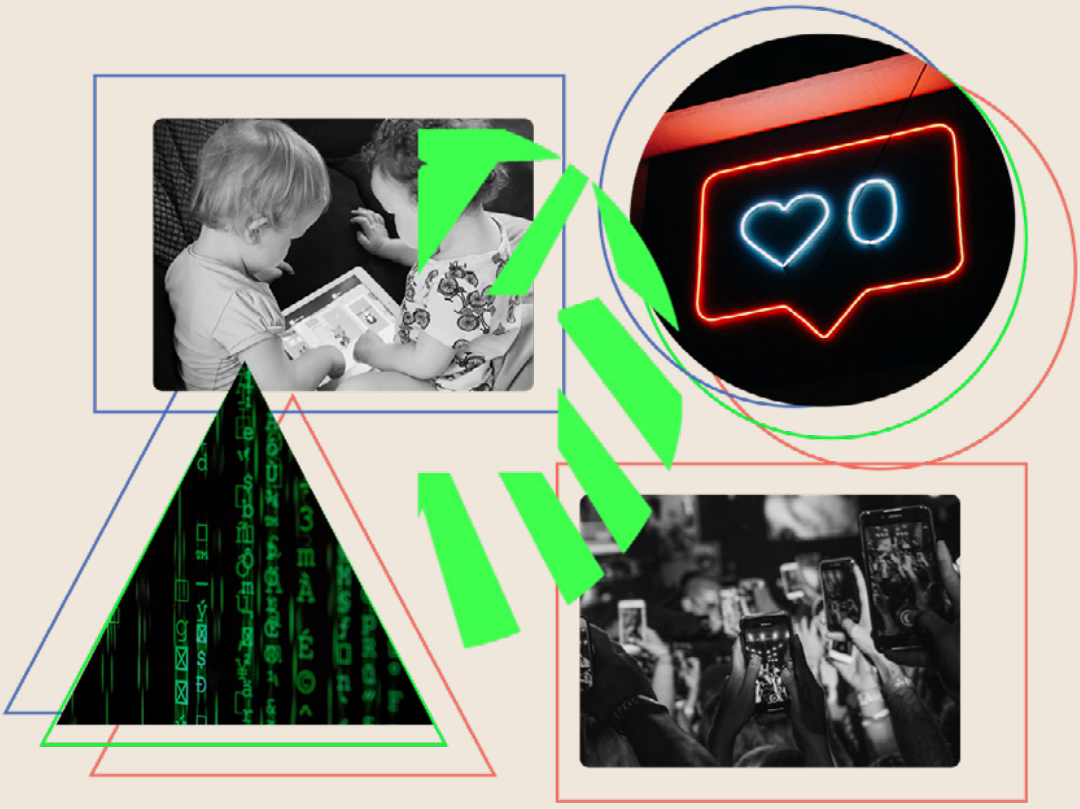
Kids & Technology Essay Series - November 2021

It's Time for a Change: Rethinking Policies to Protect Children's Rights in a Datafied World

Valerie Steeves



Centre for MEDIA, TECHNOLOGY and DEMOCRACY
McGill
MAX BELL SCHOOL of PUBLIC POLICY

About the Series

Children and youth stand to be especially impacted by the attention economy of data-driven technologies, educational tools that support surveillance and data collection, and toxic online environments. Engaging with a broad network of interdisciplinary scholars, this project aims to understand and address the impact of media technologies on children and youth against a broader data privacy governance agenda. The project convenes leading experts, policymakers, and impacted stakeholders to question the challenges posed by digital technologies to children and youth.

About the Author

Valerie Steeves

Full Professor, Department of Criminology at the University of Ottawa

Valerie Steeves is a Full Professor in the Department of Criminology at the University of Ottawa. Her main area of research is in human rights and technology issues. Professor Steeves has written and spoken extensively on online issues, and has worked with a number of federal departments, including Industry Canada, Health Canada, Heritage Canada, the Department of Justice and the Office of the Privacy Commissioner of Canada, on online policy. She is also a frequent intervener before parliamentary committees, and has worked with a number of policy groups, including the International Council on Human Rights Policy (Geneva, Switzerland), the House of Lords Constitution Committee on The Impact of Surveillance and Data Collection upon the Privacy of Citizens and their Relationship with the State (United Kingdom), and the Children's Online Privacy Working Group of the Canadian Privacy and Information Commissioners and Youth Advocates.

