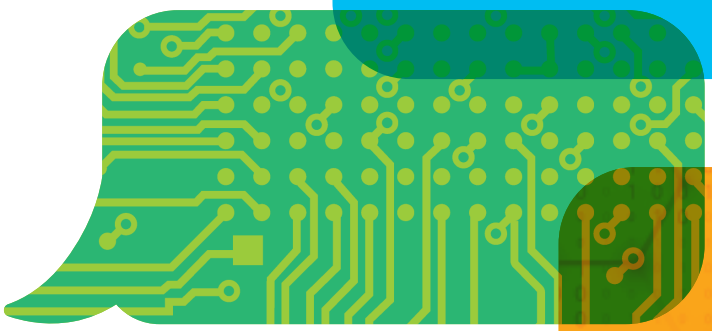
ALGORITHMIC AWARENESS

CONVERSATIONS WITH YOUNG CANADIANS
ABOUT ARTIFICIAL INTELLIGENCE AND PRIVACY



MediaSmarts

Algorithmic Awareness: Conversations with Young Canadians about Artificial Intelligence and Privacy

This report can be downloaded from: mediasmarts.ca/research-policy

Cite as: Brisson-Boivin, Kara and Samantha McAleese. (2021). "Algorithmic Awareness: Conversations with Young Canadians about Artificial Intelligence and Privacy." MediaSmarts. Ottawa.

Written for MediaSmarts by:
Kara Brisson-Boivin, PhD
Samantha McAleese

MediaSmarts
205 Catherine Street, Suite 100
Ottawa, ON Canada K2P 1C3
T: 613-224-7721
F: 613-761-9024
Toll-free line: 1-800-896-3342
info@mediasmarts.ca
mediasmarts.ca
@mediasmarts

This research was made possible by the financial contributions from the Office of the Privacy Commissioner of Canada's contributions program.

Table of Contents

Key Terms

Algorithm: A set of step-by-step instructions for solving a problem or completing a mathematical or computational task. Algorithms sort data to find patterns and make predictions or recommendations. The term is often used to refer specifically to computer programs trained to make predictions.

Artificial intelligence: The simulation of human intelligence (for example, learning or problem solving) in machines programmed to think like humans and mimic their actions. Examples include speech recognition, translation between languages, image and facial recognition, and decision-making.

Autocomplete: A feature that predicts and suggests the rest of a word or phrase a user is typing into a search engine, text message, or other application, based on what they or other users have entered in the past. An example of a prediction and suggestion algorithm.

Behavioural advertising: A technique used by online advertisers to target ads to consumers by collecting information about their browsing behaviour followed by the use of a sorting and recommendation algorithm to match ads with consumers who are most likely to respond to them. Behavioural advertising means that two people who look at the same video or website may see completely different ads based on their *data profile.*

Bias: In this context, bias means when an algorithm delivers an unfair result based on inaccurate assumptions or stereotypes. Bias can come from the designer's decisions: for example, an algorithm used to predict the final grades of students who were unable to finish the semester might base its conclusions partly on how students from that school typically performed in the past. Due to an assumption that students from schools in lower-income communities usually get lower grades, the algorithm will lower students' grades in those schools. This algorithm effectively punishes students for being poor. Bias can also occur when a *machine learning* algorithm is trained on biased data. An algorithm that decides whether or not to grant mortgages based on past mortgage applications could, unless specifically corrected, be *biased* by previous racist practices of "redlining" or denying mortgages to Black people.

Behavioural data: Information about a user's past behaviour used to inform behavioural advertising, like the pages browsed on a website or the time spent on a website, app, or game. For example, a user who has watched many videos about games will be more likely to be shown an ad for games.

Contextual advertising: A technique used by online advertisers to present targeted ads to consumers based on what they are currently *doing* or have *recently done*, such as what videos they are now watching or the search they have just performed. Because it does not draw on the user's data profile or behavioural data, it is generally considered less intrusive than behavioural advertising. For instance, a search engine that recommended ads based on *contextual* data would show you ads based on what you just searched for, while one that used *behavioural data* would lead you to ads based on all of your past searches.

Content spiral: Sometimes called a recommendation spiral, this refers to getting caught up in a seemingly endless loop of viewing online content provided by a platform's recommendation algorithm, such as on YouTube or Twitter. The user continues to view even slightly related content, spiraling from topic to related topic, potentially losing track of time.

Data broker: Companies or entities that buy or otherwise collect information (data) about users and sell that information to interested companies, individuals or other data brokers to establish data profiles on people. Some data brokers also provide services that allow them to collect data (such as search engines or video sites), while others simply buy information collected by others. Companies that own several platforms, like Google, essentially act as their own data brokers, by sharing data between the platforms. These companies then sell the recommendations that come from that data, but not the data itself, to advertisers.

Filter bubble: Coined by internet activist Eli Pariser and sometimes called a preference bubble, this refers to a unique universe of online information for each of us that can alter the way we encounter ideas and information and understand the world around us. Algorithms collect data about what we like and selectively try to predict similar content that we may also like. Filter bubbles can result in a narrow view of the world since they often hide information and opinions that differ from ours. Filter bubbles are a unique type of *echo chamber* with environments where users only encounter information or opinions that reflect and reinforce their own, resulting in confirmation bias.

Machine learning: A collection of algorithms and programming trained on large amounts of data to improve how computers search for patterns, make predictions or perform tasks. Most applications described as "artificial intelligence" are examples of *machine learning*. In some cases, machine learning can filter data through self-adjusting networks of code inspired by neurons in the human brain; this is sometimes called *deep-learning* or *neural networks*.

Introduction

This research study, *Algorithmic Awareness: Conversations with Young Canadians about Artificial Intelligence and Privacy,* combined game-based learning with discussion and reflection to gain insight into how young Canadians understand the relationship between artificial intelligence (AI), algorithms, privacy, and data protection. There is, to date, very little research on how youth interact with and are impacted by AI. This research project aimed to create the space for young people to (a) learn more about AI and algorithms and their repercussions on privacy rights; and (b) help design youth-friendly education tools to build awareness and *meaningful* understandings of data collection and sharing practices that will allow them to better protect their privacy rights.

Insufficient knowledge of AI and algorithms contributes to exclusion from online spaces, tech-facilitated discrimination, exposure to harmful content, and various privacy risks. As the Office of the Privacy Commissioner of Canada reminds us, "every day there are new, creative ideas on how businesses can derive more profit from our personal information,"[1] and it is becoming increasingly difficult for individuals to "demystify complex business relationships and complicated algorithms to make informed choices."[2] This is especially true of children and youth who are often the target audience for new AI and algorithm-based technologies, apps, games, and platforms. Given that young people "are growing up in a world surrounded by AI," we need more robust algorithmic literacy tools, resources, and programs to help them become "more critical consumers," to maintain control of their personal information, and "motivate them to help shape [the] future" of this technology.[3]

This qualitative research project gave youth an opportunity to:

- Reflect on how they interact with AI in their day-to-day lives;
- Learn more about how AI and algorithms work;
- Understand the implications of AI and algorithms on their privacy;
- Inform new tools and resources to educate themselves and their peers about the relationships between AI and privacy; and
- Share all of these insights with academics, policymakers, and representatives from the educational and technological sectors.

We facilitated eight online focus groups with 22 participants ages 13 to 17. Participants played a game prototype designed and facilitated by MediaSmarts'

[1] Office of the Privacy Commissioner of Canada. (2018). "The strategic privacy priorities." Retrieved from: www.priv.gc.ca/en/about-the-opc/opc-strategic-privacy-priorities/the-strategic-privacy-priorities/
[2] Ibid.
[3] Hao, K. (2019). "Kids are surrounded by AI. They should know how it works." Retrieved from: www.medium.com/mit-technology-review/kids-are-surrounded-by-ai-they-should-know-how-it-works-ae15756f1085

Director of Education and our Media Education Specialist. ***#ForYou: A Game About Artificial Intelligence and Privacy***, is intended to help children and youth learn more about artificial intelligence, algorithms, online privacy, and data security. It is designed as a scaffolded learning experience allowing for in-depth discussions with participants after each phase of the game.

From the start, youth were troubled by processes of algorithmic data collection, especially inferred data gathered through machine learning. Of particular concern to young people was the future—unknown or unanticipated—uses of their information, specifically as they prepare for post-secondary education, the job market, and eventually the responsibilities of adulthood (including apartment or housing applications, financial services, and healthcare services).

In the first phase of gameplay, we invited players to imagine themselves as content creators for a popular video-sharing site such as YouTube or TikTok. We introduced participants to the idea of optimization, or the purposes for which a video site might optimize its algorithm (for example, engagement, virality of content or daily use). Participants also learned about the factors that a recommendation algorithm might consider in deciding how much to boost a video, such as how many times it had been viewed, liked, or shared. In this way the first phase of the game demonstrated to participants how algorithms use various factors to sort, select, filter and recommend content and how that affects which videos are recommended to them and, as a result, which videos and content creators become popular. The observations and discussions following this first phase of gameplay mainly centred on how recommendation algorithms impact online experiences and environments. Youth quickly pointed out how algorithms impact the spaces and places within which they engage, particularly the breadth and depth of content available to them and how the pressure to optimize for recommendation factors affects the quality of this content.

In the second phase of gameplay, we introduced participants to the idea of monetization. Participants learned that for videos to make money it's important that they – and the ads that accompany them – reach and resonate with not just the *most* people, but also with the *right* people. This audience targeting, which is the main selling point of online advertising, requires gathering and analyzing information about the people watching their videos. By the end of the second phase of gameplay, participants saw how recommendation algorithms rely on user data to generate assumptions about user likes, interests, purchases, and behaviours. Youth saw how algorithms collect, analyze, and make inferences about users based on their information—discussions with participants following this phase of gameplay centred on the value of personal information for algorithmic systems. Young people also reflected on their privacy concerns regarding the corporate uses of their data and personal information.

In the third and final round of gameplay, participants learned about machine learning, artificial intelligence, data brokerage, and how algorithms rely on proxies to make inferences about users and identify patterns that might not otherwise have been apparent. The objective of this round was to expose how algorithms are trained or modified on data sets and demonstrate how these ongoing and automatic training processes lead to assumptions about individual preferences. Having participants link data cards through proxies including race, gender, or sexual orientation catalyzed discussions about how these AI processes can sometimes lead to faulty, problematic, or dangerous assumptions, contributing to bias, prejudice, and discrimination in online and offline spaces. Participants also traded data cards with other players to replicate processes for how data collected about them is shared and used by data brokers. Youth questioned the ethics of machine learning algorithms in that they often rely on information that users might not know they are providing. This led to further discussions about rights, responsibilities, and protections related to personal information, behaviours and activity, and privacy online.

The key findings from these focus groups, along with examples of the *#ForYou* game prototype, are highlighted in this final report. The interactive and scaffolded focus group format (introduction, gameplay, discussion) proved to be a generative approach to research and stressed the importance of **open and ongoing discussions with youth about algorithms, artificial intelligence, and privacy.**

Algorithms and Artificial Intelligence: What We (Don't) Know

A Black Box

In science, computing, and engineering, a black box is a device, system, or object that can be viewed in terms of its inputs and outputs without any knowledge of its internal workings. **Machine learning algorithms are black boxes:** we can identify what data goes into them, and we can know and experience the impacts of their outcomes, but because they are trained on data and iterate themselves over time their implementation is opaque, even to their designers. In fact, experts say algorithmic systems **'refuse to be known'**[4] since their value is in their opacity—in keeping their inner workings or performance a trade secret. The secrecy surrounding how algorithms do and do not work makes it challenging for users to understand what they are and what they do. While we can know algorithmic inputs and outputs and identify what an algorithm has been optimized for, most people (and young people, particularly) lack the level of algorithmic literacy required to fully understand the operation and impacts of algorithmic systems in their online and offline lives.

Algorithms are instructions for solving a problem or completing a task.[5] [6] Recipes and math equations are everyday examples of algorithms. Algorithms are everywhere on the web; the internet runs on algorithms. We can think of algorithms as the recipes or equations that coders use to take information and produce things that help us achieve (or in some cases prevent) all sorts of tasks, including searching for information, sending emails, browsing social media, consulting GPS mapping systems, streaming music or TV shows, dating, recognizing voice-activated commands, language translation, recognizing faces, sorting photos, driving a car, buying a home, and applying for university or a job. More and more of these algorithms are not simple recipes that are transparent to their designers but are created through machine learning, or 'artificial intelligence.' The relatively short history of artificial intelligence is marked by milestones in which programming and software became increasingly adept at mastering tasks previously performed only by people. This progress has been frequently represented through game play, such as by defeating human masters of games such as Chess or Go.[7]

---

[4] Gillespie,T., MacPhee, C., and J. Reddeb. (2020). "Panel presentation on AI & Algorithms." eQuality Project. Annual General Meeting. Virtual. Retrieved from: www.equalityproject.ca/resources/ai-algorithms/

[5] See: Rainie, L, and J. Anderson, (2017). "Code-Dependent: Pros and Cons of the Algorithm Age." Pew Research Center, *Internet and Technology.* Retrieved from: www.pewinternet.org/2017/02/08/code-dependent-pros-and-cons-of-the-algorithm-age

[6] The Algorithmic Literacy Project (2020). "Educational Guide: Diving Deeper into Algorithms." Kids Code Jeunesse (KCJ) and The Canadian Commission for UNESCO (CCUNESCO). Retrieved from: www.algorithmliteracy.org/data/resources/en/Algorithm-Literacy-Education-Guide.pdf

[7] In 1950, computer programs learned how to play, and eventually beat (in 1962), a master of checkers. In 1997, IBM's computer Deep Blue defeated a world chess champion, and in 2016, AlphaGo, created by Google unit DeepMind,

As AI and algorithmic systems honed new powers of perception, big tech companies acquired talented programmers and state-of-the-art technology to bolster their core business of targeting ads anticipating our next purchase, view, or listen. Of utmost importance is that algorithms and AI learn from **behaviour**, what we *do* online, and from **information**, who we are online—the information we input when signing up for apps and services and the information we share about ourselves in various online spaces. Based on this information, algorithms can limit the options available to us and potentially influence our understandings of the world.[8] However, while the decisions algorithms make for us impact our lives, we also influence algorithmic decision-making with our online interactions.[9] Still, knowing an algorithm is not as simple as opening the black box to discover what is inside since "algorithms are difficult for people to grasp, most users likely do not appreciate just how big a role they play in what they see online."[10]

Most of the youth (ages 13 to 17) that we spoke to through this research study admitted to having little to no background knowledge regarding algorithms or how they work. Our icebreaker discussions with youth ranged from silence, blank stares, and admissions of "I don't really know" (Madelyn, 14) to head bobs and shoulder shrugs to astute observations identifying algorithms as "math equations and codes that can be used for an outcome" (Sahil,15). Regardless of their prior knowledge, it was clear from these initial discussions that **young Canadians learn about algorithmic systems almost exclusively through experience.** When we asked youth to explain what an algorithm was, most of their initial responses relied on a recent example of an algorithmic interaction, one they have had on platforms using a recommendation algorithm (e.g., Instagram, Twitter, TikTok, and YouTube):

> Like on social media, it [the algorithm] tracks what you like, and that's an algorithm figuring out what to show you based on what you've seen and liked in the past. (Hailey, 16)

defeated a world champion player of the board game Go. See: Simonite, T. (2018). "The Wired Guide to Artificial Intelligence." Wired Magazine. Retrieved from: www.wired.com/story/guide-artificial-intelligence/.

[8] Dignum,V., K., Pigmans, S., Vosloo, S. and M. Penagos. (2020). "Policy Guidance on AI for Children." UNICEF, The Office of Global Insight and Policy." *The United Nations Children's Fund.* 1-48. Retrieved from: www.unicef.org/globalinsight/media/1171/file/UNICEF-Global-Insight-policy-guidance-AI-children-draft-1.0-2020.pdf

[9] The Algorithmic Literacy Project (2020). "Educational Guide: Diving Deeper into Algorithms." Kids Code Jeunesse (KCJ) and The Canadian Commission for UNESCO (CCUNESCO). Retrieved from: www.algorithmliteracy.org/data/resources/en/Algorithm-Literacy-Education-Guide.pdf

[10] Klawitter, E., and Hargittai, E. (2018). ""It's like learning a whole other language": The role of algorithmics kills in the curation of creative goods." *International Journal of Communication*, *12*, 3490-3510.

