Kids & Technology Essay Series - November 2021

Facial Recognition & Canadian Youth

Luke Stark

PUBLIC POLICY FORUM
FORUM DES POLITIQUES PUBLIQUES
PPF

Centre for MEDIA, TECHNOLOGY and DEMOCRACY

McGill

MAX BELL SCHOOL of PUBLIC POLICY

Table of Contents

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

Luke Stark

Assistant Professor, Faculty of Information & Media Studies (FIMS),
Western University

Luke Stark is an Assistant Professor in the Faculty of Information and Media Studies at Western University in London, ON. His work interrogating the historical, social, and ethical impacts of computing and AI technologies has appeared in journals including The Information Society, Social Studies of Science, and New Media & Society, and in popular venues like Slate, The Globe and Mail, and The Boston Globe. Luke was previously a Postdoctoral Researcher in AI ethics at Microsoft Research, and a Postdoctoral Fellow in Sociology at Dartmouth College; he holds a PhD from the Department of Media, Culture, and Communication at New York University, and a BA and MA from the University of Toronto.

Introduction

The town of Lockport, New York is just east of Niagara Falls, under forty kilometres from the Ontario border. For the past several years, the town has been at the epicenter of a local controversy with implications not just for its own citizens and for the United States more broadly, but for Canada too. In early 2018, the Lockport City School District, like other school districts across the United States, responded to the murder of 17 students at Parkland, Florida's Marjory Stoneman Douglas High School with a flurry of new physical security measures in its schools. Among these infrastructural changes was the installation of "dozens" of security cameras, equipped with video analytics software purportedly able to perform object and facial recognition. The software, which the district's Director of Technology called "cutting edge" and "a model (for school security)," was sold to the Lockport school district by a surveillance technology company called SN Technologies Corporation — a firm that happened to be headquartered just across the lake in Gananoque, Ontario[1].

Facial recognition technologies (FRTs) are of increasing interest to Canadian institutions such as universities, police departments, and immigration/national security agencies. FRTs are also an appealing avenue for advertising and commercial data collection on the part of big box retailers, social media platforms, and specialized digital application developers in jurisdictions around the world, including those in Canada. And Canadian firms like SN Technologies stand to gain from the development and sale of these systems around the world. Canadian youth—whose lives are often especially influenced by institutions like schools interested in social control and who are a coveted demographic for digital advertising and commerce — sit at the intersection of these two avenues by which FRTs are set to be deployed in Canada[2].

The link between Lockport, NY and Gananoque, ON is also a reminder that policy discussions and public activism around FRTs in the United States and around the world are already influencing our societal conversations about these technologies in Canada — and that we have the chance to listen to the concerns of young people here in Canada, in the United States, and elsewhere to avoid making critical mistakes. Here, I unpack what the public and private deployment of FRTs aimed at or particularly affecting Canada's youth suggests about the deployment of these technologies by governments and businesses more broadly. Today's young people are already voters, consumers, and social advocates. Their responses to these technologies and the ideologies behind them should lead Canadians to engage in a critical and necessary discussion about whether FRTs are worth the cost—not only in the monetary sense, but also in their far-reaching negative social effects.

What are Facial Recognition Technologies (FRTs)?

Facial recognition is a catchall term for a number of closely related computer systems which seek to variously identity, recognize, and analyze human faces in data from digital images or videos. According to the Canadian Civil Liberties Association (CCLA), "Facial recognition uses the physical characteristics of our face to create a mathematical model that is unique to us, just like a fingerprint[3]." Facial recognition technologies (FRTs) are a form of computer vision (CV) — mechanisms through which computer scientists train digital systems to perceive "three-dimensional shape and appearance of objects in imagery[4]." FRTs are a particularly widely-used form of biometrics, or technologies that measure physical and behavioral data from our human bodies to identify us[5].

Facial recognition technologies first identify a pattern of light and dark pixels in a two-dimensional image corresponding to the average configuration of shadows and highlights of a human face. The system then extrapolates depth to estimate facial geometry, "and makes many measurements, such as the distance between eyes, length and width of face, etc.[6]" The system then converts these measurements into a digital "faceprint." Not all FRTs perform the same functions. For example, facial detection systems simply seek to identify that a face is present in an image at all, without being able to say much about what sort of a face it is. Facial identification systems try to match the image of a specific face with the images contained in a pre-labeled database, in order to ascertain someone's identity. And facial analysis systems purport to be able to guess certain characteristics of a person, such as their age, gender, or race from a faceprint with a high degree of accuracy.

Despite the claims of their proponents, the practical utility of FRTs is dubious at best: in many cases, they just don't work as advertised. Researchers have found that FRT systems fail to recognize and correctly identify Black faces[7], as well as the faces of other visible minorities[8]; misidentified members of the United States Congress as criminals[9]; and failed up to eighty percent of the time when piloted in public by the police[10]. These technical failings suggest that the deployment of FRTs in public spaces and by public institutions risks exposing Canadians to an inaccurate technology in high-stakes situations.