Her current research focuses on children's use of networked technologies, and the use of big data for predictive policing. She is the Principal investigator of The eQuality Project, funded by the Social Sciences and Humanities Research Council of Canada, which is examining young people's experiences of privacy and equality in networked spaces. She is also a co-investigator of the Big Data Surveillance project, funded by the Social Sciences and Humanities Research Council of Canada, where she is co-leading (with Stéphane Leman-Langlois) research Stream Three: Governance. This stream is examining the use of big data for policing and other forms of social control. In addition, Professor Steeves was the lead researcher on the Young Canadian in a Wired World project (YCWW) from 2004–2020.

It’s Time for a Change: Rethinking Policies to Protect Children’s Rights in a Datafied World

In 1998, I attended a brainstorming session with a provincial government department interested in using new information and communications technologies to streamline services for young people. The discussion was driven by a series of graphics that sought to represent new data governance structures to support service delivery, and the introductory slides were filled with variations of decision trees that mapped the potential flows of data across the system. My first question was to ask about the tiny graphic at the bottom right hand corner of the slide: an indistinct dot that was separate and apart from the riot of connectivity in the tree. The presenter responded by expanding the dot until we could see that it was actually a stick figure. He then said, “That’s for the people. We didn’t know what to do with them so we put them in the corner.”

At the time, I thought this exchange was indicative of a failure of policy rooted in a disconnect between data and the people that that data was about. Now, on my darker days, I look back on that graphic fondly. At least the programmers who designed the system still had an instinct that somehow, somewhere, people needed a place in the picture that was recognizably whole, and weren’t just a bundle of data points distributed across the bureaucracies of power.

If we were to draw that stick figure now, the young person it represented wouldn’t be left free floating in the corner. They’d be pinned, boxed and constrained by the vectors that rifle through their data on an ongoing basis, both for their own protection and for someone else’s profit.

Policymakers have allowed this to happen because the networked world has been conceived of as a binary place that brings great benefits and some risks to children. From this perspective, the task of policymakers is to free up commercial innovation (to increase the collective benefits) while dealing piecemeal with issues as they arise (to mitigate the individual risks) (Steeves, 2015a). The policy options we've accordingly relied upon to deal with risks almost always call upon parents, teachers and other concerned adults to embrace surveillance as the corrective (Steeves, 2016b). This is rooted in the belief that demanding children's passwords, monitoring their texts and logging their keystrokes will help keep kids "safe" from individual bad apples and leave corporations free to continue to make apps that kids enjoy (Bailey et. al., 2020).

Policymakers have allowed this to happen because the networked world has been conceived of as a binary place that brings great benefits and some risks to children.

The cyberbullying debate is an important window into the weaknesses of this binary approach. On the surface, when we pass legislation and create policies that open children up to increased surveillance to protect them from online harassment, we claim to be filling holes in an otherwise seaworthy technological ship. The ship needs to remain unfettered so it can continue to chart new waters. The law, which is generally seen as slow and being pulled along in its wake, needs to "catch up" to provide a remedy for some of the unanticipated shoals the ship encounters along the way, like cyberbullying and online predation[1].

I argue that we need to invert this picture, for three reasons. First, it fails to problematize the fact that online policies were created precisely to enable corporations to use surveillance to generate profits, and that it is this surveillance that predisposes young people for certain kinds of conflict. In other words, rather than being unable to catch up to technology, the law was amended well before the technology was built precisely to enable the kind of data flows that often cause problems for young people. Second, it implies that surveillance is the solution to online harassment, and not part of the problem itself; and who better to keep an eye on young people than the companies that own the technologies that already collect and analyse their data on an ongoing basis? This implication gives tech corporations a free pass because they can accordingly position themselves as allies in the battle against harassment. Third, and perhaps most important, it relies on an understanding of online life that's completely out of step with young people's needs and experiences.