> Once your information is out there, it's basically impossible to get it offline... basically, anything you do online—it's just there, forever. (Claire, 15)

In other words, youth are learning about algorithms primarily from their interactions *with* algorithms. While this can provide them with some insightful observations about the uses and misuses of their information and concerns about their privacy, it is knowledge gained in fragments and in hindsight. Accordingly, participants often expressed a sense of powerlessness and a lack of control when it came to the influence and impact of algorithms and AI in their lives. Some of this sense of powerlessness, or the lack of control youth experienced, stems from not knowing what algorithmic systems *actually* know about them:

> **You never really know what information they [algorithms] are taking, so I think that too—like you don't know what they [algorithms] know. (Mia, 15)**

Not knowing what algorithms know about them is particularly difficult for youth to remedy since, as noted above, algorithms are black boxes that 'refuse to be known.'[11] However, research demonstrates that "simply understanding the basics of algorithms—that they exist, that they influence visibility, and that they can be gamed or manipulated if carefully observed—can be a sufficient differentiator when it comes to the material consequences of algorithms."[12]

Children and youth are interacting with algorithms and AI daily. AI is embedded in toys, video games, voice-activated assistants, and learning apps and educational software. "Algorithms provide recommendations to children on what videos to watch next, what news to read, what music to listen to and who to be friends with."[13] Along with these direct interactions is the potential for children and youth to be indirectly impacted by AI systems, as this technology is increasingly being integrated in decision-making systems embedded in healthcare practices, educational outcomes, and welfare subsidies, and housing applications.[14] [15] However, little work has focused

[11] Gillespie,T., MacPhee, C., and J. Reddeb. (2020). "Panel presentation on AI & Algorithms." eQuality Project. Annual General meeting. Virtual. Retrieved from: www.equalityproject.ca/resources/ai-algorithms/

[12] Klawitter, E., and Hargittai, E. (2018). ""It's like learning a whole other language": The role of algorithmic skills in the curation of creative goods." *International Journal of Communication*, *12*, 3490-3510.

[13] Dignum,V., K., Pigmans, S., Vosloo, S. and M. Penagos. (2020). ""Policy Guidance on AI for Children." UNICEF, The Office of Global Insight and Policy."" *The United Nations Children's Fund.* 1-48. Retrieved from: www.unicef.org/globalinsight/media/1171/file/UNICEF-Global-Insight-policy-guidance-AI-children-draft-1.0-2020.pdf

[14] Ibid.

[15] In the Canadian context, the use of AI technology has been primarily in law enforcement contexts (in predictive policing and social media surveillance) and there is not yet any confirmation that AI systems are being used in the social service sector.

on how youth interact with and are likely to be affected by AI,"[16] and research suggests we know even less about the long-term or future consequences of algorithms, especially for children and youth.[17] [18] Furthermore, MediaSmarts' research[19] has highlighted how **youth often do not have the opportunities to communicate their opinions or advocate for their privacy and data protection rights** in these contexts.

Given the impact that AI has, and will continue to have, on the lives of youth in Canada, "it is critical that young people have a basic understanding of what AI is and the ethical, societal, and privacy- and safety-related implications of these technologies."[20] Additionally, given that everything we do through digital technology is "now capable of being indefinitely captured, shared beyond our span of control, and brought up again completely out of context,"[21] **it is essential that we have open and ongoing discussions with youth** about this reality. Rather than grounding their online (inter)actions in fear and uncertainty, or concerns about a lasting 'digital stigma,' we can encourage youth through public education initiatives and educational resources, such as the game MediaSmarts designed through this research, to learn more about their privacy rights in ways that empower and motivate them to use AI to their advantage. For example, we know that AI shows promise in improving access to education,[22] meeting individual learning needs,[23] and mental health supports.[24] So then, as others have asked, "[h]ow can we most effectively equip young people to navigate the privacy and safety issues that

[16] 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 www.cyber.harvard.edu/publication/2019/youth-andartificial-intelligence/where-we-stand
[17] See: Dignum,V., K., Pigmans, S., Vosloo, S. and M. Penagos. (2020). ""Policy Guidance on AI for Children." UNICEF, The Office of Global Insight and Policy." *The United Nations Children's Fund.* 1-48. Retrieved from: www.unicef.org/globalinsight/media/1171/file/UNICEF-Global-Insight-policyguidanc e-AI-children-draft-1.0-2020.pdf
[18] Klawitter, E., and Hargittai, E. (2018). ""It's like learning a whole other language": The role of algorithmic skills in the curation of creative goods." *International Journal of Communication*, *12*, 3490-3510.
[19] See: McAleese, S., M., Johnson, and M., Ladouceur. (2020). "Young Canadians Speak Out: A Qualitative Research Project on Privacy and Consent." MediaSmarts. Ottawa.
Steeves,V., S., McAleese, and K.,Brisson-Boivin. (2020). "Young Canadians in a Wireless World, Phase IV: Talking to Youth and Parents about Online Resiliency." MediaSmarts. Ottawa.
www.mediasmarts.ca/sites/default/files/publication-report/full/report_ycwwiv_talking_youth_parents_online_resiliency.pdf
[20] Hasse, A., Cortesi, S., Lombana-Bermudez, A., and Gasser, U. (2019). "Youth and artificial intelligence: Where we stand." Youth and Media, Berkman Klein Center for Internet & Society. Retrieved from www.cyber.harvard.edu/publication/2019/youth-andartificial-intelligence/where-we-stand
[21] Office of the Privacy Commissioner of Canada. (2018). "The strategic Privacy Priorities." Retrieved from: www.priv.gc.ca/en/about-the-opc/opc-strategic-privacy-priorities/the-strategic-privacy-priorities/
[22] Rizzotto, L. (2017). "The future of education: How A.I. and immersive tech will reshape learning forever." Medium. Retrieved from: www.medium.com/futurepi/a-vision-for-education-and-its-immersive-a-i-driven-future-b5a9d34ce26d
[23] Dignum,V., K., Pigmans, S., Vosloo, S. and M. Penagos. (2020). "Policy Guidance on AI for Children." UNICEF, The Office of Global Insight and Policy." *The United Nations Children's Fund.* 1-48. Retrieved from: www.unicef.org/globalinsight/media/1171/file/UNICEF-Global-Insight-policy-guidance-AI-children-draft-1.0-2020.pdf
[24] D'Alfonso, S., Santesteban-Echarri, O., Rice, S., Wadley, G., Lederman, R., Miles, C., Gleeson, J., and Alvarez-Jimenez, M. (2017). "Artificial Intelligence-Assisted Online Social Therapy for Youth Mental Health." *Frontiers in Psychology*, *8*, 796.

surround AI-based applications?"[25] [26] As a first step, we need to allow young people to articulate their privacy, safety, and data protection concerns in order to understand the unique experiences of youth and to then work alongside them to meaningfully address these concerns.

The Return of the Privacy Paradox

While we have previously written about the privacy paradox in our study on privacy and consent,[27] this phenomenon re-emerged when talking to youth about AI and algorithms. The opacity and lack of understanding surrounding algorithms create what is referred to in the literature as a **privacy paradox:** while people care deeply about protecting privacy and data in online spaces, their behaviours often do not coincide with this desire for privacy and data security. This paradox is often framed as an individual problem, suggesting that it is up to individual users to familiarize themselves with privacy policies and settings. But, as Sonia Livingstone points out, "we cannot teach what is unlearnable."[28]

The Office of the Privacy Commissioner of Canada (OPC) has made great strides in shifting the onus for privacy and data protection from individuals onto corporations and online businesses.[29] However, AI challenges our traditional notions of consent, transparency, and accountability. In fact, in late 2020, the OPC released proposed policy reforms to the *Personal Information Protection and Electronic Documents Act* (PIPEDA) to address the novel (privacy) risks posed by AI.[30] As the report[31] highlights, "aggregated and inferred data about us has become more valuable and poses greater risks than almost any type of personal information shared. Aggregation and inferences are particularly strengthened by AI." Algorithms highlight not just the prevalence of the privacy paradox but its accompanying *information paradox*: algorithms refuse to be known while collecting as much knowledge (data and information) about users as possible since data is the fuel that powers AI.

---

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

[26] Montgomery, K. C., Chester, J., and Milosevic, T. (2017). "Children's privacy in the big data era: Research opportunities." *Pediatrics*, *140*(Supplement 2), S117-S121.

[27] McAleese, S., M., Johnson, and M., Ladouceur. (2020). "Young Canadians Speak Out: A Qualitative Research Project on Privacy and Consent." MediaSmarts. Ottawa.

[28] Livingstone, S. (2018). Time to Rethink Truth and Trust. Retrieved from: www.blogs.lse.ac.uk/medialse/2018/10/08/time-to-rethink-truth-and-trust/

[29] See the OPC Guidelines for Meaningful Consent: www.priv.gc.ca/en/privacy-topics/collecting-personal information/consent/gl_omc_201805/#_seven

[30] Cofone, I. (2020). "Policy Proposals for PIPEDA Reform to Address Artificial Intelligence." Report prepared for the OPC. www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/pol-ai_202011/

[31] Ibid.

MediaSmarts' research[32] [33] [34] [35] has established that youth not only care about privacy, but also put a significant amount of effort into managing their privacy and security online by changing their privacy settings and making use of various privacy strategies such as selecting audiences, limiting screenshots, and negotiating consent with their peers. However, as MediaSmarts' research on privacy and consent highlights,[36] current standards for online consent processes hide information, discourage engagement in the consent process, and allow users to accept terms of service without reading the entire agreement or privacy policies. "This means that most youth continue to be online without much knowledge of how their data is collected and what is done with it."[37] A lack of algorithmic literacy resources for young people—and the trusted adults in their lives, including parents, guardians, and educators—can exacerbate feelings of powerlessness regarding managing online privacy and security. In fact, many of the youth we spoke to in this study expressed a resignation that "they must 'pay to play' and the currency is personal information."[38]

> I feel like a lot of my information is already out there, which I know isn't good... because [corporations] can sell your information to third parties...I feel like I have no privacy sometimes. I guess that's really what my concerns would be. (Hailey, 16)

If you tell a large corporation what you're interested in, at that point, I think it's no longer your personal data. (Logan, 17)

Any information that I give a website, I'm choosing to give that website my information, and kind of allowing them to do whatever they want with it. (Tyler, 16)

In our initial conversations with youth, before we engaged in game-based algorithmic literacy training, they were resigned to what they saw as an acceptable level of

[32] See: McAleese, S., M., Johnson, M., Ladouceur. (2020). "Young Canadians Speak Out: A Qualitative Research Project on Privacy and Consent." MediaSmarts. Ottawa.
[33] Steeves,V., S., McAleese, and K.,Brisson-Boivin. (2020). "Young Canadians in a Wireless World, Phase IV: Talking to Youth and Parents about Online Resiliency." MediaSmarts. Ottawa. www.mediasmarts.ca/sites/default/files/publication-report/full/report_ycwwiv_talking_youth_parents_online_resiliency.pdf
[34] Johnson, M., V. Steeves, L. Regan Shade, and G. Foran. (2017). "To Share or Not to Share: How Teens Make Privacy Decisions on Social Media." Ottawa: MediaSmarts.
[35] Steeves, V. (2014). "Young Canadians in a Wired World, Phase III: Online Privacy, Online Publicity." MediaSmarts. Ottawa.
[36] McAleese, S., M., Johnson, and M., Ladouceur. (2020). "Young Canadians Speak Out: A Qualitative Research Project on Privacy and Consent." MediaSmarts. Ottawa.
[37] Ibid.
[38] Micheti, A., Burkell, J., and Steeves, V. (2010). "Fixing broken doors: Strategies for drafting privacy policies young people can understand." *Bulletin of Science, Technology & Science,* 30(2), 130–143.

privacy loss as a matter of necessity for participation in the online spaces within which they engage.

While there is very little research that looks at how the rapid rise in AI technology[39] impacts young Canadians and their privacy rights, youth have been concerned about surveillance and monitoring since MediaSmarts began conducting research 20 years ago.[40] However, as corporate monitoring,[41] data mining, and information brokering become routine in young people's lives, not only are they more aware of the extent to which such activities occur,[42] [43] but they describe these processes as **weird, scary, unsettling, worrying, concerning,** and above all **creepy.**

[39] Cortesi, S. et al. (2019). "Youth and Artificial Intelligence: Where We Stand," *SSRN Electronic Journal*.
[40] Environics Research Group (2001). "Young Canadians in a Wired World the Students' View." Media Awareness Network. Ottawa.
[41] Corporate monitoring refers to efforts by companies to monitor and track all online or computer-based activities and tasks for example; tracking communications (such as emails and text messages), browser history, or social media posts.
[42] See: Johnson, M., R. Riel, and B. Froese-Germain. (2016). "Connected to Learn: Teachers Experiences with Networked Technology in the Classroom." MediaSmarts/Canadian Teachers' Federation. Ottawa.
[43] Steeves,V., S., McAleese, K.,Brisson-Boivin. (2020). "Young Canadians in a Wireless World, Phase IV: Talking to Youth and Parents about Online Resiliency." MediaSmarts. Ottawa.

From the start, youth were troubled by processes of algorithmic data collection, especially inferred data gathered through machine learning. Almost all participants shared at least one anecdote of a disturbing encounter with algorithms or artificial intelligence. Examples include:

- Unwanted location tracking that sent them ads for local restaurants and services;
- Buying shoes online or looking up prom dresses and being subsequently inundated with advertisements for those same items;
- Talking with friends about a hobby such as axe-throwing and having search engines recommend ads for the activity without having searched for it themselves; and
- News stories or events, such as Brexit and the Cambridge Analytica scandal, that serve as examples of potential algorithmic influence on political outcomes.

Along with their initial concerns about what algorithms knew about them, young people were concerned about how algorithmic recommendations might affect the scope of content available to them and the decisions they are making online.

Algorithmic Imbalances: Bias and Digital Inequality

Algorithms and AI analyze data and make inferences at unprecedented speed and scales through methods shaped by the commercial and political agendas of those (companies) who created them. As a result, the potential for widespread exclusion and discrimination of certain groups and individuals is substantial.[44] "The concern for a world where AI systems are deployed unchecked has raised questions about the impact, governance, and accountability of these technologies."[45] Of particular importance is **concern about how algorithmic design, or its unintended or unanticipated use, can reinforce pre-existing social inequalities**—this unanticipated result is referred to in the literature as **algorithmic bias.**[46] [47] [48] In her book *Weapons of Math Destruction*, Cathy O'Neil analyses how algorithms and machine learning in various fields (including education and advertising) increasingly reinforce pre-existing social inequalities. Similarly, Safiya Noble argues in *Algorithms of Oppression*

[44] Dignum,V., K., Pigmans, S., Vosloo, S. and M. Penagos. (2020). "Policy Guidance on AI for Children." UNICEF, The Office of Global Insight and Policy." *The United Nations Children's Fund.* 1-48. Retrieved from: www.unicef.org/globalinsight/media/1171/file/UNICEF-Global-Insight-policy-guidance-AI-children-draft-1.0-2020.pdf
[45] Ibid
[46] See: O'Neil, C. (2016). "Weapons of Math Destruction—How Big Data Increases Inequality and Threatens Democracy." Crown Books. New York.
[47] Noble, S. (2018). "Algorithms of Oppression—How Search Engines Reinforce Racism." New York University Press. New York.
[48] Perez, C.C. (2019). "Invisible Women: Data Bias in a World Designed for Men." Abrams Press. New York. 1-272.

that algorithms (specifically the Google search algorithm) are discriminatory and reinforce systemic racism.[49]

Algorithmic bias can be found across platforms and can have impacts ranging from inadvertent privacy violations to discrimination based on race, gender, sexuality, and ethnicity. Suppose the data used by algorithms, or to train machine learning, does not sufficiently reflect the varied characteristics of users. In that case, the results may be biased against them.[51] Bias can also enter into algorithmic and AI systems because of pre-existing social, cultural, and institutional inequalities that can impact decisions regarding how data is collected, selected, coded, or used to train algorithms. Furthermore, as noted above, training algorithms on past data or data that was not collected for the specific case can reinforce or amplify historical patterns of systemic bias and discrimination.[52]

For Example: In 2015, Amazon scrapped a recruitment tool that was biased against women candidates. This was because the computer's models were trained on data sets for vetting resumes that reflected male dominance in the tech industry.[50]