Yet at a more fundamental level, the technical failings of FRT systems as currently designed simply reinforce unsolvable conceptual problems with these technologies. As a number of scholars have observed, FRTs produce and sustain the categories they claim to simply describe, making assumptions about a person's gender expression, ethnicity, or age and giving these categorizations social weight as if they were immutable facts [11]. Because these systems are designed to classify and compare human faces, facial recognition technologies are intrinsically racializing — meaning they produce and reinforce racial categories[12] — and are thus inherently racist[13]. These conceptual problems are especially acute for facial analysis systems, including those that seek to analyze traits like human emotional expression[14]. FRTs also have particular problems analyzing gender: most of these systems incorrectly treat gender as a binary trait, and so frequently misgender trans and non-binary people[15]. Claims that facial analysis can identify sexual orientation or criminality from photographs are not only inaccurate[16] — they perpetuate the incorrect conceptual idea that interior character traits can be "read" from exterior signals and signs. Such systems are part of the broader phenomenon of "physiognomic AI" — artificial intelligence systems whose designers claim, wrongly, that can make such judgements[17].

On top of these technical and conceptual problems, physiognomic AI systems like facial recognition technologies pose grave threats to Canadians' personal privacy, civil liberties, and capacity for democratic participation. In 2013, a report from the Office of the Privacy Commissioner of Canada observed that, "Facial recognition brings a new dimension to surveillance in that it makes it much easier to identify individuals in a very short period of time[18]." Scholars have termed facial recognition "the perfect tool for oppression," because of how easily governments and large institutions can use facial data to track the movements of ordinary people, and the ways in which facial surveillance can be used to target protestors and chill dissent[19]. Facial recognition systems therefore combine the worst of all worlds: they're fundamentally unable to grapple with the diversity of Canadians at a technical and conceptual level, they don't work well, and yet are still able to be used for enormous harm.

FRTs and Canadian Youth

Canadian youth, like other young people around the world, are increasingly impacted by a variety of AI systems including FRTs. A recent report from UNICEF warns that the "human and child rights risks and limitations [associated with FRTs] are great[20]," and include that recognition of children and youth faces is even more inaccurate than faces from the adult population[21]. Even the most optimistic use cases involving FRTs and youth, such as using them to identify missing children[22], are fraught with the many technical and social problems I have already described[23]. Canadian youth are both particularly exposed to the harms of facial recognition technologies and particularly concerned about them. After conducting focus groups of Canadian youth focusing on digital inclusion, Shade et al observed that, "the persistent commercialization and datafication (systematic collection and analysis of massive amounts of data sets) of [the participants'] communicative practices raise ethical tensions and privacy concerns about whether they can maintain control of their digital identity over their life cycle." Canadian youth are not only concerned about digital privacy and safety, but also about how to be creative and expressive online and off without undue corporate and government surveillance[24]. Without proper safeguards regulating, limiting, and banning facial recognition technologies, FRTs have the potential to deepen the challenges for Canadian youth around engaging in social

FRTs produce and sustain the categories they claim to simply describe, making assumptions about a person's gender expression, ethnicity, or age and giving these categorizations social weight as if they were immutable facts.

and political activities with fear of chilling effects, and making sure their personal data is kept private.

Facial recognition technologies are popping up in a variety of Canadian contexts relevant to young people. Here, I spotlight three areas where Canadian youth have likely already been exposed to FRTs and their effects: education, policing, and commercially available social media applications. These case areas highlight the range of situations in which youth in are likely to encounter FRTs, and the particular challenges those technologies bring for young people. Given the broader problems with FRTs, these case studies also point to the need for a wide-ranging policy response to facial recognition at the federal, provincial, and municipal levels, to deal with the adverse impacts of FRTs on Canadian youth and on Canadians of all ages.

FRTs in Canadian Education

The use of FRTs in schools is one element of a broader set of issues around student privacy in Canada. In 2019, the Supreme Court of Canada ruled that secondary school students have a reasonable expectation of privacy over their own bodies while at school[25], but questions remain over whether, when, and where biometric surveillance technologies like facial recognition are "reasonable." Andrejevic and Selwyn describe four possible uses for FRTs in educational contexts: security, attendance monitoring, proctoring/controlling access to learning materials, and assessing student engagement and learning outcomes[26]. These use cases can apply in elementary, secondary, and post-secondary institutions, though the latter two use cases have—thus far—been more frequently deployed at the secondary and post-secondary levels.

Closed circuit television (CCTV) cameras are increasingly common in Canadian elementary and secondary schools, with recordings subject to provincial privacy and data protection regulations[27]. The ubiquity of CCTV cameras for security monitoring in American schools has provided an already-existing material and rhetorical infrastructure over which more complex digital analytic systems such as facial recognition can be built: if cameras are already in place within a school, upgrading them is less noticeable than adding them in the first place.

