CHAPTER 3

Framing the Challenges of Digital Inclusion for Young Canadians

Leslie Regan Shade, Jane Bailey, Jacquelyn Burkell,
Priscilla Regan, and Valerie Steeves

Abstract

This paper reports on The eQuality Project's initial findings from focus groups conducted in the fall of 2018 and winter of 2019 with a diversity of youth (ages 13–17) in three Canadian cities about their perspectives and experiences of privacy and equality in networked spaces. Focus groups explored online activities and platforms used by participants, whether and how privacy was an essential aspect to their enjoyment, online experiences where they felt unwelcome or disrespected, and their strategies to mitigate these constraints. We use a modified version of the Institute of Museum and Library Services' digital inclusion framework to link the perspectives and apprehensions of the young people we interviewed to emerging digital policy questions. These include access (availability, affordability, inclusive design, and public access), application (across various sectors and uses like education, workplaces, employment, economic development, health, public safety, and civic engagement), and adoption (uptake and relevance, privacy and data rights, safety, and digital literacy). We conclude with several policy suggestions, including holding platform companies accountable and transparent about their data collection and privacy protection practices through producing coherent and well-designed terms of service; ensuring funding for enriched digital literacy programming for schools,

parents, and young people in order to strengthen digital skills and knowledge about the dynamic nature of datafication; and bringing the voices of diverse Canadian youth into policy-making to ensure that intersectional perspectives and digital justice are core components for a rights-respecting networked environment.

In May 2019, Canada's House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) hosted the second International Grand Committee (IGC) on Big Data, Privacy and Democracy. The meeting brought together politicians from Canada, the United Kingdom, the European Union, Morocco, Argentina, Brazil, Singapore, Mexico, Ecuador, and Trinidad and Tobago to discuss heightened concerns surrounding big tech regulation and the need to reaffirm domestic policy commitments. Parliamentarians signed the Ottawa Declaration, which supported an "unwavering commitment to foster market competition, increase the accountability of social media platforms, protect privacy rights and personal data, and maintain and strengthen democracy" (ETHI, 2019, p. 7). The declaration also called on digital platforms to "follow applicable competition and antitrust laws, to strengthen their practices regarding privacy and data protection, to increase their algorithmic accountability, and to improve the manner in which these platforms prevent digital activities that threaten social peace or interfere in the open and democratic processes around the world" (ETHI, 2019, p. 7).

At the conclusion of the three-day hearing, ETHI Chair Bob Zimmer remarked that policy-makers should protect children from the "surveillance capitalism" business model of the major high-tech companies. Stated Zimmer, "the whole drive, the whole business model is to keep them glued to that phone despite the bad health 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, para. 6).

As evoked by Zimmer, "surveillance capitalism" referred to testimony by scholar Shoshana Zuboff, who detailed its attributes in her magisterial 2019 book of the same title, subtitled "The Fight for a Human Future at the New Frontier of Power." In her written testimony to the IGC, Zuboff wrote that surveillance capitalism "declares private human experience as free raw material for translation into

production and sales. Once private human experience is claimed for the market, it is rendered as behavioral data for computation and analysis. While some of these data may be applied to product or service improvements, the rest is declared as a proprietary behavioral surplus. This surplus is defined by its rich predictive value" (ETHI, 2019, p. 5).

