YOUNG CANADIANS IN A WIRELESS WORLD, PHASE IV

ONLINE PRIVACY AND CONSENT

MediaSmarts

MediaSmarts

MediaSmarts is a Canadian not-for-profit charitable organization for digital media literacy. Our vision is that people across Canada have the critical thinking skills to engage with media as active and informed digital citizens. MediaSmarts has been developing digital media literacy programs and resources for Canadian homes, schools, and communities since 1996. MediaSmarts also conducts and disseminates original research that contributes to the development of our programs and resources and informs public policy on issues related to digital media literacy.

Website

mediasmarts.ca

Report Key Contact

Dr. Kara Brisson-Boivin
Director of Research
kbrisson-boivin@mediasmarts.ca

Report Credits

MediaSmarts Research Team:
Dr. Kara Brisson-Boivin, Director of Research
Dr. Samantha McAleese, Research and Evaluation Associate

Research Firm

Environics Analytics

Recruitment support

Lynn Huxtable, Senior Director, Administration and Education Relations, MediaSmarts
Environics Analytics

Data Analysis

Dr. Kara Brisson-Boivin, Director of Research, MediaSmarts
Dr. Samantha McAleese, Research and Evaluation Associate, MediaSmarts
Matthew Johnson, Director of Education, MediaSmarts
Marc Alexandre Ladouceur, Media Education Specialist, MediaSmarts

Report Design and Communication Support

Tricia Grant, Director of Marketing and Communications, MediaSmarts
Melinda Thériault, Marketing and Communications Assistant, MediaSmarts
Penny Warne, Web Manager, MediaSmarts

Advisory Committee

Dr. Jacquie Burkell, Professor, Faculty of Information & Media Studies, University of Western Ontario
Dr. Wendy Craig, Professor, Department of Psychology, Queens University
Dr. Faye Mishna, Professor, Factor-Inwentash Faculty of Social Work, University of Toronto
Dr. Leslie Shade, Professor, Faculty of Information, University of Toronto
Dr. Valerie Steeves, Professor, Department of Criminology, University of Ottawa

Suggested Citation

MediaSmarts. (2022). "Young Canadians in a Wireless World, Phase IV: Online Privacy and Consent." MediaSmarts. Ottawa.

Acknowledgements

Phase IV of Young Canadians in a Wireless world was made possible by financial contributions from the Canadian Internet Registration Authority (CIRA).

cira

MediaSmarts would like to thank the youth advisors who reviewed and provided valuable input on the survey questionnaires for Phase IV of Young Canadians in a Wireless World.

Land Acknowledgement

MediaSmarts acknowledges that it is based on the traditional unceded and occupied lands of the Algonquin Anishinaabeg. With gratitude, we acknowledge the territory to reaffirm our commitment and responsibility to building positive relationships with Inuit, First Nations, and Métis peoples from coast to coast to coast.

We strive to ground our research processes in care and reciprocity, and this includes being in a constant state of learning – especially when it comes to understanding the digital well-being and experiences of Indigenous peoples and communities across Canada. We commit to creating and maintaining respectful processes and relationships that recognize and seek to address power imbalances across the digital media literacy landscape.

Table of Contents

EXECUTIVE SUMMARY

Young Canadians in a Wireless World (YCWW) is Canada's longest-running and most comprehensive research study on young people's attitudes, behaviours, and opinions regarding the internet, technology, and digital media. MediaSmarts has surveyed over 20,000 parents, teachers, and students through this study since 1999. The study is currently in its fourth phase, and this report is the third in a series of reports that will be published on our website.

Like in previous phases of YCWW, we designed two surveys – one for students in grades 4 to 6 and one for grades 7 to 11. In both surveys, we organized questions into various categories:

- Digital devices at home
- Screen time at home
- Technology at school
- Online privacy and consent
- Trust
- Relationships and technology
- Handling online problems
- Opinions on various digital topics
- Digital and media literacy
- Demographics

From October to December of 2021, surveys were administered online to 1,058 youth across Canada. A total of 79 students participated in a classroom-based survey, and 979 youth participated in a GenPop (general population) survey.

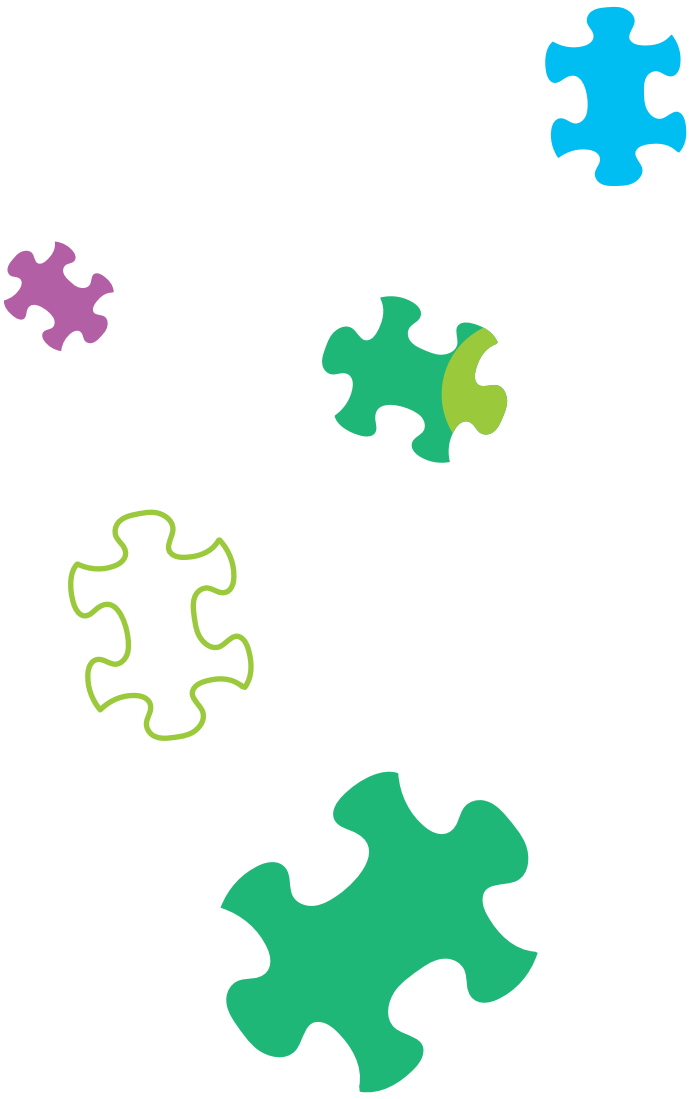
After several collaborative data analysis sessions, the MediaSmarts research team decided on the following topics and themes for the Phase IV reports:

- Life Online
- Encountering Harmful and Discomforting Content Online
- Privacy
- Online Meanness and Cruelty
- Sexting
- Digital Media Literacy

Phase IV will conclude with a Trends and Recommendations report to be released in 2023.

This report highlights findings related to online privacy and consent. We report on how youth share and protect their personal information online and how they manage their identities in online spaces. We also summarize findings related to how youth do or do not engage in various privacy practices – such as reading terms of service or using privacy settings. This report includes findings on how youth feel about various forms of interpersonal and corporate surveillance online and through digital technology. Finally, we touch on the importance of setting boundaries and building trust and how various rules and practices in the home and between adults and youth can impact online privacy.

We want to thank all students, parents, teachers, principals, and school administrators across Canada who engaged with this project in one way or another during Phase IV. YCWW remains the cornerstone of our work at MediaSmarts, and we are grateful for the support – in all forms – that sustains it.



INTRODUCTION

Young Canadians in a Wireless World (YCWW) is Canada's longest-running and most comprehensive research study on young people's attitudes, behaviours, and opinions regarding the internet, technology, and digital media. MediaSmarts has surveyed over 20,000 parents, teachers, and students through this study since 1999.

The findings from YCWW are used to set benchmarks for research on children's use of the internet, technology, and digital media and have informed policy on the digital economy, privacy, online safety, online harms and digital well-being, digital citizenship, and digital media literacy, among other topics. This research is also used to inform other projects at MediaSmarts and at other organizations, including academic institutions, within our vast and growing network of research partners.

The study is currently in its fourth phase. In 2019, MediaSmarts' research team conducted focus groups to get a kid's-eye-view of what is working for young people online and what needs to be changed or improved so that they get the most out of their online experiences. Additional focus groups with parents helped to round out discussions about what is needed to foster (collective) online resiliency. This qualitative work helped us prepare for a quantitative survey that began in 2021.

Phase IV of YCWW culminates in a series of research reports that will be published on the MediaSmarts website. Topics include:

- Life Online
- Encountering Harmful and Discomforting Content Online
- Privacy
- Online Meanness and Cruelty
- Sexting
- Digital Media Literacy

As in previous phases of this study, Phase IV will also conclude with a Trends and Recommendations report.

A departure from previous phases is the inclusion of a longer research methods report as part of the full series of YCWW reports. While each report will contain a brief section on the research method, this separate report offers a deeper dive into the methodological decisions and processes undertaken by the MediaSmarts research team during Phase IV of YCWW. The various pivots and adaptations taken during this phase deserve elaboration and will be of interest to other researchers who have made, and continue to make, shifts in their work due to the COVID-19 pandemic.

Overview: Young Canadians in a Wireless World

What follows is a summary of the previous three phases of YCWW and an introduction to Phase IV, which began with a qualitative research report published in January 2020.

Phase I (2000-2001) of YCWW involved 1,081 telephone interviews with parents across Canada and 12 focus groups with children ages 9-16 and parents of children ages 6-16 in Montreal and Toronto. The quantitative component of Phase 1 involved 5,682 self-administered paper-based surveys conducted in French and English classrooms in 77 selected schools across ten Canadian provinces.

At the time, parents were excited about the prospects of having their children use new technologies to help them learn and prepare for their future employment; they tended to exercise benign neglect online, trusting their children to come to them if they ran into problems. Youth participants felt that online media were completely private because adults did not have the skills to find them there, and they enjoyed a wide range of creative uses such as identity play and exploring the adult world. They also tended to trust corporations, calling them "friends."

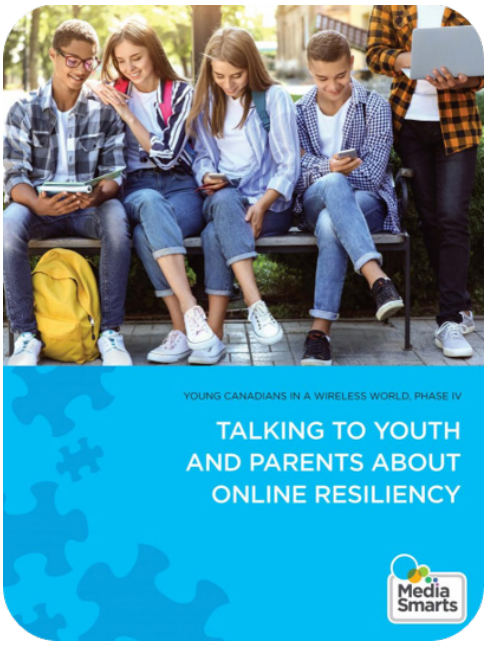
In Phase II (2004-2005), we conducted 12 focus groups with children ages 11-17 and parents of children ages 11-17 in Edmonton, Montreal, and Toronto. Additionally, 5,272 self-administered quantitative paper-based surveys were conducted in French and English classrooms in 77 selected schools across Canada with students in grades 4 to 11. We were pleased that 302 of the 319 classrooms from Phase I participated in Phase II.

Although youth participants still enjoyed many online activities, they were becoming aware of how often they were being monitored online. In response, they developed several strategies to keep their online lives private. On the other hand, adults were beginning to conclude that young people were mostly "wasting their time" playing games and chatting (precisely the things that drew youth online in the first place).

Phase III (2011-2014) involved ten one-hour key informant interviews with elementary and secondary teachers representing five regions across Canada: the North, the West, Ontario, Quebec, and the Atlantic. In addition to these interviews, MediaSmarts conducted 12 focus groups with children ages 11-17 and parents of children ages 11-17 in Calgary, Ottawa, and Toronto. The quantitative component of Phase III involved 5,436 surveys in school boards and schools in all ten provinces and all three territories.