Algorithms are "only as good as the data that humans feed them. As their builders are learning, the data used to train deep-learning systems isn't neutral. It can easily reflect the biases – conscious and unconscious – of the people who assemble it."[53]

Participants described a number of situations where they had encountered or were concerned about algorithmic bias. For example, 17-year-old Ethan, who self-identified as a "kid of colour," described his concern—based on his experience with police officers at his school using racial profiling to "look for certain kids"—that racial profiling[54] was going to be regular practice in facial recognition technology. Also of concern to them was how algorithms and AI potentially limit the breadth and depth of content available to users due to profiling and making predictions about individuals, which could confine their possibilities for traversing online spaces. **Young Canadians are well aware that the content on their connected devices is**

[49] Technological bias is not a new issue. Inventions often favour their creators; for example, scissors, can-openers, and ledgers were all created for right-handed people (the majority of users) and had to be later adapted for left-handed users.
[50] Dastin, J. (2018). "Amazon scraps secret AI recruiting tool that showed bias against women." Reuters. Retrieved, from: www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-Scraps-secret-ai-recruiting-tool-that-Showed-bias-against-women-idUSKCN1MK08G
[51] Dignum,V., K., Pigmans, S., Vosloo, S. and M. Penagos. (2020). "Policy Guidance on AI for Children." UNICEF, The Office of Global Insight and Policy." *The United Nations Children's Fund.* Retrieved from: www.unicef.org/globalinsight/media/1171/file/UNICEF-Global-Insight-policy-guidance-AI-children-draft-1.0-2020.pdf
[52] Eubanks, V. (2018). "Automating Inequality: How High-tech Tools Profile, Police, and Punish the Poor." New York: St. Martin's Press.
[53] Vanian, J. (2018). "Unmasking A.I.'s Bias Problem." Retrieved from: www.fortune.com/longform/ai-bias-problem/
[54] According to the Ontario Human Rights Commission, racial profiling is any action undertaken for reasons of safety, security or public protection, that relies on stereotypes about race, colour, ethnicity, ancestry, religion, or place of origin, or a combination of these, rather than on a reasonable suspicion, to single out an individual for greater scrutiny or different treatment. www.ohrc.on.ca/en/what-racial-profiling-fact-sheet

customized to reflect their preferences, and they do not necessarily see this as unfavourable. However, there is a concern[55] [56] that curation based on preference may result in a preference bubble or a recommendation spiral. Preference bubbles, or filter bubbles, refer to instances where the algorithm shows users only what it thinks the user will like, filtering out content the user dislikes. The concern is that these techniques, primarily driven by business interests, can limit a user's online experience and potentially their worldview, freedom of expression, or opinion.[57] Filter bubbles are different from *echo chambers*—environments where a user only encounters information or views that reinforce their own—because they are the result of *algorithmic* filtering.

However, some scholars[58] caution that the impacts of filter bubbles may be overstated. People have always *self-selected personalization* when it comes to finding information, "they've made decisions about what newspapers to buy, what TV channels to watch, and at the same time which ones to avoid."[59] On the other hand*, pre-selected personalization* is the personalization done to people, sometimes without their knowledge, by algorithms. However, we should not assume that pre-selected personalization necessarily narrows people's access to content and, therefore, their worldviews. A study by US researchers[60] found that automation can diversify people's information diets, but this diversity might cause polarization. In other words, as people pay attention to messages from opposing sides, they become more entrenched in their original beliefs[61] and may come to an inaccurate view of how widespread their own views and beliefs genuinely are.[62] Another reason to be cautious of overemphasizing the filter bubble narrative is that algorithms and AI are continually evolving. So, how people access information is also changing. These always-already changing processes pose a challenge for understanding the impacts of algorithmic systems on our ability to access online information. Of utmost importance is that we do not use filter bubbles as a scapegoat explanation for algorithmic bias—preventing us from confronting the deeper, social causes of

---

[55] See: Dignum,V., K., Pigmans, S., Vosloo, S. and M. Penagos. (2020). "Policy Guidance on AI for Children." UNICEF, The Office of Global Insight and Policy." *The United Nations Children's Fund.* Retrieved from: www.unicef.org/globalinsight/media/1171/file/UNICEF-Global-Insight-policy-guidance-AI-children-draft-1.0-2020.pdf
[56] The Algorithmic Literacy Project (2020). "Educational Guide: Diving Deeper into Algorithms." Kids Code Jeunesse (KCJ) and The Canadian Commission for UNESCO (CCUNESCO). Retrieved from: www.algorithmliteracy.org/data/resources/en/Algorithm-Literacy-Education-Guide.pdf
[57] Ibid.
[58] See: Fletcher, R. (2020). "The Truth behind filter bubbles: Bursting some myths." Reuters Institute. The University of Oxford. Retrieved from: www.reutersinstitute.politics.ox.ac.uk/risj-review/truth-behind-filter-bubbles-bursting-some-myths
[59] Ibid.
[60] Bail, C. A., Argyle, L. P., Brown, T. W., Bumpus, J. P., Chen, H., Hunzaker, M. B. F., Lee, J., Mann, M., Merhout, F., and Volfovsky, A. (2018). "Exposure to opposing views on social media can increase political polarization." Proceedings of the National Academy of Sciences, 115(37), 9216.
[61] Fletcher, R. (2020). "The Truth behind filter bubbles: Bursting some myths." Reuters Institute. The University of Oxford. Retrieved from: www.reutersinstitute.politics.ox.ac.uk/risj-review/truth-behind-filter-bubbles-bursting-some-myths
[62] Luzsa, R., & Mayr, S. (2021). "False consensus in the echo chamber: Exposure to favorably biased social media news feeds leads to increased perception of public support for own opinions." Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 15(1), Article 3.

discrimination and inequality in algorithms and AI. Instead, **we need to examine how stereotypes can limit the possibilities available to specific groups** and how profiling and predictive analysis can restrict user's choices to formulaic content easily recognized by algorithms and AI without their knowledge.

Along with concerns about algorithmic bias is the risk that algorithms and AI may exacerbate the digital divide—the gap between those able to benefit from technology and those who cannot. While access to technology remains a risk for digital exclusion, since the areas with the most robust digital infrastructure and data will be the first to reap the benefits of algorithms and AI,[63] digital inequality scholarship emphasizes the importance of including "skill differences in understanding who gets to benefit most from their internet use."[64] In the case of digital literacy and skills, MediaSmarts' research[65] echoes what is stated in other studies: that "individuals who are more highly educated or who, in the case of children and young adults, have parents who are more highly educated, tend to possess greater levels of skill."[66] These discrepancies in digital literacy (and access) mean that algorithmic literacy remains the exclusive domain of a select few users. In the case of young Canadians, we learned that this is typically for students attending a highly specialized technical STEM (science, technology, engineering, and mathematics) education program. However, **algorithmic literacy is crucial for all users to actively engage with algorithms and AI—to take more control over their privacy and data and better understand and contest the unequal consequences of algorithmic systems.**

Advancing Algorithmic Literacy

Insufficient knowledge of AI and algorithms contributes to exclusion from online spaces, tech-facilitated discrimination, exposure to harmful content, and various privacy risks. "Every day there are new, creative ideas on how businesses can derive more profit from our personal information,"[67] and it is becoming increasingly difficult for individuals to "demystify complex business relationships and complicated algorithms to make informed choices."[68] This is especially true of children and youth who are often the target audience for new AI and algorithm-based technologies, apps, and platforms. Given that young people "are growing up in a world surrounded by AI," we need more robust algorithmic literacy tools, resources, and programmes

[63] ITU (2018). "Module on Setting the Stage for AI Governance: Interfaces, Infrastructures, and Institutions for Policymakers and Regulators." Retrieved from: www.itu.int/en/ITUD/Conferences/GSR/Documents/GSR2018/documents/AISeries_GovernanceModule_GSR18.pdf
[64] Klawitter, E., and Hargittai, E. (2018). ""It's like learning a whole other language": The role of algorithmic skills in the curation of creative goods." International Journal of Communication, 12, 3490-3510.
[65] Brisson-Boivin, K. (2018). "The Digital Well-Being of Canadian Families." MediaSmarts. Ottawa.
[66] Klawitter, E., and Hargittai, E. (2018). ""It's like learning a whole other language": The role of algorithmic skills in the curation of creative goods." International Journal of Communication, 12, 3490-3510.
[67] Office of the Privacy Commissioner of Canada. (2018). "The strategic privacy priorities." Retrieved from: www.priv.gc.ca/en/about-the-opc/opc-strategic-privacy-priorities/the-strategic-privacy-priorities/
[68] Ibid.

to help them become "more critical consumers," to maintain control of their personal information, and "motivate them to help shape [the] future" of this technology.[69]

Algorithmic literacy does not only refer "strictly to being able to read and write in code" but also involves "being aware of the presence of algorithms… and the increasing role they play, both for good and for bad."[70] Building a "fundamental vocabulary" so youth can both understand and shape algorithms[71] empowers them "to exercise critical thinking in how they engage online, and to become proactive, creative users and makers rather than passive consumers."[72] The youth we spoke to for this project expressed both a need and a desire for algorithmic literacy:

> When it comes to algorithms and codes, I think that many kids should at least have a chance to learn it… I think that most schools should at least have an option to provide that kind of learning… some kids might find a new interest in it. (Ethan, 17)

I think it would be a useful thing. Perhaps just like a one-day course, and if people are actually interested in finding out more, they could pursue it a bit. But I think it is useful, especially in the [digital] age. (Andrew, 15)

Yeah. I definitely wish that we could understand more what is going on because technology is kind of taking over our lives, but we don't know about it. (Nicole, 14)

I mean, I even learned so much tonight that I didn't know before, and I definitely think it would be super valuable to be learning in schools. (Erin, 17)

We have come across a few algorithmic literacy projects designed for youth. The first one is a Canadian initiative called ***The Algorithmic Literacy Project*** and is a

---

[69] Hao, K. (2019). "Kids are surrounded by AI. They should know how it works." Retrieved from: www.medium.com/mit-technology-review/kids-are-surrounded-by-ai-they-should-know-how-it-works-ae15756f1085
[70] Oldridge, M. (2017). "Algorithmic Literacy." Medium. Retrieved from: www.matthewoldridge.medium.com/algorithmic-literacy-1d9b5f087142
[71] Waters, J. (2020). "The Canadian Primer to Computational Thinking and Code: A Kids Code Jeunesse Introduction to Algorithmic Literacy." Kids Code Jeunesse. Retrieved from: www.algorithmliteracy.org/data/resources/en/KCJ_Computational_Thinking_Primer_EN.pdf
[72] Kids Code Jeunesse & CCUNESCO. (2021). "The Algorithm Literacy Project." Retrieved from: www.algorithmliteracy.org

partnership between Kids Code Jeunesse and the Canadian Commission for UNESCO.[73] The project aims to make youth "algorithm literate" as "they are emerging as digital citizens and future decision-makers in a world where they'll need to learn how to protect their data and use technology responsibly."[74] Their website provides discussion guides, educational guides, primers, and resources for families to learn about algorithms, AI, and coding together.

AI4ALL is another initiative based in the United States, a non-profit "dedicated to increasing diversity and inclusion in AI education, research, development, and policy."[75] *AI4ALL's* education efforts include summer programs for high school students, a college pathways program that provides for experiential learning opportunities, and an open learning program that "empowers high school teachers of all subjects to bring AI education to their classrooms through a free, adaptable AI curriculum and teacher resources."[76]

A third initiative, the ***AI and Children*** policy project at UNICEF focuses strongly on children's rights and brings together international experts to "develop a draft policy guidance on promoting children's development in AI strategies and practices."[77] While not a direct service initiative, this policy project provides essential insight and direction for adults who are responsible for "protecting and upholding child rights in an evolving AI world."[78] Public consultation with researchers, non-profit organizations, international organizations and governments contributed to important requirements and recommendations for developing child-centred AI, including involving parents and educators, considering the different realities of children, and including children and youth in decision-making processes.[79]

These three initiatives demonstrate that advancing algorithmic literacy and improving our capacity to protect and uphold child rights online is a priority internationally. Not only will teaching children and youth about algorithms and AI better prepare them for careers in technology, it will also give them the knowledge and tools required to protect themselves and their information in digital spaces.

[73] The United Nations Educational, Scientific and Cultural Organization.
[74] Kids Code Jeunesse & CCUNESCO. (2021). "The Algorithm Literacy Project." Retrieved from: www.algorithmliteracy.org
[75] AI4ALL. (2021). "Our Story." Retrieved from: www.ai-4-all.org/about/our-story
[76] AI4ALL. (2021). "Open Learning." Retrieved from: www.ai-4-all.org/open-learning
[77] UNICEF. (2020). "AI for children." Retrieved from: www.unicef.org/globalinsight/featured-projects/ai-children
[78] UNICEF. (2020). "Policy Guidance on AI for Children." Retrieved from: www.unicef.org/globalinsight/reports/policy-guidance-ai-children
[79] UNICEF. (2020). "AI Policy Guidance: How the world responded. Retrieved from: www.unicef.org/globalinsight/stories/ai-policy-guidance-how-world-responded

Conversations with Young Canadians about Artificial Intelligence and Privacy

The purpose of this project was to develop a prototype for an interactive, educational game that can be used to build awareness among children and youth about artificial intelligence, algorithms, and privacy. This game prototype catalyzed discussion and reflection on how youth interact with AI in their day-to-day lives and how it impacts their experiences with digital technology, their movement through the online world, and their privacy – both online and offline.

The following research questions guided this project:

- How do youth in Canada understand the relationship between artificial intelligence, algorithms, and privacy?

- How do youth interact with AI in their day-to-day lives, and how do they understand the implications of AI and algorithms on their privacy online?

In answering these questions and testing the game prototype in a series of eight focus groups with 22 youth participants, we have confirmed the need and desire for additional algorithmic literacy resources among young Canadians along with a series of other recommendations calling for more awareness, transparency, protection, control, and engagement.

Research Method

From November 2020 to January 2021, we conducted **eight focus groups with 22 young people ages 13 to 17**. Participants were recruited via social media, a departure from our usual process due to the COVID-19 pandemic. We shared the recruitment poster and project information on MediaSmarts' social media accounts and those of our community partners, including Youth Services Bureau (Ottawa), YWCA Canada, Boys and Girls Clubs of Canada, and Carleton University's Department of Sociology and Anthropology also agreed to distribute materials via their social networks.[80]

The focus groups, which ran for approximately two hours each, allowed participants to reflect on how they interact with artificial intelligence and algorithms in their day-to-day lives. Qualitative research methods, like focus groups, "are the most appropriate for gaining an in-depth understanding of how people perceive algorithms."[81] We wanted to know what young Canadians knew about how algorithms work and what they understood about the implications of artificial intelligence and algorithms on their privacy and data security. Each session began with a review of key terms and concepts[82] followed by icebreaker questions to gather some baseline knowledge:

1. What is an example of an algorithm you have seen in the past week?
2. How would you explain how algorithms work?
3. Do algorithms use your personal data/information? If so, how do you think they are using this information?
4. Do you have any privacy or data collection concerns when it comes to algorithms?

After this opening discussion, participants played a game facilitated by MediaSmarts' Director of Education and our Media Education Specialist. The game, ***#ForYou***, is a prototype designed by MediaSmarts specifically for this research project and intended to help children and youth learn more about artificial intelligence, algorithms, and online privacy and data security. A scaffolded learning experience (outlined below) allowed for an in-depth discussion with participants after each of the three phases or rounds.

With participant permission, the focus group discussions were audio-recorded and transcribed for analysis. We removed all identifying information from the transcripts

[80] This project received ethics approval from Carleton University's Office of Research Ethics. Project #114440.
[81] Klawitter, E., and Hargittai, E. (2018). ""It's like learning a whole other language": The role of algorithmic skills in the curation of creative goods." International Journal of Communication, 12, 3490-3510.
[82] All participants were provided with a Glossary that included key terms like algorithm, artificial intelligence, bias, data broker, and machine learning.

to safeguard participant anonymity. For the same reason, participants are identified only by pseudonym and age in this report.[83]

Pandemic Pivot

The COVID-19 pandemic presented many challenges for conducting research in 2020. In terms of recruitment and engagement with participants, a **pandemic pivot** was essential for qualitative research projects given the new public health and physical distancing guidelines.[84] Our initial plan to play a card game in person with 10-12 youth participants had to be adapted quickly, given these circumstances.

