Submission to the United Nations Special Rapporteur on The Right to Privacy
Toward a Better Understanding of Privacy: Children's Right to Privacy and Autonomy

Submitted by Valerie Steeves[1] and Jane Bailey[2] on behalf of The eQuality Project
www.equalityproject.ca

Introduction

The eQuality Project is a seven-year partnership of academic researchers, civil society groups, educators, policymakers and youth funded by the Social Sciences and Humanities Research Council of Canada and co-led by Valerie Steeves and Jane Bailey. Our research team conducts research with young Canadians between the ages of 11-17 at diverse social locations to explore their experiences of privacy and equality in a networked environment. The bulk of our work is designed to give voice to young people's concerns and to bring those concerns to policymakers so young people can participate in the policy making process. We use quantitative, qualitative and youth-participatory action methods and all of our work is informed by our youth partners and our Youth Advisory Committee.

The following provides an overview of our research findings, with special emphasis on young Canadian's views about the right to privacy and how that right is interpolated with autonomy and independence.

Privacy, Autonomy and the Task of Growing Up: Young Canadian's Perspectives

Our research participants consistently report that privacy is very important to them, and that the ability to enjoy privacy is closely tied to the ability to meet their developmental goals and to enjoy a degree of autonomy as moral actors in their own right.

Younger children, aged 11-12, seek privacy in networked spaces as a way of maintaining the boundaries around the home. Although they typically enjoy using online media to communicate with friends and family and for entertainment purposes (Steeves, 2014a), they want to avoid interactions they find offensive or upsetting. They therefore see parents[3] as an important part of their privacy infrastructure because parents help them steer clear of online pitfalls (Steeves, 2012). For example, they are more likely to be comfortable with sharing passwords and giving parents access to their online lives than teenagers (Steeves, 2014b, p. 29) because parental supervision is a key resource that enables younger children to navigate online media and make choices about the content they consume (Steeves, 2012).

[1] Valerie Steeves is a Full Professor in the Department of Criminology at the University of Ottawa in Canada. She can be reached at vsteeves@uottawa.ca.
[2] Jane Bailey is a Full Professor in the Faculty of Common Law at the University of Ottawa in Canada. She can be reached at jbailey@uottawa.ca.
[3] Our use of the term "parent' is not intended to be exclusionary. It encompasses adult caregivers and guardians who engage in the act of parenting.

At this life stage, sharing the same online spaces with parents can accordingly facilitate privacy *and* autonomy because parents can help children learn how to make their own choices. They do this by teaching their children how to assert boundaries around their online lives so their children can actively manage invasive behaviour on the part of ill-intentioned online actors. This in turn creates a manageable field of choices for young children who can then navigate the online environment in ways that make sense to them. In this case, privacy and autonomy are not so much about being "left alone". Instead, they are cultivated through respectful and supportive social relationships with parents.

These privacy practices are consistent with Frierson's conceptualization of child autonomy as rooted in environmental factors that enable children to exercise their "internal capacities for freedom and attention" (Frierson, 2016, p. 340). We would suggest that this understanding of autonomy is particularly useful for two reasons. First, it positions children as rights-holders who have an interest in and capacity for negotiating a comfortable level of privacy with other social actors. Second, it moves beyond a sole focus on protecting children from online dangers and provides space for children to participate in online media. This tripartite focus on provision, protection and participation is not only more consistent with the *Convention on the Rights of the Child*; it also recognizes that creating private spaces is an essential part of ensuring that children can enjoy their other rights, such as the right to expression, information, culture, and education. It also leaves space for recognizing that ensuring autonomy and privacy for *all* may also require social and regulatory responses to address environmental factors such as racism, sexism, and homophobia that negatively affect children from equality-seeking communities.

Privacy negotiations for older children (13-17) are more complex because teenagers are seeking to meet their developmental needs to explore the world outside the home and become autonomous individuals with their own unique identities. This is typically accomplished by developing strong peer relationships and participating in different communities. This requires a certain amount of privacy *from* the family, so teens can interact with peers and experiment with different – and new – roles. From this perspective, privacy is not about control over personal information nor solely about being "left alone"; it is about being able to assert appropriate boundaries between a young person's various social roles and relationships. Privacy is violated when these boundaries are breached.