Let's look at Instagram to see how this plays out. Instagram, which is owned by Facebook, has been a popular site among teens for the past few years[2]. Like other online corporations, the social media giant collects a vast amount of information from its young users, such as the photos they post on the site (including photos posted on accounts that are set to "private"), metadata about those photos (e.g., the time and location where a photo was taken), the content of the private messages they send and receive, and the people and content they interact with. Facebook's business model relies on click-through consent to legitimize this collection, which in turn enables the corporation to commodify the information and sell services to marketers, app developers, partners who use their analytic services, researchers, law enforcement and others (Instagram, 2018; see also Aspinall, 2019).

The legal frameworks which regulate this rely on a set of information rights, collectively called data protection, designed to give individuals some control over how corporations collect and use their personal information. The assumption is that privacy will be protected if individuals can make informed decisions about whether or not they want to disclose their information to a particular corporation (Bennett & Raab, 2006). From this perspective, if the teens on Instagram don't want their data collected, they can choose not to use the site's services. The corollary is that, once they do send a message or post a photo, the content is fair game.

This policy model didn't emerge in response to the development of the technology that drives Instagram. The regulations that enable it first appeared in the 1970s when European governments were beginning to grapple with the power of computer data processing – 20 years before the World Wide Web was created, 30 years before Mark Zuckerberg created the earliest version of Facebook, and 40 years before the Instagram app was launched.

Moreover, the model wasn't designed to protect individual rights: it was created to ensure that data would continue to flow to government bureaucracies and corporations so those organizations could then use the data for their own purposes. Although human rights concerns (especially concerns about potential discrimination) were taken into account in the first Pan-European iteration of data protection principles in 1973, one year later those concerns were overtaken by competing interests in administrative efficiency and profit (Steeves, 2016a). The push and pull between data protection and human rights has continued until today but, for the most part, data protection notions of individual control have continued to restrict the more rights-driven discourses of human dignity even in the European Court of Human Rights (Hughes, 2015).

When Canada first turned its mind to private sector data protection legislation in the 1990s, it was because Europe threatened to cut off international data flows unless we enacted similar rules. Privacy was accordingly positioned as a commercial issue and, once again, competing narratives around policies rooted in human rights were marginalized (Steeves, 2016a).

Children were an important part of this shift. The Canadian policymakers of the day argued that young people were natural technology users who needed free rein so they could drive the development of the information economy (Shade, 2011). Data protection was a necessary part of the puzzle because it would create the trust that would in turn encourage young people to use new technologies and, in doing so, open up their data for commercial purposes (Steeves, 2015a). Rights-based counter arguments that this would commercialize childhood in unprecedented ways were dismissed. For example, senior general counsel for the Department of Justice, Elizabeth Sanderson, argued before a Senate Committee that, although the government was "sympathetic" to a human rights approach that would situate young people as rights holders in their own right, enshrining human rights principles "would create a good deal of uncertainty and quite possibly may pose obstacles to many government programs and policy" (Canada, 2001), including e-commerce policy.

Moreover, the consent model of data protection has failed to create trust in the information marketplace.

This privileging of data protection as a strategy to grow the information economy has not served young people well. In the early days, many flocked to the Web as an adult-free zone where they could play with their identities, explore the adult world and otherwise meet the developmental needs of growing up. They were largely unaware of the commercial nature of the sites they frequented and tended to think of "big companies" as trustworthy friends (Environics, 2000, p. 41). But by 2004, these more emancipatory uses of networked tech were beginning to shut down, because so many of their interactions were being monitored. Young people experienced this as "spying" and saw it as evidence that adults didn't trust them to act appropriately and come to them for help when they encountered a problem (Steeves, 2012).

Moreover, the consent model of data protection has failed to create trust in the information marketplace. Many young people report that they no longer

see corporations as trustworthy, but as "creepy" organizations that keep their data even when they take steps to exercise some control by deleting it. They also report that the corporate privacy notices that are intended to create transparency and support informed consent are purposely convoluted and impossible to understand because corporations want to hide what they are doing (Steeves, 2012).

The policy response to cyberbullying has just complicated this mix. Both qualitative (Steeves, 2012; Steeves, McAleese & Brisson-Boivin, 2020) and quantitative research (Steeves, 2014) indicates that young people demonstrate a high level of resiliency when it comes to dealing with the kind of individual meanness that concerns adults. Moreover, the use of surveillance and punishment to keep them "safe" actually makes it harder for them to navigate the online environment, because the surveillant nature of the adult gaze often means that they are called to account for speech that is taken out of context. For example, two 13-year-old racialized girls in Toronto reported that they were threatened with suspension because they compared tans after a March break holiday. When one of the girls said she was darker, the conversation was picked up and she was accused of racist bullying (Steeves, 2012).