With respect to children and youth, Zuboff (2019) describes in her book how "young life now unfolds in the spaces of private capital, owned and operated by surveillance capitalists, mediated by their 'economic orientation,' and operationalized in practices designed to maximize surveillance revenues. These private spaces are the media through which every form of social influence—social pressure, social comparison, modelling, subliminal priming—is summoned to tune, herd, and manipulate behavior in the name of surveillance revenues" (p. 456). The suggestion that the commercial model of big tech should be constrained because of its impact on the well-being of children signifies an important potential shift in Canadian policy-making. From the early days of the web, children have been mobilized to support the relatively unregulated growth of networked technologies: typically presenting children as naturally facile with technology, policy-makers have been both enthusiastic about connecting young Canadians so they can become the information innovators of the future, and loath to regulate tech companies because it might stifle that innovation (Shade et al., 2005). As problems such as access to pornography and cyberbullying have been identified, legislators have stopped short of interrogating how the commercial model that drives networked spaces sets young people up for conflict and erodes their privacy. Instead, they almost universally have responded by placing children under "protective" surveillance that further erodes that privacy (Bailey, 2015; Steeves, 2016). To explore policy options that better reflect the perspectives and experiences of young people, we conducted a study in the fall of 2018 and winter of 2019 called *This Is What Diversity Looks Like: What Young People Need to Enjoy Privacy and Equality in Networked Spaces*, which aimed to explore youth experience of online privacy and equality, including their experiences of what is afforded them and what constrains them in networked activities and platforms.[1] To examine the relationship between social location, privacy, and equality, we adopt an intersectional approach designed to support young people in creating networked spaces where they feel included and able to participate fully (Bailey & Steeves, 2015;

Bailey et al., 2019). For this study, our focus groups included LGBTQ, Indigenous, racialized, and general population youth (ages 13–17) from diverse geographic locations: a mid-sized central Canadian city, a large central Canadian city, and a mid-sized western Canadian city.

In the study, we asked young people about the various elements and opportunities they felt ensured their inclusion in online spaces, and whether privacy played a key role in their enjoyment of their activities and platforms. We also asked youth whether and how schools, government, and tech companies could make online spaces more welcoming and inclusive of youth. This chapter discusses our preliminary findings. We organize our discussion around a modified version of the Institute of Museum and Library Services' (IMLS) digital inclusion framework (the IMLS Framework) to connect the perspectives and concerns of the young people we interviewed to emerging policy questions about a range of online issues, including access (availability, affordability, inclusive design, and public access), application (across various sectors and uses like education, workplaces, employment, economic development, health, public safety, and civic engagement), and adoption (uptake and relevance, privacy and data rights, safety, and digital literacy) (PPF, 2018, pp. 2–3).

Moving from Surveillance Capitalism to Digital Inclusion

A plethora of social scientists have provided evidence that networked environments are complicated ones for children. Although young people report that they enjoy the easy sense of connectedness with friends and family, and have incorporated devices into a variety of daily tasks, they have also consistently raised concerns about the surveillance they experience at school, at home, and in the marketplace (Steeves, 2005, 2014). As Kathryn Montgomery (2015) notes, this surveillance is rooted in the "economic imperatives and powerful e-commerce business models" designed to "monitor and monetize [young people's] behaviors as well as their interactions with friends and acquaintances" (pp. 772–773).

Policy-makers have typically responded to these concerns by enacting consent-based data protection legislation that purports to give young people (and their parents) a degree of control over the ways in which young people's information is collected, used, and disclosed (e.g., in the United States, the *Children's Online Privacy Protection Act* [COPPA], and in Canada, the *Personal Information*

Protection and Electronic Documents Act [PIPEDA]). However, data protection has been an incomplete corrective, primarily because young people have a different conception of privacy. From their perspective, they are required to disclose information about themselves in order to participate in the online world. But this does not mean that they are comfortable with others collecting and using that information (Marwick & boyd, 2014; Steeves, 2015). For example, it is remarkable that 95 percent of young Canadians surveyed in 2013 reported that marketers should not be allowed to see what they post on social media, in spite of the fact that the young people have technically consented to their posts' disclosure to the public (Steeves, 2014).

Because of this, numerous policy organizations are incorporating human rights-based approaches to more fully protect children in networked environments. For example, the European Union's *General Data Protection Regulation* (GDPR) has supplemented children's general data protection rights with age-specific provisions that restrict profile-based marketing and prohibit algorithmic decision-making that significantly affects a child's rights (Steeves & Macenaite, 2019). And, for its part, the UN Committee on the Rights of the Child (CRC) is developing a "General Comment" on children's rights in relation to the digital environment (2019) to support states and NGOs to interpret the 30-year-old Convention on the Rights of the Child (CRC) for the digital age and to outline the types of policy responses that are needed to ensure that young people can fully participate in online life.