Parents often report that, although they would like to give their teens more privacy and autonomy, they are afraid that their children might fall prey to online dangers unless they are constantly monitored (Steeves, McAleese & Brisson-Boivin, 2020; Steeves, 2012). In other words, parents of teens are more likely to prioritize protection over provision and participation. No doubt this prioritization is at least in part affected by public messaging from corporations and governments that emphasizes and promotes surveillance and monitoring as good parenting (Steeves & Marx 2010). This makes it extremely difficult for teens to obtain the privacy they need to use networked technology for their own purposes because, as 14-year old Penny put it in 2019, "there is no hiding" so "I'm always terrified that I'm going to like, say something wrong or somebody's going to take it in the wrong way" (Steeves, McAleese & Brisson-Boivin, 2020, p. 20; see also Steeves, 2012). It can also be particularly challenging for 2SLGBTQ+ youth who wish to explore their sexual and gender identities using networked technologies, but who are not ready to "be out" to parents (sometimes out of fear of responses) (Bailey & Steeves 2017, p. 83).

"It's like, I'm your kid. You should have a little bit of faith in me… Trust" (16-year-old Tejal in res, 2020).

From the teen's perspective, the most worrisome aspect of a lack of privacy vis a vis their parents is that it indicates that their parents do not trust them. This in turn makes it more difficult for teens to trust parents when they do encounter online difficulties because they are afraid that going to a parent will mean that they lose control over the outcome (Steeves, 2012). However, our qualitative research suggests that when parents do respect their teens' privacy and trust them to exercise their autonomy in a mature way, teens have the space they need to use networked media in creative ways and come to parents for help when they need it (Steeves, McAleese & Brisson-Boivin, 2020, p. 19). (As discussed below, however, neither teens nor adults are well-equipped to meaningfully address the often-times invisible corporate manipulation of children and their data that is endemic in the current for-profit data-in-exchange-for-services model of the internet.)

"Yeah, like it's kinda weird [for teachers] to like creep on kids" (11-year-old Hayden in res, 2020).

The interaction between privacy, autonomy, and trust also plays out in the educational setting. All of our participants are aware of the fact that they are under constant electronic surveillance when they use technology at school (Steeves, 2012; Steeves, McAleese & Brisson-Boivin, 2020) and this surveillance affects their rights in unexpected ways. For example, content filters and monitoring software installed to protect them frequently make it difficult for young people to access good educational material because it is inappropriately blocked (Johnson, Riel & Froese-Germain, 2016). This invasion of privacy limits their rights to information and education. In like vein, they are often required to complete tasks which require privacy, like writing for reflection, with equipment that constantly broadcasts their work to school monitoring software; knowing the teacher may be watching interferes with the task itself, constraining their autonomy as learners through a lack of privacy (Steeves, McAleese & Brisson-Boivin, 2020). These constraints can have particularly acute effects on youth from equality-seeking communities, including 2SLGBTQ+ youth seeking information relating to gender and sexuality that over-broad filtering technologies may prevent them from accessing (Livingstone & Mason 2015).

In addition, since their social interactions at school can be captured and taken out of context, they worry about being unfairly disciplined (Steeves, 2012; Bailey & Steeves, 2017). This puts them in the awkward position of having to craft their communications for two audiences, their classmates and any teachers who may be listening in. They describe this as "scary" and "creepy" (Steeves, McAleese & Brisson-Boivin, 2020, p. 13). Once again, this loss of privacy also makes it more difficult to develop relationships based on trust and to go to a teacher for help because they worry that they will lose control over the outcome (Steeves, 2012; Bailey & Steeves, 2017).

These problems are likely to be exacerbated with the introduction of personalized learning apps driven by artificial intelligence. These apps rely upon extensive surveillance and data collection to algorithmically sort children as learners. This loss of privacy may constrain children's autonomy, as decisions about what they learn and how they learn it will be determined by the apps (Regan & Jesse, 2019). It also reconstructs the classroom in ways that make it difficult for children to get the private space they need for reflection and synthesis (Regan and Steeves, 2019), limiting their right to education. And, like other algorithmic sorting technologies, the privacy intrusions occasioned by personalized learning apps are likely to have disparately negative effects on children from equality-seeking communities (Regan & Bailey, 2020), often due to racist, classist, and sexist stereotypes built into such technologies.