This adult hyper-vigilance also makes it more difficult for young people to get help when they do need it, because they fear that they will lose control over the meaning of the interaction and be forced into the socially unacceptable role of tattle-tale (Steeves, 2012). It also interferes with the strategies that do tend to work for them, such as ignoring insulting comments, mobilizing online peer interventions that repair any reputational harm they experience or confronting the aggressor face-to-face (Steeves, 2014). And, if worse comes to worst and they aren't able to deal with it themselves, they can capture it and create a record that they can take to adult authorities, making online bullying easier to deal with than offline harassment (Steeves, 2012).

What young people do want help with is the structural harassment that too often constrains their online experiences (Bailey & Steeves, 2015; Brisson-Boivin, 2019). From their perspective, this harassment is rooted in the environment itself because the corporations that own the platforms they use, like Instagram, flood their online social spaces with marketing material that replicates stereotypes (Bailey & Steeves, 2015). This creates significant pressure to post content that conforms to commercialized constructions of the perfect body, lifestyle and friend network. This pressure is widespread, especially among

teens, who often report that they feel exhausted by trying to make the grade (Michaelson & Steeves, 2020). Moreover, algorithms search for content that will attract the most attention because this maximizes advertising revenue: this privileges harassing and offensive content because anger is a prime driver of views (Berger & Milkman, 2012).

Research respondents in 2015 described it this way. A girl who is "authentic" and "never really scared to say what she wants or act in any way that she wants" offline will be "just bashed" online because she doesn't conform to the online image of female "looks" that is epitomized in online ads and celebrity posts. That bashing is likely to go viral because everyone follows the "drama" that ensues (p. 162). Recent focus groups have reported that this behaviour is consistent with broader online trends, where women and other marginalized groups are frequently demeaned, dismissed and threatened by adult users who tend to attract large audiences (Steeves, et al., 2020).

It's important to remember that young people are resilient and do not just passively accept media content; they continue to use networked tech for their own purposes in creative and important ways.

It's important to remember that young people are resilient and do not just passively accept media content; they continue to use networked tech for their own purposes in creative and important ways. But at the same time, it's no wonder that they find online life exhausting. It's time policymakers looked beyond simplistic understandings of bullying as an individual harm and began to unpack how the commercial design of platforms – and the data collection that drives that design – creates ideal conditions for viral harassment, because that harassment has real consequences. In the latest UK survey, over two-thirds (69%) of 13- to 17-year-olds report that social media has a mostly negative (24%) or neutral (45%) effect on teens. Negative ratings are linked to bullying/spreading of rumours (27%), negative effects on personal relationships (17%), "unrealistic views of others' lives" (15%), distraction and addiction (14%), peer pressure (12%), negative mental health outcomes (4%) and "drama" (3%) (Anderson & Jiang, 2018).

Instagram has come under particularly strong pressure to fix its platform, because it too often "contain[s] a flood of toxic behavior, extreme content and misinformation" (Roose, 2019). Moreover, the visual nature of photo sharing

tends to magnify the impact of stereotypical and hateful images (Steeves & Bailey, 2013), making Instagram a difficult space for the majority (70%) of young people who report concerns about the casual prejudice they find there (Brisson-Boivin, 2019).

Facebook's response to these problems has been typical of the tech industry. Rather than creating private spaces that would give young people more control over their online reputations, it has focused on technological fixes that are consistent with its business plan. And that business plan is predicated on the continuing collection and commodification of young people's data. It has also turned the focus back on their young users by arguing both that they misbehave online (and therefore cause the problem) and that they are unlikely to report bullying to the platform when they are victimized by it (and therefore exacerbate the problem). Facebook's solution is to develop an algorithm that can identify cyberbullying electronically so it can be automatically removed from Instagram's platform without any user intervention[3] (Roose, 2019).

At the very least, this algorithmic solution ignores evidence from its young users that the corporation routinely refuses to remove the content that young people flag as problematic (Bailey & Steeves, 2017). A streamlined complaints procedure that gives young people more control over their content would likely be a simpler and stronger corrective. But, more importantly, relying on an algorithm deflects attention away from the commercial model that sets young people up for conflict. Indeed, it entrenches that commercial model further because it legitimizes the ongoing collection and analysis of their data as a form of protective surveillance.