First, **we had to adapt our recruitment strategy** (outlined above). While recruiting online via social media was a new approach for MediaSmarts, it did allow us to increase our reach. Instead of only meeting with youth who live in Ottawa, we connected with participants from across Ontario, Alberta, and British Columbia. All project consent forms were sent via email and signed electronically by participants (and parents/guardians when required).

Second, **we had to adapt our gameplay.** Initially, MediaSmarts' education team designed the #ForYou game prototype to be played in person. After working with a graphic designer to create the cards for the game, the research team decided to shift to Roll20, a "virtual tabletop" where participants could create a free account and were not required to download or install any additional software to participate.[85] We also offered to create player accounts and provide login details for participants who did not wish to register themselves.

Finally, **we had to facilitate the focus groups via Zoom** – a platform we chose because of familiarity, ease of use, and recording capability.[86] Like other researchers, we quickly noted the benefits and drawbacks of shifting from an in-person model to facilitating focus groups online.[87] [88, 89] For us, the benefits included connecting with young people outside of Ottawa, eliminating travel time, and the ability to

---

[83] See Appendix A for more information about participants and focus groups.
[84] Centre for Critical Qualitative Health Research. (2020). "Considerations for Conducting Qualitative Health Research During COVID-19 at the University of Toronto." Doing Science Differently. Retrieved from: www.ccqhr.utoronto.ca/2020/08/10/considerations-for-conducting-qualitative-health-research-during-covid-19-at-the-university-of-toronto/.
[85] Roll20. (2021). www.roll20.net. We chose this platform because of its popularity among gamers and because of its simplified and accessible privacy and consent policies.
[86] All participants were notified via consent forms and again at the start of the focus groups that the sessions would be recorded. We clarified that we were only keeping the audio recording for transcription purposes but that participants were not required to have their cameras on if they did not feel comfortable.
[87] Dos Santos Marques, I.C. et al. (2020). "Implementation of Virtual Focus Groups for Qualitative Data Collection in a Global Pandemic." The American Journal of Surgery.
[88] Dodds, S. and A. C. Hess. (2021). "Adapting Research Methodology during COVID-19: Lessons for Transformative Service Research." Journal of Service Management 32 (2), 203–17.
[89] Hinkes, C. (2020) "Conducting Focus Groups in a Global Pandemic." International Journal of Social Research Methodology. 1–7. Thank you to Chloe Martin for her research assistance for this section of the report.

communicate and record additional information using the chat function throughout the focus group sessions. Drawbacks included a lack of non-verbal communication (as many participants chose to keep their cameras turned off), connectivity issues (which sometimes resulted in inaudible contributions), and difficulty collaborating during gameplay – something we anticipate would have looked much different had we been able to meet in person.

Despite these challenges, our experience facilitating online focus groups was a success. We will take lessons learned forward with us in subsequent research projects, especially since we anticipate the continued practice of conducting qualitative research in online spaces.

#ForYou

The game prototype for ***#ForYou*** was designed by MediaSmarts' Director of Education and our Media Education Specialist. ***#ForYou*** is a card-based pattern-matching game that helps children and youth understand the role that algorithms play in their online and offline lives and the value of their personal information to companies that use algorithms. The game primarily focused on recommendation algorithms, as they are the variety that young people encounter most often, but players also learned about other forms of sorting and predictive algorithms. The game was designed to be played collaboratively, with several players representing video or content makers and one player representing The Platform.[90]

#ForYou is a game comprised of three phases:

1. The Popularity Phase: Players try to solve The Platform's algorithm to get their video as widely viewed as possible.

2. The Advertising Phase: Players draw on user data to solve the algorithm to get their advertisements seen by the right audience.

3. The Machine Learning Phase: Players repeat the gameplay of the advertising phase, with the addition of proxy data and data brokerage.

[90] During the focus groups, the Director of Education played the role of the Platform to provide the participants with a consistent experience.

Each round is played with various cards, including Optimization Cards, Algorithm Cards, Boost Cards, Video Cards, Ad Cards, Audience Cards, and Data Cards.

At the beginning of each phase, players were introduced to different terms, concepts, and processes such as *recommendation algorithms*, *personal information*, *information brokers*, and *proxies*. This real-time learning, coupled with discussion questions between each round, allowed participants to reflect on their own experiences with algorithms and artificial intelligence and think more intently about privacy implications. Examples of discussion questions asked after each phase of gameplay are listed below:

Popularity Phase Debrief

- Do you think the way an algorithm is designed affects how much time we spend on a platform?
- Do you think an algorithm that recommends similar content might lead to a spiral? Is this a good thing or a bad thing? Why?
- Is it up to you or the platform to make sure the content you see is appropriate? Why?

Advertising Phase Debrief

- Why do you think it is more valuable for an algorithm to use information about you rather than information about what you have done on a platform?
- Do you think it is fair for a platform to base a recommendation on what the algorithm thinks it knows about you to target content to your friends and vice-versa?
- Do you think it is fair that what you do on one platform may affect what you see on another?

Machine Learning Phase Debrief

- How did you feel linking ads through proxies like race, sexual orientation, or gender?
- Do you think a platform has a responsibility to make sure its algorithms are not prejudiced or biased?
- Would you want to know why you were recommended something online?
- Is this your first time learning about algorithms? Do you learn about algorithms or artificial intelligence in school? At home? Do you want to learn more?

This **interactive and scaffolded focus group** format (introduction – gameplay – discussion) proved to be a generative approach to research on algorithms, AI, and privacy. We outline the insights and experiences shared by youth participants throughout this scaffolded, game-based learning and discussion process in the remainder of this report.[91]

[91] Refer to Appendix B for screenshots of the #ForYou gameplay on the Roll20 platform.

Algorithms Among Us

In the first phase of gameplay, we invited players to imagine themselves as content creators for a popular video-sharing site. We introduced participants to the idea of optimization, represented by five Optimization cards:

- **Stickiness:** using an algorithm to make sure that users keep watching videos instead of leaving the platform;
- **Watch time:** using an algorithm to try to make users spend as much time watching videos as possible;
- **Virality:** using an algorithm to try to make users share the videos they watch with as many people as possible;
- **Engagement:** using an algorithm to get users to like, comment on, and reply to as many videos as possible; and
- **Daily use:** using an algorithm to make sure that users return to your site as frequently as possible.

Participants also learned about the factors that a recommendation algorithm might consider in deciding how much to boost a video, such as recency (referred to as "freshness" in the game), the number of interactions (likes vs. dislikes), views (to date), shares, and subscribers. Scoring was weighted[92] to demonstrate that algorithms do not consider all of these factors with equal importance, and based on their scores, the participants tried to guess which three algorithm cards (the factors) the platform player placed in what order for the round.

Players played two rounds of the game in this first phase. In the second round, players could artificially boost their videos by playing a card used to describe how content creators and platforms try to 'game' the algorithm by artificially increasing one of the factors listed above. Boost cards included hidden pop-ups,[93] retweet rooms,[94] like farms,[95] Google bombs,[96] sock puppets,[97] and controversy.[98] In addition to playing boost cards, participants could also play any additional video cards with the same topic (e.g. sports, reviews, music, etc.) as the cards already on the table;

[92]Three algorithm cards are selected per round. Each match with the first algorithm card is worth three points, each match with the second is worth two points, and each match with the third is worth one point.
[93] Hidden pop-ups open an ad or video in a new window without telling you. Doubles the views score for the video it's played on.
[94] Retweet rooms are groups of accounts that all share each other's posts, making them look briefly more popular. Doubles the freshness score on the video it's played on.
[95] Like farms are groups of accounts or devices used to fake likes on a video. Doubles the like score for the video it's played on.
[96] Google bombing is making misleading websites to control what shows up in a Google search for a word. Doubles the links score for the video it's played on.
[97] A sock puppet is a fake account used to make it look like someone follows or agrees with you. Doubles the subscribers score for the video it's played on.
[98] Videos and posts that are controversial get a lot more reactions than ones that aren't. Doubles the Shares score for the video it's played on.

this simulated the most basic form of algorithmic recommendation, in which content similar to what was just watched is recommended.

As they played this first phase of the game, participants saw how algorithms use various factors to sort, select, and filter content. The observations and discussions following this first phase of gameplay mainly centred on how recommendation algorithms impact online experiences and environments.

Algorithmic Architecture: The Environment

After this first phase of gameplay, youth quickly pointed out how algorithms impact the spaces and places within which they engage. Specifically, the breadth and depth of content available to them and how the pressure to optimize for recommendation factors (such as likes, shares, and subscribers) impacts the quality of this content. Participants explained that there were instances when they felt algorithmic *pre-selection* was advantageous, like when watching videos for fun, looking for how-to or tutorial videos, or researching a specific topic for a project. Hailey (16) gave the example of how she uses YouTube exclusively for sewing tutorials, and the videos are "all right there, I don't have to search for something to do which is helpful."

However, participants also highlighted what they see as a concerning tension: that while their connected devices have the potential to provide them with the world at their fingertips, algorithms are narrowing their access to the online world. Participants of all ages described an algorithmic content narrowing effect through which youth see an **excess, overload, or saturation** of *similar* content. For example, Jacob (14) explained how he felt he had learned all he needed to know after watching one video about a specific quest in a video game. But, after viewing that one video, he got "tons of videos with the same content," which were just "useless," and it was "annoying" because he already knew what to do. Madelyn (14) agreed, emphasizing "it's hard to get [similar] content off your recommended videos and maybe you don't want that content anymore…and you can't find a way to find those [different] videos."

> You get sick and tired of the content; it's [the algorithm] like, 'Oh, you like this? Take *every* single bit of information!' (Conor, 15)

The content saturation that youth described in our discussions was not surprising given that recommendation algorithms always prioritize similar content, and users typically resort to the default architectures of the apps, platforms, or websites they use and access. In fact, 70% of YouTube views

come through the recommendation engine (the 'up next' sidebar),[99] and 50% of Google searches are 'zero-click searches,' meaning users do not click on *any* search hits but remain on the results page.[100]

After playing the first round of the ***#ForYou*** game, participants demonstrated a stronger awareness of algorithmic architectures (especially default settings) and a keen sense for recognizing when content creators or platform designers were manipulating the online environment to game the algorithm and reach peak optimization. Trends and hashtags[101] were the primary examples used by participants to describe how attempts to boost recommendation factors impacted the quality of the content they could access online. Charlotte (16) gave an example of how video creators often tailor their content to what they think the algorithm is optimizing for:

> *Among Us*[102] is huge right now, and YouTube creators are making *Among Us* videos because it's really popular right now…and they want to appeal to the masses…because they just want views and people are going to watch what is interesting right now so [creators] have to be able to adapt to that.

Nathaniel (17) agreed:

> YouTubers were all playing [*Among Us*] to try to bank off the algorithm promoting that game specifically.

Participants, like Charlotte and Nathaniel, were able to make connections between the content saturation they were witnessing and the content creator's strategies of using trends as a way to try to boost views, likes, and shares and optimize for stickiness, watch time, virality, engagement, and even daily use. Participants also pointed out how strategies to optimize algorithms "cycled" across platforms:

> There's an expression I've heard that the internet is basically three websites posting images of each other, which is fairly accurate. Whatever gets popular on YouTube gets popular on Twitter, and whatever gets popular on Twitter inevitably leaks into YouTube or Reddit or *everything*. (Logan,17)

Participants described how trends and trending topics moved seamlessly across platforms through algorithmic architectures, saturating these spaces with trendy 'attention grabbers.' Participants were also aware that trending topics are evolving

[99] Jaffari, A. (2019). "How the YouTube Algorithm Works (Or Why Your Videos Aren't Getting Views)." Shopify Social Media Blog. Retrieved from:www.shopify.ca/blog/youtube-algorithm
[100] Longtail UX (2019). "Google's Hogging Half Your Traffic: How to Get It Back." Search Engine Journal. Retrieved from: www.searchenginejournal.com/googles-hogging-half-your-traffic-how-to-get-it-back/341831/
[101] A hashtag is a word or phrase preceded by a hash sign (#), used on social media websites and applications, especially Twitter, to identify digital content on a specific topic.
[102] Among Us is an online multiplayer social deduction game developed and published by the American game studio Innersloth.

since, as Nathaniel (17) explained, trends come and go, so users will not likely see the same thing forever. However, the use of trends remains a key boosting strategy. So while the content of the trend may change, youth are still seeing trending topics, hashtags, and content-with-the-most-engagement at the top of their feeds.

Participants also described situations where they had seen bots (or AI) generate controversy or content creators share dangerous or violent content as boosting strategies. Participants gave examples, including videos of snowboarding stunts, '1000 degree knives,'[103] and depictions of self-harm and suicide.[104] According to participants, reactions to videos like this have resulted in changes to the content they see and ultimately changes to the architecture of online spaces. For example, Sahil (15) described how platforms are now engaging in more thoughtful content curation or take-downs, and Charlotte (16) explained how platforms are including warnings or cautions, particularly for content that provides for political or health and science information – especially in the case of COVID-19.

> There is a little black bar under the pictures, and it leads you to a website with [reliable] information, or it will warn you if there is misleading information in the video. (Charlotte, 16)

Participants expressed a particular concern when algorithmic content narrowing or saturation generated what youth say is a false sense of social consensus on the platform.

> My concern is that certain ideas or certain topics are exaggerated by these boosters and… even though people aren't into the topic, they will see it on a trending page… and they will keep clicking it, and that will exaggerate how much people are actually interested in that [topic]. (Andrew, 15)

Participants were particularly concerned when a false sense of social consensus was generated for political topics, such as elections, or issues with negative social consequences, such as climate change or flat earth theories. Logan (17) described this as "prioritizing trends over actual information."

Participants were aware of the impacts of algorithms in their online environments, and they were frustrated by a sense of powerlessness to change this algorithmic architecture.

[103] Videos where creators heat knives with blow torches and cut things.
[104] One participant cited the case of Logan Paul, who filmed the corpse of a man who had hanged himself and then posted it on his YouTube channel. After a few days of promotion, the video was removed by YouTube for violation of the platform's terms of use.

> There's not much that can really happen when it comes to what you see on the internet because it's being controlled by someone else. (Ethan, 17)

Participants were also troubled about what they were missing as a result of content narrowing or saturation. Having heard some of their peers describe their experiences with recommended content, participants grew concerned that the content saturation they were seeing was *different* from the content saturation their peers were seeing. While algorithmic pre-selection was seen seen favourably because it provided participants with unique content for *them* – – based on their preferences (or interests) and their online interactions (what they do online) – they also worried that "we don't even know what we are missing out on" (Ethan, 17).

Youth did appreciate and enjoy algorithmic content curation in particular contexts: when it made their searching more efficient, and when it provided them with relevant and easily accessible content. **However, they expressed frustration with the filtering effects of algorithms and AI because it constrained their ability to navigate online spaces and limited the breadth and depth of content they could explore.** Youth were especially displeased with how algorithms and AI were also attempting to influence their behaviour and agency.

Algorithmic Influence: The Experience

When it came to their online experiences, discussions of content narrowing came up again, but this time concerning how participants felt they were being sucked into endless feeds. We explained that this experience was called a **content spiral** (or recommendation spiral) and refers to getting caught up in a seemingly infinite loop of algorithmically-recommended online content. These spirals typically start with content such as a YouTube video and lead the user to spiral from topic to related topic, potentially losing track of time. Almost all of the participants responded with an anecdote of how recommendation algorithms, particularly those optimizing for watch time and stickiness, resulted in a content spiral for them. Participants described these spirals as '**mindless scrolling**,' '**boredom**,' '**rabbit holes**,' and '**focus thieves**.' More importantly, participants differentiated between *passive* uses of the internet that resulted in spirals versus *active* uses that avoided spirals, including '**surfing vs searching**' and '**procrastination vs productivity**':

> Especially for Instagram and YouTube, they have an algorithm deciding what content to show you... to keep you there in the moment, so it can keep you online... or make you want to stay online for way longer. (Nathaniel, 17)

If the algorithm is really good, you can go down a rabbit hole… and that will make you spend a lot of time [on the platform]. (Charlotte, 16)

I think they *want* to keep you on there for a long time. (Nicole, 14)

> [Platforms] are trying to reel you in. I spend a lot of time scrolling, and I don't even realize all the time that's gone by until I look at the clock, and I'm like, 'Oh my goodness, I just spent an hour scrolling through social media.' (Erin, 17)

Participants were aware that algorithmic pre-selection was pushing them towards more passive uses of the internet. They were also aware that content creators were using optimization strategies to influence their behaviour, something participants found to be incredibly aggravating. Here, most participants described clickbait content (or an Easter egg), which is text or a thumbnail designed to attract attention and entice users to follow the link and read, view, or listen to the content that ends up being either misleading or sensationalized.