In this third phase, adults began feeling overwhelmed by the reported dangers their children faced online, especially around cyberbullying. Youth participants indicated that cyberbullying was much less worrisome than adults feared; however, they felt that the protective surveillance they were being placed under in response to cyberbullying, and other perceived dangers, was stultifying and equated it to being "spied on" by family

members and teachers. They also argued that this kind of surveillance made it much more difficult for them to receive help from trusted adults when needed. Youth were also much less comfortable with the corporations that owned the sites and apps they used and questioned the regulatory model of click-through consent that meant others could collect and use their data. For example, 95% of the students surveyed said that the corporations that own the social media sites they use should not be allowed to see what they post there.



Phase IV of YCWW began with a qualitative research report that outlines findings from focus groups with youth ages 11 to 17 and a second set of focus groups with their parents in Toronto, Halifax and Ottawa. Generally, we discovered that young people are conscious about spending too much time online or on their digital devices and are also worried about the impact of misinformation on their online and learning experiences. Youth told us that they do not always want to rely on technology in school and some expressed feeling "creeped out" by the various forms of surveillance technology used in the classroom. Other findings related to teacher and parental controls over content and access to technology – both at school and at home – and how young people navigate or sometimes push back against those controls in favour of more creative uses like community engagement and self-expression. We also heard how these controls could contribute to an erosion of trust between young people and the adults in their lives.

Phase IV of YCWW also began with a name change to the project: from *Young Canadians in a **Wired** World* to *Young Canadians in a **Wireless** World*. This change in language speaks to shifts in digital technology and the online world since 1999 from a 'wired' to 'wireless' technological landscape that presents new opportunities and challenges for youth, parents, educators, policymakers, and the tech sector.

The findings from the qualitative portion of Phase IV helped us develop the surveys used in the quantitative portion. The following section on methods will outline the research plan for this quantitative research, the required shifts we made to that plan due to the COVID-19 pandemic, survey design, participant recruitment, data analysis, and a discussion of some limitations and considerations readers should keep in mind as you read through this report.

METHODS

Survey Design and Administration

As in previous phases of YCWW, we designed two surveys to explore the attitudes, activities, benefits, and challenges young people hold and experience when they are online and using digital devices – one for students in grades 4 to 6 and one for grades 7 to 11.[1] We organized questions into various categories:

- Digital devices at home
- Screen time at home
- Technology at school
- Online privacy and consent
- Trust
- Relationships and technology
- Handling online problems
- Opinions on various digital topics
- Digital and media literacy
- Demographics

The survey for youth in grades 4 to 6 had 82 questions, and the survey for youth in grades 7 to 11 had 100 questions. The additional questions in the second survey for older youth covered topics like sexting, pornography, and racist or sexist content.[2]

Also following from previous phases of YCWW, we planned to recruit participants from schools across Canada and hoped to survey between 6,000 and 8,000 students in the fall of 2020. Despite strong support for YCWW and MediaSmarts from school board representatives, fewer than half (n=25) confirmed their participation in Phase IV, citing complications related to the COVID-19 pandemic. Due to this low uptake, we extended the project timeline and adjusted our recruitment strategy and survey administration options, primarily by including a GenPop survey to reach a total of 1,000 participants.

From October to December of 2021, surveys were administered online, with the support of our partners at Environics Research Group, to 1,058 youth across Canada in two ways:

1. A total of 79 students participated in the classroom-based survey.
2. A total of 979 youth participated in a GenPop (general population) survey.

---

1 If you are interested in viewing the surveys used in Phase IV of *Young Canadians in a Wireless World*, please contact our Director of Research at info@mediasmarts.ca.

2 Both surveys, along with all the required consent documents, recruitment texts, teacher instructions and method of analysis, were approved by the Carleton University Research Ethics Board.

Young Canadians in a Wireless World: Phase IV Quantitative Survey Participation			
	Younger Grades 4 to 6 Ages 9 to 11	**Older Grades 7 to 11 Ages 12 to 17**	**Total**
Classroom Survey	28	51	79
GenPop Survey	371	608	979
Total	399	659	1058

Data Analysis

To reduce bias in reporting the survey data, MediaSmarts' research team engaged in a collaborative analysis process. We started by reviewing the initial analysis report provided by the team at Environics and used this document to identify the key themes for individual reports. We then revisited the data with our own queries informed by the literature, contemporary discussion and debate around the various topics, and MediaSmarts' established expertise in digital media literacy.

For each report, we identified a lead analyst who offered their initial thoughts on the outline of the report, including the themes and critical data points to be included. Discussion among the research and education teams at MediaSmarts helped confirm (or triangulate) the themes for each report and served to expand on the story we wanted to share based on the survey responses. We then began writing the themed reports based on the outcomes of this collaborative analysis process.

Limitations and Considerations

When we began planning this project in 2019, our initial goal was to reach 6,000 to 8,000 participants. While we did not reach this target—primarily due to the COVID-19 pandemic—we still reached over 1,000 survey respondents, thanks to participating principals and teachers and our research firm partner: Environics. Please read this report for full details on our recruitment strategy, including the pandemic pivots we made to reach our study goals.

Of note in this latest phase of YCWW is the additional demographic data (see Appendix A) we collected to help us understand how gender, race, disability, and sexual orientation might influence what young Canadians are experiencing online. We recognize the limits of making definitive claims due to our sample size, but our analysis

of this data reveals important snapshots and stories about young people's attitudes, behaviours, and opinions regarding the internet, technology, and digital media based on these various identity markers. We think this data is especially important given that it was collected during a global pandemic when so much of our lives were thrust online. We will continue to collect these demographic data in future projects and continue to work with other researchers and community partners to enhance and encourage an intersectional approach to digital media literacy studies.

We are also aware of the gaps in geographic representation – especially when it comes to representation from Northern Canada (Nunavut, Yukon, and the Northwest Territories). While complications related to the COVID-19 pandemic are partially to blame, ongoing challenges related to the digital divide in Canada also contribute to this low representation. MediaSmarts remains committed to closing the digital divide and will continue to work with partners on future projects that centre the experiences of young people in rural, remote, northern, and Indigenous communities.

The reports in this series present survey data alongside other research and evidence that support analysis and provide important context. Where it makes sense, we speak to the findings alongside our other research projects and draw on the expertise and insights of other researchers.

Finally, not only will the findings be used to inform a series of recommendations for educators, policymakers, and decision-makers in various sectors, but they will also inform future research projects at MediaSmarts.

We want to thank all students, parents, teachers, principals, and school administrators across Canada who engaged with this project in one way or another during Phase IV. YCWW remains the cornerstone of our work at MediaSmarts, and we are grateful for the support – in all forms – that sustains it.

ONLINE PRIVACY AND CONSENT

There is no question that Canadian youth enthusiastically use digital technology to communicate and publish content (see our Life Online report). That does not mean, however, that they do not value their privacy. In fact, youth in our survey are both more likely to participate in online spaces than when we conducted the Phase III study in 2013 and to take steps to actively manage who sees the content they post and limit the collection of their personal data. While it may seem paradoxical for young people's lives to have become both more public and more private, when viewed within the context of how youth conceptualize privacy, it becomes clear that having control of one's privacy is not a barrier but a *necessity* to be able to participate online.

Protecting Information and Managing Identities

8 in 10 youth say that they do not share their personal information online, and 9 in 10 say that they would address unwanted personal content posted about them by others.

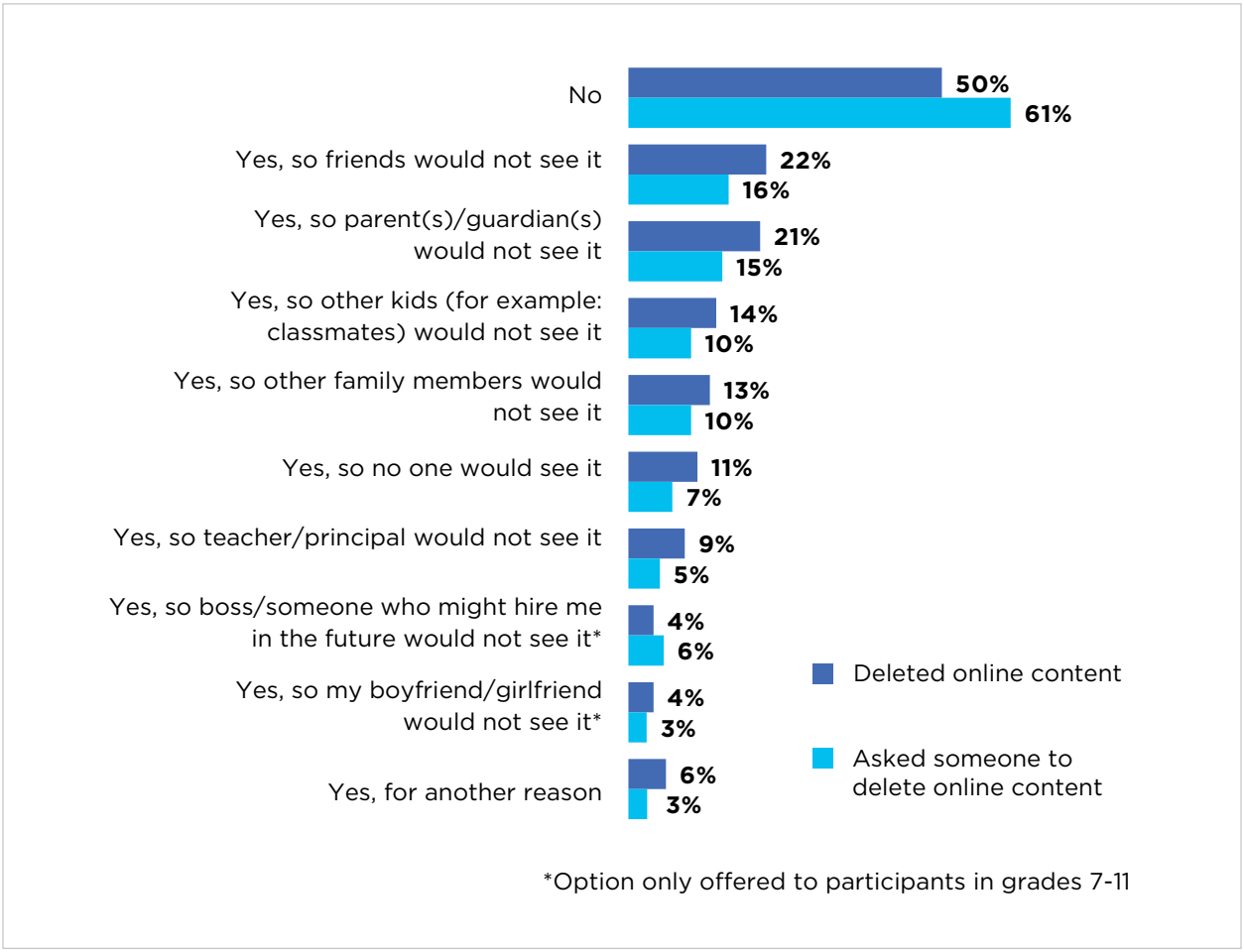
Half (50%) of youth have posed as someone else online or used a fake account to engage in various online spaces.

The first set of questions about privacy in the YCWW Phase IV survey focused on how young people share, protect, and manage their personal information online. When it comes to sharing personal information, eight in ten (82%) youth say they do not share things like their home address, phone number, or full birthday anywhere online. While there are some demographic differences (for example, **LGBTQ+** youth and youth with a disability are more likely to say they share personal information online), this initial finding demonstrates that young people are generally mindful of what they post and share while engaging in online spaces.

LGBTQ+ is inclusive of any participant who identified as lesbian, gay, bisexual, asexual, questioning, or any other diverse sexual orientation.

Regarding other kinds of content, such as photos, comments, videos, and memes, we asked participants if they had ever deleted anything after posting it to prevent someone else from seeing it. Half (50%) of participants said they did this, and 39% of youth said they had asked someone else to delete content posted about them without their consent or approval. **Figure 1** summarizes why youth either delete or ask others to delete content.

Figure 1: Deleting Online Content



Girls (13%) and LGBTQ+ youth (17%) are more likely to delete online content so that no one can see it (compared to 7% of boys and 10% of heterosexual youth). While the number of participants who identified as transgender and gender diverse is not large enough to be statistically significant (n=13), 7 in 10 indicated that they had deleted online content so someone else would not see it, and 6 in 10 have asked others to delete online content about them.

White youth are more likely to delete online content (23%, compared to 16% of **racialized youth**) and to request that others delete online content about them (16%, compared to 13% of racialized youth) so that their parents or guardians do not see it. **Youth with a disability** are more likely to delete online content (63%, compared to 44% of youth without a disability). Finally, younger participants are more likely to say that they have never deleted online content (57%, compared to 46% of older youth) and are less likely to request that someone else deletes online content about them (66%, compared to 58% of older youth).