This mix of surveillance and profit is particularly difficult for young people, who have little choice but to reveal the intimate details about their lives to tech companies because the infrastructure they use to learn, play and work requires it. But from their perspective, the mere fact that they post content online or instant message a friend does not mean that they have consented to it being collected and used, because that information is still private in a social sense. They do not protect that privacy solely by deciding not to disclose information; they protect it by controlling (or seeking to control) who looks at it once it is posted (Steeves, 2016b).

The rules they have developed to do this are rich and nuanced, and grounded in their social relationships. For example, contrary to the popular notion that young people are comfortable posting anything, they are incredibly careful about crafting

and curating a particular online image. From their perspective, participating on social media platforms like Instagram is less about being social, and more about being seen to be social. They do this, in part, by only selecting photos that are unlikely to attract any negative attention. Photos that actually reveal personal details of their lives are kept offline because they are "random" and not what the online audience is looking for (Johnson, et al., 2017).

At the same time, they are highly aware of how the commercial nature of the platforms they use shapes the images that surround them and opens them up for negative feedback. Even when they are critical of the "amazing", "perfect", "awesome" people who have "professional people doing their hair" that appear in online ads, entertainment and celebrity blogs (Steeves, 2015a, pp. 163-164), they feel badly about not being able to look like them. As one research participant in 2015 concluded: "I think social media is great at giving [young people] this fantasy world but at the same time I think it's also really easy to sort of make them feel really bad about themselves" (p. 167) because the online marketplace places such unrealistic demands on them.

As Shoshana Zuboff notes, this bad feeling is not an accident, it is a business strategy:

> … 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, modeling, subliminal priming—is summoned to tune, herd, and manipulate behavior in the name of surveillance revenues" (Zuboff, 2019, p. 456).

It is also a business strategy that is out of keeping with young people's express wishes. It is particularly noteworthy that 83 per cent of over 5,000 Canadian young people between the ages of 11 and 17 surveyed in 2013 reported that the corporations that own the platforms they post their data on should not have any access to that data. The percentage rose to 95 when it came to online marketers (Steeves, 2014, p. 36).

The problems inherent in the existing e-commerce framework (Montgomery, 2015) are beginning to attract the attention of policymakers. For example, after Canada hosted the second meeting of the International Grand Committee on Big Data in November 2019, the Chair of the House of Commons Committee on Ethics, Access to Information and Privacy, Bob Zimmer, called for action to protect young people from the "surveillance capitalism" they find online. Zimmer noted, "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, para. 6).

Those jurisdictions with strong human rights frameworks have made the most progress in this regard (Steeves & Macenaite, 2019). For example, the European Union's General Data Protection Regulation has called for "special protection" for children, limiting the use of profiling for marketing purposes (Recital 38) and the use of automated decision-making where there are legal consequences for a child (Recital 71). However, the majority of the General Data Protection Regulation's special provisions for children tinker with the existing approach, and continue to put the principle burden on children and their parents to limit their disclosures (Steeves & Macenaite, 2019).

I suggest that policymakers would be better served by adopting a rights-based approach that explicitly draws on human rights discourses[4]. The United Nations Convention on the Rights of the Child is a particularly important touchstone when it comes to responding to online harassment and abuse because it balances the need to protect children with the equally important need to enable them to participate fully in decisions about their own lives. It explicitly requires signatory states to respect children as rights-holders in their own right, and to work to ensure that they can enjoy their rights to privacy, free speech, access to information and their own culture in a social environment that is also free from harassment and discrimination (Steeves, 2017).

Perhaps most importantly, a rights-based approach rejects the notion that young people are data points to be commodified and calls upon policymakers to ensure that the frameworks that govern their online lives are in the best interests of the child.

As much as I think about that stick figure from 1998, I also think of a day in 2009 when I was doing research on Club Penguin. Club Penguin was an online playground that had been created by three Canadian fathers to give their kids a non-commercial social media site where they could play and socialize. In 2007, they sold the platform and its parent company to Disney for $350 million. At the time, the site had 11 million accounts, including 700,000 subscribers who paid $5.95/month to access special content (Jordan, 2008).