The IMLS Framework is a useful tool in this process because it goes beyond informational control and aims to identify "interventions which seek to increase access, remove barriers, develop digital skills, and empower people who might be otherwise marginalized and excluded from the design and use of digital technologies" in order to "ensure that everyone can benefit from digital technologies in their lives" (*Ontario Digital Service*, 2017). We suggest that a modified version of the IMLS Framework will enable policy-makers to begin to ask the right questions that will help inform the development of a rights-respecting networked environment in which young people from diverse social backgrounds can meaningfully access networked technologies and thrive online without fear of discrimination. In Table 3.1 we provide questions that we deem to be relevant and merit further research and analysis, even though not all of these were addressed by participants in our focus groups.

Table 3.1: Some Policy Questions on IMLS Framework

Elements	Policy Questions
Access: Availability Affordability Inclusive design Public access	Do young people and their families have access to affordable high-speed broadband in their homes? Are there sufficient, affordable, and accessible spaces for young people to gain public access to digital technologies? Are digital technologies inclusively designed so everyone can use them effectively and safely? Are school-based technologies implemented in ways that promote inclusion and respect privacy?
Application: Across various sectors and uses: - education - workplaces - economic development - health - public safety - civic engagement	Are all young people able to equally benefit from the use of digital technologies? Can digital technologies enhance educational, economic, healthy, and civic engagement for all young people in ways that enhance their privacy and enable them to participate in decisions about their lives?
Adoption: Uptake and relevance Privacy and data rights Safety Digital literacy	How can young people gain the knowledge and skills to effectively use digital technologies, including cell phones, smart tablets, and laptop computers? Do teachers and parents have the support they need to help young people become digitally literate? Are tech companies being held accountable to ensure they design technologies that respect young people's needs for privacy and participation?

Adapted from: PPF (2018).

Young Canadians' Perspectives of Digital Inclusion: A View from the e-Trenches

Our study asked a central research question: What factors enable youth from diverse social locations to participate fully in networked spaces and activities, and enjoy a lived equality online? Using the IMLS Framework of access, application, and adoption, we present preliminary findings from our focus groups.

Access

Cell phones were the primary means of accessing the Internet for virtually all of the focus group participants. They were also important storage devices for multiple types of content, making the prospect of losing one's phone quite upsetting. Emma, a 16-year-old participant who thought they'd lost their phone put it, "I had lots of things in my phone that I didn't really realize, like contacts and like old photos, like screenshots. So, I guess it's just like small things." Laptops, iPads, and Chromebooks were other common means for gaining Internet access, although use of these devices was more frequently associated with doing schoolwork either in school or at home. In a number of cases, focus group participants shared these devices with others, such as family members. For example, Xiu, a 13-year-old participant, reported sharing with "only my family so like it's safe."

Application

The focus group participants primarily connected with the Internet for leisure and education purposes, although occasionally their leisure pursuits involved information gathering that could be associated with civic engagement. Connectivity related to leisure pursuits involved both communicating with others and seeking out entertainment. While most of our participants communicated with family and friends primarily through cell phone texting, they also used Snapchat and Instagram, with some of them curating their Instagram to differentiate public from private audiences of friends and family. WeChat's video call function was also a popular means for Chinese newcomer focus group participants to communicate with family and friends who were still in China. As Xiu put it, "[s]o other than you can talk with them, so you can also see them

is more convenient. It's like when you see them and talk to them in real life."

The focus group participants' leisure pursuits involved seeking out entertaining content (such as Vines and memes) on platforms and apps such as Instagram, Amino, Kik, Tumblr, YouTube, Netflix, and Twitter, and gaming sites such as Fortnite. In some cases, participants' entertainment-seeking activities were also forms of community building. Members of our LGBTQ focus group who use Amino, for example, described it as an opportunity to connect with others from around the world with shared interests such as fandoms. Similarly, for some of the Chinese newcomer focus group participants, watching Netflix became a way of gaining cultural capital that then allowed them to participate in face-to-face conversations in school about popular shows. They also used Chinese platforms such as Bilibili in order to gain access to popular culture from their homeland. In certain cases, information seeking on public issues was part of our participants' leisure activities. For example, several followed prominent public figures such as politicians (Donald Trump), tech gurus (Elon Musk), and well-known entertainers (Lin-Manuel Miranda) on Twitter.

