible parenting

For their part, parents are under increasing pressure to monitor their children online. Part of this reflects a neo-liberal regulatory regime that places the burden of protecting children on parents. Data protection legislation purports to give parents control by requiring web sites that target children to solicit parental consent before collecting, using and disclosing personal information from children, by convention those who are less than 13 years of age. This in effect creates a binary switch: parents either consent or their children cannot participate in the online community. It also does little to push back against the commodification of children's online interactions, in effect legitimizing the site's surveillance practices through the contractual mechanism of informed consent.

In addition, online companies have been active promoters of media education initiatives that promote parental surveillance. Companies like Microsoft, Google, and Verizon routinely sponsor public education sites that link parents directly to monitoring software and urge them to use online filters and other technical controls to protect their children. These controls enable parents to block 'risky' sites, create a permanent log of their children's online activities, capture their children's online discussions in real time so they can 'listen in' without their child knowing, and run their child's wall posts, profile information, instant messages, emails and posted comments through artificial intelligence software that will alert the parent by email or text when the software detects potential stalkers, bullying or suicide conversations (Marx and Steeves 2010: 13).

In spite of the fact that social science research repeatedly indicates that children are highly unlikely to be randomly subjected to these kinds of communications, marketers for parental control software expressly play up this construction of online risk. For example, PC Tattletale tells parents, 'The Internet Is A Dangerous Place For Your Child … Studies have shown that one in five children have received some type of sexual (*sic*) related solicitation online. With an 87% growth rate of children online and not being monitored, now is the best time to begin a proactive stance in your children's lives to prevent your children from being witness to the virtually infinite number of dangers online.' Not placing your child under surveillance 'is just asking for trouble' because 'No matter how much you trust your child to do the right thing, there are just too many peer pressures and other dangers lurking in cyberspace.' With parental monitoring software, 'you can relax knowing that you have a "secret back door" that you can use to see exactly what they see, and what they are doing online. Do NOT risk your child becoming a potential victim. Take Control of Your Child's Online Experiences And Keep Them Safe' (quoted in Marx and Steeves 2010: 13).

Marx and Steeves argue that parental surveillance is presented 'as an essential part of effective and loving parenting' (13), because parents cannot trust their children to talk to them about their online experiences. Again, PC Tattletale is illustrative: 'Without Parental monitoring software you have no way of knowing what your kids do or where they go when they're online. And even if they are not supposed to, we all know that your child WILL go online unsupervised if they think that no one will find out!' (quoted in Marx and Steeves 2010: 14). From this perspective, early concerns about invading children's online privacy are superseded by the imperative to keep children safe from proliferating unknown and unknowable risks. Trust is replaced by monitoring, and the companies that own the sites children inhabit become well placed not only to provide surveillant tools to parents but also to actively monitor children on their sites to protect them from 'inappropriate' content and communications. In this way, corporate surveillance is normalized and recedes into the background.

It's fantastic plastic being plastic

It is in the background that corporate surveillance is the most powerful. Unlike the panoptic gaze of parental control software, which seeks to encourage the child to internalize the watcher, corporate surveillance seeks to invisibly manipulate the child's identity play to privilege behaviours and identities that conform to the needs of the marketplace.

As Grimes and Shade (2005) point out, children's social networking sites – like Club Penguin, Webkinz and Neopets – are modeled on a system of commerce that includes stores, a service industry, job opportunities and currency (including a banking system, a stock market and daily inflation reports, in the case of Neopets). Participating in this system of commerce is an essential part of participating in the virtual community. On Neopets, for example, children play games and get jobs to earn Neopoints so they can buy food and toys for their virtual pets. The Neopets Marketplace creates scarcity by selling limited quantities of virtual products for virtual currency over very short periods of time. Since goods sell out in seconds, children are encouraged to impulse shop. Moreover, this kind of 'play' also reflects the 'enormous focus placed on exchange and acquisition that pervades the game's activities and features. Thus a member's economic status can significantly limit or greatly enhance access and enjoyment of the site' (ibid: 185). Since these virtual worlds are instructive, 'teaching children models for being and experiencing the world,' they encourage children to believe that the objective of play and social interaction is to acquire consumer goods.

Surveillance reinforces and deepens these lessons, by privileging certain kinds of identities. Early behavioural targeting involved directly collecting personal information from children and then using it to solicit product. For example, when 'Jenna' filled out a personality survey on eMode in 2000, she was told that she was a politician. The site then directed her to a diet site (one of their corporate sponsors) so she could 'prep her bod for success' (Steeves 2006: 175). However, with the advent of social networking, children are now encouraged to reveal personal details on an ongoing basis. That information is then analyzed and used not only to solicit product but to structure the child's online environment. I personally experienced one of the most powerful examples of this when I was doing research on a popular social networking site. Before I registered, I was served news items about world events. As soon as I registered as a 16-year old girl, the world news disappeared, and I was inundated with celebrity gossip and ads for plastic surgery and various diets.

Branded sites like Club Penguin, Webkinz and Barbie.com use the information they collect to create a personal relationship between the child and the brand by encouraging the child to interact with the brand as if it were a person. Girls playing on Barbie.com, for example, are asked to help surprise Ken by helping Barbie plan a special day for him. Barbie can also reach out from the screen and interact with the child in the physical world. For $1.99, Barbie will call a child to wish her Happy Birthday, read her a bedtime story or give her advice about how to get along with her siblings. The site tells girls, 'Wow! You could get a call from *your best friend – Barbie*!' (ibid: 178, emphasis added).