In the Phase IV survey, we asked youth to self-identify regarding race (see Appendix A for a breakdown of the response categories). When we say 'racialized' throughout this report, we are referring to youth who identified as Indigenous, African/West Indian, South Asian, Middle Eastern, or South/Latin American.

In the Phase IV survey, we asked participants to self-identify regarding physical disabilities, intellectual/cognitive/learning disabilities, and mental illness. The breakdown for each is available in Appendix A. When we say disability throughout the report, we are referring to any of the three categories.

There were some significant changes in these questions compared to the Phase III report in 2014. In particular, youth were less likely to want to hide content from all audiences: the number of participants who had deleted content so that no one would see it declined from 24% in Phase III to 11%, and the number who had asked someone else to delete something so that no one would see it dropped from 24% in Phase III to just 7%. This provides further evidence for the findings in some of our qualitative research since Phase III that youth are more concerned about managing audiences – determining *who* sees *what* – than with deleting content completely.

Moving from this, we asked participants what they would do if someone posted a photo or video of them online that they did not want other people to see (in other words, without their consent). Nine in ten youth said they would act if this happened, and most (64%) indicated that they would ask the person to take the content down (see **Figure 2**).

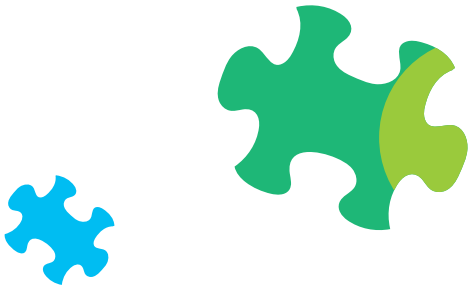
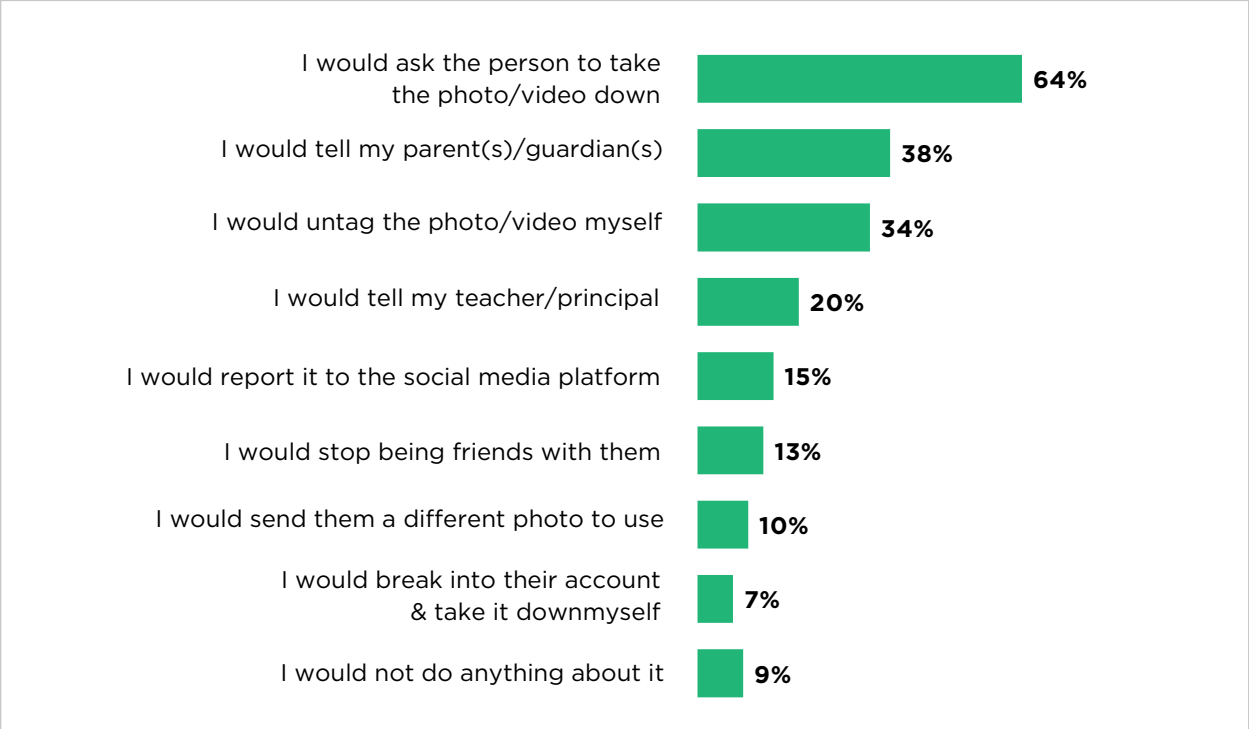


Figure 2: Addressing Unwanted Personal Content Posted by Others

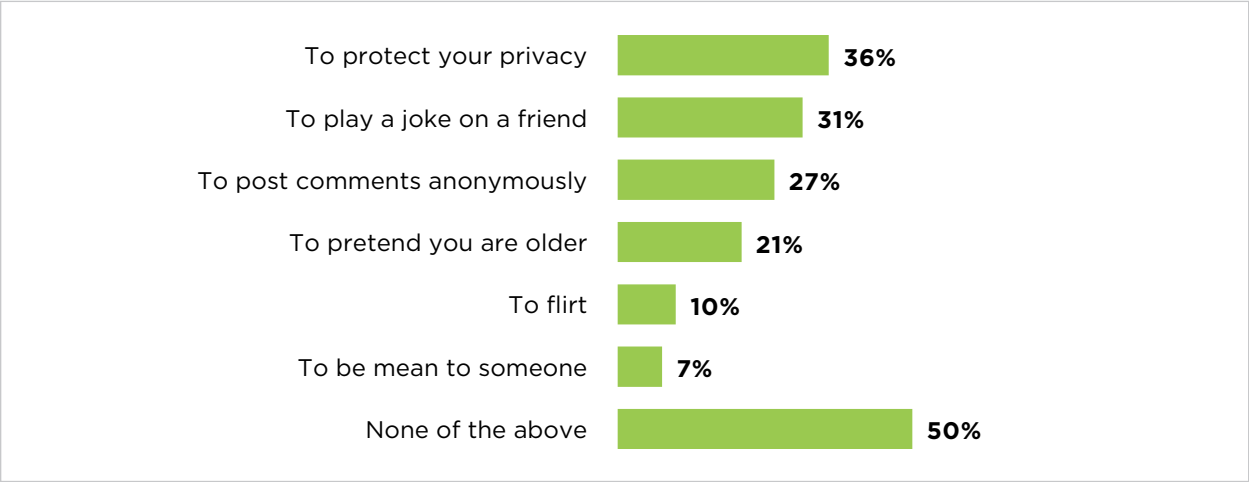


Boys are slightly more likely to do nothing (11%, compared to 7% of girls), and girls are more likely to ask the person to delete the content (68%, compared to 59% of boys), tell a parent or guardian (43%, compared to 34% of boys), or tell a teacher (22%, compared to 18% of boys). Transgender (86%) and gender-diverse youth (83%) (n=13) are most likely to ask the person to delete the content. LGBTQ+ youth are somewhat more likely to ask the person to delete the content (69%, compared to 63% of heterosexual youth), tell a parent or guardian (41%, compared to 37% of heterosexual youth), and tell a teacher or principal (24%, compared to 19% of heterosexual youth). See Appendix B for graphs that visualize demographic differences in the responses to this question.

Older youth are more likely to do nothing about the posted content (10%, compared to 6% of younger youth), untag themselves from the post (37%, compared to 29% of younger youth) or report the content to the platform where somebody posted it (17%, compared to 12% of younger youth). Younger youth, on the other hand, are considerably more likely to tell a parent or guardian (47%, compared to 33% of older youth) or a teacher (27%, compared to 15% of older youth). White youth are more likely to ask the person who posted the content about them to delete it (67%, compared to 58% of racialized youth) or untag themselves from a post (37%, compared to 29% of racialized youth). Youth without a disability are more likely to respond to this situation by telling their parents (41%, compared to 31% of youth with a disability), while youth with a disability are more likely to untag themselves (39%, compared to 32% of youth without a disability).

The last question we asked to help us understand how young people manage their identities online was whether participants have ever said they were someone else online (see **Figure 3**). Half (50%) of participants said they have posed as someone else or used a fake account online, and most (36%) say they do this to protect their privacy. Another 27% indicated that they do this to post comments anonymously.

Figure 3: Fake/Impersonated Online Accounts



Generally, older youth are more likely to report using fake accounts in online spaces (52%, compared to 46% of younger youth). Boys are somewhat more likely to use fake accounts (53%, compared to 47% of girls) and primarily do so to play a joke on a friend. Transgender youth are most likely to use fake accounts to play a joke on a friend (71%, n=7), and gender-diverse youth are most likely to use fake accounts to protect their privacy and post comments anonymously (33%, n=6). Racialized youth are more likely to use fake accounts specifically to protect their privacy (40%, compared to 35% of white youth). Youth with a disability are more likely to use a fake account, for all the above reasons, than those without a disability.

Other notable findings related to the use of fake accounts in online spaces include:

- Youth with their own smartphone are more likely to use a fake account for all the above reasons compared to youth without their own smartphone.
- Youth who share personal information online are more likely to use a fake account for all the above reasons compared to youth who say they do not share personal information online.
- Youth who say they know how to protect themselves online are more likely to use fake accounts to protect their privacy.

Engaging in Privacy Practices

Almost half of participants (48%) say they never read privacy policies or terms of service, and just over half (52%) of youth use privacy settings when using digital devices or engaging in online spaces.

Most participants (60%) say that they use privacy settings to hide the content they post online from strangers.

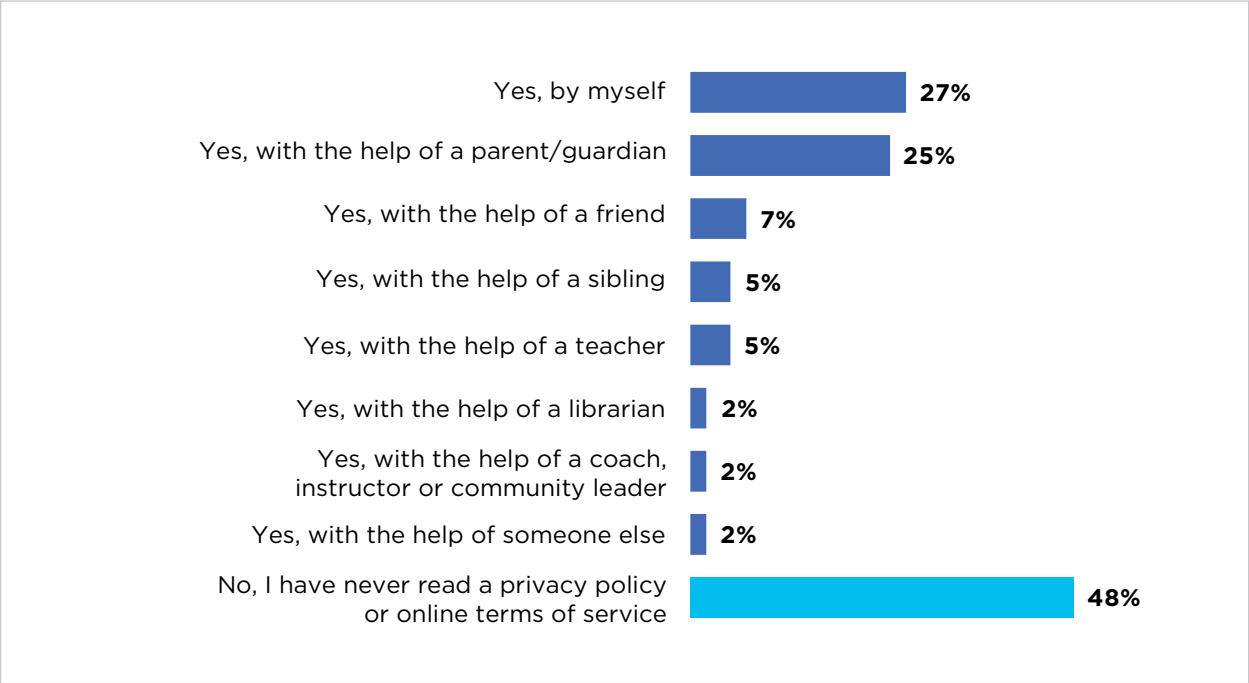
This section of the report summarizes findings related to how young people engage with privacy policies and settings. Stereotypes about young people suggest they do not read privacy policies or terms of service because they do not care about online privacy.[3] However, our qualitative research on privacy and consent shows that most youth (and many adults) do not read these documents because they are too long and too complicated and not because they do not care about protecting their personal information.