Music was another popular online leisure pursuit for our participants, who use platforms and apps such as Spotify, iTunes, BlackPlayer, and QQ (which one Chinese focus group participant, Tommy, age 14, characterized as "a Chinese version of Spotify"). For one of our participants, algorithmically generated recommendations, such as on Spotify, were a generally inaccurate and unwelcome product of a for-profit agenda. Emma noted, "I'll be less likely to listen to [a recommendation] or enjoy it, simply because I've decided in my mind that this might just be because of money."

Email, Google Drive, and Google Docs were platforms that our participants generally only used to connect with educational activities. Google Drive, in particular, was considered by some as stressful because of its association with homework assignments. As Tommy put it, "Every time I use Google Drive, I need to do a lot of school stuff, like assignments and it's pretty stressful." While Skype and Facebook were considered by Tommy to be "kind of old," or as platforms used mainly by older people, both were still used to a limited extent by some participants. For example, one participant used Skype for English lessons, while other participants found they had to use Facebook in order to access school communications, information

about volunteer opportunities, and, to a lesser extent, news. On the other hand, several found that access to certain content was blocked while they were in school, which as Annie, age 13, commented, "can sometimes get annoying."

Adoption

Based on a preliminary analysis of the focus group comments, we focus on several adoption issues related to safety, privacy, and what government or corporations might do. A more complete analysis of the focus groups is underway, but our early review reveals a number of relevant insights.

Regarding safety, the focus group participants identified four main sources that negatively affect their online experiences, especially on social media: other people, corporations, malevolent anonymous interactions, and being hacked. The main source of concern is other people—specifically negative, inappropriate, mean, self-serving, harassing, or nasty posts and messages (e.g., use of the "n" word, calling things "so gay," and intentional or ignorant ways of silencing members of marginalized communities). There was a recognition that, as Tommy put it, "These things happen all the time" but also that, as Emma commented, they "feel bad for all of the people involved." Interestingly, the main response to such negative posts is "to ignore them" (Malinda, age 14). Participants also engage in proactive behaviour, for example, with respect to posting of photos. As one trans participant, Josh (age 16), related:

> But like, if they're taking a picture of you without asking you, without saying anything, it's like they could be, like, posting it—they could be, like, taking this to make fun of me. They could be, like, taking—like taking this for, like, some weird, like, malicious intent. Like, it's just creepy. That's weird and it happens a lot with that, like—cosplayers [costume players]—have to, like, basically be like, "Please don't take photos of me without asking because it's creepy."

These comments mirror the results of earlier studies of online behaviour of youth that indicate the importance, and creativity, of self-management. The participants in our groups accepted that there was a likelihood of somewhat nasty behaviour from other people yet

demonstrated a confidence in handling and moving past it. Their responses reflect learning from experience to develop the necessary skills. In some cases, participants reported this type of management behaviour but with a sense of resignation that it might not help. As Andrew, a 13-year-old racialized participant, said: "I don't know what happened after that. I don't care about that anymore."