Canadian elementary and secondary school boards have been less quick than their US counterparts to turn to FRTs as a school security measure. Lax gun control laws and the high frequency of school shootings in the United States have led many American school districts to embrace an ethos of school securitization to the point of “surveillance theatre.[28]” According to one industry report the US market for school security technologies was worth $2.7 billion in 2017[29]. For instance, the Lockport City School District began to investigate additional physical security measures in earnest after the 2012 Sandy Hook school shooting and was referred to the surveillance technology firm SN Technologies Corporation by an outside security consultant with ties to the company[30]. The school district spent $1.4 million on SN Technologies’ Aegis software suite, which includes facial and object detection and recognition, as well as a “forensic search engine” which is able to “quickly review video unattended and search for specific people.[31]” Before entering the education market, SN’s products were deployed in locales such as prisons and casinos[32].

We need to ask what models of education, human learning, and the ideal student are generated and perpetuated by using FRTs and other similar biometric technologies in the classroom, both when the classroom itself is entirely virtual and when these technologies are used as part of a hybrid learning system.

The lack of widespread deployment of FRTs for security purposes in Canadian elementary and secondary schools thus far is a positive sign. However, FRTs remain part of a broader debate around the deployment of digital learning tools in Canada — a topic gaining salience given the expansion of online learning in many jurisdictions as necessitated by the COVID-19 pandemic. FRTs are often components of classroom learning management systems used to mediate — and monitor — student activities[33]. For instance, platforms like Proctorio[34], Proctortrack[35], and D2L’s Brightspace use facial identification as a proctoring tool for online tests and exams[36]. Brightspace is the Virtual Learning Environment (VLE) for all Ontario K-12 public schools[37] and is used by postsecondary institutions like Ottawa’s Carleton University[38]. The use of Proctortrack at Ontario universities has led to recent student protests[39], and Proctorio recently sued a University of British Columbia employee in what he claims is an attempt to chill his criticism of the company’s products[40].

Brightspace and other learning management systems also incorporate a variety of behavioral analytics techniques into their products, including information on whether students have read materials or watched videos, and how frequently students have engaged via the platform[41]. These analytic techniques have the potential to be combined with FRT data to create granular surveillance and assessments of students, particularly when many are learning via online platforms. With an increasing emphasis on social and emotional learning on the part of many educators, these types of data analysis threaten to become more common both inside and outside the traditional classroom even after the COVID-19 pandemic has subsided[42].

A recent report from the University of Michigan lays out many of the particular dangers around using FRTs for any purpose in educational institutions, whether at the elementary, secondary, or post-secondary level. The report identifies five general consequences of using FRTs that stand to be particularly acute in school settings. First, FRTs exacerbate racism in schools, amplifying surveillance that disproportionally falls on visible minority students. Second, FRTs normalize surveillance more broadly, chilling certain types of behavior and leading to a loss of privacy. Third, FRTs help school administrators define the "acceptable student," in terms of behavior, social norms, and ideal academic trajectory. FRTs also produce data about students that can be commodified by educational institutions and learning management platforms. And lastly, since FRTs are error prone and do not work as advertised, their deployment in schools will "institutionalize inaccuracy," baking error into any school that relies on these systems[43]. The report's authors conclude that "the use of facial recognition be banned in schools"— a recommendation that Canadian jurisdictions should follow for primary, secondary, and post-secondary education. We need to ask what models of education, human learning, and the ideal student are generated and perpetuated by using FRTs and other similar biometric technologies in the classroom, both when the classroom itself is entirely virtual and when these technologies are used as part of a hybrid learning system.

Facial recognition technologies are especially dangerous and deleterious in educational contexts. Many United States jurisdictions, including New York State lawmakers, have arrived at this conclusion. The Lockport City School District piloted facial recognition in its schools in 2019, leading to widespread concern from parents, teachers, and civil liberties groups[44]. In May 2020, after a concerted effort by Lockport City School District parents and non-profit groups such as the New York Civil Liberties Union, the New York State Department of Education announced they would no longer approve the funding of biometric projects involving facial recognition; in July the state legislature passed a two-year moratorium on the use of facial recognition in schools[45]. Canadian youth, and their parents can build on the work of their American counterparts to ensure that FRTs never see the inside of schools across the border in the first place.

FRTs in Canadian Policing

While FRTs are not yet widespread in Canadian schools, they are becoming increasingly pertinent to another Canadian institutional context: policing. As in education, the use of FRTs in law enforcement and national security activities disproportionally impacts particularly disenfranchised groups of Canadian youth, including Black and First Nations people and others who are visible minorities. Individuals who are part of these racialized groups are already subject to heightened state surveillance and racist disadvantage in Canadian society more broadly[46].

