Chapter 11

Terra Cognita: The Surveillance of Young Peoples' Favourite Websites

Valerie Steeves

In 1999, when MediaSmart's Young Canadians in a Wired World Project was initiated, marketers were found to be among the first sector to have taken notice of the children who were beginning to flock to the Internet. Branded playgrounds seamlessly blended commercial content into advergames, product spokes-characters sought to build relationships between children and products, and quizzes and other forms of interactive media encouraged them to divulge personal information in exchange for opportunities to win contests or points (Center for Media Education, 1996; United States, 1998). Many of the children and parents we spoke to at the time saw this as a positive aspect of their online lives. From their perspective, these activities were not just fun; sites that belonged to corporations they "knew" were trustworthy and they felt that the brands they encountered online were "friends" with whom they could safely interact (Media Awareness Network, 2004, p. 13).

Although concerns about the potentially deceptive nature of commercial practices targeting young people had been raised as early as 1996 (Center for Media Education, 1996), legislators in North America and Europe largely saw the profusion of children's sites through the lens of economic growth. They accordingly sought to balance concerns about commercialization with the needs of the emerging online marketplace through the enactment of privacy laws (Steeves, 2015b). These laws typically require transparency and/or consent mechanisms to enable children

(and their parents) to make informed decisions about the information they choose to disclose to the corporations that own the sites they visit (Grimes, 2008; Steeves, 2015a, 2015b).

Since those early days of the Net, websites have developed increasingly sophisticated methods to collect vast amounts of data about young people as they chat, surf and play online. The goal of this surveillance is to deepen children's relationships with commercial products through the use of micro-targeted "one-on-one" marketing and communications strategies that create a cognitive, emotional and behavioural relationship between the child and the brand (Montgomery, 2015). However, after privacy legislation was put in place to protect children, policymakers — who were increasingly focused on children's online exposure to offensive content and contact with potentially dangerous strangers (Steeves and Bailey, 2013) — largely lost interest in what Cairns calls "the third 'C': commercialism" (Cairns, 2008, p. 240).

A growing number of academics have called for a reinvigorated debate around the effect of commercial surveillance in children's networked spaces (Buckleitner, 2008; Grimes, 2008, 2015b; Grimes and Shade, 2005; Hasebrink et. al., 2007; Montgomery, 2007, 2015; Nairn, 2008; Steeves, 2006, 2007). This chapter seeks to contribute to that debate by providing a snapshot of surveillance practices used on popular web sites. It also presents quantitative findings regarding young people's attitudes towards this surveillance. I argue that, contrary to popular conceptions, many young people have outgrown their early infatuation with online commercial content; they are both increasingly skeptical about commercial surveillance and dissatisfied with the kinds of privacy protections that were intended to protect them from commercial manipulation.

Moreover, the ubiquity of commercial collection on the sites they inhabit strongly suggests that current regulations do little to restrict surveillance, but instead legitimize the rampant commodification of their online communications. Accordingly, I call for more nuanced and critical regulatory interventions that can better insulate children from marketplace logics and push back against the ongoing commodification of the networked spaces in which they play, learn and mature.

Methodology

In 2013, as part of Phase III of the Young Canadians in a Wired World Project,[1] we surveyed 5,436 young people aged 9-17 in schools across Canada. Participants were recruited through school boards and schools and parental consent was obtained. All recruitment documents, consent forms, survey instruments and methods of analysis were approved by the University of Ottawa Research Ethics Board. Statistical analysis was conducted by Directions Research, Inc.[2]

Among other things, participants were asked to identify their five favourite sites on the Internet. This resulted in a list of more than 3,000 individual sites. The sites on this list were ranked according to the percentage of participants who included them on their favourite five, and a list of the top 50 sites was generated. Content analysis was then used to identify the presence, length

---

[1] The data was collected as part of MediaSmart's Young Canadians in a Wired World Project. The Project has collected qualitative and quantitative data in three phases, the first in 2000-2001, the second in 2004-2005, and the third in 2012-2013. Full reports on each phase of the project can be found at http://mediasmarts.ca/research-policy.

[2] For full details, see AUTHOR, 2014, pp. 42-50.

and complexity of privacy policies, and the number of trackers and other forms of surveillance on each site.

The Top 50 — An Overview

Although there is a great deal of diversity in the 3,000 sites participants listed in total, the top 50 list is made up of specific types of sites (see Tables 1 and 2). Gaming sites are the most prevalent (21 sites), followed by social media (13 sites), sports and entertainment (8 sites), informational tools (4 sites), online stores (3 sites) and free email services (2 sites). Slightly more than half (27) of the sites are intended for a general adult audience; the remaining 23 specifically target young people. All of the 50 sites on the list collect personal and non-personal information and 48 of them — with the exception of Wikipedia (no. 10) and Animal Jam (which is operated by the National Geographic Society) — use that information to generate profit.