Young Canadians report similar concerns about privacy and autonomy on social media because they know that their communications are being monitored by corporations. This loss of privacy is particularly problematic because online privacy helps them access the information they need to explore their own identities as emerging adults. It is noteworthy that between 20 to 40 percent of 17-year-olds in 2015 reported that they use online resources to learn more about their physical health, mental health, relationships and sexuality (Steeves, 2014a, p. 16). Our most recent focus groups suggest that this private access to online resources is particularly important to teens that belong to equality-seeking communities. For example, our trans participants report that the Internet is often a lifeline because it gives them access to information about their bodies and connects them to other trans youth. However, since privacy is essential to this process and corporate data collection disrupts that privacy, they are now turning away from online resources because they know that their private searches are constantly being collected by corporations (Steeves, et. al, 2020). Once again, a lack of privacy interferes with young people's ability to enter into relationships of trust and exercise their autonomy in ways that make sense to them, with particularly negative effects for youth from equality-seeking communities.

The corporate collection and use of children's data is a key element of understanding how the online environment works against privacy, autonomy and equality. As Zuboff notes, corporations rely upon "a new economic order that claims human experience as free raw material for hidden purposes of extraction, prediction, and sales" (Zuboff, 2019, preface). This practice embeds "a new global architecture of behavioural modification" (*ibid*) into young people's daily lives that is predicated upon constantly collecting their data and using those data to manipulate their choices (Sussler, Roessler & Nissenbaum, 2019). Since the algorithms that drive this commercial extraction privilege commercially successful representations, children's online spaces are wallpapered with ads and other marketing content that contains gender, racial and other stereotypes. Young people are then expressly and publicly judged (though the like button, comments and other functionalities) on their ability to mimic these representations. This both magnifies inequalities and sets young people up for conflict (Bailey & Steeves, 2015).

Our research participants describe these corporate practices as "creepy" (Steeves, 2012; Bailey & Steeves, 2015) and "stalkery" (Steeves, McAleese & Brisson-Boivin, 2020). Menah's (aged 14) comments are typical. When she was explaining why she no longer used Wattpad to write stories, she said, "I don't want [the] people that like own it, to know what I want … I definitely don't want like a bunch of strangers knowing it, so yeah" (p. 21). Knowing that "everything nowadays, every electronic camera – it always has someone behind it listening and recording and gathering everything that's happening" (Sachi, aged 15, p. 21) means that young people are no longer willing to use networked media for self-expression and community building (Johnson et al., 2017; Steeves, McAleese & Brisson-Boivin, 2020). As 16-year-old Tejal put it, posting anything personal "makes no sense' because "if you hit share, then like it's everywhere already" (Steeves, McAleese & Brisson-Boivin, 2020, p. 21; see also Johnson et al., 2017).

Policy Implications and Recommendations

Our participants tend to see civil and criminal legal avenues as remedies of last resort, except in the most extreme circumstances (Bailey & Steeves, 2017). Not only do they note that legal remedies are inaccessible due to expense and delay, they also worry that involving the law will blow things out of proportion, potentially exposing someone already harmed to further publicity rather than minimizing the damage (e.g. of an online attack) or repairing and redressing affected relationships (Bailey & Steeves, 2017).

> "It would be blown up into like a larger thing than it really was …. It's just it could get a lot further than I'd want it to go and I have no control in stopping it because it's like gone to the police and now they want to make a court date out of it" (15-year-old Morgan, Bailey & Steeves, 2017).

Based on their lived experiences, our participants prefer policy approaches that are more consistent with an understanding of privacy, autonomy and equality as related social values, negotiated in and through relationships, and heavily affected by environmental factors such as corporate, parental and educational surveillance and monitoring, as well as structural discrimination. They call for policy responses aimed at creating a healthy online environment, rather than individualistic approaches grounded in controlling young people through surveillance. Unsurprisingly, privacy plays a critical role in creating and maintaining that environment.

Our participants seek responses that:

- avoid reliance on further surveillance, which already makes it difficult for them to exercise their rights to privacy, autonomy, equality, access to information and free expression (Bailey & Steeves, 2017);
- minimize corporate access to and use of their data (Steeves, 2014b);
- minimize publicity relating to online attacks (e.g. through community-based platform moderation and small-scale interventions by teachers (Bailey & Steeves, 2017);
- support young people in repairing their own reputations and relationships (e.g. through administrative bodies offering mediation and restorative justice services) (Bailey & Burkell, 2020); and
- prevent harmful online behaviour at its source, rather than simply reacting to it (e.g. through anti-racism, anti-sexism education) (Bailey & Steeves, 2015; Bailey & Burkell, 2020).