On YouTube, the family blog channel… it would have the most insane things happening in the thumbnail—it would be a kid falling off a bannister, or a pool full of gummy worms, and in a thirty-minute video, there would be a two minute part sort of related to the thumbnail. (Nathaniel, 17)

Especially on YouTube, it's like 'we BLEW UP our house,' but it's one firework in the backyard, and you're really disappointed, but then it makes you want to go search for more of that stuff, so it keeps you locked in. (Hailey, 17)

Participants saw clickbait[105] as pure attention-grabbing content. They did not like being '**duped**,' '**scammed**,' and '**manipulated**' by this content which admittedly had them coming back for more, hoping that they would see something unique or exciting.

Participants were also aware that algorithms could train users to return to online spaces regularly or habitually, making passive or what they called 'mindless' online engagement a part of their everyday experience.

[105] Major platforms like Facebook have adjusted their algorithms, or are using AI and machine learning, to reduce the reach of clickbait content on the platforms; however, our conversations with youth indicate that clickbait is still a predominant issue when it comes to recommended content.

> Once we watch a recommended video, we stay on the platform for a long period of time and then the next day, we spend time on that platform. We go back, watch more videos. It keeps cycling. (Jacob, 14)

> When you are there for a long time, you become attached to the site, so it becomes... more part of your routine. (Sahil, 15)

However, regular or daily engagement also highlighted how algorithmic accuracy is 'weird' and 'creepy.' As Kate (16) explains, "it's weird that it [the algorithm] does that [recommends accurate content] almost every time." In some cases, participants described being thrown a curve-ball by the algorithm where for example, it tried to recommend they watch something they would not normally engage with to broaden the number of videos the algorithm could recommend. However, participants thought this could backfire if algorithms went 'off the script' and somehow 'messed up the formula.'

Following this first phase of gameplay, participants demonstrated an awareness of algorithmic opacity; they were aware that algorithms were influencing their behaviours, and they knew *why* but could not fully explain *how* this was happening. Most participants pointed to the effects of monetization and corporate business models:

> Time is money, right? If they steal away as much of your time as possible, then they are almost literally stealing from you. (Tyler, 16)

Participants felt content creators, even those following trends or using manipulative tactics, were doing 'what they had to' under these constraints. Logan (17) estimated that 90% of user content creation involved figuring out the algorithm, including drawing people in through clickbait. **Participants were resigned to the fact that algorithmic environments and algorithmically-generated experiences created a feedback loop of mostly low-quality, over-saturated, pre-selected content.**

Both content narrowing and passive engagement have important implications for the agency of users, particularly young users, to shape algorithmic systems. For example, participants explained how, when searching for information, they had to more consciously engage as active users rather than passively accepting recommended content. As Nathaniel (17) explained, since "everything we are being shown is related to some trend," when conducting research for an assignment, he has to actively *avoid* trends and search more consciously for accurate information. Many participants echoed this sentiment, explaining that they try their best to exercise their agency, especially when searching for information since recommendation algorithms produced an excess of *trendy* information rather than reliable or trustworthy information. While participants were surprised and 'creeped-out' by the accuracy of algorithmically recommended entertainment content, they were

skeptical of an algorithms' ability to present them with accurate information about news content.

Trust, Responsibility, and Control

After the first phase of gameplay, participants were **already calling for algorithmic transparency** so that they could better understand *how* content was being recommended to them and, as a result, how algorithms were impacting their online environments and experiences. While participants did not like being '**duped**,' '**scammed**,' or '**tricked**' by content creators, creators also played a role in demystifying algorithms for young people. For example, Nicole (14) explained how TikTokers sometimes leave messages at the end of their videos telling viewers to 'share, copy, link,' highlighting the factors that will help boost their videos in the recommendation algorithm. However, participants expect more transparency from platforms so that they may better understand the relationship between the platform's goal(s) for optimization and the factors they consider in reaching that algorithmic optimization.

Participants felt a tension between the way algorithms frequently recommended "outrageous" content such as conspiracy theories (which eroded their trust in platforms) and what they saw as the value of algorithms filtering out inappropriate or low-quality content (a process that builds trust in platforms). For example, participants saw advantages in using algorithms to restrict or filter content, especially for younger children and even commented on regulations restricting 'Easter eggs'[106] for kids. In fact, some participants identified that YouTube Kids was a result of platforms having to address regulations, specifically the Children's Online Privacy Protection Rule (COPPA) in the United States. Echoing findings from previous MediaSmarts research,[107] [108]participants differentiated between the needs of younger children and those of older youth.

Participants explained that children needed technical fences to keep them from accessing inappropriate content and that children were at a higher risk of being sucked in by content spirals. However, these protective factors for children were seen as barriers for older teens and youth to exercise their agency in online spaces. **Participants were clear that platforms, users, and, in the case of young children, parents all have a role to play when it comes to algorithmic responsibility.** Younger participants (ages 13-14) were more likely to discuss the role of parents as

[106] Similar to clickbait, an Easter egg is a term used to describe a message, image, or feature hidden in a video game, film, or other, online medium.
[107] Steeves,V., S., McAleese, and K.,Brisson-Boivin. (2020). "Young Canadians in a Wireless World, Phase IV: Talking to Youth and Parents about Online Resiliency." MediaSmarts. Ottawa.
[108] McAleese, S., M., Johnson, M., Ladouceur. (2020). "Young Canadians Speak Out: A Qualitative Research Project on Privacy and Consent." MediaSmarts. Ottawa.

gatekeepers (blocking and controlling children's access to connected devices and specific sites and apps), rule setters (making sure kids weren't spending too much time on devices) and educators (helping kids develop their algorithmic literacy to learn more about the influence of algorithms in their lives). Most participants were quite clear about the ethical responsibility that platforms have to ensure that younger users do not see inappropriate content. But, as Logan (17) explained, while platforms have to take responsibility for the content they are sharing, it's up to users to "tell them to do that" – to hold them accountable.

Most participants expressed a desire to translate what they were learning through gameplay into more active and **critical digital media engagement.** Part of building that critical engagement, particularly for young users, is raising their awareness about the effects of algorithms specifically as they shape online environments and potentially influence user behaviour. Since the vast majority of users (95%)[109] do not adjust the default settings on platforms, awareness and knowledge building is a powerful component of algorithmic literacy that can address young people's feelings of powerlessness and **increase their capacity and agency to influence algorithmic design and decision making.**

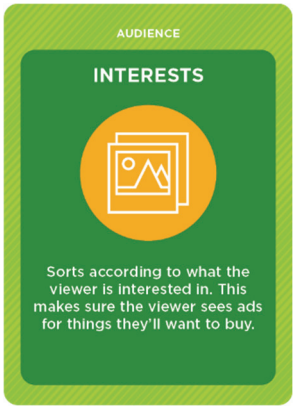
[109] Arthur, C. (2013). "Why the default settings on your device should be right the first time." The Guardian. Retrieved from: www.theguardian.com/technology/2013/dec/01/default-settings-change-phones-computers

Under the Algorithm's Lens

In the first phase of gameplay, participants focused on the objective of having their video reach the *most* people. They did so by trying to guess which factors (e.g. views, likes, shares) the recommendation algorithm considered to be most important for to reach peak optimization (e.g. stickiness, engagement, virality). Having established these basics regarding algorithmic optimization and the factors recommendation algorithms might use to boost video content, we added a new layer of complexity: monetization.

In the second round of gameplay, we introduced participants to the idea of monetizing their videos by including ads.[110] To make this explicit, participants were told that to earn advertising revenue content creators must ensure that their content (and the accompanying ads) reach and resonate with not just the *most* people but also the *right* people. This monetization process involves gathering and analyzing data about the people watching their videos. In this round of play, the algorithm is made up of three audience factors, each of which represents an aspect of the audience that the advertiser would like to reach:

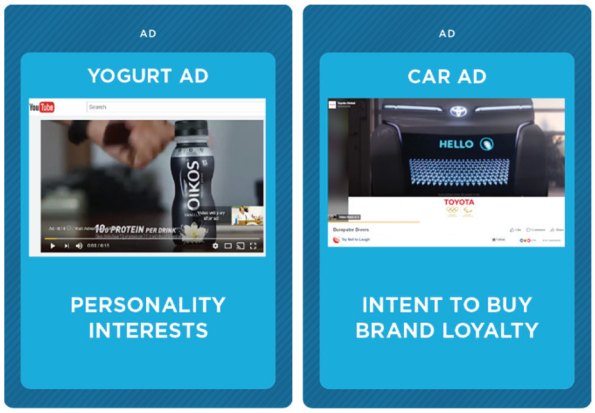
- **Age:** viewers who are of the right age to be interested in the product;
- **Intent to Buy:** viewers who are actively looking to buy the product;
- **Interests:** viewers whose interests suggest they might want to buy the product;
- **Brand Loyalty:** viewers with an established loyalty to the brand (or not wasting money on viewers with an established loyalty to a competing brand);
- **Personality:** viewers whose personality profile suggest they might want to buy the product;
- **Location:** viewers in an appropriate place to buy the product; and
- **Income:** viewers whose income matches the appeal of the brand (high for luxury brands, low for budget brands, etc.).



As in the first phase, The Platform player weighted these factors[111] to demonstrate that algorithms do not consider them all with equal importance.

[110] MediaSmarts' research has shown that young Canadians often do not understand how the online platforms they use or the content creators featured on them make money, or how their personal data was of value to those platforms. See: Johnson, Matthew, Valerie Steeves, Leslie Regan Shade and Grace Foran. (2017). To Share or Not to Share: How Teens Make Privacy Decisions on Social Media. Ottawa: MediaSmarts.
[111] Three algorithm cards are selected per round. Each match with the first algorithm card is worth three points, each match with the second is worth two points, and each match with the third is worth one.

Participants again played two rounds of the game. In the first round, players each placed a single Ad card and received a score from The Platform player. Based on their scores in the first turn, participants then tried to guess which three audience cards the platform player had placed and in what order.



In the second round, players could draw on Data cards to increase their score and solve the algorithm. Data cards represent a source of information about users, such as their search history, interactions on a platform, IP address, previous purchases, profile information, and GPS signal, that allow the video and ad to be targeted to the correct audience. Within the game, Data cards allow an ad to be targeted to one of the audience factors listed above, doubling its value. For example, a "search history" card targets "intent to buy" (because a user's search history can show whether or not someone is actively interested in buying a product) and can be played on any Ad card with "intent to buy" as a factor.[112]

As they played the second phase of the game, participants saw how algorithms collect, analyze, and make inferences about user information. The observations and discussions following this phase of gameplay centred on the value of personal information for algorithmic systems and the corporate uses of data and personal information.

Algorithmic Accuracy: The Value of Personal Information

After this second round of gameplay, youth understood the connection between the value of personal data in targeting user content and monetization. Participants were acutely aware that accuracy is vital if platforms want to generate revenue through advertisements and, more importantly, that accuracy required information about users. Without accurate user information, platforms run the risk of wasting time and money targeting the wrong people.

> If they [platforms] are recommending a really expensive hair dryer, but you're 12 years old, and you have no job, that doesn't make any sense because you can't afford it. But if [the algorithm knows] you are a middle-aged person who can afford it, then it makes sense. (Rachel, 14)

[112] If intent to buy was the top factor in the algorithm the player would get double the points.

Most participants believed that personal information about who you *are* is often more valuable in algorithmic recommendations than personal information about your online interactions (what you *do*). For the most part, they thought this was because personal information is less likely to change, or at least less frequently than your interests change. Claire (15) explained that information about who you are tells platforms "what you actually want," whereas interests and brand loyalty "changes all the time."

> You can get more information, or more precise information, [about a user] if you use personal information. (Andrew, 15)
>
> Personal information makes ads more specialized. (Charlotte, 16)
>
> It's more important for [platforms] to use personal information because then you can actually understand what [users] are interested in. (Ethan, 19)

Participants reasoned that the more algorithms know about users, the more algorithmic factors or "tricks" they could use to target ads. For example, Nathaniel (16) explained the goal of algorithmic optimization, specifically stickiness, "boils down to advertising" since the longer a platform can keep users engaged, the more advertisements they can show to those users.

Participants were quick to point out the advantages and disadvantages of algorithmic uses of personal information. Most participants had few reservations about the use of personal information by algorithms recommending relevant entertainment and leisure content. These sorts of recommendations were seen as 'low stakes', and participants valued relevance as a favourable outcome. However, **participants were particularly concerned about the use of personal information in algorithmic decision-making for housing applications and loans.** Even if not directly relevant to them yet (given their age), these sorts of recommendations were seen as having significant future consequences.

While participants highlighted relevance as a primary advantage of algorithmic accuracy, it was still seen as "creepy" and "invasive" because participants did not know what algorithms *actually* knew about them and where they were getting this information. Ethan (17) explains this tension in his efforts to find an apartment near the university he will attend in the Fall: while he sees suitable options for places to live, he "is skeptical" about what information the algorithm is using to show him these ads and where it gets this information about him in the first place.

> [Algorithmic accuracy] does have that creepy factor where it [the algorithm] knows everything about me, but there is this other hand where they are [algorithms] helping you out in a way…by gearing different things towards you (Erin, 17)

Despite the benefits of accuracy, some participants wished ads were based exclusively on interests or what they *do* online rather than who they *are* (or say they are) online, even if this produced less accurate ads. Nathaniel (17) expressed nostalgia for the 'old days' when YouTube showed you many "random, unrelated ads" that you did not have to think about. Participants also emphasized that audience factors are moving targets; age changes, interests and brand loyalty changes, and even your personality can change. This was cause for concern since youth quickly figured out that accuracy requires a significant amount of corporate surveillance and data collection.

Algorithmic Assumptions: Corporate Uses of Data

In this second phase of gameplay, participants learned firsthand how algorithms potentially collect, share, and analyze user data to target ads, and this shed entirely new light on what they had thought were advantages to algorithmic uses of their personal information. Participants disliked the idea that algorithms were comparing them to other users 'like them.' They especially disliked the idea that their online information was being 'lumped' into categories of aggregate data to train algorithms and machine learning without their knowledge and, more importantly, without their consent. Participants thought they were receiving content recommendations *for them* because they were a unique user with unique interests. However, after this second round of gameplay, participants realized that algorithms are not necessarily providing recommendations *for them*. Instead, algorithms are sometimes making guesses based on other users who are *like them.* For some participants, this was the first time they had made this connection:

> Wait, what do you mean? You mean it [an algorithm] uses your information to target what your friends like? (Stacey, 13)

Many participants grew concerned that they were getting recommendations because of who they were 'friends' with online and vice-versa, and how their online information and interactions were being used to make recommendations to their 'friends.' Participants quickly figured out that what they had initially thought was algorithmic accuracy was actually an algorithmic assumption.
Logan (17) emphasized that there were contexts where comparison by social association 'made sense' (like with advertisement) and contexts where comparison felt inappropriate (like with banking).

> I don't like the whole idea of like a social credit score, where if you 'hang out' with undesirable people, your score will go down, but I think a more generalized approach where like this group of people likes these things, we [the platform] should show them [more]...is entirely fair. (Logan, 17)

However, many participants found it "annoying" that they were being compared to other teens assumed to be *like them*. As Kate (16) explains, "the people you are friends with online might be completely different from you," and as Mia (15) expands, "if you don't identify with a certain group of people," then the recommended content is irrelevant. Participants were concerned that users were being homogenized by algorithmic assumptions and that data sharing across algorithmic architectures resulted in further content saturation. Mia (15) explained that if platforms shared a similar data profile or 'picture' of her, she would just get more of the same content everywhere.

> If you go on and search an app to see certain content and a different app to see different content but because of data sharing, you are only seeing one type of content... Like on Instagram, you're looking at pictures of dogs, and then on Facebook, that's all you see; it can get annoying because... then it's everywhere. (Mia, 15)

Participants were quick to point out that they thought algorithms were more likely to get it 'wrong' than right when making assumptions, particularly about user groups, which could have negative consequences for both platforms and users:

> It could be harmful for the company because they could be giving you ads that you're not even a little bit interested in based on the interests of your friends. But, it could also be harmful for the person themselves because like they are being [made] into people that they are not, they don't fully identify with. (Kate, 16)

In some cases, when algorithms made incorrect assumptions, it was humorous. For example, Rachel (14) described a scenario where she and her friends were getting the same yogurt ads, but one of her friends was lactose intolerant. However, participants described these processes of corporate surveillance and algorithmic assumption as 'creepy' and questioned why algorithms assumed they were looking at or interested in the same things as their friends. Sahil (15) and Nicole (14) also

pointed out that if users are sharing a device[113], they will get inaccurate ads and recommendations "because other people [particularly parents] are on the device doing something that you normally wouldn't do or wouldn't watch and this messes up the algorithms."