After YouTube, which is the most popular site across all age groups, social media dominate the top 10 favourites (nos. 2, 4, 5, and 6) (see Table 3). This preference for social media is particularly pronounced among participants aged 13-17; it is remarkable that teenaged girls selected social media sites for five of the top seven slots (see Table 4). Although younger respondents[3] tend to prefer gaming sites, Facebook (no. 4 for boys and no. 2 for girls) and Twitter (no. 10 for boys and no. 7 for girls) both make their top 10 lists, even though the sites expressly forbid children under age 13 from participating (see Tables 6 and 7). In addition, three

[3] Aged 9-12

of the five gaming sites on the top 10 list for young girls (nos. 4, 5 and 8) incorporate elements of social media into their design.

This preference for social media is also reflected in the finding that children's use of social media definitely tends to start young, and grows across age groups. Thirty percent of the 11-year-olds we surveyed reported that they have created their own social media pages where they post their own comments or photos. By age 12, the percentage of children posting content on their own sites doubles to 60 percent, and from age 13 to17, the percentage rises from 76 to 90 percent. Young people who use social media also tend to do so fairly frequently; more than three quarters of respondents in all age groups who post content reported that they do so at least once a month. Accordingly, a large number of teens are disclosing personal information on social media as a matter of course.

Social media has clearly increased the amount of digital information young people reveal as they go about their daily lives. But the growing popularity of social media has also changed the kinds of online surveillance young people experience. In 2005[4], when half of the top 10 were gaming sites (Steeves, 2005), information was typically collected in the background as children surfed the sites and played the games available to them. Since many of the sites did not require registration to play, there was an element of (restricted) anonymity for the children who frequented them. In contrast, social media is predicated upon express disclosure on the part of site users who identify themselves by their "real" names. Although information about the links

[4] Respondents to the 2005 survey listed their top three sites, not their top five sites.

they click, the content they "like" and with whom they communicate continues to be collected in the background, that information is used in combination with the information they voluntarily disclose to create highly detailed, individualized profiles which are, in turn, used to shape their interactions (Montgomery, 2015).

The kind of voluntary disclosure common on social media is also becoming more prevalent on other types of platforms. Most notably, a number of the gaming sites on the list now incorporate chat functions so players can talk to each other as they play. Even though pseudonyms may be used, the information collected from their conversations is linked to an IP address and helps to build individual profiles of unique players. Moreover, a number of sites encourage users to log in using their Facebook or Google Plus accounts, which enables site owners to link their online behaviours with their real names and locations. Accordingly, the space for anonymous online play enjoyed in 2005 has largely been replaced with an expectation that users will publicly perform a singular and "real" identity that is often linked to their name, their physical location and their physical appearance as portrayed in photos.

The collection of children's information in 2013 is also significantly shaped by the fact that *more* young people now tend to congregate on the *same* sites, and that many of these same sites are owned by a small number of large high-tech companies. Again the contrast with the 2005 list is striking, as none of the sites of the top 10 list in 2005 attracted the votes of more than one fifth of the respondents and there was no concentration of corporate ownership. For example, the no. 1 site in 2005 (Addicting Games) was selected by only 18 percent of respondents, and more than

half of the sites on the 2005 list attracted the support of less than five percent of respondents (Steeves, 2005). By way of contrast, a remarkable 75 percent of respondents in 2013 voted for top-site YouTube, and the next three most popular sites garnered the support of one quarter or more of respondents, respectively. Even the no. 10 site on the 2013 list was selected by 10 percent of respondents (see Table 4). Again, this differs markedly from 2005 when more than half of the sites on the top 10 list were selected by less than five percent of respondents.

In addition, although all of the 10 top sites in 2005 were owned by corporations,[5] eight out of 10 were relatively small companies whose main business was tied to online gaming or music. The large corporations on the list included YTV, a television station targeting youth, and Candystand, an advergaming site created by Nabisco, Inc. to market its candy products. This differs sharply with the picture in 2013, when two corporations in particular dominated the top 10: Google (which also owns YouTube); and Facebook (which also owns Instagram). Other high-tech giants, including Twitter, Yahoo (which owns Tumblr) and Microsoft (which owns Hotmail) also made the 2013 top 10.

This concentration of ownership in a small number of large tech corporations is a significant factor in young people's experiences of surveillance. Although the commercialization of young people's online environment has been taking place for some time (Davies, 2010), the commercial agenda behind children's favourite sites — disclosure of personal and/or non-personal

[5] Addictingames (no. 1), Miniclip (no. 2), Neopets (no. 3), Ebaumsworld (no. 4), Newgrounds (no. 5), Runescape (no. 6), Funnyjunk (no. 7), Candystand (no. 8), YTV (no. 9) and Launch (no. 10).

information in exchange for free access to content — is more deeply entrenched when the major players, like Google and Facebook, operate integrated information collection systems across the sites they own as well as the sites owned by their (largely unnamed) corporate partners and use the information they collect for marketing purposes. As Montgomery notes, "The entire digital media enterprise has been structured to facilitate and maximize user interaction with brand promotion and marketing, and to enable continuous monitoring and analysis of all these interactions in real time" (2015, p. 3-4).