In the spring of 2020, the use of FRTs by Canadian police became a public scandal after the revelation that police forces including the Toronto Police Services, the Ontario Provincial Police, and the RCMP had all used the facial recognition database of Clearview AI[47], a company whose facial recognition technology is built on a database of three billion images of people collected, possibly illegally, from social media platforms like Facebook[48]. According to the New York Times, Clearview had been used by over six hundred police forces globally as of early 2020[49]. Clearview, which reportedly has ties to far-right and white supremacist activists[50], allows users to link an image to a person's name, address, phone number, and other personally identifiable information[51]. After the use of Clearview by Canadian police forces was reported in the press, the Office of the Privacy Commissioner of Canada, along with its provincial counterparts in British Columbia, Alberta, and Quebec, launched a joint investigation into the company's Canadian operations and whether they complied with Canadian data privacy legislation[52]. In July 2020, Clearview announced it would pull out of the Canadian market — though Canadians had little recourse if they wanted their images removed from the company's database[53].

Despite Clearview's retreat, FRTs remain popular with Canadian police and national security agencies. Toronto Police began using facial identification technology in 2018[54], and York Regional Police spent $1.68 million on facial recognition and identification technologies in 2019[55]. The Calgary police force have used FRTs for several years[56], and other forces across the country are purportedly considering deploying such systems[57]. The Vancouver airport has begun to replace prior biometric identification systems like iris scanning with facial recognition for certain classes of travelers[58], and national security agencies like CSIS have reportedly been coordinating with law enforcement agencies around biometric data collection for several years[59]. And the Canada Border Services Agency (CBSA) recently disclosed they had tested facial recognition on over three million passengers at Toronto's Lester B. Pearson International Airport in 2016[60].

In response to the increasing use of FRTs in policing, a coalition of human rights and civil society groups published an open letter to Public Safety Minister Bill Blair in July 2020, urging the federal government to ban the use of facial recognition technologies by Canadian law enforcement and intelligence agencies[61]. The letter called for a wide-ranging and meaningful set of public consultations on all aspects of facial recognition technologies in Canada and changes to relevant Canadian privacy laws.

> The CCLA describes facial recognition as "an extreme form of carding, because it renders all of us walking ID cards." In this already troubling milieu, facial recognition technologies will invariably make a bad situation worse, exacerbating police racism and burdening minority communities with further surveillance.

The increased use of FRTs by police forces across Canada have particularly grave implications for Canadian youth who are members of visible minority groups. In Canada, both Black and Indigenous communities are over-policed, and with anti-Black and anti-Indigenous racism in Canadian police departments of concern to international organizations like the United Nations[62]. One such form of over-policing is carding or "street checks," roughly analogous to "stop and frisk" policies in the United States; these practices involve stopping and questioning individuals (including asking for identification cards) for non-specific reasons[63]. Carding disproportionally affects members of visible minority groups, especially young people. As one scholar observes, “Street check practices interfere with youth on the streets, where young people frequently gather for social purposes; members of the groups who are disproportionately targeted by police practices are aware of the discriminatory practices, and experience feelings of injustice and disempowerment as a result of street checks.[64]” An independent report commissioned by the Ontario government in 2018 found that these practices resonated with historical forms of racist surveillance, such as the Off-Reserve Pass System for Indigenous people and ownership records for enslaved Black people, and perpetuated racist forms of surveillance in the present[65]. Another report found that visible minorities are more likely to be stopped by police per capita in cities across Canada[66]. In Halifax, Black people are six times more likely than white people to be stopped by police[67], while in Toronto, Black people are seventeen times more likely to be detained[68].

The CCLA describes facial recognition as “an extreme form of carding, because it renders all of us walking ID cards.[69]” In this already troubling milieu, facial recognition technologies will invariably make a bad situation worse, exacerbating police racism and burdening minority communities with further surveillance. Moreover, without clear laws governing the use of biometric data in Canada, the data collected by FRTs in certain educational contexts could also theoretically be diverted for use by law enforcement agencies. As the CCLA observes, “the use of Clearview points to a larger crisis in police accountability when acquiring and using emerging surveillance tools[70]” — including how data obtained in one institutional context is used in another. Given that street checks already disproportionally affect young Canadians, this sort of potential data creep is just one more reason to ban facial recognition in both education and law enforcement entirely.