While participants were concerned that data sharing and algorithmic assumptions were eroding the one silver-lining (accuracy and relevance) that they had seen in giving up their data, they were even more troubled by realizing that their data was often collected and sold by data brokers. Participants expressed strong feelings that this was **scummy**, **unfair**, **wrong**, and **unethical**. Some participants were willing to accept a certain level of data sharing within companies, citing the relationship that Instagram and Facebook or Google and YouTube share, but outside of these connections – to other platforms, apps, or companies—— and without their knowledge and consent, youth essentially considered this unacceptable.

> It's [information brokering] a pretty scummy thing to do, in my opinion…I would rather they [companies] not do it. (Ethan, 17)

> You think that only one app has your information, but then it turns out that they are connected to a bunch. It's not fair because it [the platform] doesn't really tell you; it just does it by itself. (Nicole, 14)

Participants commented on the potential social and political implications of information brokering, especially since users were almost always unaware of these processes. Many participants were concerned that information brokering was covered somewhere in the platform's terms of service or privacy policies. However, echoing findings from previous MediaSmarts' research on privacy and consent,[114] participants did not read these policies because they are too long and inaccessible (Sahil, 15).

When it came to selling user's information without their knowledge, meaningful consent, or without properly compensating users for their data, youth felt like online businesses crossed an ethical line:

[113] MediaSmarts' study on The Digital Well-Being of Canadian Families has found it is often the case that especially young children share 'family devices.' www.mediasmarts.ca/sites/default/files/Publication-report/full/Digital-Canadian-Families.pdf

[114] See: McAleese, S., M., Johnson, M., Ladouceur. (2020). "Young Canadians Speak Out: A Qualitative Research Project on Privacy and Consent." MediaSmarts. Ottawa.

I don't think it's fair because we haven't given them [platforms] permission to take our data, but then they [platforms] are the ones usually benefitting from it. (Rayleigh, 13)

That's [data brokering] just way over the line. Like how with Brexit, people's data was sold to political organizations, and they would be shown ads and stuff, and I mean, that's just like, *come on*?! (Nathaniel, 17)

It [data brokering] should be illegal…you are not putting your information in for Facebook so another random person can have it…I don't know if it would be considered stealing… under the terms of the law? (Erin, 17)

Participants were clear that selling their data without their knowledge and meaningful consent was a "violation of their privacy" (Erin, 17). While they were concerned that platforms had a legal carte blanche when it came to how algorithms and AI used their personal information, for the most part, participants were resigned to the fact that their personal information was the price they had to pay for online participation:

That's one thing that you are giving up when you give [platforms] your personal information, is the right to privacy. (Sahil, 15)

In the context of recommendation algorithms, participants worried that if they did not give up their right to privacy, they would no longer reap the benefits of algorithms and AI, specifically content curation, relevance, and efficiency. Sahil (15) referenced Californian laws which allow users to opt-out of the sale of their information, saying he would "prefer that option." However, he also worried that if he did opt-out then online services could become less appealing to use because they would not recommend the content "you want to be recommended."

Again, participants pointed to the effects of monetization and corporate business models as an explanation for this violation of their privacy. As Tyler (16) explains, most websites are 'free' when we sign-up, but really, we "pay with our data." Participants thought this was a "smart" way to make money but also felt it infringed

on their privacy rights and information protection. Some participants were at a loss with how to manage this problem since the terms of service and privacy policies were unreadable and buried this information. As Sahil (15) explained, if platforms were clear and upfront about how they were using our data under corporate monetization models, it would "shock and scare us," so that's why the platforms put this information in the "fine print" – so "they've technically told users, but users would not have read it." Of particular concern is that youth are trying to fill these knowledge gaps themselves. Sometimes they turn to unreliable sources and are unnecessarily frightened by misinformation and conspiracy theories about how their information is collected and shared.[115] Some participants imagined alternative solutions or models: where they could *choose* where their information is shared and for what purposes, or where they could *pay* for an account where the platform could not sell their information. Once again, most **participants agreed that algorithmic transparency was essential and would go a long way in providing users with the knowledge and capacity to make better decisions about their information and privacy.**

Trust, Responsibility, and Control

The second phase of gameplay increased participants' knowledge and awareness of the value of their personal information in algorithmic decision-making. There were contexts in which the use of their personal information "made sense," such as recommending relevant advertisements and entertainment content. However, participants had concerns that their information was, in unidentified ways, being used and sold for training algorithms and for making assumptions about user groups. Again, participants were calling for algorithmic transparency to understand better *how* algorithms and AI use their information.

Many participants anthropomorphized or attributed human characteristics or qualities to algorithms and AI. This is understandable given that AI refers to the simulation of human intelligence and action in machines and that most users lack the algorithmic literacy to be able to understand these operations effectively. When it came to algorithmic uses of their personal information, participants described algorithms as **pushy, unfair, scammy,** and **manipulative.** Interestingly, in their gameplay and discussions of their interactions with algorithms and AI, we observed that youth began to demonstrate a parasocial relationship with the technology. Parasocial interactions refer to a kind of one-sided psychological relationship between users and their mediated encounters with performers, celebrities, or

[115] For example, Stacey (13) explained that she heard about a conspiracy theory regarding TikTok recording what users are talking about to improve their algorithmic accuracy.

personas.[116] Parasocial interactions become parasocial relationships after repeated experiences with the persona cause the user to develop illusions of intimacy or friendship.[117] Meaning construction and parasocial relationships with *technology*, rather than with celebrities or mediated personas, have been traced over time, beginning with early learning connected toys in the 1980s[118] [119] to smart toys[120] and *embodied* AI in voice-activated assistants such as Alexa and Siri.[121] However, there are gaps in the literature regarding understanding parasocial relationships with *unembodied* AI, especially algorithms, which we began to see in this study. This parasocial relationship with algorithms highlighted a tension regarding trust: on the one hand, youth described algorithms and AI as they would a trusted friend who curates and sorts online content *for them.* On the other hand, after discovering that their data was often sold and used in aggregate by algorithms to make assumptions about users, participants expressed frustration with what they saw as a violation of their privacy and trust.

> For some websites, you don't want to give them the information, like maybe you don't trust them…but for others you are perfectly fine giving your information and if they share information with each other then you feel bad about it. (Claire, 15)

> I don't feel safe [when algorithms use my personal information]. I know professional companies are secured and stuff like that, but… when it comes to sites I do trust, I definitely wouldn't be happy if I found out some people know my personal information. (Jacob, 14)

Again, participants were frustrated with "not knowing how algorithms work" and felt that they were owed a clear explanation regarding the algorithmic uses of their personal information. In fact, some participants highlighted that selling user data would not be "completely unethical" if platforms were fully transparent about doing so. But, as Tyler (16) described, platforms rarely, if ever, tell users "exactly how their information is being used." Along with transparency, participants emphasized that rather than an 'all or nothing' approach, they wanted to make *choices* regarding what information they shared, in what contexts, and whether or not this information could be shared outside of these specific contexts. Further, the **participant's felt that a user's decisions to protect their data should not impact the quality of the user experience.** Participants had high expectations of platforms regarding privacy and

[116] Horton, D. and Wohl, R. (1956). "Mass communication and para-social interaction: Observation on intimacy at a distance". Psychiatry. 19 (3), 215–229.
[117] Rubin, R. and McHugh, M. (1987). "Development of Parasocial Interaction Relationships". Journal of Broadcasting & Electronic Media. 31 (3), 279–292.
[118] Liebers, N., and Schramm, H. (2019). "Parasocial Interactions and Relationships with Media Characters-An Inventory of 60 Years of Research." Communication Research Trends, 38(2), 4–31.
[119] Turkle, S. (1995). "Life on the screen: Identity in the age of the internet." New York: Simon and Schuster.
[120] Steeves, V. (2020). "A dialogic analysis of Hello Barbie's conversations with children." Big Data & Society.
[121] Lovato, S. and A.M. Piper. (2019). "Young Children and Voice Search: What We Know From Human-Computer Interaction Research." Frontiers in Psychology, 10(8).

information protection; they felt that platforms had almost exclusive responsibility to *clearly* explain how user information was being used and obtain meaningful consent to use it, therefore protecting this information.

Further, the control strategies that young people are currently trying to deploy against algorithmic uses of their data are mostly unsuccessful. Nathaniel (17) mentioned a friend who is adamantly against getting a Facebook profile because of the Cambridge Analytica and Brexit scandals. However, in this second phase of gameplay, Nathaniel reasoned that this friend probably could not avoid data brokerage by refusing to get a Facebook account, which was "just not fair" because it completely defeats his friend's purpose in avoiding these social media accounts. Participants like Hailey (17) described their efforts to "try to be careful when sharing their information online," citing instances where they felt it was necessary to include personal identifiers – for example, when filling out university applications. **Youth also pointed to cases in which they thought data collection was invasive and unnecessary**, such as when making a clothing purchase at online retailers, "because there is a pretty solid chance that information could be passed on and sold."

Participants also described attempts to game or manipulate algorithms by not using personal accounts or information and entering false or misleading information. For example, Logan (16) explained his own efforts to manipulate the Google ad algorithm by inputting false user information in his profile and customer service reviews:

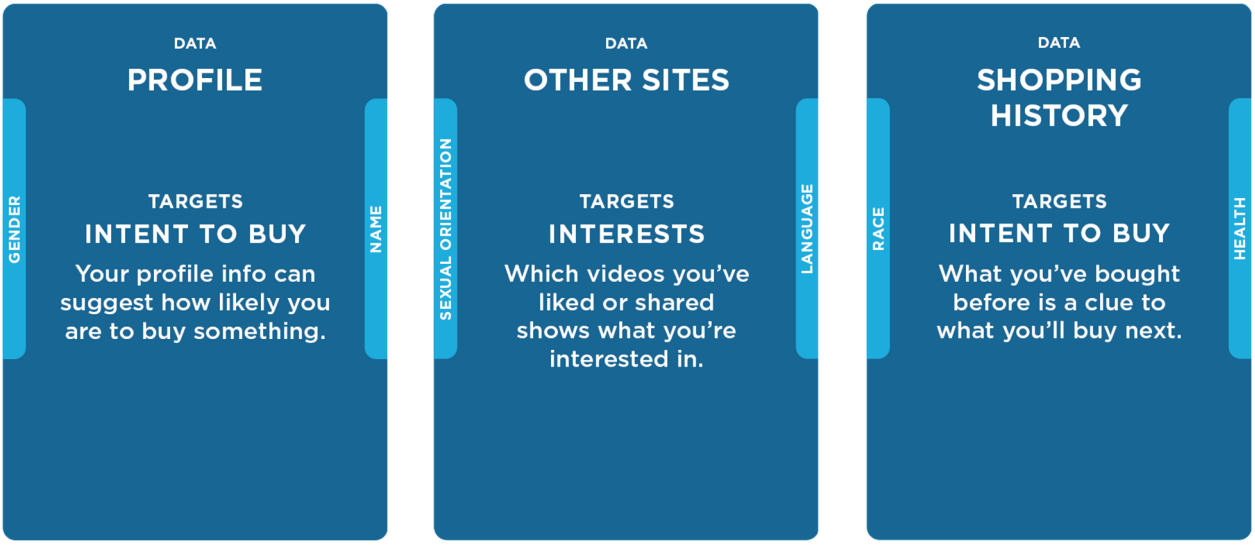
> **Google thinks I'm like 200 years old because I set it up when I was too young [with a false age] so I keep getting ads for Cialis *laughs*... You know, if one week I say I make $300,000 a year [Google] gives me a bunch of car ads, and if I say I make negative $10, then it doesn't. (Logan, 17)**

Again, participants had high expectations of platforms; they wanted to have control over algorithmic decision-making especially for "things that mattered, like banking" (Logan, 17). Algorithmic transparency would not only work towards addressing the apathy and powerlessness described by participants but it would also increase their algorithmic literacy, specifically their ability to better understand *how* algorithms and AI use their data which will potentially allow them to raise *other* privacy and information protection issues that they may be unaware of. **Algorithmic literacy efforts must also help youth understand that some of their agency and control comes from how they interact with and can influence algorithmic factors through their online (in)actions.** For example, *not* liking, re-tweeting, or posting content is one way to curb recommendation algorithms by not feeding the algorithm information. However, participants also expressed a desire for a clearer way to communicate dislikes and errors in algorithmic assumptions.

By the end of the second phase of gameplay, participants understood that recommendation algorithms rely on user data to generate assumptions about people's likes, interests, purchases, and behaviours. Inaccurate recommendations were seen as annoying: the frustrating outcome of not understanding how algorithmic decision-making happens, which generated privacy concerns for participants since they were unsure how their data was being used and potentially sold. Perhaps even more importantly, as they would learn in the third and final phase of gameplay, algorithmic decisions were not just inaccurate; they were in some cases biased or prejudiced towards entire groups of people, which could have material consequences in their offline as well as online lives.

The (Algorithmic) Ties That Bind Us

In the third and final round of gameplay, participants learned more specifically about machine learning, artificial intelligence, data brokerage, and how algorithms rely on *proxies* to make inferences and identify patterns that might not otherwise have been apparent. The objective of this round was to expose how algorithms are trained or modified on data sets and demonstrate how these ongoing and automatic training processes lead to assumptions about individual preferences. Having participants link Data cards through **proxies** such as race, gender, or sexual orientation also catalyzed discussions about how these AI processes can sometimes lead to faulty, problematic, or dangerous assumptions, contributing to bias, prejudice, and discrimination in online and offline spaces.



The gameplay in this round was similar to round two. On the first turn, each player placed one Ad card to guess which audience characteristics the algorithm was optimized for. The Platform player then scored the Ad cards, providing players with clues about which Audience cards were in the algorithm and in what order. The second turn is where things got more exciting and interactive. Players were allowed to play additional Data cards by connecting them using the proxy text along the sides of the cards to match and make links. The proxy text on the cards represented things that a machine learning algorithm might be able to infer about a person based on data like race, gender, name, sexual orientation, language, friends, and health. Players also had a chance to broker (trade) their data cards with other players to obtain cards with matching proxy text. This brokering exercise showed participants how quickly data profiles come together, especially when online businesses can share or buy and sell personal information.

After playing this round, we asked participants how they felt about linking ads through proxies and talked about their thoughts and experiences with algorithmic-

facilitated bias and prejudice. This round led to further discussions about rights, responsibilities, and protections related to personal information, behaviours and activity, and privacy online.

Putting the Pieces Together

This round, even more so than the previous two, elicited several 'aha' moments from participants. Many admitted not knowing what proxy data was or never really thinking about how things like race, gender, health status, or sexual orientation could be inferred from other data and used to build more complete data profiles mobilized by online businesses.

> I didn't realize how much the [platform] could connect all of that just with machine learning and AI. (Andrew, 15)

> I never knew what proxy meant. I've learned a lot. (Jacob, 14)

> I didn't realize how linked some different things are… I didn't realize how you could connect all of the different cards together. It really made sense when I looked at it, but I never really thought about that before. (Kate, 16)

After learning about these processes, youth were very interested in talking more about machine learning and the impacts of artificial intelligence on their lives – both online and offline. This third round of gameplay encouraged youth to reflect on aspects of the digital world that they typically do not spend much time thinking about as users or consumers.

> It was kind of cool to see how the little things can fit into the bigger subjects, like how your shopping history shows what you intend to buy, or like your profile… Those things can work into a bigger category that you wouldn't assume. (Stacey, 13)

> It's interesting how much the algorithms and stuff can connect different things. (Mia, 15)

Participants also quickly pieced together how beneficial these connections and categorizations are for platforms, acknowledging that these algorithmic ties are good for business. Getting "the right information on someone" (Ethan, 17) by tracking their interactions and behaviour online and making generalizations, or reducing people down to "their raw materials" (Nathaniel, 17) made sense to youth from a business perspective.