Certainly advertising is ubiquitous on the top 50 sites: 49 are populated by advertisements[6], ranging from ads for site products/services and traditional ads for third parties, to "pre-roll" ads on videos, sponsored content, product placement and advergames. But the real goal is to less to advertise and more to blend marketing messages into the social environment in a seamless and natural way (Calvert, 2008). Instagram summarizes it well on their Sponsored Photos and Videos page: "Our aim is to make any advertisements you see feel as natural to Instagram as the photos and videos many of you already enjoy …".

The naturalization of commercial content in children's play and social interaction is also normalized through games and other activities that present commerce as a form of play/ entertainment (Nansen et. al., 2012; Chung and Grimes, 2005). This is key to understanding how commercial surveillance shapes young people's online experiences, because the information corporations collect is used to encourage certain kinds of identities that are consistent with

[6] The exception is Wikipedia (no. 10), which is an advertising-free site.

commercial messaging. For example, sites on the top 50 list like Webkinz and Club Penguin encourage children to earn points to buy things for their virtual pets. Girlsgogames.com contains a series of Shopaholic Games, where players go on shopping sprees for dresses, shoes, makeup, jewelry and fast food in glamorous locales like Paris, Milan and Hawaii. Weheartit reinforces shopping as entertainment through the Swag tag, where young people can post photos of their latest purchases. Even Animal Jam, operated by the non-profit National Geographic Society, greets new users with a treasure box which one of the animals points out by saying, "Hey look, free stuff!" and then encourages the child to purchase new clothes and items for their virtual house. They are then asked, "What would you like to do next?" and given four options (in the following order): Go to your den (a virtual home they can decorate with virtual purchases); Shop for new clothes; Play games; and Go on an adventure. Even as they play or go on an adventure, they are greeted with ads such as this one encouraging them to upgrade their den: "Introducing the BEACH HOUSE, the incredible NEW DEN filled with huge ROOMS, great VIEWS, and your own PRIVATE BEACH!! Pick up your own BEACH HOUSE in the Diamond Shop today!"

As Grimes notes, the "type of play afforded is noteworthy in both its limited scope and its close alignment with consumerist values … In the process, economic priorities not only come to shape and constrain the field of play, but also impose a particular, deeply ideological, vision of what children's play looks like" (Grimes, 2015b, p. 129).

Regulatory Compliance

As noted above, the current privacy regime is built upon an uneasy compromise that sought to encourage online commerce through the commodification of user data while still providing some protection for children's privacy. Although early concerns raised by the US-based Center for Media Education focused on the impact of deceptive trade practices that disguised market research labs as children's playgrounds, the American legislative debate was quickly overtaken by data protection discourses that reduced the issues to informational control (Steeves, 2015b). The American model accordingly focused on mechanisms that would promote informed parental consent for children under age 13 to any collection and use of a child's personal information. In keeping with other data protection laws, information collectors were required to be transparent about their information practices and provide access so individuals could see and correct the data collected from them. But the crux of the regime rested on the requirement that web sites seeking to collect personal information from children under 13 were required to first obtain permission from their parents. Children 13 years and older, on the other hand, could consent on their own behalf.

Although Canada, Europe and Australia have typically relied on general data protection legislation to regulate sites aimed at children, the reach of the American model is evidenced by the ways in which non-American sites have adapted to American standards. This is most clearly reflected in the fact that the *de facto* age of consent for many non-American sites is 13, even though domestic laws regarding the ability of mature minors to consent on their own behalf

mandate a different age[7]. This dominance of the American approach is at least partly based on the popularity of American sites among non-American children. In the Canadian context, for example, more than half of the top 50 favourites (32) are owned by US-owned corporations.[8] Only seven are Canadian[9]; and the remaining 10 sites are owned by corporations in the United Kingdom, the Netherlands, Luxembourg, Switzerland, Hong Kong and Sweden.[10]

On the positive side, all of these jurisdictions have data protection laws in place that require corporations to make their information practices transparent and provide children (and/or their parents) with certain rights to control their information. And at first blush, the regulatory regime appears to be working. All 50 sites had a privacy policy posted on the site and 46 could be located with a single click from the site's home page (see Table 5). The vast majority (92%) were easy to find: the links on 12 sites were highly visible and particularly easy to find and the links on 34 sites were clearly visible to a user interested in learning about the site's information practices and willing to scroll down to the bottom of the page[11]. Only four were hard to find, because of nondescript icons (friv.com and kizi.com) or because the user was required to click on

---

[7] See, for example, Miniclip (based in Switzerland), Y8.com (based in Hong Kong), Webkinz and YTV (based in Canada) and Girlsgogames and Agame (based in the Netherlands).

[8] This includes four companies which were purchased by US firms: Skype (which originated in Estonia); ask.fm (which originated in Latvia); Weheartit (which originated in Brazil); and Minecraft (which originated in Sweden).

[9] Webkinz, Family.ca, YTV, NHL, Bitstrips, TSN and Wattpad.

[10] Based on a whois search: Friv.com, Poptropica, Moshimonsters, Sumdog are based in the UK; Girlsgogames and Agame in the Netherlands; Pornhub in Luxembourg; Miniclip in Switzerland; Y8 in Hong Kong; and MovieStarPlanet in Sweden. There is no information on andkon indicating where the site owner is located, and whois did not have locational information for the URL registrant.

