Taking Online Rights Seriously: Ensuring Children's Active Participation in Networked Spaces

An NGO Report submitted with respect to the 5th/6th Review of Children's Rights in Canada (Convention on the Rights of the Child)

Submitted by The eQuality Project

Valerie Steeves, JD, PhD
Department of Criminology
University of Ottawa
Room 14045
120 University Private
Ottawa, ON K1N 6N5

March 1, 2020

Introduction

The eQuality Project (EQ) is a seven-year partnership of academic researchers, educators, policymakers, civil society groups and youth funded by the Social Sciences and Humanities Research Council of Canada. Together, we examine young people's interactions with networked technologies, paying particular attention to their experiences of privacy and equality in online spaces.

EQ is co-led by Valerie Steeves and Jane Bailey, both professors at the University of Ottawa. Since EQ's inception in 2015, we have conducted eight qualitative and mixed methods research projects exploring young people's perspectives about their online lives, including their experiences of privacy, surveillance, equality, discrimination, reputation, self-presentation, gender and sexuality in online spaces. Our work is intersectional and focuses in particular on the needs of marginalized communities of children.

In addition, Steeves has collected qualitative and quantitative data on young Canadians' experiences with networked technologies since 2004 as the lead researcher of EQ partner MediaSmart's Young Canadians in a Wired World research program. Steeves has also worked with EQ partner UNICEF Canada on the Global Kids Online Project to generate quantitative data to help inform the international debate about children's online rights.

EQ also develops educational and outreach material designed to engage young people in an ongoing dialogue about their relationship with technology. For example, in our most recent outreach initiative, we worked with EQ partner The Alberta Teachers' Association to challenge Albertan students to disconnect from their devices for a week so they could see how their tech use shapes their activities. Over 10,000 Albertan students participated in the challenge, and are currently posting their findings on an online community page designed to connect them with other students in the province.

All of our work is informed by our Youth Advisors and focuses on the need to ensure that the voices of young people are heard in the policy debate about their rights. To help us meet this challenge, we are working with our Youth Advisors to design a Youth Summit in 2021 where young Canadians will participate in a deliberative dialogue with policymakers to articulate the kinds of policy responses they need to best protect their rights in online spaces.

Young Canadians in an Networked Environment – Twenty Years of Data

In the past 20 years, networked media has been embedded into the lives of young Canadians and they are now among the most networked children in the world. The devices they use have brought them a number of benefits: they are able to connect to a wide array of informational resources; they enjoy interacting with popular culture products; and they use apps to help organize their lives and connect with their friends and family (Steeves, 2014a). However, the benefits of networked technology have shrunk over the past two decades, primarily because children have been increasingly subjected to privacy invasions and surveillance in an attempt to protect them from online harms and to enrol them into a surveillance capitalist economy (Steeves, 2016). This loss of privacy has made it more difficult for them to enjoy their rights to expression, access to information, freedom of association, education and play.

The Problem with Protective Surveillance

Our early research reported that children and young people aged 11-17 liked networked technology because they gave them a way to meet their developmental needs to explore the adult world and experiment with various identities. Children perceived the Internet to be private because adults were unaware of young people's activities and did not have the technical skills to find them online (Steeves, McAleese & Brisson-Boivin, 2020). This sense of privacy let children participate in online communities, access information and cultural materials, associate freely, and exercise their right to expression.

However, as young people flocked to the Internet, adults became concerned that children could encounter offensive content and ill-intentioned strangers online. The policy response was to increase surveillance of children in order to protect them from harm (Steeves, 2016; Bailey, 2016). Keystroke trackers, filters, adults demanding passwords to children's social media accounts, and other forms of monitoring became a common part of the online landscape, both at home and in school.

This protective surveillance has constrained young people's ability to participate in online life. For example, identity play and exploration have been shut down by the fact that young people cannot control who has access to their online data. This means that they are now accountable to all their audiences for all their online activities, subjecting them to micro level of controls for behaviours that can be taken out of context (Steeves, 2014a). They also worry that a mis-step in youth will affect their ability to work in the future (Bailey & Steeves, 2015).

> Two best friends in Toronto were comparing their tans after a March break holiday. A teacher saw their comments and the girls were disciplined by the principal for racist bullying because both girls were black (Steeves, 2014s).