From a rights perspective, the commercialization of that playground should give us pause. Are we really protecting children when we make it impossible for them to communicate with each other?

Not surprisingly, Disney quickly commercialized the site, embedding marketing material for its products throughout the games, adding virtual bling for paid subscribers, and collecting user data to improve its services. Perhaps more surprisingly, it also enlisted its young users to help it fight cyberbullying. Each paid subscriber was asked to join the Penguin Secret Agency and get their own spyphone, F.I.S.H. (Factual Informative Spy Book) and virtual key to Headquarters. Children were told that their duty as a secret agent was to report any other players who broke the rules by using bad language, sharing personal information, or being rude or mean. Reporting was facilitated by simply clicking on the other user's player card. Children who did so were given special rewards (Marx & Steeves, 2010, p. 208).

Needless to say, this created a lot of conflict on the site. Non-subscribers began to resent subscribers whose penguin avatars often shuffled through the virtual playground laden down by multiple hats, pets and other purchased paraphernalia. The day I was online just happened to be the day of an organized protest. Non-subscribers were unable to talk about their concerns or challenge the commercialization of the space, because their ability to communicate had been limited to select phrases (such as "I love Club Penguin!"), for their own "safety". They were, however, allowed to throw virtual snowballs at each other. So on that day, one penguin posted the message, "Throw snowballs at subscribers!!" and the result was a flurry of virtual snow.

From a rights perspective, the commercialization of that playground should give us pause. Are we really protecting children when we make it impossible for them to communicate with each other? Should we be pathologizing their natural

inclination to share personal information with friends at the same time that we allow large corporations to solicit and commodify that very information and use it to steer their behaviour? How do we design an online environment that provides children with the opportunities they need to really connect and engage?

As Gillespie notes, it will be impossible to answer these kinds of questions without "a deep understanding of the economic relationships and social assumptions" (Gillespie, 2014, p. 177) embedded in the algorithms that drive the new economy. To do this, we need policy tools that call upon regulators to directly interrogate these assumptions and test them against children's dignity.

Endnotes

1 This argument is so strong that sexualized cyberbullying was used to justify lawful access legislation that significantly increased police powers of surveillance, in spite of the fact that the harm it sought to correct (the non-consensual exchange of sexual images of minors) was already criminalized under Criminal Code provisions barring the distribution of child pornography. I am not arguing against the resultant Criminal Code section prohibiting the non-consensual distribution of intimate images. What I am suggesting is that, by refusing to sever that provision from lawful access legislation that had been defeated in the House of Commons on three previous occasions, the government effectively held protection for girls and women hostage to a new police surveillance regime that had been soundly rejected by Canadians because of its negative implications for citizen privacy.

2 According to a survey of American teens by the Pew Research Center, approximately 70 percent of 13 to 17-year-olds used the social media site in 2018 (Anderson & Jiang, 2018).

3 Because of the difficulty in determining what content is and is not bullying, the algorithm will work in tandem with a team of human employees who will be more sensitive to "context" (Roose, 2019).

4 For an example of what that might look like in practice, see UNICEF, 2014.

References

Anderson, Monica and Jingjing Jiang. (2018). *Teens, social media & technology 2018*. Washington, DC: Pew Research Centre.

Aspinall, Georgia. (2019, August 22). No, Instagram is not changing its privacy policy but you should know what you've already agreed to. *Grazia*. Retrieved from: https://graziadaily.co.uk/life/in-the-news/instagram-privacy-policy/.

Bailey, Jane, Jacquelyn Burkell, Suzie Dunn, Chandell Gosse and Valerie Steeves. (2020). AI and technology-facilitated violence and abuse. In Florian Martin-Bariteau and Teresa Scassa (Eds.), *Artificial intelligence and the law in Canada*. Toronto: LexisNexis.

Bailey, Jane and Valerie Steeves. (2017). Defamation law in the age of the internet: Young people's perspectives. Toronto: Law Commission of Ontario

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

Bailey, Jane and Valerie Steeves. (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*. Farnham, UK: Ashgate Publishing, 41-66.

Bennett, Colin and Charles Raab. (2006). *The governance of privacy: Policy instruments in global perspective*. Cambridge, Massachusetts: MIT Press.