A second source of negativity identified by our participants is the behaviour of corporations, especially in terms of what participants fear is going on behind the scenes. For example, on Instagram, Shan (age 13) related that, "Every time I download something, they would also say, like, 'Oh, we can—can we access your camera?' and all that, and I'm… Yeah, that's kind of creepy. Especially when they don't need the camera. So, I just… Yeah, I would—I would uninstall it if it does that." There is also a sense that some of the corporate offerings made to be attractive in ways that are misleading—for example, Snapchat (and its Snap Map), which Josh described as a "dangerous platform because people get, like, this sense of, like, 'Oh, it's—it's gonna disappear, so I can say whatever'… But … nothing on the internet is ever gone." When asked who *should not* see their information, participants of one focus group centred attention on data sharing and integration across multiple platforms owned by the big corporations, specifically mentioning Google, Apple, Instagram, and Amazon. Julie (age 15) gave as an example the targeted ads that appear on Instagram after searching on Amazon, noting that the practice "kind of scares me. Because like, then you know for sure that they're kind of collecting data on you" and "Instagram and Amazon, they're like two completely different apps, and seeing them somehow have a relationship, well, it's kind of like, woah." Julie also raised concerns about covert monitoring of activity (e.g., microphone, camera, texts), noting that "sometimes it seems like your phone is listening to you" because you can be talking to someone about a product and then you get an ad for it later on. The same issue came up in another focus group with a similar response from participants; as Annie exclaimed, "So, they could, like, see what I've talked about with other people? … That feels … weird, like I'm spied on." George, a 17-year-old participant referred to this as "extreme capitalism," while Luke, a 15-year-old participant, described it as "Big Brother." Participants voiced frustration with the tech companies—that they were neither transparent with their practices nor held accountable for overstepping what was expected.

A third source of negativity, mentioned less than the above two, relates to people with malicious intent outside of one's social circle. Participants expressed concerns about online anonymity because they wanted to make sure they were not talking to, as Cody (age 14) described, a "dangerous person." A fourth concern emanated from experiences of being hacked, which also affected future behaviour: George discussed an experience in which hackers "broke into my account, changed the password, and then started posting, like, a bunch of, like, pornography from my account until the account got deleted. So, that's just why I'm really anxious."

In terms of measures that might address the negativity online, participants believed much of the responsibility had to rest with social media users themselves. For example, Shan commented, "When I think of, like, people posting, like, mean stuff on social media, I don't really think that's the social media's responsibility to fix that." An interesting exchange in one focus group with Chinese newcomers included a list of "do's and don'ts" including "make the right decisions" and "don't talk to strangers" (Janaan, age 13); "don't tell someone your personal information" (Ken, age 13); "be polite, trying to control yourself, not saying bad words or your comments to other people, otherwise they'll fight back to you" (Malinda); and, "don't follow fake accounts" and "don't watch some videos … like violence or pornography" (Andrew).

Participants do not generally read privacy notices or terms of service, which they find too long (as 16-year-old Patrick said, "to force you not to read it"), purposely hard to understand, "convoluted," and difficult to understand ("they can sometimes sneak things in there that just flips everything on its head," said Alex, a 14-year-old demigirl). In two focus groups, participants did note that they were more likely to look at the notices after the Facebook—Cambridge Analytica scandal.

Participants did not believe there was much that the government or corporations could do to mitigate the negativity. Some participants thought the government or corporations should block sites or take down comments that were hateful or racist, but most participants had a more nuanced view, noting the difficulties of making these distinctions and recognizing the potential negative implications for freedom of speech. A number of participants had reported issues to social media sites but were concerned that the sites lacked "context" to evaluate photos or comments and would likely

take down reported posts because, as Emma exclaimed, "What's the easy way out? 'Let's just delete the post.'" Annie emphasized that platforms could assist with "security improvements" that reduced the possibility of account hacking. In general, participants seemed to think that corporations were motivated by money and the government by rich people—and that there was not much either could, would, or should do.