[11] Very visible links were clearly labelled"Privacy" or "Privacy Policy" in regular or larger size font and typically easily found at the bottom of the home page without scrolling). Visible links were labelled "Privacy" but in smaller font. Although they were also typically located at the bottom of the page, the user was required to scroll down through a significant amount of content.

a general link to “FAQ” (andkon.com) or “More” (ytv.com) before finding a link to “Privacy Policy”. Interestingly, all four of the hard-to-find links were on sites specifically targeting children.

The length of the privacy policies varied significantly, from a minimum of 54 words on andkon.com to a maximum of 7,250 words on Skype. On average, policies on children’s sites are approximately 60 per cent as long as policies on adult sites (2,044 and 3,468 words, respectively). However, the language in four fifths of both children’s and adult policies was not highly accessible (i.e. written in short sentences, without technical terms) and policies on children’s sites were slightly more likely — 35 percent compared to 30 percent of adult sites — to be written in inaccessible ways (i.e. long, compound sentences, undefined legal and technical terms).

The length and inaccessibility of the policies may pose barriers to children who are attempting to learn what happens to their information on these sites. It is noteworthy that 68 percent of our survey respondents mistakenly agreed with the statement, “If a website has a privacy policy, that means it will not share my personal information with others.” A similar percentage (65%) report that no one has ever explained a policy to them, which suggests that they are often struggling with policies without assistance from adults. But even students who have had a policy explained to them may need additional support, as they are *more* likely to agree with the above statement (70.3%) than those who have not had an explanation (66.7%).

Part of the confusion may also be based in the ways in which the policies talk about privacy. Many contain statements that they value user privacy in spite of broad collection, use and disclosure practices. Bitstrips is typical: "At Bitstrips, we respect the privacy of our users … By using the Service, you consent to our collection and use of personal data as outlined therein." Others use empowering language and/or collapse privacy concerns into security and safety. For example, Google's privacy policy states:

> We know security and privacy are important to you – and they are important to us, too. We make it a priority to provide strong security and give you confidence that your information is safe and accessible when you need it. We're constantly working to ensure strong security, protect your privacy, and make Google even more effective and efficient for you. We spend hundreds of millions of dollars every year on security, and employ world-renowned experts in data security to keep your information safe. We also built easy-to-use privacy and security tools like Google Dashboard, 2-step verification and Ads Settings. So when it comes to the information you share with Google, you're in control.

Social media sites in particular tend to valorize "sharing" and "control." For example, Facebook's privacy policy starts with the statement that, "We give you the power to share as part of our mission to make the world more open and connected," and continues to say, "You're in charge. We're here to help you get the experience you want." Twitter's policy has a similar tone: "Our Services are primarily designed to help you share information with the world. Most of the information you provide us through the Twitter Services is information you are asking us to

make public." However, it then goes on to list items that the site considers public, moving quickly from "the messages you tweet" which are clearly intended by the user to be distributed to other information that is not so easily understood as "public", including:

> … the metadata provided with Tweets, such as when you Tweeted and the client application you used to Tweet; the language, country, and time zone associated with your account; and the lists you create, people you follow, Tweets you mark as favorites or Retweet, and many other bits of information that result from your use of the Twitter Services.

In this way, any conflict between the social value of privacy to the user and the commercial value of disclosure to the corporation collapses. If there is a privacy issue, it is generally seen as the responsibility of the user or his or her parents. Twitter concludes the above paragraph by telling users, "When you share information or content like photos, videos, and links via the Services, you should think carefully about what you are making public." Kizi tells its users that it collects "non-personal information," such as IP address and click-through data, and suggests, "For the protection of your privacy, we ask that you avoid sending us any and all personally identifiable information." MovieStarPlanet states, "…we strongly encourage parents and guardians to take an active role in promoting online safety." Animal Jam advises, "Parents, you can take steps to protect your kids too. To learn more about how to protect your child online, read the helpful information provided by the FTC."

Accordingly, the regulatory framework provides for some level of transparency, but the length, wording and tone of policies may make it difficult for young people to fully understand the extent to which information about them is collected and commodified, and places the burden of limiting surveillance on them and/or their parents. Moreover, the adult sites on the top 50 list typically side-step any additional protections that may be afforded for children by posting blanket prohibitions telling young people they are not to use their services. The majority (20 out of 27) include a provision that children under 13 are simply not allowed to access their services[12]. Skype restricts users to those who are old enough to participate under the laws of the user's country of residence. The remaining sites are e-stores that either: restrict users to those 18 and over (Netflix, Porn Hub, eBay); require children under 16 to have their parents access their services (Kijiji); or sell merchandise to children under 13 only through a shared family account (iTunes). Although the practical impact of these clauses is questionable, given the fact that these sites all appear of the list of young people's favourites, they provide evidence to support a legal defence should any of these corporations be faced with law suits or other processes seeking to hold them accountable for their collection and use of children's information. As Nansen et. al. (2012) conclude, "the architectures of participation … are shaped not solely for the benefit of participants.. just as much for the benefit of the digital object itself and for its value to owners. Web 2.0 is not just a user or social model, but also a technical and business model" (p. 1222).