Based on what we have been fortunate enough to learn from young people over the last 20 years about their needs, aspirations and experiences we advocate for policy approaches grounded in the UN Convention on the Rights of the Child principles relating to protection, provision and participation.

Protection – Ensuring that children's privacy and autonomy rights flourish requires new measures of protection that move beyond a data protection approach toward a human rights-based approach. A human rights-based approach should include creation of no-go zones that prohibit profiling children for marketing purposes and other invasive practices. Prohibiting such activities moves beyond data protection models based on "consent" to data collection and use, recognizing that children's human rights to privacy, autonomy and equality are inalienable and thus cannot be contracted away.

Provision – Children's privacy and autonomy rights will not flourish unless they are provided with an environment in which commercial activity is zoned, which necessitates creation of public infrastructure for non-commercial educational and social spaces.

Participation – Measures aimed at ensuring the flourishing of children's privacy and autonomy must be grounded in children's participation. Children from a wide variety of social locations must be recognized and supported participants in policy-making processes relating to their privacy and autonomy, as a reflection of their internationally-recognized right to participate in decision-making about matters directly affecting them. Further, young people must be assured the right to participate in protecting their own privacy by ensuring that corporate, governmental and parental practices do not impede their ability to exercise their own strategies for controlling their audiences.

Works Cited

Bailey, J. and Steeves, V. (2015). *eGirls, eCitizens*. Ottawa: University of Ottawa Press.

Bailey, J. and Steeves, V. (2017). *Defamation law in the age of the internet: Young people's perspectives*. Commissioned by the Law Commission of Ontario. Online: http://www.lco-cdo.org/wp-content/uploads/2017/07/DIA-Commissioned-Paper-eQuality.pdf. Retrieved 25 September 2020.

Bailey, J. and Burkell, J. (2020). Legal remedies for online attacks: Young people's perspectives. *The Annual Review of Interdisciplinary Justice Research*, 9, 110.

Bailey, J. and Regan, P. (2020). Big data, privacy and education applications. *Education and Law Journal, 29(1)*, 55.

Frierson, P.R. (2016). Making room for children's autonomy: Maria Montessori's case for seeing children's incapacity for autonomy as an external failing. *Journal of Philosophy of Education*, *50*, 3, 332-350.

Johnson, M., Riel, R. and Froese-Germain, B. (2016). *Connected to learn: Teachers' experiences with networked technologies in the classroom*. Ottawa: MediaSmarts/Canadian Teachers' Federation.

Johnson, M., Steeves, V., Shade, L.R. and Foran, G. (2017). *To share or not to share: How teens make privacy decisions about photos on social media*. Ottawa: MediaSmarts.

Livingstone, S. and Mason, J. (2015). Sexual rights and sexual risks among youth online. London: LSE. Online: http://eprints.lse.ac.uk/64567/1/Livingstone_Review_on_Sexual_rights_and_sexual_risks_among_online_youth_Author_2015.pdf. Retrieved 25 September 2020.

Regan, P.M. and Jesse, J. (2019). Ethical challenges of edtech, big data and personalized learning: Twenty-first century student sorting and tracking. *Ethics and Information Technology, 21*, 167-179.

Regan, P.M. and Steeves, V. (2019). Education, privacy, and big data algorithms: Taking the persons out of personalized learning. *First Monday, 24*, 11.

Steeves, V., Bailey, J., Burkell, J., Regan, P.M., and Shade, L.R. (2020). [This is What Diversity Looks Like]. Unpublished raw data.

Steeves, V. (2014a.) *Young Canadians in a wired world, phase III: Life online*. Ottawa: MediaSmarts.

Steeves, V. (2014b.) *Young Canadians in a wired world, phase III: Online privacy, online publicity*. Ottawa: MediaSmarts.

Steeves, V. (2012.) *Young Canadians in a wired world, phase III: Talking to youth and parents about life online*. Ottawa: MediaSmarts.

Steeves, V., and Marx, G.T. (2010). From the beginning: Children as subjects and agents of surveillance. *Surveillance & Society*, 7(3-4), 192.

Steeves, V., McAleese, S. and Brisson-Boivin, K. (2020). *Young Canadians in a wireless world, phase IV: Talking to youth and parents about online resiliency*. Ottawa: MediaSmarts.

Susser, D., Roessler, B., and Nissenbaum , H. (2019). Online manipulation: Hidden influences in a digital world. *Georgetown Law Technology Review, 4*, 1, 1-44.