First, and not all that surprising, given what we know from previous research, almost half of the participants (48%) say they never read privacy policies or terms of service for the websites they visit or apps they use (see **Figure 4**). Those who do read these documents mainly do so by themselves (27%) or with the help of a parent or guardian (25%). Very few reported that this is something they do with a teacher (5%) or a librarian (2%).

There are some demographic differences related to reading privacy policies or terms of service. For example, older youth are considerably more likely to have read these documents on their own (33%, compared to 16% of younger youth), and when younger youth do read these documents, they are more likely to do so with the help of a parent or guardian (34%, compared to 20% of older youth).

3 Adorjan, M., & Ricciardelli, R. (2019). A new privacy paradox? Youth agentic practices of privacy management despite "nothing to hide" online. Canadian Review of Sociology, 56(1), 8–29.

Figure 4: Reading Privacy Policies or Terms of Service



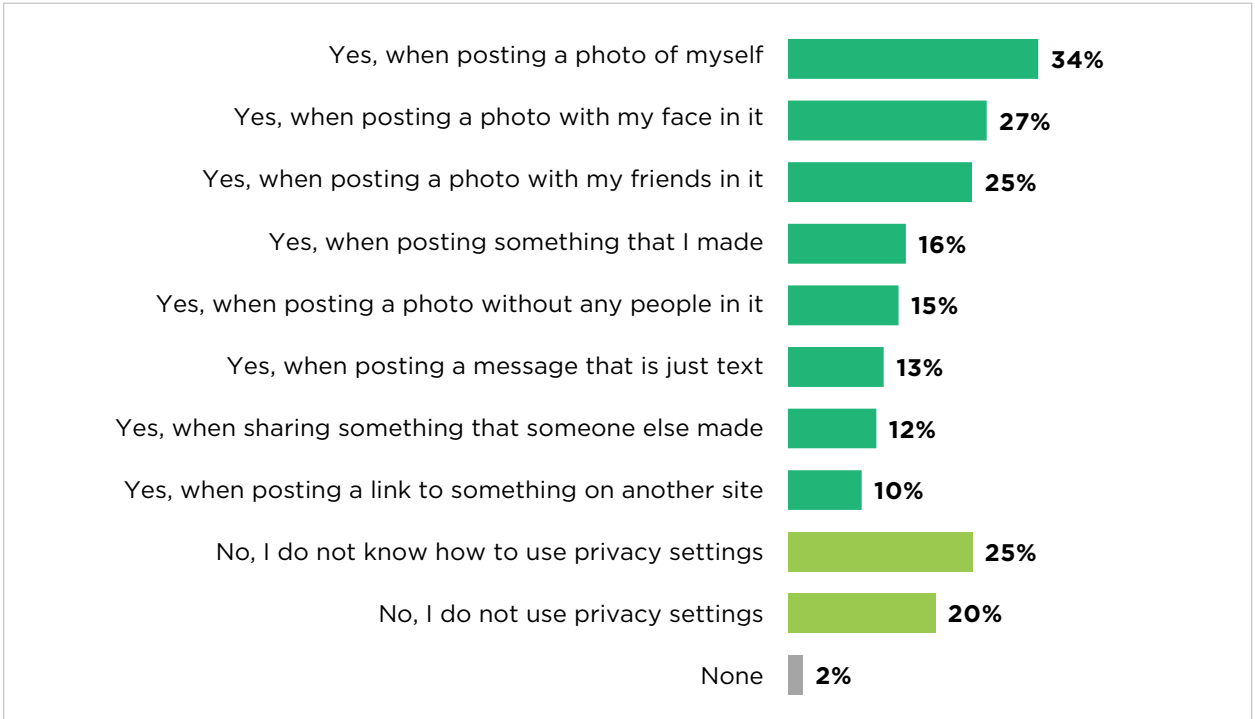
Additional analysis related to this question about reading privacy policies or terms of service reveals the following:

- Youth who say they share personal information online are more likely to read privacy policies or terms of service (75%, compared to 45% of youth who say they do not share personal information online) and primarily by themselves or with the help of a parent or guardian.
- Youth who feel the internet is safe are somewhat more likely to read privacy policies and terms of service (53%, compared to 46% who do not feel the internet is safe). Similarly, youth who say they know how to protect themselves online are more likely to read these documents (52%, compared to 42% of youth who say they do not know how to protect themselves online).
- A worryingly large number of youth (63%) mistakenly believe that the presence of a privacy policy means a website will not share their personal information with others. Interestingly, those who believe this are *more* likely to say they have read a privacy policy or terms of service (54%, compared to 44% of youth who do not believe this).

This last point is concerning as it highlights the opacity of many privacy policy documents produced by various online platforms. We know that many platforms, specifically social media platforms, share and broker personal information regularly. But this survey result tells us that these practices are not made clear in privacy documents, and therefore, many young people are interacting in these online spaces with a false sense of privacy and security.

Next, we asked participants whether and when they use various privacy settings on social networking sites or websites (see **Figure 5 and see Appendix C for graphs that visualize demographic differences in the responses to this question**). Here we learn that slightly more than half of youth (52%) make use of privacy settings when engaging in online spaces and primarily when posting photos of themselves online (34%), posting a photo with their face in it (27%), and posting a photo with their friends in it (25%). Girls (56%, compared to 47% of boys), transgender (57%, n=7), gender diverse (100%, n=6), older youth (56%, compared to 46% of younger youth), heterosexual youth (54%, compared to 42% of LGBTQ+ youth), and youth with a disability (62%, compared to 49% of youth without a disability) are all more likely to use privacy settings. These findings align with other research on privacy and consent, highlighting that young people "seem to change privacy settings more often than older people."[4]

Figure 5: Use of Privacy Settings



4 Custers, B., van der Hof, S., & Schermer, B. (2014). Privacy expectations of social media users: The role of informed consent in privacy policies. Policy & Internet, 6(3), 268–295.

Additional analysis related to this question about using privacy settings reveals the following:

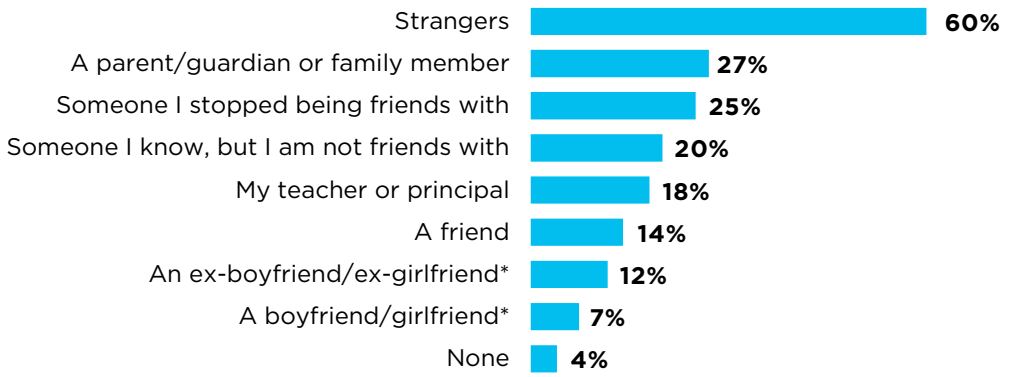
- Youth who share personal information online are more likely to use privacy settings on websites or apps (75%, compared to 47% of youth who say they do not share personal information).
- Youth who talk to people they have only met online (not in person) are more likely to say they use privacy settings (62%, compared to 36% of youth who do not talk to online-only contacts).
- Youth who post videos of themselves online are more likely to say they use privacy settings (64%, compared to 36% of youth who do not post videos of themselves).
- Youth who read privacy policies or terms of service are more likely to use privacy settings (67%, compared to 37% of youth who do not read these documents).
- Youth who say they know how to protect themselves online are more likely to use privacy settings (55%, compared to 40% of youth who do not believe they know how to protect themselves online).

Just less than half (46%) of participants said that they do not use privacy settings at all. One-quarter (25%) of youth said they do not use these settings because they do not know how – younger youth (35%, compared to 19% of older youth) and LGBTQ+ youth (33%, compared to 23% of heterosexual youth) are more likely to report that this is the reason they do not use privacy settings.

Later in the survey, we asked participants about what they would like to learn more about when it comes to various digital media literacy topics, and 37% of respondents said that they would like to learn more about how to use privacy settings. We will address this in more detail in our forthcoming report focused specifically on digital media literacy.

Further, most participants in this study (60%) say they use privacy settings to hide content from strangers (see **Figure 6**). Other top answers indicate that young people use privacy settings to hide content from a parent or guardian or another family member (27%), someone they stopped being friends with (25%) or someone they know but are not friends with (20%).

Figure 6: Who Content is Hidden From

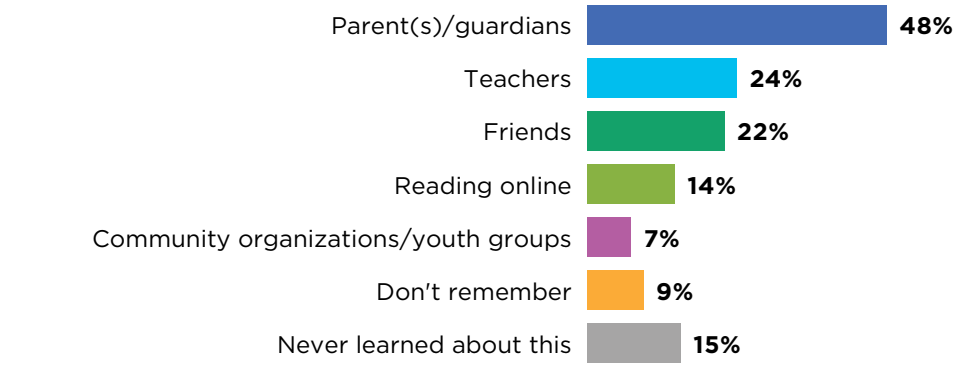


Girls are more likely to use privacy settings to hide content they post from strangers (64%, compared to 52% of boys) and acquaintances (24%, compared to 15% of boys), while boys are slightly more likely to use privacy settings to hide content they post online from parents or other family members (30%, compared to 24% of girls). Gender-diverse youth (n=6) are more likely to use privacy settings to hide content from strangers (83%) and someone they stopped being friends with (50%). Older youth are also more likely to use privacy settings to hide content from strangers (64%, compared to 49% of younger youth) and people they used to be friends with (27%, compared to 19% of younger youth). Younger youth are more likely to use privacy settings to hide content from parents, guardians, or other family members (30%, compared to 25% of older youth) or friends (17%, compared to 12% of older youth). LGBTQ+ youth report using privacy settings to hide the content they post online from former friends (41%, compared to 23% of heterosexual youth) and former romantic partners (29%, compared to 10% of heterosexual youth). Finally, youth with a disability are more likely to use privacy settings to hide content from parents or other family members (36%, compared to 23% of youth without a disability) and friends (20%, compared to 11% of youth without a disability).

As mentioned previously, 37% of respondents said they would like to learn more about how to use privacy settings; an increase from the previous phase of this study.[5] When we asked how or from whom they are *currently* learning about privacy settings, most participants (48%) said they were getting this information from their parents or guardians (see **Figure 7**).

5 In Phase III of YCWW, conducted in 2013 with a sample size of 5,436 students in grades 4 to 11 from across Canada, 31% of youth said they would like to learn more about privacy settings.

Figure 7: Learning About Privacy Settings



Some demographic differences of note based on further analysis indicate that:

- Girls are more likely to learn about privacy settings from their teachers and parents or guardians, while boys report that they learn about such things from their friends.
- Gender-diverse youth (n=13) are most likely to learn about privacy settings from parents or guardians.
- Older youth say they learn about privacy settings from their friends and by reading related content online, while younger youth say they learn about them from teachers or do not learn about them at all.
- Heterosexual youth report learning about privacy settings from parents, teachers, or friends, while LGBTQ+ youth are more likely to say that they have never learned how to use them.
- Racialized youth are more likely to mention learning about privacy settings from various sources, but especially from friends and through reading content online.
- Youth without a disability are more likely to say that they have never learned about privacy settings, and youth with a disability say that they do not know or do not remember where they learned about how to use these settings.