By interacting with a brand online, children learn to 'trust' them and think of them as 'friends.' They also become 'role models for children to emulate, in effect embedding the product right into the [child's] identity' (ibid: 179). An interview with Hilary Duff posted on Barbie.com in 2005 illustrates this process well. Duff tells the girls, both in text and in audio,

> I was the biggest Barbie fan when I was younger, and I still admit I love Barbie. I just think that she's so pretty, and she's so motivated. She's had a lot of jobs. I think she's a really good, positive role model for young girls to look up to…. And I always looked up to Barbie when I was younger, and I think that she's such an inspiring, cool, hip, and trendy role model for girls to look up to, so I'm very excited. And she loves pink—just like me! (ibid)

However, as Livingstone (2008) points out, children's online experiences are shaped by both technical and social affordances. Technology and social practice are therefore coequal in that they mutually shape each other to frame potential acts of agency. This potential is evident in the move from wholesale acceptance of corporate surveillance on the part of children in 1999 to the distrust and resistance expressed by children in 2007. Again, Club Penguin is exemplary. In the process of research, I witnessed an impromptu ‘protest’ in a Club Penguin village. As Grimes and Shade (2005) note above, the site emphasizes exchange and acquisition in ways that create varying levels of social capital between players. The differences are reinforced by the fact that only paying members can buy the ‘coolest’ swag for their penguins from CP catalogues. It is not unusual to see a penguin waddling through the site wearing multiple hats, sun glasses, MP3 players and other paraphernalia. This has created animosity between non-members and members (who tend to be heavily burdened with goods). In spite of the fact that Club Penguin strictly limits what children can say and do in order to keep them ‘safe,’ children find ways to get around surveillant controls to express themselves and resist the constraints that are built into the site itself. For example, one member started a massive melee by yelling, ‘Throw snow balls at members!!’ The penguins quickly took sides and non-members hurled insults at the members. Members responded by expressing anger and calling non-members names.

Regan and Steeves (2010) argue that the surveillance built into the online environment contains potential spaces of empowerment in which online users can turn the surveillant gaze aside, or turn it back on itself by reclaiming the publicity inherent in what appears to be a private space. They illustrate their point with an incident that occurred at George Washington University. Campus officials were monitoring students’ Facebook pages to identify and prosecute under-aged drinkers. The students responded by posting a Facebook invitation to a ‘cake party.’ When the officials arrived to intervene, they found an empty room with a cake and no alcohol. Regan and Steeves conclude:

> … the top-down surveillance embedded in the site was reversed – the uni-directional gaze was transformed by a concerted resistive behaviour that unmasked both the watcher and the limits of the watcher’s control. This indicates that top-down surveillance will be

> tolerated unless and until it disrupts the social interaction that is the primary reason young people participate in a [social networking site]. The site provides a private space in which they can deepen their social interactions, shape and present themselves, and experiment with social roles; and nodal surveillance is central to these forms of empowerment. However, the fact that they are also watched 'from above' provides an opportunity to publicize that private space and use it to 'talk back' to the institutional watcher who seeks to constrain and control their social interactions. (161)

In sum, the ability to watch and be watched is central to young people's desire to use the net to explore their identities and try on a variety of social behaviours. At the same time, the net has opened up this previously private world of identity play and social interaction to the invisible gaze of corporations that seek to manipulate the online environment for their own purposes. For their part, many parents now employ invasive methods of surveillance that diminish both the trust between parent and child and the child's ability to develop resiliency by encountering risks and learning from mistakes. This surveillance is driven by moral panics about children and technology, as well as a neo-liberal regulatory environment that seeks to maintain surveillance as a way to fuel the information marketplace. Children's experiences accordingly provide an excellent context in which to map the contradictory ways in which surveillance is implemented as an organizational principle within online spaces.

References

Burkell, J., Steeves, V., and Micheti, A. (2007) *Broken doors: Strategies for drafting privacy policies kids can understand*, Ottawa: Office of the Privacy Commissioner of Canada.

Disney.com. (2011) Club Penguin. Available HTTP: http://www.clubpenguin.com/ (accessed 15 January 2011).

Grimes, S. and Shade, L.R. (2005) 'Neopian economics of play: Children's cyberpets and online communities as immersive advertising in Neopets.com,' *International Journal of Media and Cultural Politics*, 1(2): 181-98.

Estrin, M. (2007) 'Behavioural marketing – Getting ads to the right eyeballs,' *iMedia Connection*. Available HTTP: http://www.imediaconnection.com/content/14559.asp (accessed 15 January 2011).

Livingstone, S. (2008) 'Taking risky opportunities in youthful content creation: Teenagers' use of social networking sites for intimacy, privacy and self-expression,' *New Media & Society*, 10(30): 393-411.

Livingstone, S. and Bober, M. (2003) '*UK children go online: Listening to young people's experiences*,' London: Economic and Social Research Council.

Marx, G. and Steeves, V. (2010) 'From the beginning: Children as subjects and agents of surveillance,' *Surveillance and Society*, 7(3): 6-45.

Media Awareness Network. (2004) *Young Canadians in a wired world, phase III: Focus groups*. Ottawa: Media Awareness Network; 2005a. *Young Canadians in a wired world, phase III: Student Survey*; 2005b. *Young Canadians in a wired world, phase III: Trends and recommendations.*

Montgomery, K. (2000) 'Digital kids: The new on-line children's consumer culture' In D. G. Singer and J. Singers (eds.) *Handbook of children and the media*, pp. Thousand Oaks, California: Sage Publications.

Regan, P. and Steeves, V. (2010) ‘Kids R Us: Online social networking and the potential for empowerment,’ *Surveillance & Society*, 8(2): 151-65.

Steeves, V. (2006) ‘It’s not child’s play: The online invasion of children’s privacy,’ *University of Ottawa Law and Technology Journal*, 3(1): 169-88.