Privacy Loss Leaders for Canadian Youth

Public institutions like schools and police forces are in theory accountable to Canadian citizens and subject to public debate over their use of facial recognition technologies. But what about the many private sector and commercial FRT applications popping up in Canadian offices, malls, and on our smartphones?[71] Canadian firms such as Deloitte Canada, KPMG, and Shell have begun to use facial recognition as part of their hiring and candidate screening protocols through companies like HireVue, which until recently deployed FRTs as part of their automated assessment batteries testing and evaluating job candidates[72]. The increased use of facial recognition by human resources companies as a mechanism to screen job candidates in certain sectors mean young people are faced with a novel set of opaque technological hurdles to getting a job. Canadian retail management companies like Cadillac Fairview have also piloted FRTs in their shopping centers[73], with the company recently admitting it used facial recognition technology to collect over five million images in order to analyze the age and gender of shoppers without mall patrons' knowledge or consent[74]. One Toronto area supermarket, mirroring similar developments in the United States[75], has even proposed an FRT system whereby customers pay with accounts linked to their faces [76]. The various commercial uses of FRTs are under-regulated, meaning all Canadians, including young people, are at the mercy of obscure privacy policies and consent notices regulating FRT surveillance in places like malls and other quasi-public private spaces.

Yet the most ubiquitous form of facial recognition technology in Canada is likely sitting in your hand or pocket as you read this sentence. Smartphones from companies like Apple, Samsung, and Huawei all feature sophisticated cameras equipped with various kinds of facial detection, recognition, and analysis software. For instance, the iPhone X's TrueDepth camera "captures accurate face data by projecting and analyzing over 30,000 invisible dots to create a depth map of your face and also captures an infrared image of your face." According to Apple, the camera then "transforms the depth map and infrared image into a mathematical representation and compares that representation to the enrolled facial data.[77]" The iPhone X uses this facial recognition data in its FaceID system allowing users to unlock the phone.

One especially common and popular use for smartphone facial recognition systems like the TrueDepth camera is to power animated "skins," "lenses," or "filters" – software applications which allow a user to digitally manipulate, augment and mask their face[78]. Social media platforms like Facebook Messenger, Instagram, Snapchat, and TikTok all incorporate these "augmented reality" or AR filters into their camera and video interfaces. This phenomenon is hardly unique to Canada, and young people are often the target user group for these filters[79]. A variety of services also allow users to create and share their own AR animated filters on platforms like Snapchat and Instagram[80].

By routinizing the process of engaging with FRTs, these apps make the wider dangers of FRT less viscerally appreciable to consumers.

Animated AR filters are significant vectors for youth marketing, and Canadian corporations have invested heavily in custom filters and lenses which reflect and burnish their brands; companies like Vancouver-based Geofilter Studios are specialty third-party design firms for these custom filters serving companies around the world[81]. The Canadian federal government has commissioned AR filters for promotional purposes, with departments including Canadian Heritage and Global Affairs purchasing Snapchat lenses in 2016[82], and Elections Canada using filters to promote voting during the 2019 federal election[83].

While it's not unreasonable to reach Canadian youth via channels they use on a daily basis, the widespread and uncritical embrace of animated AR smartphone filters built on top of facial recognition technology is a major boon for the development of FRTs, and a major problem for advocates seeking to curtail the use of facial recognition. The biggest problem with these AR filters is that they can't work without taking measurements of a user's face. In May of 2020, four Illinois teenagers sued TikTok under the state's strict biometric privacy law, claiming that the app had collected facial geometry data on the teens using facial recognition without their explicit consent[84]. It's not always easy to determine whether facial geometry data is being stored on a user's phone, or sent back to the app; it's also often unclear whether apps are using facial geometry to refine and improve their facial recognition systems.

Animated AR applications, much like other features such as TouchID, also serve as "privacy loss leaders." These every-day, even fun applications of facial recognition acclimatize smartphone users – especially children and young people – to FRT engagement and surveillance[85]. By routinizing the process of engaging with FRTs, these apps make the wider dangers of FRT less viscerally appreciable to consumers[86]. Apple's Animoji and Memoji are a good example of the ways AR filters accustom users to facial tracking through seemingly innocuous social applications. According to Apple, "Animojis track more than fifty muscle movements," in order to produce animated avatars of various animals that track to a user's facial movements and speech. In June 2018, Apple launched Memoji — customizable animated avatars of a user's own face —to complement its Animoji characters. While interacting with others via these animated avatars seems harmless, doing so just reinforces facial recognition's centrality to animated social media and augmented reality systems.

Conclusion: What Can Young People Do?

Facial recognition is now widely available and appealing to corporations and governments, and these systems' many downsides haven't stopped their spread. Given the popularity of smartphone-based facial recognition technology alongside its increasingly common use in areas like hiring, policing, and even education, what should Canadian youth do about the proliferation of these technologies—both to safeguard their rights to privacy and robust democratic participation and to ensure their advocacy for the responsible assessment of FRTs benefits all Canadians?