Questioning (Corporate) Surveillance

Three-quarters (74%) of youth think that family members should be allowed to use devices or apps to track where they are, but only 2% of youth agree that online companies (like marketing companies) should be allowed to track their location.

Most youth want their content seen by their friends (75%) or their parents, guardians, or other family members (68%). However, few want their content to be accessible to the police (8%), online companies (6%), or future employers (3%).

Just over half (55%) of youth trust online companies to make good decisions about their privacy and safety online.

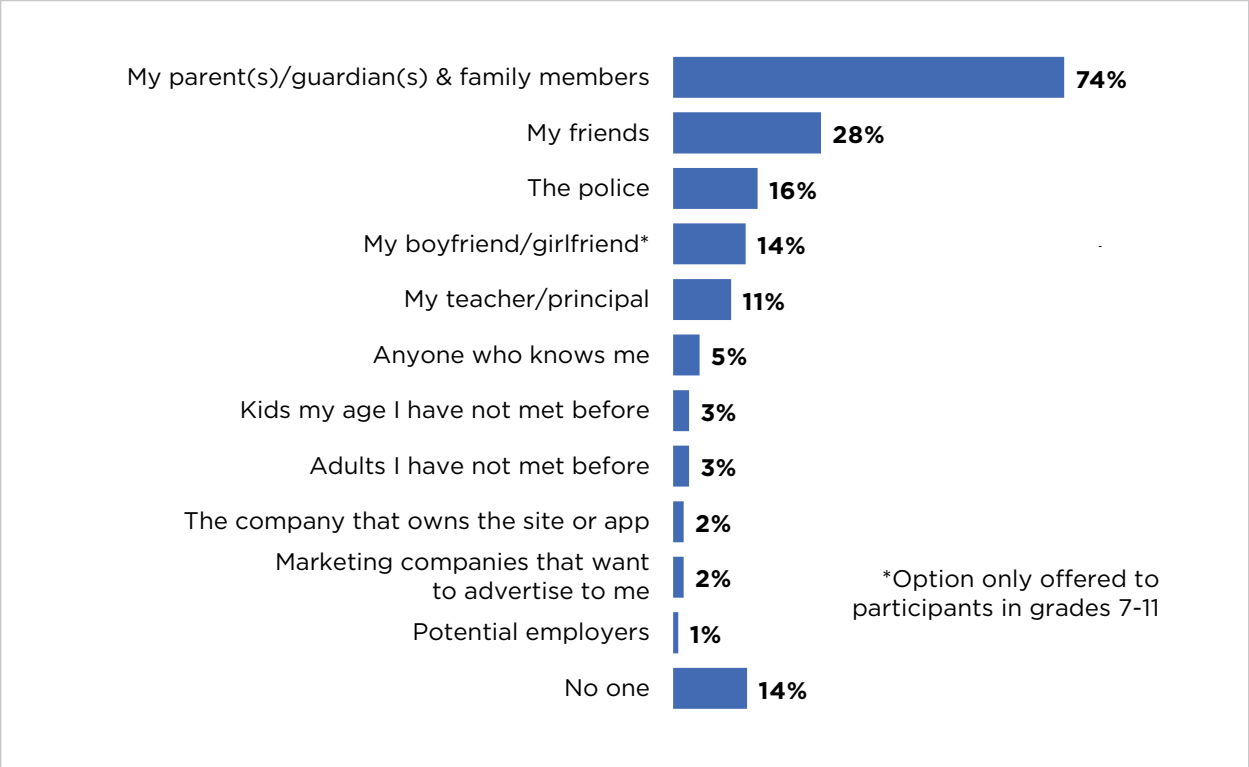
In our first report in the YCWW Phase IV series – Life Online – we reported on questions we asked participants about school email accounts and the use of online learning management systems at school. To recap:

- Seven in ten (72%) youth say that their school has given them an email account.
- Seven in ten (71%) youth say that they must use an online learning management system for school.

We bring these findings up again in this report on privacy to speak to them alongside findings from the qualitative portion of YCWW Phase IV. In our focus groups with youth, we heard that while school email accounts and online learning management systems might make it easier for students to work collaboratively and communicate with teachers, there were also serious concerns about surveillance. For example, Myah (aged 12) described the teacher monitoring the platform as "scary" and worried that her teacher or other school staff were reading the messages she was writing to her friends. Francine (aged 11) also shared these concerns and explained how she and her friends address every email message to its intended recipient and then add "and Hi to everyone else" to make it known that they knew educators were listening. This "creepiness" and surveillance facilitated by school-based tech and platforms reduced their trust in the technology and their teachers. Future research that focuses more specifically on the use of technology and online learning platforms in the classroom would be valuable to understand the concerns and experiences of both students and teachers.

In the Phase IV quantitative survey, we also asked participants about tracking location apps on their devices and whom they think should be allowed to use these functions (like GPS) to see where they are. Three-quarters (74%) of youth think that family members *should* be allowed to use devices or apps to track where they are, and many (28%) also would not mind if their friends did this (see **Figure 8**).

Figure 8: Tracking Location Apps on Devices



Older youth are more likely to say that their friends could use these apps to track their location (32%, compared to 20% of younger youth), and younger participants were more likely to be ok with their parents or other family members using tracking apps on their devices (81%, compared to 70% of older youth).

Compared to our YCWW Phase III survey,[6] there has been a significant decrease in the number of youth who believe the police should be able to track their location (35% in 2013, compared to 16% in 2021).

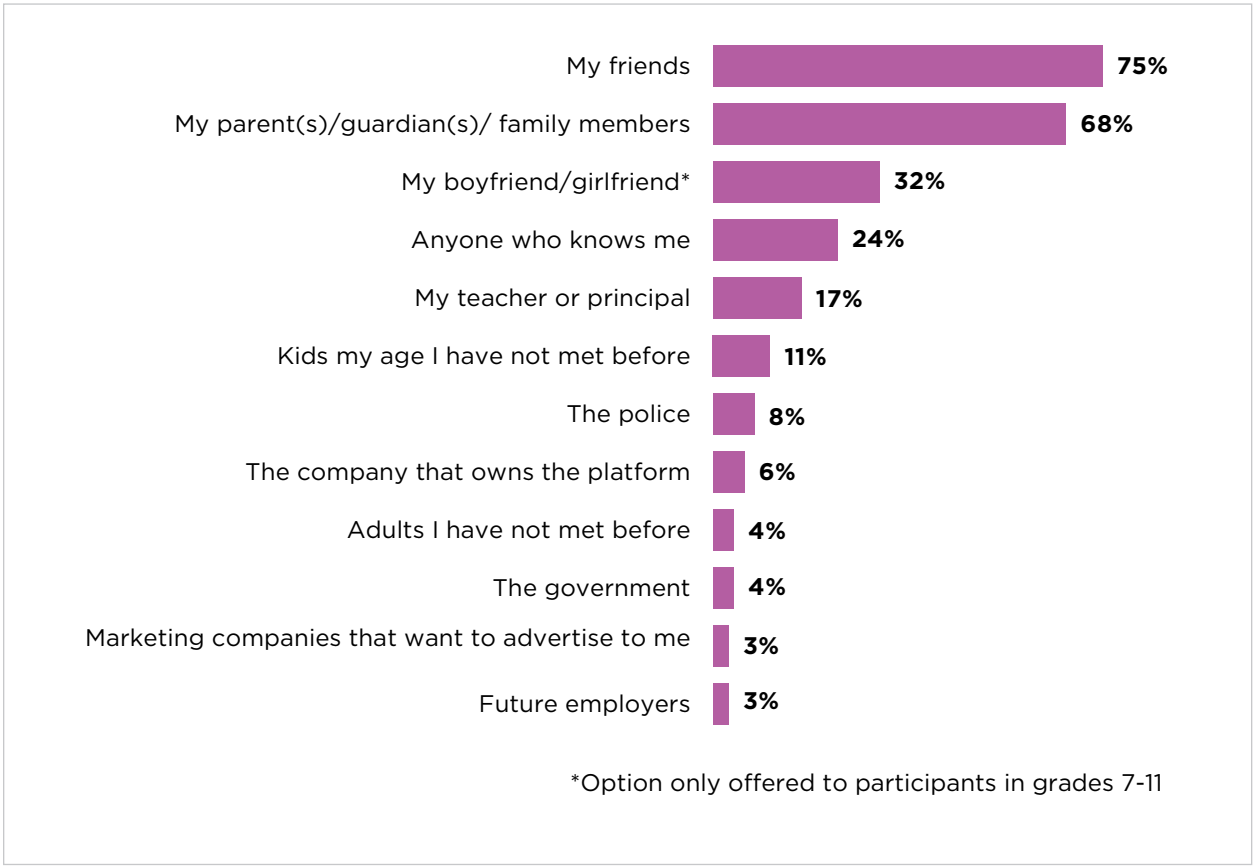
Of note here is that only 2% of participants agree that either the company that owns the sites or apps they are accessing or marketing companies that want to advertise to them should be allowed to track their location. This aligns with findings from our qualitative research on privacy and consent, in which some youth were concerned about the

6 Phase III of YCWW was conducted in 2013 and included a sample size of 5,436 students in grades 4 to 11 from across Canada.

granularity of location data collected by online companies and wanted to see clear limits placed on such data collection. For example, there was an agreement that users should have to *opt-in* to location settings on devices and apps rather than discover that they are being tracked unknowingly. In other words, young people do not want corporations to take and use their data without their explicit and meaningful consent.

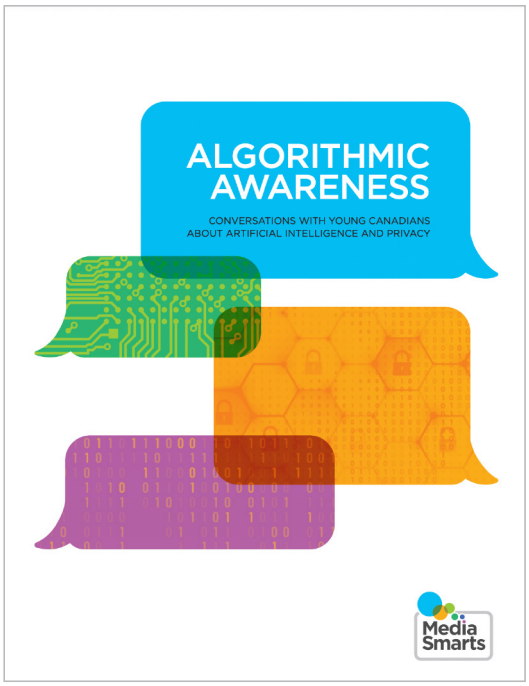
We also asked participants who should be able to see what they post on social networking platforms (see **Figure 9**). Responses tell us that while most youth want their content to be seen by their friends (75%) or their parents, guardians, or other family members (68%), few want their content to be accessible to the police (8%), the company that owns the platform (6%), adults whom they have never met before (4%), the government (4%), marketing companies (3%), or future employers (3%). Compared to our YCWW Phase III survey[7], there has been a significant decrease in the number of youth who believe the police (8% in 2021 compared to 28% in 2013), companies that own the site or app (6% in 2021 compared to 17% in 2013), or the government (4% in 2021 compared to 20% in 2013) should be able to see the content they post online.

Figure 9: Who Should See Social Media Posts



7 Ibid.

These findings are consistent with our two recent qualitative projects on privacy and consent and artificial intelligence and algorithms. For example, in these studies, participants expressed concern over how personal data scraped from social media sites might be used by employers in hiring and firing decisions. Andrew (aged 16) described this as "a breach of privacy" or "blackmail" and was concerned about the permanence of data and how employers might use all kinds of information to make unfair assumptions about a person. Others shared worries about how some employers use artificial intelligence or machine learning to make hiring decisions and questioned the fairness of such practices – especially for those who already experience racism, marginalization, and discrimination. These concerns about the uses (and future consequences) of personal data taken from social media engagement led to recommendations for data erasure policies[8] and other practices that might help youth (and others) gain more control over how their data is shared and used.