[12] The exception is again Wikipedia. The site does not impose age restrictions on young users, but it is also a non-profit site that does not commodify their information.

But perhaps the most important test of the value of the current framework is whether or not it limits surveillance in the first place. Our analysis indicates that commercial collection on these sites is rampant: 48 of them[13] used trackers to continually collect the data users drop as they chat, play and entertain themselves (see Table 5). The number of trackers per site ranged from 1 to 15, with an average of 5 trackers per site.[14] Moreover, of the 40 sites that have privacy settings, only 6 were set to private by default[15]. The remaining sites were either set to public (16) or contained a mixture of public and private defaults (24). This suggests that the regulatory framework acts less to protect young people's privacy, and more to legitimize the commercial collection and use of their data by providing a veneer of privacy protections that do little to nothing to limit commercial surveillance.

Surveillance and Control of Young People's Communications

The ubiquitous presence of acceptable use policies or "community standards" on young people's favourite sites (found on 42 of the top 50 sites[16]) also reshapes the kinds of surveillance they experience. These policies set out strict behavioural guidelines that are almost always defined

---

[13] Data was collected by using Ghostery, an app that identifies over 2,000 trackers, including cookies, tags, web bugs, pixels, widgets and beacons. The number of trackers on sites can fluctuate. This data was collected in October 2014. All sites of the top 50 list except Wikipedia and friv.com used at least one tracker.

[14] The most common trackers were Google Analytics, Google AdSense, DoubleClick, NewRelic, and ScoreCard Research Beacon, and Facebook, Twitter and Google widgets.

[15] Although there are twice as many children's sites with private defaults (4), compared to adult sites (2).

[16] The remaining eight either do not allow users to create profiles, post content or communicate with each otherNetflix, Friv, Andkon, Family.com, Coolmath-games, and Coolmath4kids), or they limit communication to product reviews that are vetted and pre-approved by the site before they are posted (iTunes) or messages between individuals who have accepted a "friend" request (Kizi).

and imposed by the corporation.[17] On the majority of sites (78%), users are expected to both comply with guidelines and monitor other users to ensure their compliance. The removal of non-compliant content is at the discretion of the site owners — Tumblr is the only site that even contacts the user accused of misbehaviour before taking action — and active moderation is common, especially on children's sites.

These practices not only normalize corporate surveillance, which takes on a protective function, but extend the surveillant gaze of the corporation by enlisting users as informants. Club Penguin has made this explicit, through the creation of its Penguin Spy Agency. Children who sign up to work for PSA are told that "*your duty* (as an agent) is to report any penguin that says bad words, asks or reveals personal information or is rude, mean or breaks any of the other rules." This kind of peer surveillance reshapes the online environment to encourage conformity to corporate and commercial values (Marx and Steeves, 2010).

Chat among young children is also subjected to particularly tight controls on Webkinz, Club Penguin, Poptropica, Roblox, and Animal Jam. All five sites enable parents to limit their children's communications to stock words and phrases, and threaten to remove privileges from those who disobey the rules. The language is often quasi-criminal, as in Webkinz' notice to parents that:

[17] Only Wikipedia relies on norms and solutions negotiated by members of the Wiki community.

> Breaking any of the Rules may lead to one's account being silenced or banned from KinzChat PLUS for a period of time, or permanently, depending on the severity of the offense. For serious or repeat offenses one's account may also be banned permanently from the website.

However, the surveillant gaze behind the enforcement of these rules is legitimized by positioning the corporate site owner as a guardian of the young person's safety. The corporation is no longer a threat to privacy but is actively monitoring the child and ready to take action to keep her safe — from others or from herself. As Roblox states, the site has:

> … a team of of moderators who are constantly keeping an eye on discussion forums, fielding abuse reports from members, and screening uploaded content. These moderators follow our policies in regard to swearing and obscenities, messages and content of a sexual or violent nature, and any sort of aggressive or threatening communication … [an] infringing member is immediately suspended or permanently expelled.

From this perspective, the potential harm is not a loss of privacy vis-a-vis the corporation, but the possible harms of publicity: the child may be approached by malicious strangers or ill-intentioned peers; or the child may act badly in public as a result of his or her own poor judgment (Steeves and Bailey, 2013). Surveillance is presented as the solution and the commercial nature of corporate surveillance accordingly recedes from view.

Concluding Thoughts — Young People's Attitudes about Commercial Surveillance and the Need for Better Regulation

Given the ubiquity of constant monitoring on our respondents' favourite websites, one might assume that young people are comfortable with commercial surveillance. However, the qualitative research that preceded our Phase II survey suggested that many young people are either ambivalent about corporate surveillance or see it as a "creepy" form of "stalking" (Steeves, 2012). To test this, we asked our survey respondents who *should* be able to see what they post on social media. Less than one fifth (17%) reported that the company that owns the site should be able to see their content, and only five percent thought marketing companies that want to advertise to them should have access to their posts. The numbers are even lower when it comes to website/app companies or marketers tracking their location (4% and 1%, respectively).