Conclusion: Digital Inclusion to Digital Justice

In May 2019, Innovation, Science and Economic Development Canada (ISED) released their *Digital Charter* emphasizing three broad areas of concern—the future of work, the impact of innovation, and trust and privacy. Echoing earlier discourses, youth are positioned in the report as needing to be prepared for the "workplace of the future," through adequate digital skills and literacy, especially in STEM fields. Youth were also mentioned with respect to strengthening PIPEDA rules (e.g., making it easier to delete content and withdraw consent) to give them greater control over their personal information and reputation. A sidebar on "What Young Canadians Said" (ISED, 2019, p. 11) mentions their belief that access is fundamental, especially to improve digital government services and online resources for education. It further mentions that strong digital literacy initiatives in a climate of misinformation and improving privacy, trust, and consent through transparent agreements are needed for a democracy. The *Digital Charter* made no mention of regulating tech companies, nor did it specify what a rights-respecting networked environment with elements of the IMLS Framework would entail. The *Digital Charter* commitment to address online hate appears to be primarily connected with Canada's decision to sign on to the Christchurch Call to Action,[2] which focuses largely on terrorism and radicalization and came about in response to an attack at a mosque in Christchurch, New Zealand. While these are no doubt important equality issues, there is a notable lack of attention to day-to-day acts of discrimination, corporate monitoring, and other forms of negativity that undermine inclusivity in digital spaces.

For young people, the persistent commercialization and datafication—the systematic collection and analysis of massive amounts of data sets—of their communicative practices raise ethical tensions and privacy concerns about whether they can maintain control of their digital identity over the course of their life cycle (Smith & Shade,

2018). Digital inclusion aims to improve quality-of-life and economic well-being (Rhinesmith, 2016), and is a constituent element of digital justice, "concerned with fair and equitable access to technologies and skills; appropriate instructional approaches and design tailored to different groups; and safe, secure and inclusive spaces online" (Pelan & Smythe, 2019, para. 1). Digital justice includes data literacy, which extends core components of digital literacy (an ability to critically understand and create digital media content and tools), to encompass an awareness of datafication processes, design, and policies. Seen through an intersectional lens (Bailey et al., 2019), and reflected in our findings, digital justice highlights how the intersectional social location of youth shapes their online experiences, and how corporate platforms, through infrastructural design, opaque algorithms, and complex and obfuscatory terms of service and privacy policies, can stifle online equality for youth.

Writing during the current global pandemic of COVID-19 palpably highlights the pertinence of digital inclusion as outlined by the IMLS Framework of access, application, and adoption. An affordable and universal Internet is a basic necessity when social distancing measures and shelter-in-place orders shutter schools and businesses. Online learning that relies on platforms and programs that are privacy- and equality-protective offers potential for reducing the negative effects of interruptions in learning. However, any advantages it may offer will only benefit those children and families who possess basic domestic Internet access. For these reasons, as Michael Geist notes in Chapter 10 of this book, policy goals must go beyond consideration of cultural consumption to include the broader objectives of providing universal and affordable access. Moreover, ministries of education and school boards should ensure that all software programs used for education comply with young people's rights, under the UN Convention on the Rights of the Child, to education and privacy, as well as to participate in decisions that platforms make that affect them.

We conclude with several policy suggestions. The first is that platform companies must be held accountable and become more transparent about their data collection and privacy protection practices through producing coherent and well-designed terms of service. Only a few participants in our focus groups read the privacy policies on the social media sites they use. Patrick's response was typical: "No. It's too long … to force you not to read it." Shan said that she tried to

"start reading the privacy … like, conditions" but that, "I don't really … understand anything." Annie stated that she sometimes skimmed through the terms of service for "anything that really … pops out or that seems … bad … but not usually," while George related that platform companies "know that nobody reads the terms."

Our participants were both cynical and resigned about the power of social and other platform companies. Alex expressed distrust with platform companies because "they can sometimes sneak things in there that just flips everything on its head. Like Facebook and that big privacy leak." When participants were asked how they felt about behavioural marketing, Alex stated, "Violated … but it's the price you have to pay." Luke addressed the surveillance capitalism inherent in online media, stating that, "it's really difficult to find an actual, like, good-natured website that's trying to do stuff. They want to make money and so, they're going to pretty much … get into every little bit of your life that they can to generate the most profit. They're going to just … just … they, like, watch you."