In addition, this protective surveillance is making it more difficult to access information because of concerns that others will be able to see what they do online. This is particularly problematic

> [Going online] helped a lot … that was kind of central to discovering, like, different identities and me kind of realizing that straight wasn't the only thing that existed … but there's, like, a tab where you can see what people are liking … and I was like, oh, God, what if, like, someone sees I like this … that's not safe (Steeves, et al., 2020).

for the LGBTQ children we have spoken with, who rely on networked communication to learn about their bodies/sexuality and to find community with other LGBTQ youth. As protective surveillance at schools and at home has increased, they have become less likely to turn to online resources because of fears that they will be outed before they are ready (Steeves, et al., 2020).

The most unfortunate outcome of this surveillance is that it signals a loss of trust between children and the adults who care for them. Children refer to it as "spying" and "stalking", and report that it makes it harder for them to get help from parents and teachers when they need it because they fear that they will lose control over the outcome if they ask for help (Steeves, 2014).

The Problem with Corporate Surveillance

With the exception of Wikipedia, the sites young Canadians visit and the apps they use at home and in school are almost exclusively owned by for-profit companies. The commercial agenda that fuels those profits is based on the seamless collection and commodification of the data that people create as they surf, shop, chat and play. Zuboff (2019) calls this surveillance capitalism: "a new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales … in which the production of goods and services is subordinated to a new global architecture of behavioral modification" (Preface).

Corporate data practices affect children in a number of ways. Sites and apps are typically wallpapered with marketing material that reinforces stereotypes by privileging narrow representations of youth, gender, race and sexuality, because these narrow representations attract audiences and help to sell product. Children who do not fit into these stereotypes – particularly girl children – are often set up for conflict with others because their (in)ability to conform to the stereotype is literally quantified by features like the Like button. Moreover, children who do not conform are often subjected to online judgment and harassment, creating a disincentive for them to participate in online life (Bailey & Steeves, 2015). It is no surprise that, in this environment, children are now reporting a discomfort with posting photos of themselves or revealing their interests online (Johnson et al., 2017), and that the more emancipatory uses of networked technologies are being replaced by the passive consumption of online popular culture (Steeves, McAleese &Brisson-Boivin, 2020).

Corporate algorithms also use children's data to create profiles, and then, based on those profiles, feed children content to "nudge" them to a particular outcome, whether it is to buy a particular product or to use a particular educational resource. These algorithms often replicate real-world stereotypes, in effect automating discrimination in the marketplace and in school

(O'Neil, 2016) and further constraining the kinds of subjectivities young people can inhabit online.

Most importantly, young Canadians reject the commercial model that drives many of their online activities. In a 2013 survey of over 5,500 Canadian students, 95 percent agreed with the statement that the corporations who own social media sites should not be able to see what users post there (Steeves, 2014b). Policymakers are beginning to agree. At the conclusion of the second International Grand Committee on Big Data, Privacy and Democracy in May 2019, the Chair of the House of Commons Standing Committee on Access to Information, Privacy and Ethics, Bob Zimmer, commented:

> … the whole drive, the whole business model is to keep them glued to that phone despite the bad health that that brings to those children – our kids. It's all for a buck…We're responsible to do something about that. We care about our kids. We don't want to see them turned into voodoo dolls, to be controlled by the almighty dollar and capitalism (Blanchfield, 2019).

Comments on the State Report

Given the centrality of networked technologies in the lives of young Canadians and the prominence that the CRC gives to media in its provisions (Arts. 13, 17), it is surprising that the State Report only makes three passing references to online issues. This is particularly problematic, given the ways in which protective and corporate surveillance constrain a child's right to:

- free expression, including the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or *through any other media of the child's choice*" (emphasis added) (Art. 13)
- freedom of thought (Art. 14);
- freedom of association (Art. 15);
- privacy, including protection from interference with the child's communications and unlawful attacks on the child's personality (Art. 16);
- access information from a range of national and international sources, especially information "aimed at the promotion of [the child's] social, spiritual and moral well-being and physical and mental health," recognizing "the important function performed by the mass media" in children's lives (Art. 17);
- education (Art. 28) directed to the fullest development of the child's unique personality and culture (Art. 29); and
- play (Art. 31).

Paragraph 78 includes a reference to a new criminal provision prohibiting the non-consensual distribution of intimate images as a way of responding to cyberbullying. Although the provision provides an important avenue of redress for adults, its effect on children is limited because the distribution of intimate images was already an offence under pre-existing child pornography provisions. In addition, the new provision was linked to lawful access legislation that gave the state additional surveillance powers for all offences, leaving many Canadians with the impression that child protection had been used to force through general police powers that had repeatedly failed to pass the House of Commons in the past.