This raises serious questions about young people's comfort with the current regulatory framework and its attempts to "balance" online commerce and privacy. It is remarkable that 72 percent of respondents reported that they did not like it when companies use their personal information to advertise to them,[18] and three quarters indicated that they want more control over what companies do with the photos and information they post online. This desire for control is understandable given the fact that many young people:

[18] Although girls are more likely than boys to report this (78% of girls compared to 66% of boys).

> … spend very large amounts of time online, and in many ways, conduct their friendships through social networks, largely unaware of the level and intensity of scrutiny that takes place … Yet, precisely at the times in their lives when they are forging their own identities, navigating their social worlds, and developing their abilities to form and sustain lasting relationships, their personal and social interactions are increasingly shaped and facilitated by the force of the digital marketplace" (Montgomery, 2015, p. 5).

To help carve out a place for this kind of identity play and deep social connection, regulators should consider at the very least a staged regime that forbids the collection of information from very young children and relies on an age-related set of parental and child consent provisions for teenagers (Lawford, 2008). However, to protect children from life-long consequences for failed experiments, any information collected before the age of majority should be deleted when the child becomes an adult. In addition, default settings should strictly limit collection on the part of the corporation housing the site and give children much more control over exactly who sees the information they post online. "Right to be forgotten" provisions could also help young people by delinking embarrassing content from major search engines.

But a complete corrective requires a re-thinking of networked platforms. To fully protect children from commercial surveillance, governments at all levels — from national legislatures to school boards — need to devote funds to creating and maintaining commercial free zones where children can chat, play, learn and communicate. Schools and community groups need alternatives to commercialized spaces that premise networked learning on the collection of

information and/or marketing, and children need truly private spaces to think, play, make mistakes and learn, free from the kinds of surveillance that are embedded in the sites they currently frequent.

Further research is needed to gauge the extent to which this surveillance constrains healthy child development (Nairn, 2008), but we must also begin to grapple directly with the political-economic factors at play (Grimes, 2015b; Monahan, 2004). Now that children's digital culture is increasingly shaped by corporate interests (Nansen et. al., 2012), policymakers should revisit basic questions about commercialization, question the use of networked technologies that operate as "significant vectors for market infiltration", and interrogate the ways that the networked spaces inhabited by children intensify their experience of surveillance, privilege a commercial model based on the rampant corporate collection of their information and "constrain conceptions of the possible" (Bartow, 2014, p. 36).

References

Bartow, Susan Meabon. (2014). Teaching with Social Media: Disrupting Present Day Public Education. Educational Studies 50: 36-64.

Buckleitner, Warren. (2008). Like Taking Candy from a Baby: How Young Children Interact with Online Environments. Flemington, New Jersey: Media Tech Foundation.

Calvert, Sandra L. (2008). Children as Consumers: Advertising and Marketing. The Future of Children 18(1): 205-234.

Center for Media Education. (1996). The Web of Deception. Washington, D.C.: Center for Media Education.

Chung, Grace and Sara M. Grimes. (2005). Data Mining the Kids: Surveillance and Market Research Strategies in Children's Online Games. *Canadian Journal of Communication* 30(4): 527–548.

Davies, Maire Messenger. (2010). *Children, Media and Culture*. New York: McGraw Hill Open University Press.

Hasebrink, Uwe, Sonia Livingstone and Leslie Haddon. (2008). *Comparing Children's Online Opportunities and Risks Across Europe: Cross-national Comparisons for EU Kids Online*. London: EU Kids Online (Deliverable D3.2).

Grimes, Sara M. (2015a). Configuring the Child Player. *Science, Technology and Human Values* 40(1): 126-148.

Grimes, Sara M. (2015b). Playing by the Market Rules: Promotional Priorities and Commercialization in Children's Virtual Worlds. *Journal of Consumer Culture* 15(1): 110-134.

Grimes, Sara M. (2008). Researching the Researchers: Market Researchers, Child Subjects and the Problem of "Informed" Consent. *International Journal of Internet Research Ethics* 1(1): 66–91.

Grimes, Sara M. and Leslie Regan Shade. (2005). Neopian Economics of Play: Children's Cyberpets and Online Communities as Immersive Advertising in Neopets.com. *International Journal of Media & Cultural Politics* 1(2): 181–198.

Lawford, John. (2008). All in the Data Family: Children's Privacy Online. Ottawa: The Public Interest Advocacy Centre.

Marx, Gary and Valerie Steeves. (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 II: Focus Groups*. Ottawa: Media Awareness Network.

Monahan, Torin. (2004). Just Another Tool? Pedagogy and the Commodifcation of Education. *Urban Review* 36: 271-292.

Montgomery, Kathryn. (2007). Generation Digital: Politics, Commerce, and Childhood in the Age of the Internet. Cambridge, MA: MIT Press.

Montgomery, Kathryn. (2015). Youth and Surveillance in the Facebook Era: Policy Interventions and Social Implications. *Telecommunications Policy*. http://dx.doi.org/10.1016/j.telpol.2014.12.006i

Nairn, Agnes. (2008). "It Does My Head In … Buy It, Buy It, Buy It!" The Commercialisation of UK Children's Web Sites. Young Consumers 9(4): 239-253.