The most effective single action Canadian young people can take to stop the use (and abuse) of facial recognition technology is to work to elect politicians at all levels of government who support strong biometric privacy laws and laws supporting bans and moratoria on FRTs. Right now, there is a "significant vacuum" with respect to how Canadian data privacy laws[87], including the Personal Information Protection and Electronic Documents Act (PIPEDA) which regulates data privacy in the private sector and engages with the nuts and bolts of novel and rapidly developing technologies like facial recognition[88]. While the Canadian Privacy Commissioner and provincial counterparts have taken action in specific situations like the Clearview AI case[89], a systematic and robust response to facial recognition means enhancing existing federal and provincial privacy laws to regulate all forms of physiognomic AI — ideally to the point of elimination in most sectors. Outside of very few specialized and highly controlled specialist applications, like assisting surgeons, there's no reason for FRTs to be used at all — and certainly not in areas like education or hiring.

Second, Canadian youth can, to the best of their abilities, organize to demand an immediate end of the use of FRTs in schools and public institutions. While comprehensive biometric privacy laws are being debated, young people can follow the lead of advocates in the United States and elsewhere in pushing for immediate FRT bans and moratoria by their communities, school boards, and universities[90]. In Lockport, NY it was both young people and their parents whose advocacy helped halt the deployment of facial recognition in the local schools — so learning about the issues and building alliances with others is a valuable way of changing the minds of institutions tempted to deploy FRTs.

Finally, Canadian youth already working in the digital technology sector or starting their careers there, can connect with other like-minded specialists committed to producing new technologies that support values like privacy and robust, healthy democratic engagement. Digital technology developers should indeed be “listening to kids.[91]” Canadian youth deserve, and are collectively creating, innovative ways to think about how digital technologies can support their aspirations — initiatives like the Indigenous Futures Research Centre at Concordia University, dedicated to exploring how digital technologies can support Indigenous people in imagining the future of their families and communities[92]. Conversely, facial recognition technologies won’t flourish without researchers working to develop them, and while systemic change is vital, it can come not only from regulation but also from collective action within the tech sector itself[93]. Banding together to both fight problematic technologies like facial recognition, and imagine better futures supported by digital systems, isn’t easy — but it’s the best way forward for young people, and for all of us interested in a fair, just, equal, and connected Canada.

Endnotes

[1] https://www.lockportjournal.com/news/local_news/trying-for-more-secure-schools-lockport-district-turning-to-facial-recognition-software/article_f1cc9cfa-0898-5da0-ac5d-d600df21bed7.html.

[2] "According to a 2010 paper by United Way of Calgary and Area, the federal government uses several definitions of youth: Statistics Canada defines youth between 16-28 years, whereas for Human Resources and Skills Development Canada it is 15-24." https://www.youthpolicy.org/factsheets/country/canada/.

[3] https://ccla.org/facial-recognition/.

[4] Szeliski, R. (2010). Computer Vision: Algorithms and Applications (Springer), 3.

[5] Gates, K. (2011). Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance. New York: New York University Press.

[6] http://stpp.fordschool.umich.edu/sites/stpp.fordschool.umich.edu/files/file-assets/cameras_in_the_classroom_full_report.pdf, page 18.

[7] Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research, 81*, 1–15.

[8] https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.

[9] https://threatpost.com/aws-facial-recognition-platform-misidentified-over-100-politicians-as-criminals/156984/.

[10] https://www.forbes.com/sites/thomasbrewster/2019/07/04/london-police-facial-recognition-fails-80-of-the-time-and-must-stop-now/#d2d39a1bf950.

[11] MacKenzie, D. A. (2016). Performing Theory? In An Engine, Not a Camera (pp. 1–35). The MIT Press. http://doi.org/10.7551/mitpress/9780262134606.003.0001.

[12] Browne, S. (2015). Dark Matters: On the Surveillance of Blackness. Durham NC and London: Duke University Press.

[13] https://www.aclu.org/news/privacy-technology/how-is-face-recognition-surveillance-technology-racist/.

[14] Crawford, K., Dobbe, R., Dryer, T., Fried, G., Green, B., Kaziunas, E., et al. (2019). AI Now 2019 Report (pp. 1–100). New York: AI Now Institute.

[15] Scheuerman, M. K., Paul, J. M., & Brubaker, J. R. (2019). How Computers See Gender. Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), 1–33. http://doi.org/10.1145/3359246.

[16] **Physiognomy's New Clothes, Blaise Agüera y Arcas, Margaret Mitchell and Alexander Todorov.**

[17] https://twitter.com/jevanhutson/status/1296806594085359628.

[18] Canada, O. O. T. P. C. O. (2014). Automated Facial Recognition in the Public and Private Sectors, 1–16.

[19] Hartzog, W., & Selinger, E. (2018, August 20). Facial Recognition Is the Perfect Tool for Oppression. Retrieved August 20, 2018, from http://cyberlaw.stanford.edu/publications/facial-recognition-perfect-tool-oppression.

[20] *Policy Guidance on AI for Children DRAFT 1.0* (September 2020). UNICEF/Ministry of Foreign Affairs of Finland, p. 22. https://www.unicef.org/globalinsight/media/1171/file/UNICEF-Global-Insight-policy-guidance-AI-children-draft-1.0-2020.pdf.