Holding the digital industry accountable for children's online safety is the focus of the UK government. In their white paper *Online Harms* they call on tech companies whose business model relies on user-generated content to demonstrate how they fulfill a *duty of care* to "make companies take more responsibility for the safety of their users and tackle harm caused by content or activity on their services" (Secretary of State, 2019, p. 7). A duty of care is also addressed in consultations to update the 30-year-old UN Convention on the Rights of the Child through the UN Committee on the Rights of the Child's General Comment on children's rights in relation to the digital environment (2019). Acknowledging children as agentic users and rights holders in the digital sphere is thus part of the requirement that states "fulfil their fundamental duty of care to children in the digital environment" (Third et al., 2019, p. 401).

The second policy suggestion is to ensure funding for enriched digital literacy programming for schools, parents, and young people to strengthen digital skills, knowledge about the dynamic nature of datafication, and to unpack and discourage discriminatory comments and behaviours. Digital-privacy policy literacy provides knowledge about the political economy of platforms and their privacy rights with respect to meaningful consent under privacy legislation, whether PIPEDA or the GDPR. Citizenship education for school-aged youth is also an essential component of digital literacy. An innovative example

that fosters democratic engagement is the pan-Canada Student Vote, led by the registered charity CIVIX, where over 1.1 million students cast ballots in a mock 2019 Canadian federal election (CIVIX, 2019).

And finally, we need to bring the voices of youth into policy-making. With respect to the development of the CRC's General Comment on children's rights in relation to the digital environment, Canada was not among the 28 countries that submitted an initial concept note in 2019, with the exception of the submission by Global Kids Online, of which The eQuality Project is an academic partner. As the initial findings from our focus groups demonstrate, Canadian youth have rich perspectives to offer on how to create a rights-respecting networked environment.

Acknowledgements

The authors thank the Social Sciences and Humanities Research Council of Canada for their funding of The eQuality Project.

Notes

1. This research was conducted by The eQuality Project, a seven-year partnership of scholars, community organizations, educators, policy institutes, policy-makers, and youth, funded by the Social Sciences and Humanities Research Council of Canada, which explores young people's experiences with privacy and equality in networked environments, with a particular focus on youth from marginalized communities (see http://www.equalityproject.ca/our-project/). In this paper, all participants are referred to by pseudonyms and, where applicable, by their self-identification (ex: boy, demi-girl).
2. Christchurch Call to Eliminate Terrorist & Violent Extremist Content Online, May 2019. https://www.christchurchcall.com/.

References

Bailey, J. (2015). A perfect storm: How the online environment, social norms and law constrain girls' online lives. In J. Bailey & V. Steeves (Eds.), *eGirls, eCitizens* (pp. 21–53). University of Ottawa Press. https://press.uottawa.ca/egirls-ecitizens.html

Bailey, J. & Steeves, V. (Eds.). (2015). *eGirls, eCitizens*. University of Ottawa Press. https://press.uottawa.ca/egirls-ecitizens.html

Bailey, J., Steeves, V., Burkell, J., Shade, L. R., Ruparelia, R., & Regan, P. (2019). Getting at equality: Research methods informed by the lessons of

intersectionality. *International Journal of Qualitative Methods*, *18*, 1–14. https://journals.sagepub.com/doi/full/10.1177/1609406919846753

Blanchfield, M. (2019, May 29). Big data committee wraps up third and final day of hearings on Parliament Hill. *The Globe and Mail*. https://www.theglobeandmail.com/politics/article-mozilla-executive-tells-big-data-committee-he-was-shocked-when-he/

Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505.

CIVIX. (2019, October 23). *Mock federal election for students also ends in Liberal minority* [Press release]. https://studentvote.ca/canada/canadian-press-mock-federal-election-for-students-also-ends-in-liberal-minority/

Committee on the Rights of the Child [CRC]. *(2019). General comment on children's rights in relation to the digital environment*. UN Human Rights, Office of the High Commissioner, Committee on the Rights of the Child. https://www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx

House of Commons Standing Committee on Access to Information, Privacy and Ethics [ETHI]. (2019, June). *Report of the Standing Committee on Access to Information, Privacy and Ethics* (Report No. 20, 42nd Parliament, 1st Session). House of Commons of Canada. https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/report-20/

Innovation, Science and Economic Development Canada [ISED]. (2019). *Canada's digital charter in action: A plan by Canadians, for Canadians.* Government of Canada. https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00109.html

Marwick, A. & boyd, d. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, *16*(7), 1051–1067.