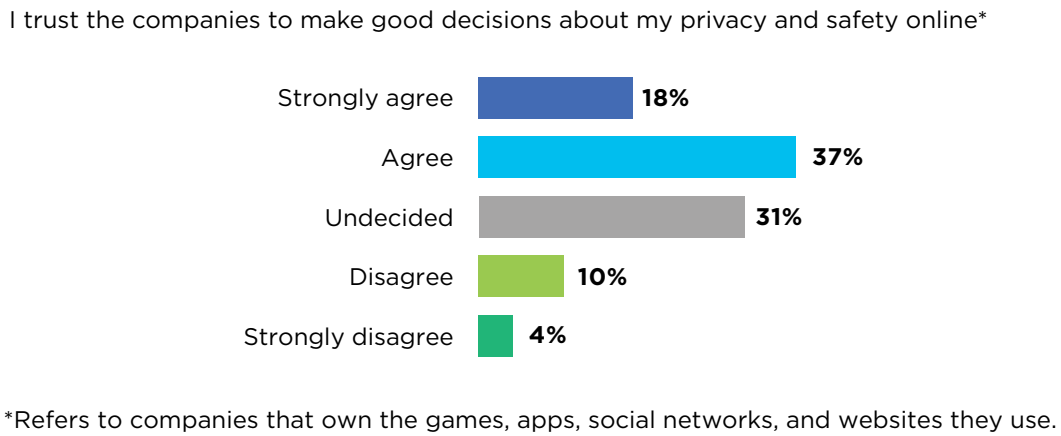


Girls are more likely to allow their parents, guardians, or family members (73%, compared to 64% of boys) to view their social media posts. Younger youth are also more comfortable with family viewing what they post online (75%, compared to 64% of older youth) and are also more likely to allow social media post views by teachers or principals (25%, compared to 13%). Older youth are most likely to allow views by their friends (79%, compared to 69% of younger youth) and are also more likely to allow anyone who knows them (29%, compared to 16% of younger youth) and strangers (5%, compared to 3% of younger youth) to see their posts. Gender-diverse youth (n=13) are also most likely to allow their friends to view their social media posts. LGBTQ+ youth are more comfortable with sharing content with peers their age whom they have not met offline (73%, compared to 64% of heterosexual youth), and we see the same with youth who have a disability (15%, compared to 9% of youth without a disability). This aligns with findings in the Life Online report that highlight the importance of online spaces and communities to LGBTQ+ youth and youth with disabilities.

8 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.

These findings about tracking and intended or preferred audience dovetail with the responses to another question we asked about trust. For example, when asked whether youth agree or disagree with the statement: "I trust companies to make good decisions about my privacy and safety online," only 55% agreed (see **Figure 10**). Boys (60%, compared to 52% of girls and 43% of transgender youth, n=7), heterosexual youth (59%, compared to 30% of LGBTQ+ youth), white youth (59%, compared to 51% of racialized youth), and youth with a disability (83%, compared to 54% of youth without a disability) were more likely to agree with this statement.

Figure 10: Trust in Online Companies



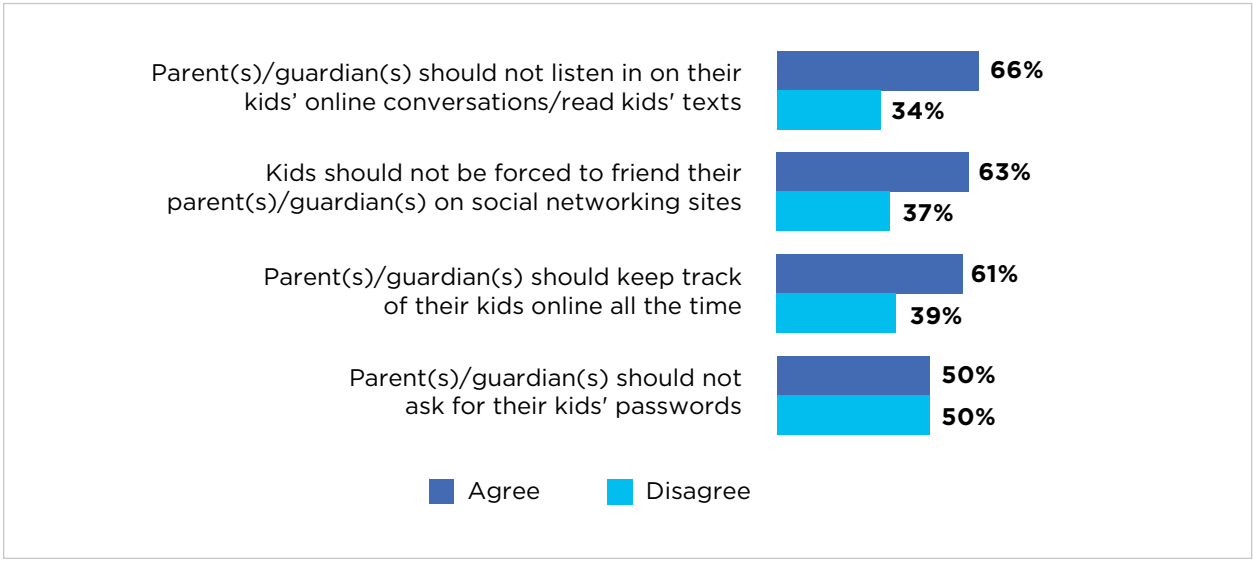
Some young people (27%) are interested in learning more about how companies collect and use their personal information, including location (a discussion that we will return to in further detail in the forthcoming report on digital media literacy). However, our previous qualitative research on privacy and algorithms has consistently found that when youth become aware of the extent and impact of corporate data collection they become considerably more interested in learning about it. The same research has also demonstrated that youth want more transparency around how their personal data is collected and shared online, more protection from the unintended consequences of these data-sharing practices, and more control over their data overall.

Setting Boundaries and Building Trust

Six in ten (61%) youth agree that parents or guardians should keep track of what their children are doing online, and almost half (48%) said that they would share their passwords with a parent or guardian. More than half of youth (51%) say they have a rule about posting their contact information online.

In this final section of the report, we summarize findings from the YCWW Phase IV survey related to how young people feel about the boundaries and rules set by adults in their lives that might impact their online privacy. First, we asked participants to agree or disagree with a series of statements (see **Figure 11**) and discovered that most youth agree that parents or guardians should respect their online privacy but are divided regarding password sharing. Additionally, six in ten (61%) youth agree that parents or guardians should keep track of what their children are doing online (which aligns with what we reported earlier in relation to the use of tracking apps on devices). This indicates that while young people think adults should have a *general* sense of what young people are doing online (e.g., what sites, apps, or platforms they are using), they are more uneasy about sharing the *specifics* of their online lives – like their texts, conversations, and posts.

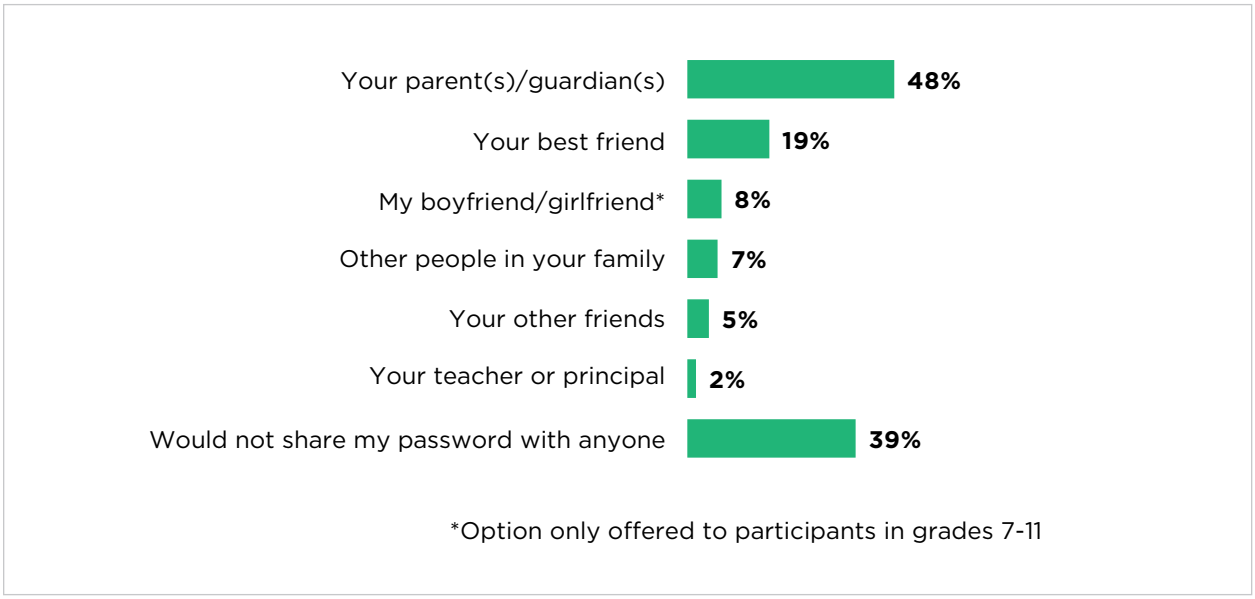
Figure 11: Parental or Guardian Control



Girls are somewhat more likely to say that their parents or guardians should keep track of what young people are doing online (65%, compared to 58% of boys), and boys are more likely to say that parents or guardians should not ask for their children's passwords (53%, compared to 46% of girls). 86% of transgender youth (n=7) agree that parents and guardians should not listen in on their kids' online conversations or read their kids' texts and that kids should not be forced to friend their parents or guardians on social networks. Racialized youth are also more likely to say that their parents or guardians should keep track of their online activities (66%, compared to 59% of white youth). Most older youth (67%) and LBGTQ+ youth (66%) agree that parents or guardians should not listen to or read their online conversations. Heterosexual youth are more likely to say that parents or guardians should not ask for their children's passwords (51%, compared to 41% of LGBTQ+ youth). Finally, youth with a disability are somewhat more likely to agree that they should not be forced to friend their parents or guardians on social networking sites (67%, compared to 61% of youth without a disability) and that parents or guardians should not ask for their children's passwords (56%, compared to 48%).

We asked another question in the survey about password sharing that confirms the results of the question above. Almost half (48%) of youth said they would share their passwords with a parent or guardian (see **Figure 12**). Others indicated that they would share passwords with a best friend (19%), a romantic partner (8%), or other people in their family (7%), whereas 39% of participants indicated that they would not share their passwords with anyone.

Figure 12: Sharing Passwords



Younger youth (60%, compared to 41% of older youth), girls (51%, compared to 46% of boys and 43% of transgender youth, n=7), LGBTQ+ youth (53%, compared to 47% of heterosexual youth), white youth (50%, compared to 46% of racialized youth) and youth with a disability (54%, compared to 46%) are more likely to share their passwords with parents or guardians.

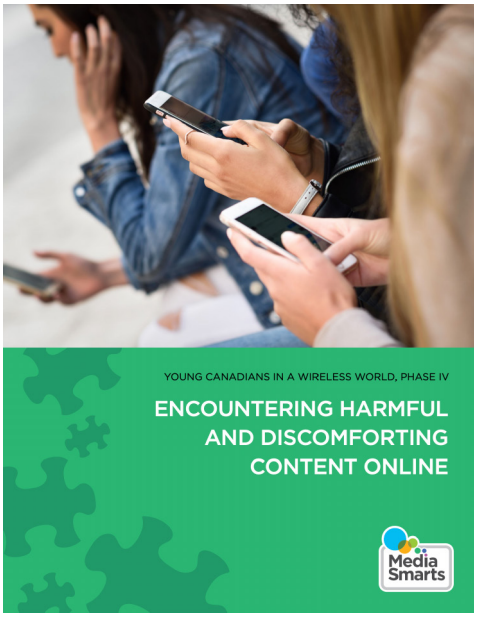
Regarding household rules for online activities related to privacy, we note that more than half of youth (51%) say they have a rule about posting their contact information on the internet. Additional analysis of questions related to adult supervision and household rules demonstrates the role that building trust and setting boundaries can play concerning how youth manage their personal information and navigate privacy online. For example, youth who usually go online with an adult are somewhat more likely to tell their parents or guardians about unwanted personal content posted by others (42%, compared to 35% of youth who are rarely with an adult online), and they are more likely to tell a teacher or principal about unwanted content (22%, compared to 17% of youth who are rarely online with an adult). Furthermore, youth who usually go online with an adult are more likely to read privacy policies and terms of service (59%, compared to 48% of youth who are rarely with an adult online) and considerably more likely to have read these sorts of policies with the help of a parent or guardian (40%, compared to 16% of youth who are rarely online with an adult). On the other hand, youth who never go online with a parent are more likely to say they do not use privacy settings (55%, compared to 42% of youth who are usually online with an adult). Additional findings related to adult supervision include:

- Youth who are usually online with an adult are least likely to hide content from a parent, guardian, or someone else in their family (23%, compared to 33% of youth who are rarely with an adult while they are online).
- Youth who are usually online with an adult are more likely to agree that their parents, guardians, or other family members should be allowed to see what they post on a social network (76%, compared to 64% of youth who are rarely online with an adult).
- Not surprisingly, youth who are usually online with an adult are more likely to say they would share their password with a parent or guardian (58%, compared to 45% of youth who are rarely online with an adult).