The other two references to online issues, i.e.:

- the role of the Canadian Centre For Child Protection's tip line in protecting children from online sexual exploitation (Paragraph 79); and
- the proposal that anti-cyberbullying initiatives will be developed as part of the Government of Canada's National Crime Prevention Strategy (Paragraph 151)

both position technology as a criminal matter alone. Although these criminal policy initiatives are an important part of the State's obligation to protect children under the CRC, the State Report's emphasis on criminal justice to the exclusion of addressing online privacy invasions and the commercialization of online spaces indicates that the State is failing to take its provision and participation obligations into account. This is particularly worrisome as, in Annex

2 What We Heard, the Report implicitly suggests that online privacy rights must be revisited as "privacy rights are perceived as protecting abusers" and technology is seen as "facilitating abuse and exploitation".

Without careful attention to the ways in which networked spaces shape a child's opportunities for communication, education, and play, and the important role that online privacy has in supporting all these activities, Canada will be unable to meet its obligations under the CRC.

Recommendations

1. Pursuant to the Privacy Commissioner of Canada's Draft Position on Online Reputation (2018), Parliament should pass legislation formally providing children with a right to be forgotten. In particular, legislation should create a remedy that enables a child to have online information about him/her/them deindexed from search engines and/or taken down, and that enables a child who reaches the age of majority to have content posted by their parents or guardians deindexed and/or removed.

2. The Privacy Commissioner of Canada should use section 5 of the Personal Information and Electronic Documents Act to prohibit the commercial collection, use and disclosure of children's personal information as it is not a purpose that a reasonable person would consider appropriate in the circumstances. Collection and use by corporations to provide services would still be allowed, but corporations should not be able to use the information they collect to provide that service to algorithmically profile children or to track them. In addition, all information collected from a child to provide services should be deleted immediately after the services are provided.

3. Canadian privacy and data protection commissioners and provincial youth advocates should reinstitute their ad hoc committee to examine the use of children's data, to identify best practices and policies to protect children's online privacy and provide them with opportunities to exercise their rights to expression, access to information, freedom of association, education, and play in networked spaces.

4. The Government of Canada should work with civil society to create non-commercial online spaces for education, communication and play to be funded through the federal budget. Canada's SchoolNet is an appropriate model to examine, as federal funds were used to support non-commercial organizations interested in creating online spaces that respected children's rights to privacy, expression, association, education and play.

Citations

Bailey, Jane. (2016). *Canadian Legal Approaches to 'Cyberbullying' and Cyberviolence: An Overview*. Ottawa Faculty of Law Working Paper No. 2016-37. Retrieved from: https://ssrn.com/abstract=2841413

Bailey, Jane and Valerie Steeves (Eds.). (2015.) *eGirls, eCitizens*. Ottawa: University of Ottawa Press.

Blanchfield, M. (2019). Big Data Committee Wraps Up Third and Final Day of Hearings on Parliament Hill. *The Globe and Mail*, May 29. Retrieved from https://www.theglobeandmail.com/politics/article-mozilla-executive-tells-big-data-committee-he-was-shocked-when-he/

Johnson, Matthew, Valerie Steeves, Leslie Regan Shade and Grace Foran. (2017). *To Share or Not to Share: How Teens Make Privacy Decisions about Photos on Social Media*. Ottawa: MediaSmarts.

O'Neil, Cathy. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown Publishing Group.

Steeves, Valerie. (2016.) Swimming in the Fishbowl: Young People, Identity and Surveillance in Networked Spaces. In Irma van der Ploeg and Jason Pridmore (Eds.), *Digitizing Identities*. London: Routledge.

Steeves, Valerie. (2014a.) *Young Canadians in a Wired World, Phase III: Life Online*. Ottawa: MediaSmarts.

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

Steeves, Valerie, Jane Bailey, Jacquelyn Burkell, Priscilla Regan and Leslie Shade. (2020). *This is What Diversity Looks Like*. Manuscript in preparation.

Steeves, Valerie, Samantha McAleese, Kara Brisson-Boivin. (2020). *Young Canadians in a Wireless World, Phase IV: Talking to Youth and Parents about Online Resiliency*. Ottawa: MediaSmarts.

Zuboff, Shoshana. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Hachette Book Group.