Montgomery, K. C. (2015). Youth and surveillance in the Facebook era: Policy interventions and social implications. *Telecommunications Policy*, *39*(9), 771–786.

Ontario Digital Service: Key priorities. (2017, May 29). Government of Ontario. Retrieved March 29, 2019, from https://www.ontario.ca/page/ontario-digital-service-key-priorities#section-9

Pelan, D., & Smythe, S. (2019, March 6). *Digital literacy and digital justice*. Brookfield Institute for Innovation + Entrepreneurship. https://brookfieldinstitute.ca/commentary/digital-literacy-and-digital-justice/?mc_cid=3c769f2243&mc_eid=9d606cc7bf

Personal Information Protection and Electronic Documents Act [PIPEDA], S.C., c. 5 (2000).

Public Policy Forum [PPF]. (2018). *Ontario digital inclusion summit: Summary report*. https://ppforum.ca/publications/ontario-digital-inclusion-summit-summary-report/

Rhinesmith, C. (2016). *Digital inclusion and meaningful broadband adoption initiatives*. The Benton Foundation. https://www.benton.org/inclusion-adoption-report

Secretary of State for Digital, Culture, Media & Sport and the Secretary of State for the Home Department. (2019). *Online harms* [White paper]. HM Government. https://dera.ioe.ac.uk/33220/1/Online_Harms_White_Paper.pdf

Shade, L. R., Porter, N., & Sanchez, W. (2005). "You can see anything on the Internet, you can do anything on the Internet!" Young Canadians talk about the Internet. *Canadian Journal of Communication*, *30*(4), 503–526. https://www.cjc-online.ca/index.php/journal/article/view/1635/1776

Smith, K. L., & Shade, L. R. (2018). Children's digital playgrounds as data assemblages: Problematics of privacy, personalization, and promotional culture. *Big Data and Society*, *5*(2), 1–12. https://journals.sagepub.com/doi/10.1177/2053951718805214

Steeves, V. (2005). *Young Canadians in a wired world, phase II: Trends and recommendations*. MediaSmarts. http://mediasmarts.ca/publicationreport/young-canadians-wired-world-%E2%80%93-phase-ii-trends-and-recommendations

Steeves, V. (2014). *Young Canadians in a wired world, phase III: Online privacy, online publicity*. MediaSmarts. http://mediasmarts.ca/ycww/online-privacy-online-publicity

Steeves, V. (2015). Privacy, sociality and the failure of regulation: Lessons learned from young Canadians' online experiences. In B. Roessler & D. Mokrosinska (Eds.), *Social dimensions of privacy: Interdisciplinary perspectives* (pp. 244–260). Cambridge University Press.

Steeves, V. (2016). Swimming in the fishbowl: Young people, identity and surveillance in networked spaces. In I. van der Ploeg & J. Pridmore (Eds.), *Digitizing identities* (pp. 125–139). Routledge.

Steeves, V. & Macenaite, M. (2019). Data protection and children's online privacy. In G. G. Fuster, R. Van Brakel, & P. De Hert (Eds.), *Research handbook on privacy and data protection law: Values, norms and global politics* [Book submitted for publication]. Edward Elgar Publishing.

Third, A., Livingstone, S., & Lansdow, G. (2019). Recognizing children's rights in relation to digital technologies: Challenges of voice and evidence, principle and practice. In B. Wagner, M. C. Kettemann, & K. Vieth (Eds.), *Research handbook on human rights and digital technology* (pp. 376–410). Elgar Online.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

Zuboff, S. (2019, May 28). Written testimony submitted to the International Grand Committee on Big Data, Privacy, and Democracy. https://www.ourcommons.ca/Content/Committee/421/ETHI/Brief/BR10573725/br-external/ZuboffShoshana-e.pdf

Page left blank intentionally