[21] Berman, G., Carter, K., García-Herranz, M. and Sekara, V. (2020). Digital Contact Tracing and Surveillance during COVID-19: General and Child-specific Ethical Issues. https://www.unicef-irc.org/publications/pdf/WP2020-01.pdf.

[22] https://ca.reuters.com/article/idUSKBN2081CU.

[23] Hasse, A., Cortesi, S., Lombana-Bermudez, A., & Gasser, U. (2019). *Youth and artificial intelligence: Where we stand.* Youth and Media, Berkman Klein Center for Internet & Society. Retrieved from https://cyber.harvard.edu/publication/2019/youth-and-artificial-intelligence/where-we-stand.

[24] Shade, L. R., Bailey, J., Burkell, J., Regan, P., and Steeves, V. (2020) “Framing the Challenges of Digital Inclusion for Young Canadians,” in Dubois, E. and Martin-Bariteau, F. (eds.), *Citizenship in a Connected Canada: A Research and Policy Agenda,* Ottawa, ON: University of Ottawa Press.

[25] http://rightswatch.ca/2019/02/16/supreme-court-of-canada-confirms-students-reasonable-expectation-of-privacy/.

[26] Andrejevic, M., & Selwyn, N. (2019). Facial recognition technology in schools: critical questions and concerns. *Learning, Media and Technology, 45*(2), 115–128. http://doi.org/10.1080/17439884.2020.1686014, 119.

[27] https://collections.ola.org/mon/7000/10317630.pdf.

[28] https://freedom-to-tinker.com/2004/07/09/security-theater/.

[29] https://technology.informa.com/600401/school-security-systems-industry-us-market-overview.

[30] https://www.lockportjournal.com/news/local_news/trying-for-more-secure-schools-lockport-district-turning-to-facial-recognition-software/article_f1cc9cfa-0898-5da0-ac5d-d600df21bed7.html.

[31] http://www.sntechnologies.ca/product/. The software is “designed to interact with your current CCTV network and is agnostic to camera brand.”

[32] https://educhatter.wordpress.com/tag/sn-tech-security-software/. An inventory of Canadian suppliers of FRTs to the global education market, and more broadly, would be a valuable research contribution.

[33] Zeide, E., & Nissenbaum, H. (2018). Learner Privacy in MOOCs and Virtual Education. *Theory and Research in Education, 16*(3), 280–307. http://doi.org/10.1177/1477878518815340.

[34] https://proctorio.com/.

[35] https://www.proctortrack.com/coronavirus-support/.

[36] https://www.d2l.com/covid-19/take-online-learning-to-the-next-level/.

[37] https://www.d2l.com/k-12/ontario/.

[38] https://www.globenewswire.com/news-release/2020/07/16/2062983/0/en/CARLETON-UNIVERSITY-CHOOSES-BRIGHTSPACE-EDUCATION-PLATFORM.html.

[39] https://lfpress.com/news/local-news/western-students-want-online-anti-cheating-program-banned-as-potential-privacy-threat.

[40] https://www.theverge.com/2020/10/22/21526792/proctorio-online-test-proctoring-lawsuit-universities-students-coronavirus.

[41] https://www.d2l.com/k-12/products/engagement/.

[42] Ben Williamson. (2019). Psychodata: disassembling the psychological, economic, and statistical infrastructure of “social- emotional learning.” *Journal of Education Policy, 36*(1), 1–26. http://doi.org/10.1080/02680939.2019.1672895.

[43] Claire Galligan, Hannah Rosenfeld, Molly Kleinman, Shobita Parthasarathy, “Cameras in the Classroom: Facial Recognition Technology in Schools,” 10-11.

[44] https://news.wbfo.org/post/facial-recognition-lockport-schools-best-technology-world-or-not-proven-work.

[45] https://www.medianama.com/2020/07/223-new-york-halts-facial-recognition-schools/.

[46] https://www.ctvnews.ca/canada/five-charts-that-show-what-systemic-racism-looks-like-in-canada-1.4970352.

[47] https://www.cbc.ca/news/canada/toronto/toronto-police-clearview-ai-1.5462785.

[48] https://iapp.org/news/a/police-call-for-external-review-on-use-of-facial-recognition/.

[49] https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[50] https://www.huffingtonpost.ca/entry/clearview-ai-facial-recognition-alt-right_n_5e7d028bc5b6cb08a92a5c48?ncid=other_email_o63gt2jcad4&utm_campaign=share_email.

[51] https://www.cbc.ca/news/canada/toronto/clearview-ai-toronto-police-ccla-privacy-1.5463823.

[52] https://priv.gc.ca/en/opc-news/news-and-announcements/2020/an_200221/.

[53] https://www.cbc.ca/news/technology/clearview-ai-canadians-can-opt-out-1.5645089.