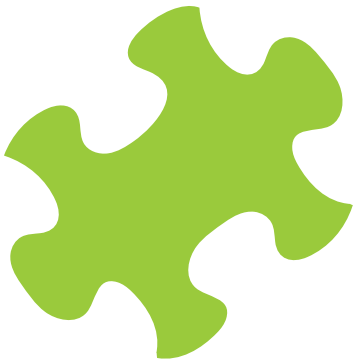
Regarding the relationship between household rules and online privacy, we note the following:

- Youth with a household rule about talking to a parent or guardian about anything that makes them uncomfortable online are more likely to talk to a parent or guardian about unwanted personal content posted in online spaces.
- Youth with a household rule about treating people online with respect are more likely to ask the person who posted unwanted personal content online to delete the content.
- Youth with household rules (in all instances of the rules we asked about) are less likely to use fake accounts or say they are someone else online. This is also true of school rules about cyberbullying. Youth who are aware of school rules about cyberbullying are less likely to use fake accounts or say they are someone else online.
- Youth with a household rule about talking to parents or guardians are less likely to hide content from their parents, guardians, or other family members and are more likely to hide content from strangers.

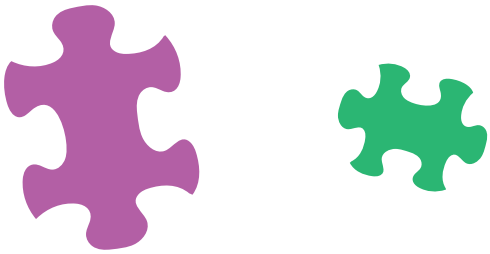
Finally, as we have noted in our previous Phase IV YCWW reports (Life Online; Encountering Harmful and Discomforting Content), collective resilience plays a vital role in how youth understand and navigate issues related to privacy online. Apart from the role of supervision and rules, we also want to emphasize trust and support as two essential pieces of the puzzle for how young people and their families build and maintain digital well-being. Here we note that youth who said they have people in their lives who can help them solve online problems are more likely to tell a parent or guardian about unwanted content posted about themselves online (42%, compared to 24% of youth who felt they do not have people to turn to for support with this problem).



NEXT STEPS



In this final section, we want to highlight the connection between young Canadians' desire to participate publicly online and their determination to take control of their privacy. Rather than being in tension, controlling which audiences see posted content and limiting unwanted surveillance are essential for youth to feel they can participate fully and openly in online spaces.



This is why it is important to emphasize the difference between what we see as *relational supervision* (more supportive approaches to protecting and managing young people's information online) and *corporate surveillance* (more concerning practices of collecting and using personal data). The survey data from YCWW Phase IV strongly confirms what we heard from youth and their parents in the qualitative phase in this regard and highlights the growing concerns that we all have about online privacy and consent.

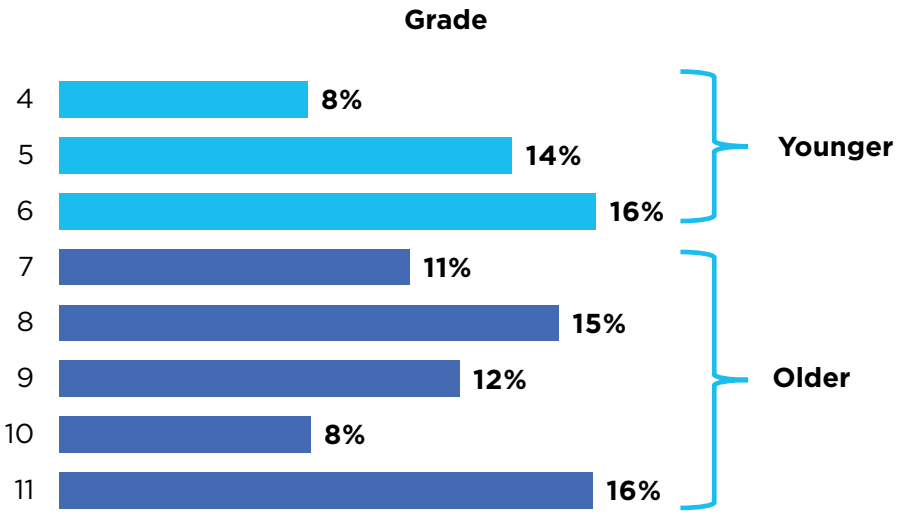
Young people across Canada are becoming increasingly aware of how their personal information is collected, used, and shared by online corporations and platforms, and they are looking for more information and resources on how to maintain control over their data. Some of this support comes from their parents or guardians, who set rules and guidelines about what they can share online, where they can share it, and with whom and review privacy settings with them. Other forms of support come from trusted adults who will listen and help youth when they report that someone is posting unwanted content about them online. This *relational supervision* plays a critical role in keeping young people safe – both online and offline – and in protecting their personal information or data. It is also essential to building trust and collective resilience.

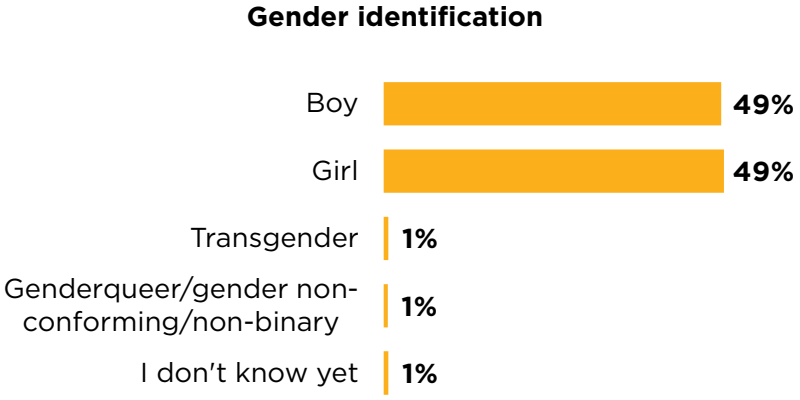
Navigating *corporate surveillance* is more complicated and requires responses and solutions that go beyond the home and the people closest to youth. While more research is needed to understand better how young people are experiencing the growing creep of surveillance in their classrooms, we have a baseline understanding of their concerns and experiences about how their personal information is constantly being collected, shared, and used by a variety of online corporate actors in several online spaces. Our recent projects on privacy and consent and artificial intelligence and algorithms highlight that young people want more digital literacy support, more transparency and accountability from online platforms, more protection from the unintended consequences of data sharing, more control over their personal data by way of *meaningful* consent processes and *clear* and *accessible* terms of service, and more opportunities to share their concerns about online privacy with policy and decision-makers.

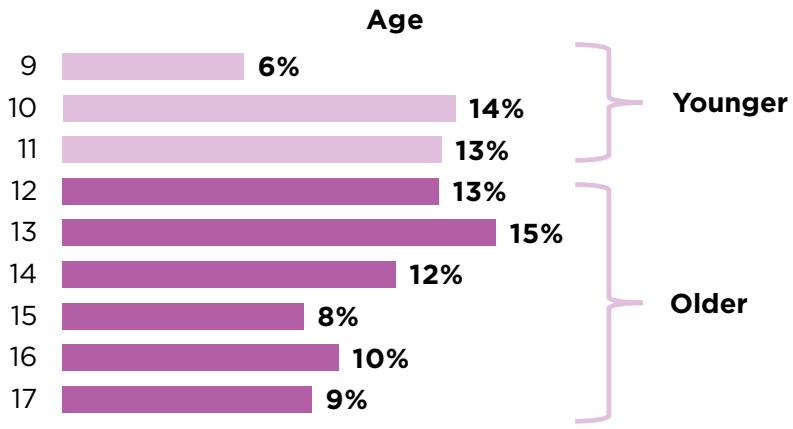
In response to these asks, MediaSmarts has recently developed and released a new algorithmic literacy resource called *#ForYou: A Game About Algorithms*. This card-based pattern-matching game helps youth understand how recommendation algorithms work and the impact of machine learning on their privacy online. The game and discussion guide help to build awareness among those who facilitate and play it and encourage more meaningful and active discussions about the things young people can do to manage their privacy and the things that must change – at a structural level – to protect their privacy rights.

APPENDICES

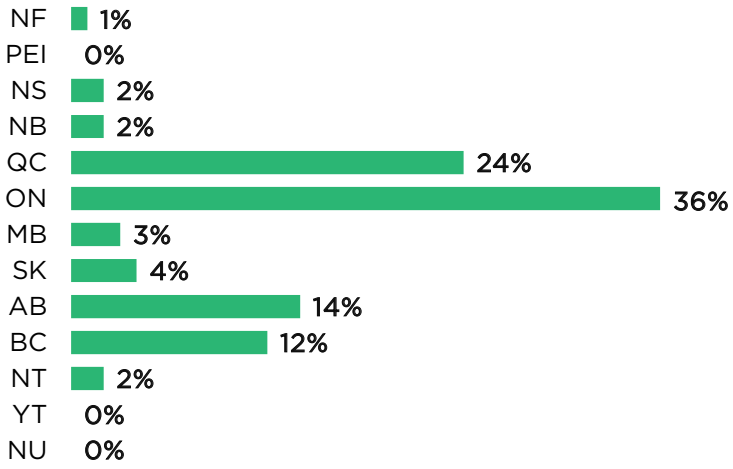
Appendix A: Demographics



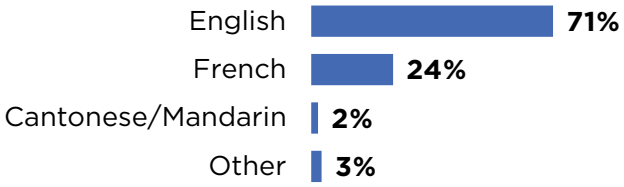




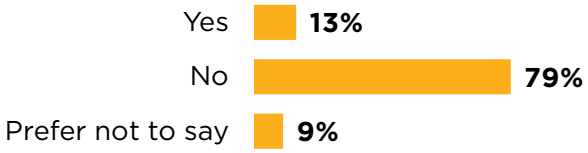
Province of residence



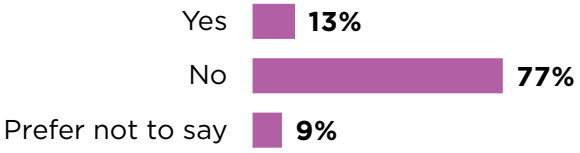
First language



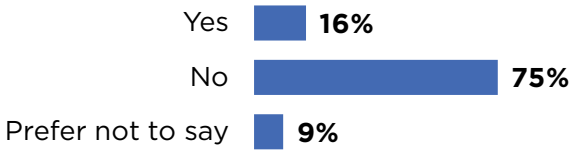
Identifies as having a physical disability



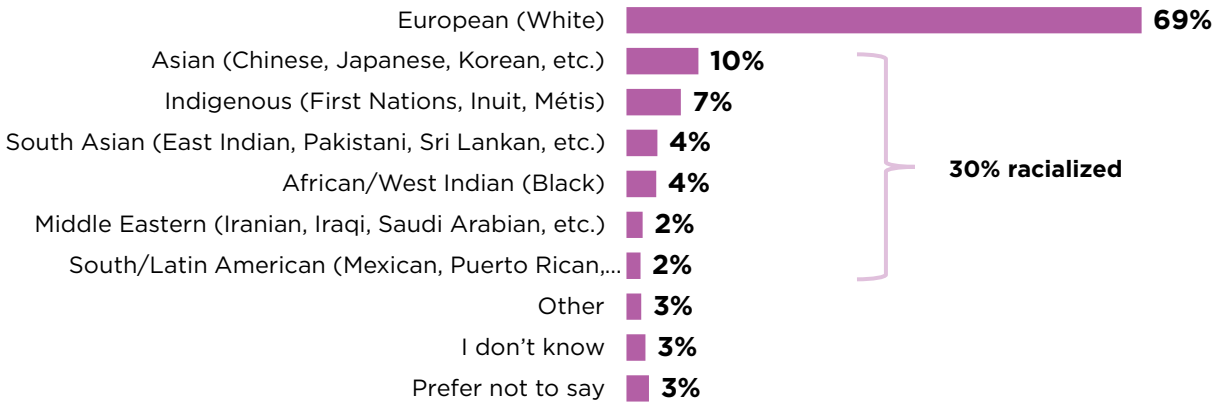
Identifies as having intellectual/cognitive/learning disability