Berger, Jonah and Katherine L. Milkman. (2012). What makes online content viral? *Journal of Marketing Research, 49*(2), 192-205.

Blanchfield, Mike. (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/.

Brisson-Boivin, Kara.(2019). *Pushing back against online hate*. Ottawa: MediaSmarts.

Canada. (2001). *Proceedings of the Standing Senate Committee on Social Affairs, Science and Technology, Issue 25: Evidence, 25*.

DitchtheLabel.org. (2019). *The annual bullying survey 2019*. Retrieved from: https://www.ditchthelabel.org/wp-content/uploads/2020/05/The-Annual-Bullying-Survey-2019-1-2.pdf.

Environics. (2000). *Young Canadians in a Wired World: Parents and youth focus groups in Toronto and Montreal*. Ottawa: Media Awareness Network.

European Union. (2016, April 27). *General Data Protection Regulation: Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*. OJ 2016 L 119/1.

Gillespie, Tarleton. (2014). The relevance of algorithms. *Media technologies: Essays on communication, materiality, and society*. Cambridge, Massachusetts: MIT Press.

Instagram. (2018, April 29). *Data policy*. Retrieved from: https://help.instagram.com/519522125107875.

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.

Jordan, David. (2008, April 1). Lane Merrifiled: Club Penguin. *BC Business Online*. Retrieved from: https://web.archive.org/web/20131203033854/http://www.bcbusiness.ca/people/lane-merrifield-club-penguin.

Marx, Gary and Valerie Steeves. (2010). From the beginning: Children as subjects and agents of surveillance. *Surveillance & Society, 7*(3/4), 192-230.

Michaelson, Valerie and Valerie Steeves. (2020). "I'll use it differently now": Using dual systems theory to explore youth engagement with networked technologies. *Canadian Journal of Public Health*.

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

Roose, Kevin. (2019, May 9). Instagram is trying to curb bullying. First it needs to define bullying. *New York Times*. Retrieved from: https://www.nytimes.com/2019/05/09/technology/instagram-bullying-teenagers.html.

Shade, Leslie Regan. (2011). Surveilling the girl via the third and networked screen. In Mary Celeste Kearney (Ed.), *Mediated girlhoods: New explorations of girls' media culture*. New York: Peter Lang, 261-276.

Steeves, Valerie. (2016a.) Now you see me: Privacy, technology and autonomy in the digital age. In Gordon DiGiacomo (Ed.), *Human rights: Current issues and controversies.* Toronto: University of Toronto Press.

Steeves, Valerie. (2015a). Pretty and a little bit sexy, I guess: Publicity, privacy, and the pressure to perform "appropriate" femininity on social media. In Jane Bailey and Valerie Steeves (Eds.), *eGirls, eCitizens*. Ottawa: University of Ottawa 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*. Cambridge: Cambridge University Press, 244-260.

Steeves, Valerie. (2017). Snoops, bullies and hucksters: What rights do young people have in a networked environment? In Nancy A. Jennings and Sharon R. Mazzarella (Eds.), *20 questions about youth and media*, 2nd ed. New York: Peter Lang.

Steeves, Valerie. (2016b). Swimming in the fishbowl: Young people, identity, and surveillance in networked spaces. In Irma can der Ploeg and Jason Pridmore (Eds.), *Digitizing identities: Doing identity in a networked world*. Routledge Studies in Science, Technology and Society. New York: Routledge, 125-139.

Steeves, Valerie. (2014). *Young Canadians in a Wired World, Phase III: Cyberbullying: Dealing with online meanness, cruelty and threats*. Ottawa: MediaSmarts.

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

Steeves, Valerie. (2012). *Young Canadians in a Wired World, Phase III: Talking to youth and parents about life online*. Ottawa: MediaSmarts.

Steeves, Valerie and Jane Bailey. (2016.) Living in the mirror: Understanding young women's experiences with online social networking. In Emily van der Meulen and Robert Heynen (Eds.), *Expanding the gaze: Gender and the politics of surveillance*. Toronto: University of Toronto Press.