Nansen, Bjorn, Kabita Chakraborty, Lisa Gibbs, Frank Vetere and Colin Macdougall. (2012). "You Do the Math": Mathletics and the Play of Online Learning. New Media and Society 14(7): 1216-1235.

Steeves, Valerie. (2006). It's Not Child's Play: The Online Invasion of Children's Privacy. University of Ottawa Law and Technology Journal 3(1): 169-188.

Steeves, Valerie. (2015a). Now You See Me: Privacy, Technology and Autonomy in the Digital Age. In Gordon DiGiacomo (Ed.), Human Rights. Toronto: University of Toronto Press.

Steeves, Valerie. (2015b). Privacy, Sociality and the Failure of Regulation: Lessons Learned from Young Canadians' Online Experiences. In Beate Roessler and Dorota Mokrosinska (Eds.), Social Dimensions of Privacy. An Anthology. London: Cambridge University Press.

Steeves, Valerie. (2007). The Watched Child: Surveillance in Three Online Playgrounds. Proceedings of the International Conference on the Rights of the Child. Montreal: Wilson Lafleur).

Steeves, Valerie. (2005). Young Canadians in a Wired World, Phase II: Trends and Recommendations. Ottawa: Media Awareness Network.

Steeves, Valerie. (2014). Young Canadians in a Wired World, Phase III: Online Privacy, Online Publicity. Ottawa: Media Smarts.

Steeves, Valerie. (2012). Young Canadians in a Wired World, Phase III: Talking to Youth and Parents about Life Online. Ottawa: Media Smarts.

Steeves, Valerie and Jane Bailey. (2013). Will the Real Digital Girl Please Stand Up?" In Hille Koskela and J. Macgregor Wise (Eds.), New Visualities, New Technologies: The New Ecstasy of Communication. Suurey, England: Ashgate Publishing.

United States. Federal Trade Commission. (1998). Privacy Online: A Report to Congress. Washington, DC: Federal Trade Commission.

[TABLES BELOW]

TABLE 1 — TOP 50 SITES BY ORDER OF POPULARITY

1. youtube.com	18. addictinggames.com (*)	35. bitstrips.com
2. facebook.com	19. clubpenguin.com (*)	36. coolmath4kids.com (*)
3. google.com	20. pubtropica.com (*)	37. kijiji.ca
4. twitter.com	21. moshimonsters.com (*)	38. fantage.com (*)
5. tumblr.com	22. reddit.com	39. nba.com
6. instagram.com	23. andkon.com (*)	40. ytv.com (*)
7. minecraft.net (*)	24. roblox.com (*)	41. agame.com (*)
8. miniclip.com (*)	25. yahoo.com	42. sumdog.com (*)
9. hotmail.com	26. skype.com	43. tsn.com
10. wikipedia.com	27. family.ca (*)	44. ask.fm
11. y8.com (*)	28. nhl.com	45. armorgames.com (*)
12. google.ca	29. coolmath-games.com (*)	46. wattpad.com
13. netflix.com	30. kizi.com (*)	47. 9gag.com
14. gmail.com	31. pornhub.com	48. itunes.com
15. pinterest.com	32. girlsgogames.com (*)	49. weheartit.com
16. friv.com (*)	33. ebay.com	50. moviestarplanet.com (*)
17. webkinz.com (*)	34. animaljam.com (*)	(* children's site)

TABLE 2 — TOP 50 SITES BY CATEGORY

Gaming Sites (21)	**Social Media Sites (13)**	**Sports & Entertainment (8)**
7. minecraft.net (*)	*Social Networking (6)*	*Media Streaming/TV (5)*
8. miniclip.com (*)	2. facebook.com	13. netflix.com
11. y8.com (*)	4. twitter.com	27. family.ca (*)
16. friv.com (*)	6. instagram.com (**)	31. pornhub.com
17. webkinz.com (*)	15. pinterest.com (**)	40. ytv.com (*)
18. addictinggames.com (*)	26. skype.com	43. tsn.com (**)
19. clubpenguin.com (*)	44. ask.fm	*Sports (3)*
20. pubtropica.com (*)	*Microblogging (5)*	28. nhl.com
21. moshimonsters.com (*)	5. tumblr.com	39. nba.com
23. andkon.com (*)	22. reddit.com	43. tsn.com (**)
24. roblox.com (*)	46. wattpad.com	(** tsn is a sports network)
29. coolmath-games.com (*)	47. 9gag.com	
30. kizi.com (*)	49. weheartit.com (**)	**Informational Tools (4)**
32. girlsgogames.com (*)	*Video or Photo Sharing (5)*	3. google.com
34. animaljam.com (*)	1. youtube.com	12. google.ca
36. coolmath4kids.com (*)	6. instagram.com (**)	25. yahoo.com
38. fantage.com (*)	15. pinterest.com (**)	10. wikipedia.com
41. agame.com (*)	35. bitstrips.com	
42. sumdog.com (*)	49. weheartit.com (**)	**Online Stores (3)**
45. armorgames.com (*)		33. ebay.com (auction)
50. moviestarplanet.com (*)	(**instagram, pinterest and	37. kijiji.ca (classifieds)