[54] https://www.thestar.com/news/gta/2019/05/28/toronto-police-chief-releases-report-on-use-of-facial-recognition-technology.html.

[55] https://www.vice.com/en_ca/article/xg8wp4/police-forces-in-canada-are-quietly-adopting-facial-recognition-tech.

[56] https://www.cbc.ca/player/play/2586405074.

[57] https://www.cbc.ca/news/canada/nova-scotia/facial-recognition-police-privacy-laws-1.5452749.

[58] https://vancouversun.com/news/local-news/yvr-to-become-first-canadian-airport-to-use-facial-recognition-at-nexus-kiosks.

[59] https://www.vice.com/en_us/article/new5q8/canadas-spies-police-and-border-agents-are-quietly-coordinating-on-biometrics.

[60] https://www.theglobeandmail.com/canada/article-ottawa-tested-facial-recognition-on-millions-of-travellers-at-torontos/.

[61] https://iclmg.ca/wp-content/uploads/2020/07/facial-recognition-letter-08072020.pdf.

[62] https://www.amnesty.ca/blog/carding-and-anti-black-racism-canada.

[63] https://www.thestar.com/news/gta/2018/12/31/police-carding-should-be-banned-in-ontario-independent-review-says.html.

[64] https://harvest.usask.ca/bitstream/handle/10388/8098/ABBOTT-THESIS-2017.pdf?sequence=1&isAllowed=y.

[65] http://www.mcscs.jus.gov.on.ca/sites/default/files/content/mcscs/docs/StreetChecks.pdf, 37.

[66] http://beta.legalaid.on.ca/strategic/wp-content/uploads/sites/4/2016/06/infographic-RCS-carding-2016-05-EN.pdf.

[67] https://www.cbc.ca/news/canada/nova-scotia/street-checks-halifax-police-scot-wortley-racial-profiling-1.5073300.

[68] https://www.cbc.ca/firsthand/m_features/heres-what-you-need-to-know-about-carding.

[69] https://ccla.org/facial-recognition/.

[70] Ibid.

[71] https://www.cbc.ca/news/technology/facial-recognition-shopping-1.3561060.

[72] https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/.

[73] https://www.cbc.ca/news/canada/calgary/calgary-malls-1.4760964.

[74] https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/nr-c_201029/.

[75] https://www.latimes.com/business/technology/story/2020-08-14/facial-recognition-payment-technology.

[76] https://nationalpost.com/news/pay-with-your-face-ontario-grocery-chain-looks-at-paying-via-facial-recognition.

[77] https://support.apple.com/en-ca/HT208108.

[78] Tilic, G. (2017). Snapchat as an advertising platform. *New Trends and Issues Proceedings on Humanities and Social Sciences. [Online]. 4*(11), 122-129. Available from: www.prosoc.eu.

[79] https://www.theverge.com/2019/8/16/20808954/instagram-face-filters-facebook-videos-effects-how-to-spark-ar-studio.

[80] https://www.highsnobiety.com/p/instagram-augmented-reality-filters/.

[81] https://www.geofilter.studio/about-us/.

[82] https://www.vice.com/en_ca/article/nz838w/trudeaus-government-has-spent-dollar20000-on-snapchat-filters-and-thats-a-bargain.

[83] https://election.ctvnews.ca/snapchat-teams-up-with-elections-canada-to-encourage-young-users-to-vote-1.4641364?cache=yes.

[84] https://www.chicagotribune.com/business/ct-biz-tiktok-illinois-biometric-privacy-lawsuit-20200513-jogjwzp4ofa67nu6pwsduxz7si-story.html.

[85] Stark, L. (2018). Facial recognition, emotion and race in animated social media. *First Monday, 23*(9). http://doi.org/10.5210/fm.v23i9.9406.

[86] Stark, L. (2016). The emotional context of information privacy. *The Information Society, 32*(1), 14–27. http://doi.org/10.1080/01972243.2015.1107167.

[87] https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/.

[88] https://www.mondaq.com/canada/privacy-protection/808754/biometric-identification-and-privacy-concerns-a-canadian-perspective.

[89] https://www.cbc.ca/news/technology/clearview-ai-stops-facial-recognition-in-canada-1.5639380.

[90] https://www.forbes.com/sites/tomtaulli/2020/06/13/facial-recognition-bans-what-do-they-mean-for-ai-artificial-intelligence/#6a3b0e8946ee.

[91] https://www.wired.com/story/ai-innovators-should-be-listening-to-kids/.

[92] https://milieux.concordia.ca/indigenous-futures/.

[93] https://www.nytimes.com/2018/10/07/technology/tech-workers-ask-censorship-surveillance.html.

Designed by Yasmeen Safaie

Centre *for* MEDIA, TECHNOLOGY *and* DEMOCRACY

McGill

MAX BELL SCHOOL *of* PUBLIC POLICY