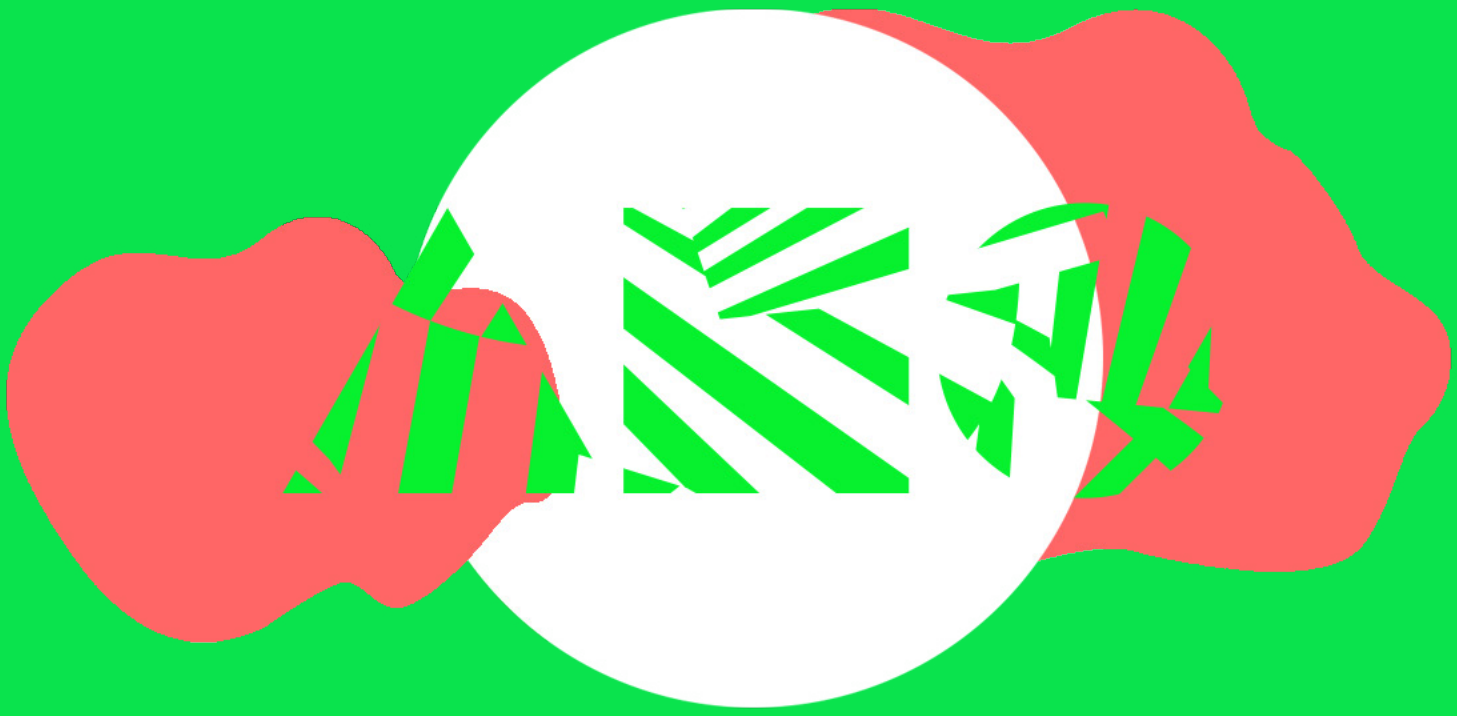
Steeves, Valerie, Jane Bailey, Jacquelyn Burkell, Priscilla Regan & Leslie Shade. (2020). *This is what diversity looks like: What young people need to enjoy privacy and equality in networked spaces*. Unpublished raw data.

Steeves, Valerie and Milda Macenaite. (2019). Data protection and children's online privacy. In Gloria González Fuster, Rosamunde Van Brakel and Paul De Hert (Eds.), *Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics*. Cheltenham: Edward Elgar Publishing.

Steeves, Valerie, Samantha McAleese, and Kara Brisson-Boivin. (2020). *Young Canadians in a Wireless World, Phase IV: Talking to youth and parents about online resiliency*. Ottawa: MediaSmarts.

UNICEF. (2014). *Children are everyone's business: Workbook 2.0*. Geneva: UNICEF.

Zuboff, Shoshana. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York: BBS Public Affairs.



Designed by Yasmeen Safaie

Centre for MEDIA, TECHNOLOGY and DEMOCRACY
McGill
MAX BELL SCHOOL of PUBLIC POLICY