TABLE 3 — TOP 10 SITES ALL RESPONDENTS

1. youtube.com	75%
2. facebook.com	57%
3. google.com	31%
4. twitter.com	24%
5. tumblr.com	12%
6. instagram.com	10%
7. minecraft.com	8%
8. miniclip.com	7%
9. hotmail.com	6%
10. wikipedia.org	5%

TABLE 4 — TOP 10 SITES BY AGE AND GENDER

Boys (aged 9-12)		**Girls (aged 9-12)**	
1. youtube.com	70%	1. youtube.com	61%
2. minecraft.net	31%	2. facebook.com	22%
3. google.com	27%	3. google.com	20%
4. facebook.com	22%	4. webkinz.com	11%
5. miniclip.com	19%	5. moshimonsters.com	10%
6. y8.com	9%	6. friv.com	9%
7. roblox.com	9%	7. twitter.com	9%
8. andkon.com	8%	8. poptropica.com	9%
9. friv.com	7%	9. y8.com	8%
10. twitter.com	7%	10. family.ca	8%
Boys (aged 13-17)		**Girls (aged 13-17)**	
1. youtube.com	83%	1. youtube.com	77%
2. facebook.com	72%	2. facebook.com	77%
3. google.com	40%	3. twitter.com	43%
4. twitter.com	24%	4. google.com	36%
5. wikipedia.org	9%	5. tumblr.com	31%
6. miniclip.com	7%	6. instagram.com	21%
7. tumblr.com	7%	7. pinterest.com	10%
8. reddit.com	6%	8. hotmail.com	8%
9. minecraft.com	5%	9. netflix.com	5%
10. hotmail.com	5%	10. wikipedia.org	5%

Site	Privacy Policies and Practices					Community Standards	
	Visibility of Link	Length (in words)	Accessible Language	Number of Trackers	Default Settings	Site Policy	Encouraged to Monitor Peers
1	Medium	3509	Medium	2	Public	Yes	Yes
2	Medium	2387	High	2	Public	Yes	Yes
3	High	3509	Medium	4	Both	Yes	Yes
4	Medium	2602	Medium	4	Public	Yes	Yes
5	Medium	4285	Medium	4	Both*	Yes	Yes
6	High	3039	Medium	2	Public	Yes	Yes
7	Medium	1410	Medium	3	Private	Yes	No
8	Medium	1943	Low	11	Both	Yes	Yes
9	Medium	7250	Medium	4	Public	Yes	Yes
10	Medium	5925	High	0	Both	Yes	Yes
11	Medium	1172	Low	6	N/A	Yes	Yes
12	High	3509	Medium	4	Both	Yes	Yes
13	Medium	2978	Medium	3	Both	No	No
14	High	3509	Medium	1	Both	Yes	Yes
15	High	1922	High	5	Both	Yes	Yes
16	Low	650	Medium	0	Public	No	No
17	High	5117	Medium	3	Both	Yes	Yes
18	Medium	6769	Low	15	Public	Yes	Yes
19	Medium	3008	Low	5	Private	Yes	Yes
20	High	3287	Low	4	Both	Yes	No
21	Medium	3093	High	3	Both	Yes	Yes
22	High	3079	High	2	Private	Yes	No

23	Low	54	High	4	N/A	No	No
24	High	3151	Medium	4	Both	Yes	Yes
25	Medium	1238	Medium	5	Both	Yes	Yes
26	Medium	7250	Medium	3	Public	Yes	No
27	Medium	1828	Medium	6	N/A	No	No
28	Medium	3785	Low	13	Public	Yes	Yes
29	High	708	Medium	6	N/A	No	Yes
30	Low	596	Medium	11	N/A	No	Yes
31	Medium	1075	Low	3	Public	Yes	Yes
32	Medium	2138	Low	5	Both	Yes	Yes
33	Medium	4312	Medium	4	Public	Yes	Yes
34	High	1648	High	3	N/A	Yes	Yes
35	Medium	2229	Low	1	N/A	Yes	Yes
36	High	708	Medium	6	N/A	No	Yes
37	Medium	2286	Medium	7	Private	Yes	Yes
38	Medium	2636	Medium	6	Private	Yes	Yes
39	Medium	6706	Low	15	Public	Yes	Yes
40	Low	1187	Low	4	N/A	Yes	Yes
41	Medium	2127	Medium	7	Both	Yes	Yes
42	Medium	2561	High	2	Both	Yes	Yes
43	Medium	2728	Low	10	N/A	Yes	Yes
44	Medium	4916	Medium	4	Both	Yes	Yes
45	Medium	1392	Low	13	Both	Yes	Yes
46	Medium	1569	Low	5	Public	Yes	Yes
47	Medium	1531	Low	4	N/A	Yes	Yes
48	Medium	3197	Low	3	Public	No	No
49	Medium	2132	Medium	10	Public	Yes	Yes
50	Medium	1008	Medium	3	Private	Yes	Yes