Alongside these acknowledgements of the benefits of machine learning, youth participants described these processes of linking proxies and brokering data as "**kinda weird**" (Claire, 15), **creepy**, **strange**, **disappointing**, and even **evil**:

> It's a little disappointing, to be honest – that it's so easy to manipulate people. (Nathaniel, 17)

> It felt kinda creepy... [sorting] people into those aspects of themselves for the sake of making money feels very strange, and I did not like it. It was super cool to play the game, but I felt a little bit evil. (Hailey, 16)

Others had their doubts about the accuracy of the results of these tracing, trading, and recommendation processes and questioned the reliance on proxies and their associated stereotypes:

> **I don't think it would necessarily be accurate all of the time. I know for me, I play hockey, and it's not necessarily a girl sport, it's more of a guy thing, so then they might start to think or give me ads for guy's things that aren't relevant to me at all because I'm a girl. (Nicole, 14)**

Nicole's concerns about stereotypes leading to irrelevant advertisements and videos bring us to a broader conversation about the material consequences of bias in AI. Youth were quick to acknowledge that **any good generated by machine learning algorithms should not be used to justify or overlook the real-world negative impacts of bias and prejudice** that are often inherent (whether intentionally or not) to these systems and processes.

Troubling Assumptions

Without too much prompting, many participants seemed quite familiar with the concept of bias in relation to digital technology, algorithms, and AI. Youth were aware of how biased data translates to "wrong answers [or] the wrong information" (Sahil, 15) and how this can have repercussions for both online businesses and users. The idea that bias is bad for business was highlighted a few times, and youth warned

that companies, websites, platforms, and apps should "be careful" (Jacob, 14) not to rely on stereotypes or categorizations:

> You have to be careful about that because if you're stereotyping something like gender or a race and showing them certain ads just because you think they will enjoy it because they are white or something, you have to be careful around that. (Charlotte, 16)

> You have to be careful about those broader categorizations because they can sometimes, or most of the time, they'll do more harm than good. (Sahil, 15)

> With machine learning, where it's pretty much a black box, you don't know what's going on, and it's hard to figure out what kind of decisions it has made – you have to be careful about what you're feeding it and what it's feeding into. (Logan, 17)

One of the main consequences of relying on biased data discussed in each focus group was discriminatory hiring practices. We provided an example scenario in the sessions about how some companies use AI to screen job applications or sort resumés. Based on the data sets used to train these processes, certain people (often racialized) will be filtered out of the application process. Youth found this profoundly unfair and once again emphasized that this bias, resulting in a lack of diversity, is terrible for business.

> If the company develops the bias, they only hire people like that, it's bad when other companies can see all of their employees are not [diverse], and it looks bad for the company. (Jacob, 14)

> I don't think it's a fair way because it's discriminating against people. There might be people who might be more eligible but who are not considered because they don't meet the requirements that the algorithm chose. (Stacey, 13)

> That's just not great to choose people for a position or a job based on anything, but especially based on race – that's not great. (Kate, 16)

In troubling these algorithmic assumptions, participants used language like "**upsetting**," "**dangerous**," "**terrible**," and "**unfortunate**." They questioned the fairness of these practices and were concerned for people who are already placed at risk of experiencing racism, marginalization, or discrimination:

> I guess there could be particular places where people might already face a lot of discrimination [and to] have a computer doing that too is kind of brutal. (Hailey, 16)

Youth also questioned the ethics of machine learning algorithms, in that they often rely on information that you might not know you are providing. The reliance on information like race, gender, or sexual orientation felt like "manipulation" to some, and there was a call for online businesses to stick to details like "age or interests" (Rachel, 14). The assumption here is that things you *do* on a platform say more about you and are less likely to lead to experiences of bias and discrimination.

> I feel like any information that they infer from you is a lot less ethical to use than information that you give them directly. (Tyler, 16)

Finally, there was an acknowledgment from participants that algorithms, or algorithmic systems, should not be left to their own devices:

> The algorithm isn't human. It doesn't understand emotions or what is right or wrong – it only understands what it's being given. (Sahil, 15)

Hailey (16) provided an excellent example of what happens when machine learning algorithms are left unchecked or when developers and platforms do not fully appreciate or anticipate the unintended consequences of relying on this technology.

> There was a bot on Twitter, and it basically let people tweet at it whatever they wanted, and it would learn from the kind of things that people would say to it and then it would tweet out sort of similar phrases. I remember reading that a group of neo-Nazis found the bot and tweeted a bunch of really awful things at it, so it started tweeting those things.

Hailey was referencing an incident from 2016 when Microsoft released an AI chatbot ('Tay') on Twitter as a "playful" experiment.[122] In less than 24 hours, the chatbot echoed the harmful and violent remarks that Twitter users were feeding it, despite efforts from the developers to include filtering processes. "Tay's adventures on Twitter show that even big corporations like Microsoft forget to take any

[122] Vincent. J. (2016). "Twitter taught Microsoft's AI chatbot to be a racist asshole in less than a day." The Verge. Retrieved from: www.theverge.com/2016/3/24/11297050/tay-microsoft-chatbot-racist

preventative measures against these problems"[123] and, as participants shared with us, it is episodes like this that erode trust in AI and demand a more intentional discussion about who is responsible for mitigating the negative (and sometimes violent and harmful) consequences of technology.

Trust, Responsibility, and Control

This final round of gameplay confirmed for participants that "what you're doing online is being remembered, and the algorithm is influenced by what you are doing online" (Kate, 16). Thinking about both the volume and permanence of personal information collected and shared every day by online businesses and platforms raised serious issues for young people. Of particular concern were the future—unknown and unanticipated—uses of their data, specifically as they prepare for post-secondary education, the job market, and eventually the responsibilities of adulthood (e.g. apartment/housing applications, financial services, healthcare services). Add bias and prejudice into the mix, and youth were also worried about ongoing marginalization and discrimination both online and in their communities. As Ethan (17) explained, if the algorithm is just recommending content, or "if it's something harmless like on YouTube" then it's "perfectly fine," but once the functioning or use of the algorithm becomes "harmful" or "puts a certain group of people at a disadvantage" then new considerations or interventions are required. These concerns, once again, shifted the discussion to issues of trust, responsibility, and control.

> If someone gets a worse mortgage or doesn't get the job, those are big life-changing events. So, that impacts people a lot. You have to be more careful than with whatever cat ad to show me or what video game they want to promote now. (Logan, 17)

There was a mixed response when we asked youth who should be responsible for managing, monitoring, or responding to algorithmic bias and AI-facilitated harm and discrimination. A few participants indicated that this was a complicated question to answer "because you can't really control what an algorithm is going to do" (Tyler, 16). For some, the responsibility lies with the developer:

[123] Ibid.

> It's hard to say because the AI learned from experiences – it's not just like, "Hmm, I'm gonna discriminate against these people for fun!" It learns from what it's taught. But, I think it's important that developers monitor what it's being taught… When the bias is harmful to people, it is the developer's responsibility to manage that. (Hailey, 16)

> I think most of the time when these machine learning algorithms become biased, that's more about whoever decided to use the algorithm's fault… Because with machine learning, you need to train it on certain data sets and if you don't train it on certain exceptions that let it know what's right and wrong, then that's kind of your fault if it becomes biased. (Tyler, 16).

Logan (17) echoed this, emphasizing that "if the data you have is biased then it has chances for the algorithm itself to become technically homophobic or racist." For others, the responsibility lies with the platform, website, app, or online business to "limit the bias" (Andrew, 15), "monitor content" (Nathaniel, 17), and make sure that "people are aware" of the potential for bias in machine-learning processes (Madelyn, 14).

> I think that the website or app should make sure that – like, it falls onto them. The prejudice that they put into the formula… it is their responsibility. (Stacey, 13)

> If a post is reported for prejudice or anything related to that, I think [the platform] should look into that immediately. For me, it's a priority. It should be taken down. (Erin, 17)

Overall, there was a sense that *someone* needs to "monitor what the algorithm is doing very closely and test it a lot to make sure that it doesn't go crazy" (Tyler, 16). Sahil (15) did not have a lot of faith in companies to take on this kind of careful monitoring, but said that it would be in their best interest to do so to make sure that people don't "feel uncomfortable visiting the site" or are fearful of experiencing violence, harm, or discrimination.

Next, there was a general call for more transparency from participants. Youth were in agreement that people need more information about how algorithms work and how we are all impacted by AI and the increased reliance on machine learning systems. This call for more transparency follows from concerns about platforms collecting "unnecessary information" without a good enough reason or without clearly asking for consent (Stacey, 13). Young people generally want to know "how [platforms] got their information and who else has it" (Henry, 13).

> I'm fine if they ask you a direct question and you answer it and submit it to them, but I think any information that you don't give them directly they shouldn't have the right to use or sell. (Tyler, 16)

> If I knew that one website was taking a lot of information and I didn't know, I would probably stop using it or figure out ways to make sure that it's not doing that anymore. (Nicole, 14)

Youth also want more transparency around content – why they see the things that they see online. They expressed that it would be "really cool" or "really insightful" to learn more about these recommendation and content curation processes. Nathaniel (16) said that more transparency "might get a lot of people to think more critically about why you are actually seeing ads" which could also contribute to a stronger focus on data privacy.

> I think it's very important for people to have the choice to learn why they are seeing certain types of ads. It gives the user more freedom over what they see or more control [over] what they see on their pages. (Ethan, 17)

> If I knew more about the reasons why I've been recommended this video, then you can understand more and you can see if the algorithm itself is recommending content for the right reasons or the wrong reasons. (Sahil, 15)

For participants, more transparency would offer more control and they felt strongly about having the right to this control. They also want this information provided in simple terms, so that it is something they can quickly and easily absorb. As Erin (17) put it, "I don't need a full-on complete report… just something simple and then I would understand." Youth want to place limits on data collection and tracking through proxies and did not seem convinced that platforms actually need to know *everything* about them.

> I think users would feel better knowing that they can have a bit more control and a bit more knowledge about what they see instead of the algorithm controlling everything. (Mia, 15)

Control also included the ability to report faults or errors in the recommendation algorithm. Tyler (16) stated quite simply: "if [the algorithm] is wrong, then I think you should be able to report it." Users were already aware of reporting features on various platforms like YouTube and TikTok, and they liked having this option so that they could play a role in determining what content is appropriate for them and flagging content that they think is "violent or something that's offensive" (Sahil, 15). Participants liked the idea of being able to respond more actively to the suggestions made by the recommendation algorithm.

> It will help you be more aware of why you are seeing what you are seeing... and being able to know how algorithms work and then learn sort of how to manipulate it to your own advantage. (Kate, 16)

At the end of this final phase of gameplay, participants had both demonstrated and expressed quite strongly the need for algorithmic literacy. **Concerns about data collection, data sharing, bias, and privacy were threaded throughout the discussions in each of the eight focus groups.** Youth participants – as a result of playing the #ForYou game – now had a better understanding of how they interact with AI in their day-to-day lives, how AI and algorithms work, and were starting to better understand the implications of AI and algorithms on their privacy.

Recommendations

This qualitative research project demonstrates once again the benefit of talking directly to young Canadians about what they do and what they experience online. Rather than speculating about their knowledge of algorithms and AI and the impact of new and ever-evolving technologies, we can know exactly what youth are experiencing and acknowledge them as experts in their own lives. The key findings from these focus groups with youth ages 13 to 17 provide researchers, educators, policymakers, and tech industry leaders with important next steps in addressing issues related to privacy online. As participants themselves highlighted, these conversations and considerations have become even more essential throughout the COVID-19 pandemic:

> I definitely wish that we could understand more what is going on because technology is kind of taking over our lives, but we don't know about it. It's just, everything is being switched onto technology. You can just do so much more nowadays, but you don't really know where your information is going. (Nicole, 14)

> Especially during the pandemic since everything has been online recently, like school and everything, and talking to all of your friends... It's definitely important to know what you're doing. (Kate, 16)

The recommendations that follow echo what participants told us about the need for more awareness, transparency, protection, control, and engagement.

Awareness

Participants issued a strong and coherent call for increased awareness about how algorithms work. Conversations with youth echoed what we found in the literature about the opacity and secrecy of artificial intelligence and its uses and impacts. So, to help expose what is in 'the black box,' children and youth require **access to more robust algorithmic literacy tools and resources.** Algorithmic literacy can help young people understand the impact of algorithms on their online experiences as well as

the potential future impact on other aspects of their lives. Educational programs should not only be about learning to code, but must also **encourage critical thinking skills that will empower young Canadians to take control over their personal information**. Algorithmic literacy curricula should be tailored to the unique needs of children and youth and should be delivered to them in the spaces and places where young people already are. For example, participants expressed a desire to learn about algorithms and AI in school or in community groups. In particular, it is essential that learning to think critically about algorithms and their impact not only be available to youth in more affluent communities or in specialized programs, as it is precisely marginalized and disadvantaged communities that are likely to feel the heaviest impact of algorithmic inequity. Along with professional development resources needed to make school and community group learning possible, some resources should also be directed towards parents and guardians, as several participants hinted to a lack of algorithmic knowledge among the trusted adults in their lives.

Transparency

Across all of the focus groups **participants emphatically called for online businesses and corporations to provide transparency about algorithmic design.** Participants demonstrated a good understanding of what information is collected about them and why, but they expressed a need and desire to know more about **how algorithms work.** Youth want more information about how data is collected, stored, and brokered and also about how these processes translate into content recommendations. Youth expressed concern that algorithms were limiting their capacity to navigate and participate in online spaces and they felt that algorithmic transparency would broaden the scope of content available to them, providing them with greater access to trusted sources of information. They described machine learning processes as “weird”, “creepy” and “scary” and are tired of feeling scammed or tricked by online businesses that do not provide clear data collection and privacy policies. **Youth expect more from platforms, apps, and websites when it comes to transparency and want to see safety and privacy considerations at the forefront of any AI-based initiatives.**

Protection

Echoing findings from our previous study on privacy and consent, **participants in this project also expressed concern about the unanticipated or unintended consequences of data collection and sharing practices.** Given the volume and permanence of the personal information they provide to online businesses, young people are particularly concerned about how their data profiles might be stored or shared and how this might have a negative impact on their futures. Youth expressed

frustration with the inaccuracy of algorithmic inference and they were concerned that algorithmic assumption was further narrowing the scope of their online experience. Participants worried about the growing reliance on AI in decision-making processes and how the bias built into these systems might potentially interfere with education, employment, financial, or social opportunities. Youth also worried about more directly harmful forms of marginalization and discrimination that could arise as a result of an increased reliance on AI. They also expressed a desire for more control over their data profiles. In response to this, **our recommendation is that policymakers consider a data erasure approach** similar to what is outlined in other jurisdictions.[124] **We also recommend that online businesses improve their privacy policies and consent practices so that users – especially younger users – have a clear understanding of what data is being collected, for what reasons, and what will happen to their data.**

Control

In line with recommendations for increased awareness, transparency, and protection is a recommendation to **give more control to young people who are engaging in online spaces.** While participants felt that it was the responsibility of developers and platforms to monitor algorithmic systems and remain aware of the harms that stem from deploying AI, they did not have full confidence in these bodies to take on that responsibility. Therefore, they ask for **more reporting features so that they themselves can hold platforms accountable by taking action when they notice that something is wrong** – whether it is because a video is recommended that they do not like or when they notice violent or discriminatory content online. Young people also want more control over the personal information that they give over to online businesses and what can be done with the information that they do provide. In this regard, we recommend **stronger and more meaningful consent processes** guided by the principles outlined by the Office of the Privacy Commissioner of Canada[125] and the solutions identified by youth in previous MediaSmarts research[126] that include:

- **Unbundling options:** allowing users to give or withhold consent to different forms of data collection and different uses of their data, particularly when their data is used in aggregate to train algorithms and machine learning technology

[124] For example, the European Union's General Data Protection Regulation (GDPR) contains a 'right to be forgotten' article that "gives individuals the right to ask organizations to delete their personal data" and offers detailed criteria that balances the needs, interests and concerns of both users and organizations that collect, store and share data. See: GDPR.EU. (2020). Everything you need to know about the "Right to be forgotten". Retrieved from: www.gdpr.eu/right-to-be-forgotten/

[125] Office of the Privacy Commissioner of Canada. (2018). "Guidelines for Obtaining Meaningful Consent." Retrieved from: www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/

[126] McAleese, S., M., Johnson, and M., Ladouceur. (2020). "Young Canadians Speak Out: A Qualitative Research Project on Privacy and Consent." MediaSmarts. Ottawa.

- **Line-by-line consent:** where the online platform makes clear what will be done with the collected data, especially by algorithmic systems, by encouraging users to read and click 'agree' to the various components of privacy and consent policies.
- **Just-in-time notices:** giving users the information they require about data collection and data uses, in real time, as they engage with various components of the app, platform, or website.

Engagement

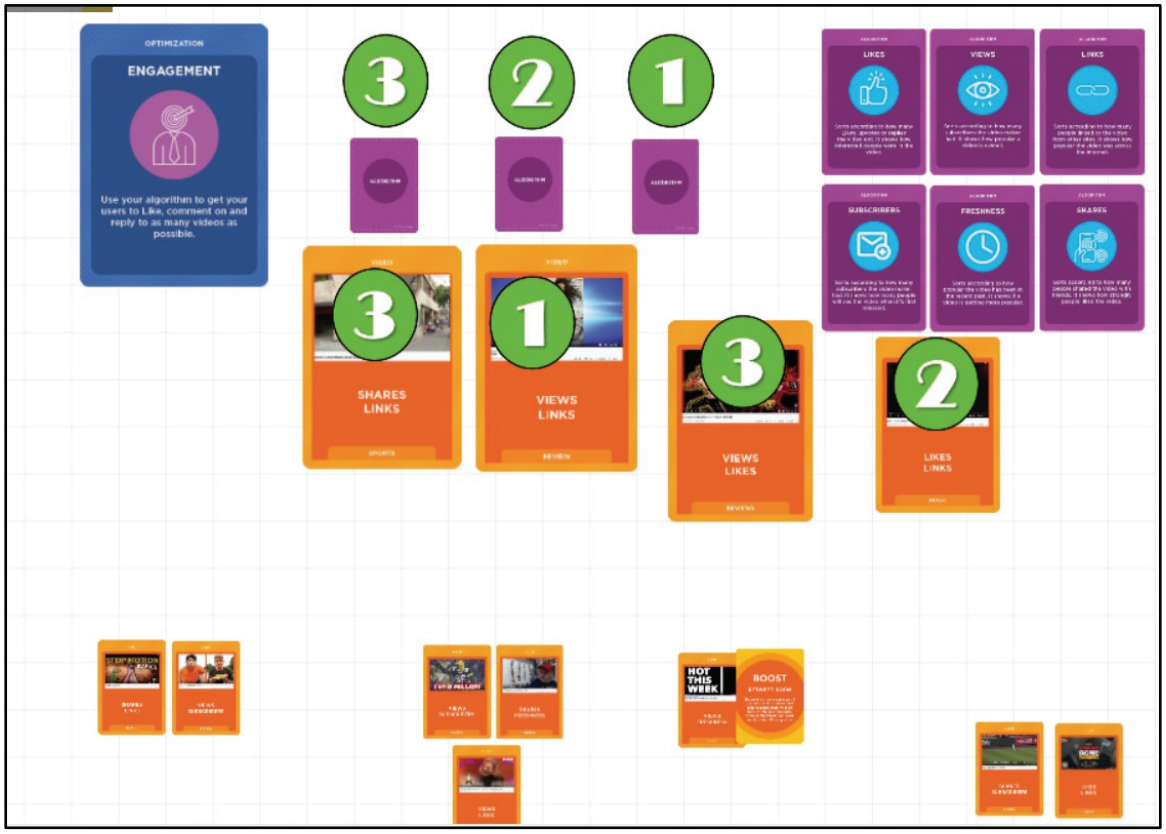
Finally, we recommend **ongoing conversations with young people across Canada about privacy online.** MediaSmarts will continue to engage with children and youth to develop new resources, tools, and supports that best address their experiences and concerns with digital technology and the online world, and we **encourage others to do the same.** Participants in this study, like in previous qualitative projects, appreciate the time, space, and opportunity to talk more intentionally about these issues that directly impact their day-to-day lives. Youth are energized by the idea that the findings from these research projects are mobilized and shared in spaces where youth are rarely included (such as parliamentary committee hearings or privacy consultation processes). We recommend **future research projects that continue to build our knowledge of algorithmic literacy levels among children and youth and projects that specifically interrogate the intersection between young people's understanding of algorithmic systems and their ability to access and verify information online.** Addressing the challenges and shortcomings of algorithms and AI, and ensuring ongoing and much needed innovation in this sector, requires that youth be recognized as experts. **We are grateful to the youth who shared their insights, experiences, and strategies for encouraging young Canadian's to learn more about their privacy rights in a way that empowers and motivates them to use AI to their advantage.**

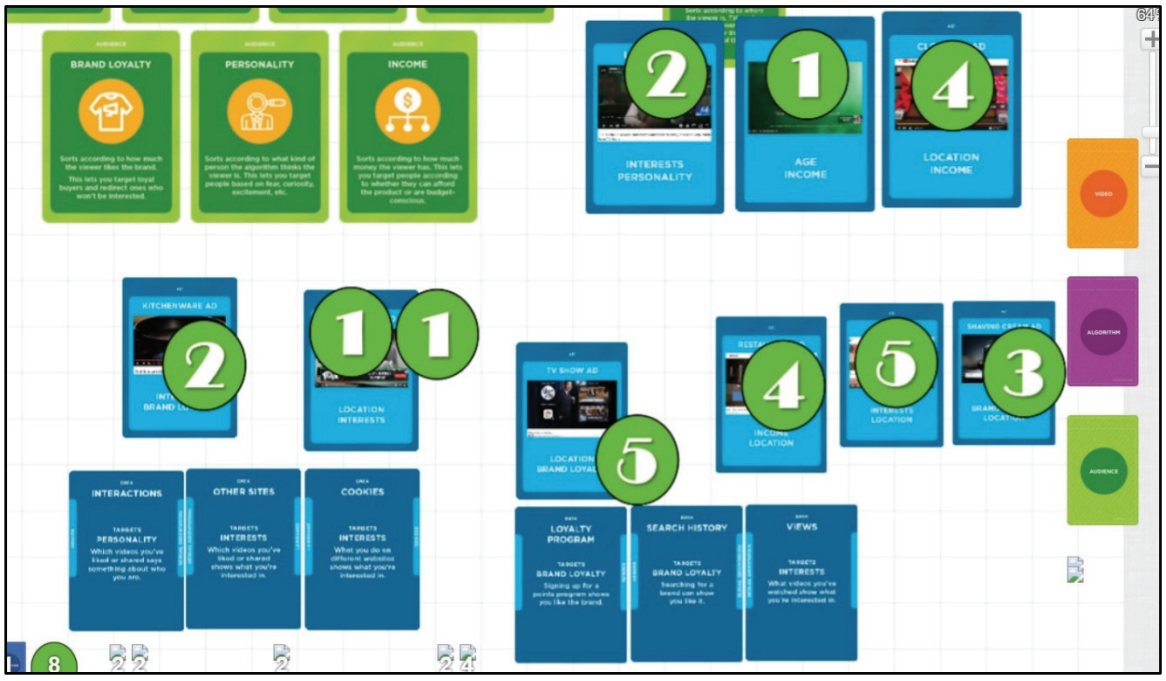
Appendices

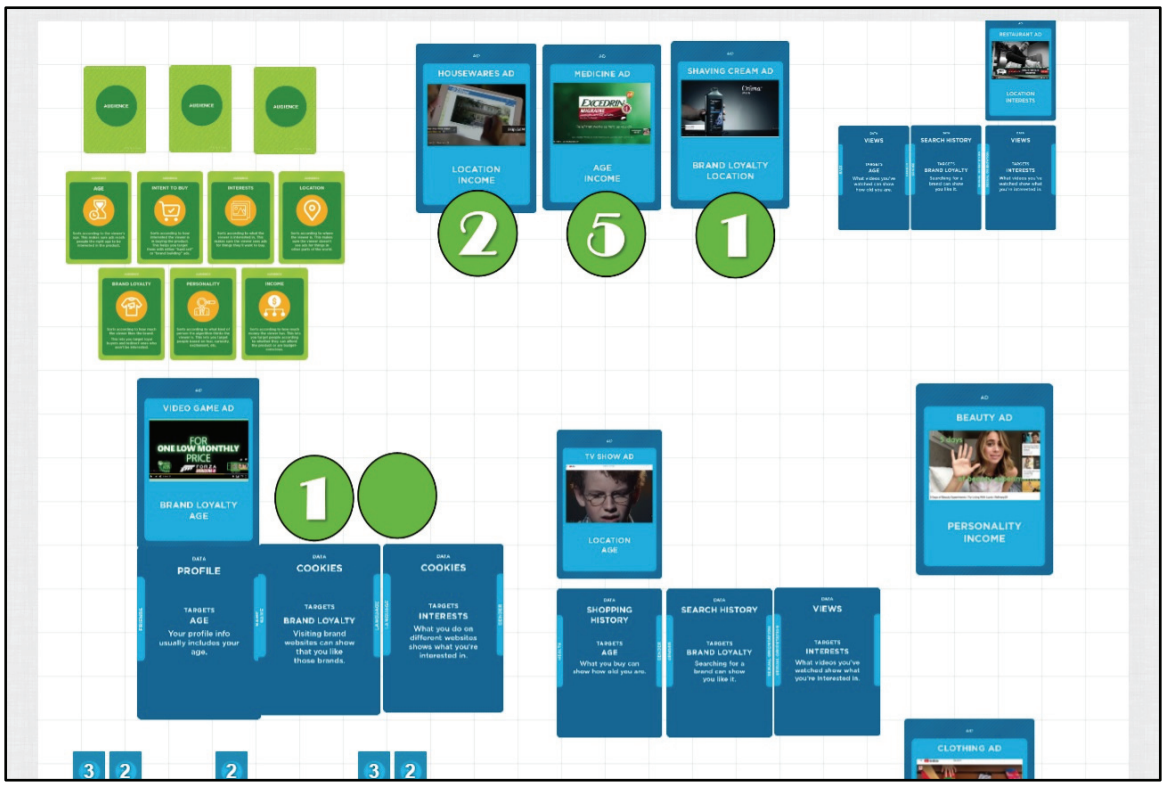
Appendix A: Participants and Focus Group

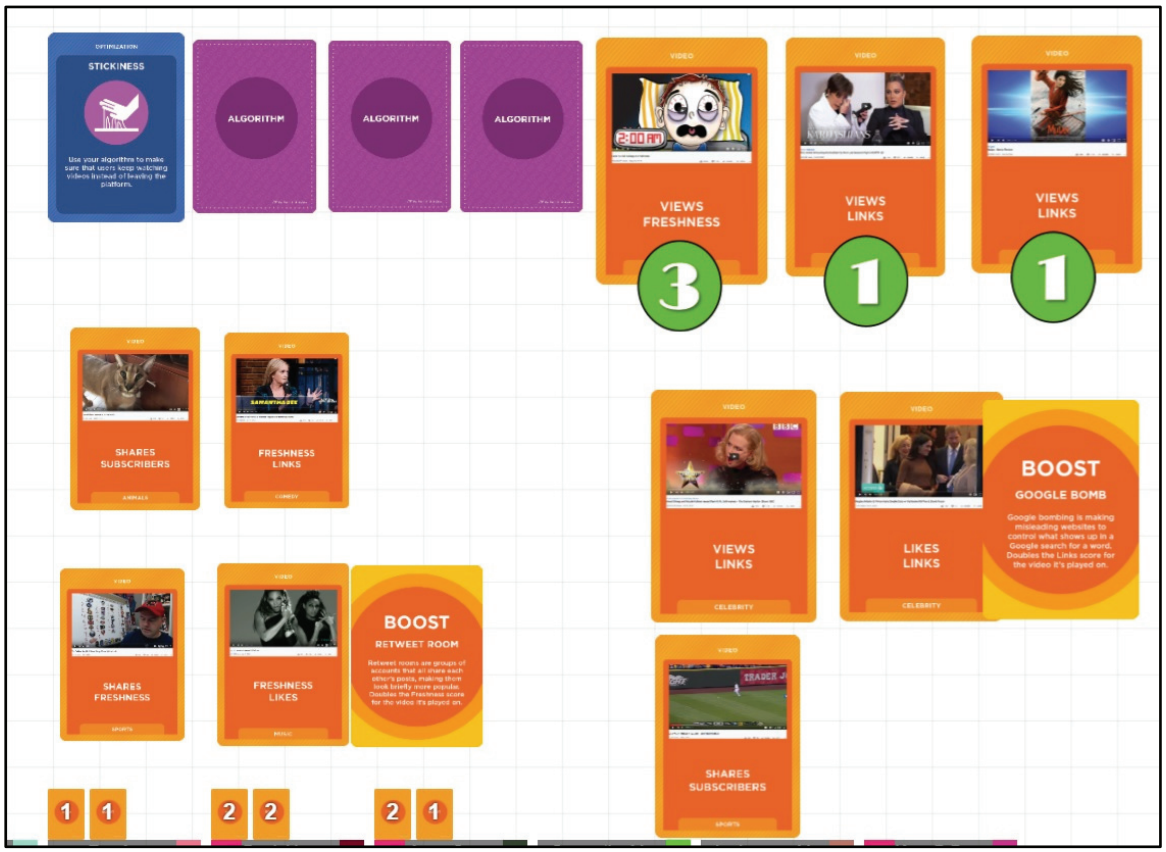
Focus Group	Pseudonym	Age	Province/Territory
1	Jacob	14	Ontario
	Madelyn	14	Ontario
	Stacey	13	Ontario
2	Aisha	13	Ontario
	Celina	13	Ontario
	Rachel	14	Ontario
3	Hailey	16	Ontario
	Claire	15	Alberta
4	Conor	15	Ontario
	Henry	13	Ontario
	Rayleigh	13	Ontario
	Nicole	14	Ontario
5	Tyler	16	Ontario
	Charlotte	16	Ontario
	Sahil	15	Ontario
6	Nathaniel	17	Ontario
	Erin	17	Ontario
7	Logan	17	Ontario
	Ethan	17	Ontario
8	Mia	15	Alberta
	Kate	16	Alberta
	Andrew	15	British Columbia

Appendix B: Gameplay Screenshots






AUDIENCE
AUDIENCE
AUDIENCE
AGE
INTENT TO BUY
INTERESTS
LOCATION
BRAND LOYALTY
PERSONALITY
INCOME
HOUSEWARES AD
LOCATION
INCOME
2
MEDICINE AD
AGE
INCOME
5
SHAVING CREAM AD
BRAND LOYALTY
LOCATION
1
RESTAURANT AD
LOCATION
INTERESTS
VIEWS
SEARCH HISTORY
VIEWS
VIDEO GAME AD
FOR ONE LOW MONTHLY PRICE
BRAND LOYALTY
AGE
1
DATA
PROFILE
TARGETS
AGE
Your profile info usually includes your age.
DATA
COOKIES
TARGETS
BRAND LOYALTY
Visiting brand websites can show that you like those brands.
DATA
COOKIES
TARGETS
INTERESTS
What you do on different websites shows what you're interested in.
TV SHOW AD
LOCATION
AGE
BEAUTY AD
PERSONALITY
INCOME
DATA
SHOPPING HISTORY
TARGETS
AGE
What you buy can show how old you are.
DATA
SEARCH HISTORY
TARGETS
BRAND LOYALTY
Searching for a brand can show you like it.
DATA
VIEWS
TARGETS
INTERESTS
What videos you've watched show what you're interested in.
CLOTHING AD
3
2
2
3
2


OPTIMIZATION
STICKINESS
Use your algorithms to make sure that users keep watching videos (instead of leaving the platform).
ALGORITHM
ALGORITHM
ALGORITHM
VIDEO
VIEWS
FRESHNESS
3
VIDEO
VIEWS
LINKS
1
VIDEO
VIEWS
LINKS
1
SHARES
SUBSCRIBERS
FRESHNESS
LINKS
SHARES
FRESHNESS
FRESHNESS
LIKES
BOOST
RETWEET ROOM
Retweet rooms are groups of accounts that all share each other's posts, making them look briefly more popular. Doubles the Freshness score for the video it's played on.
VIEWS
LINKS
CELEBRITY
LIKES
LINKS
CELEBRITY
BOOST
GOOGLE BOMB
Google bombing is making misleading websites to control what shows up in a Google search for a word. Doubles the Links score for the video it's played on.
SHARES
SUBSCRIBERS
1
1
2
2
2
1