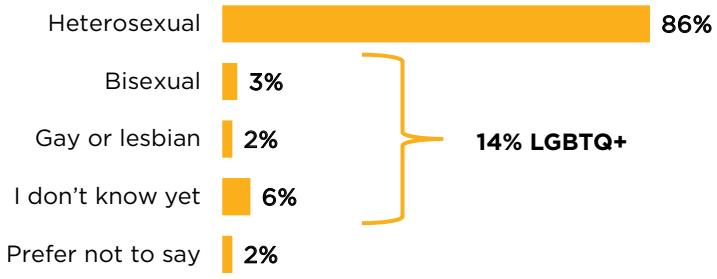
Identifies as having a mental illness



Race identification

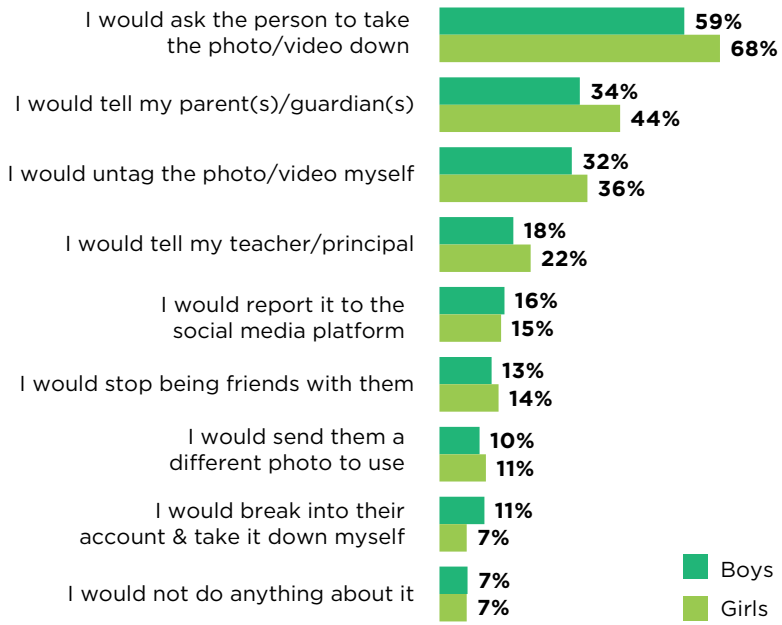


Sexual orientation

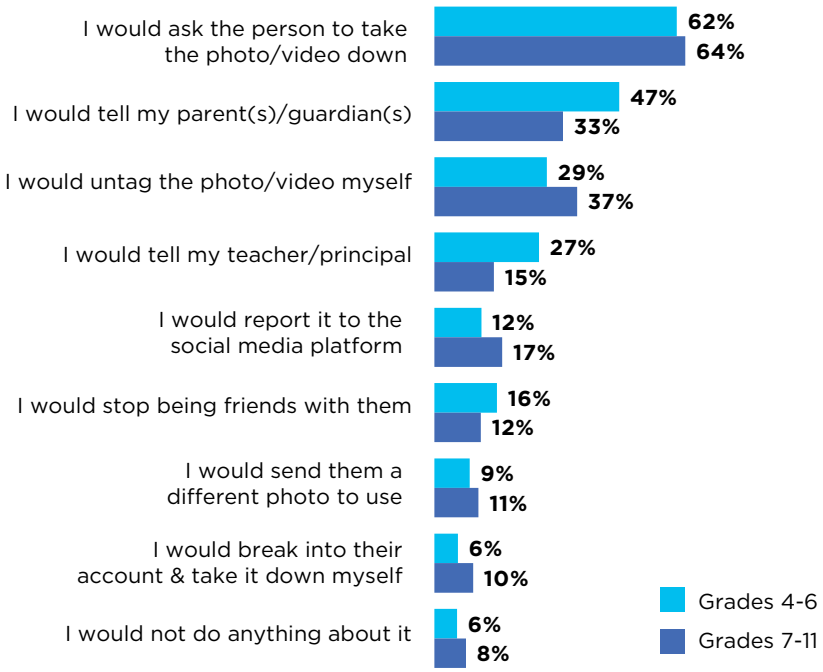


Appendix B: Addressing Unwanted Personal Content Posted by Others – Demographic Differences

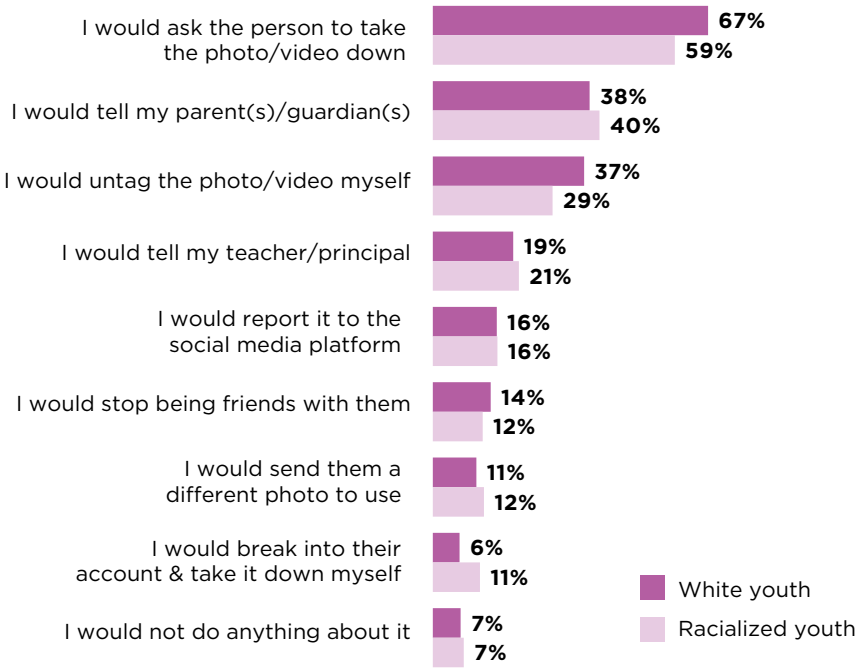
Addressing Unwanted Personal Content Posted by Others – Gender



Addressing Unwanted Personal Content Posted by Others – Grade

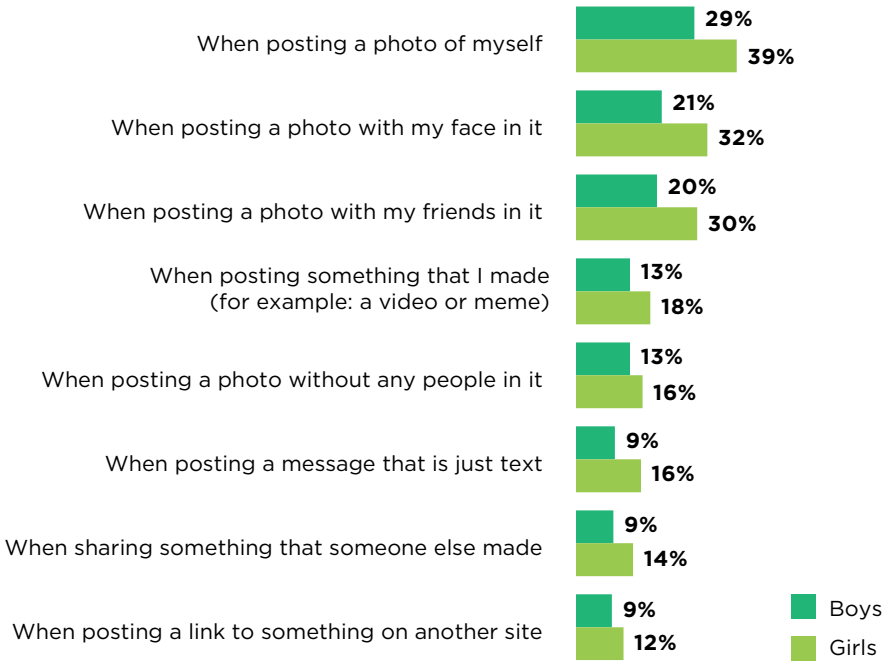


Addressing Unwanted Personal Content Posted by Others – Race

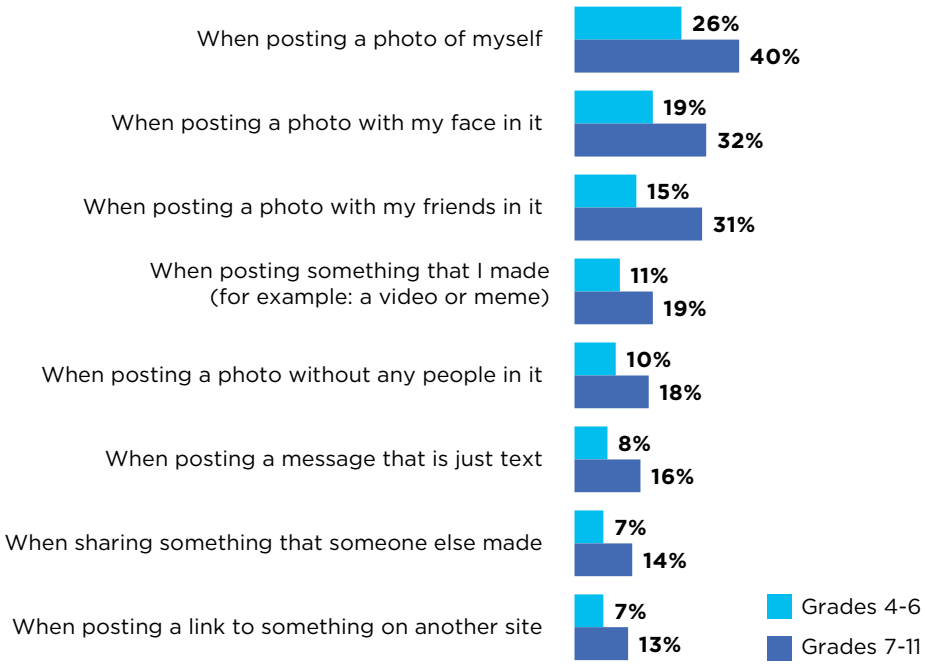


Appendix C: Specific Use of Privacy Settings – Demographic Differences

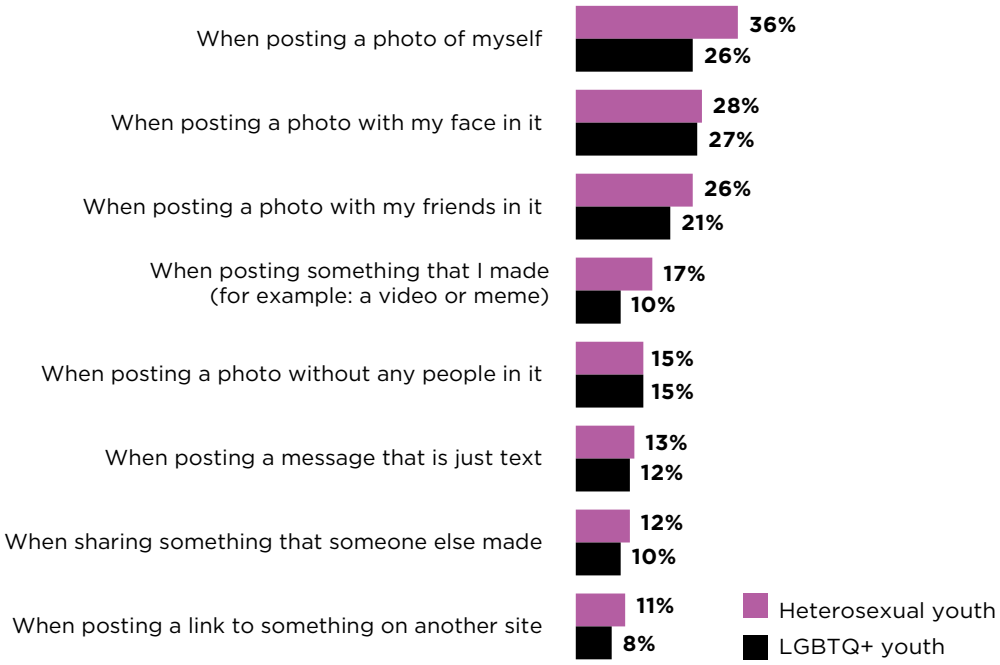
Specific Use of Privacy Settings – Gender



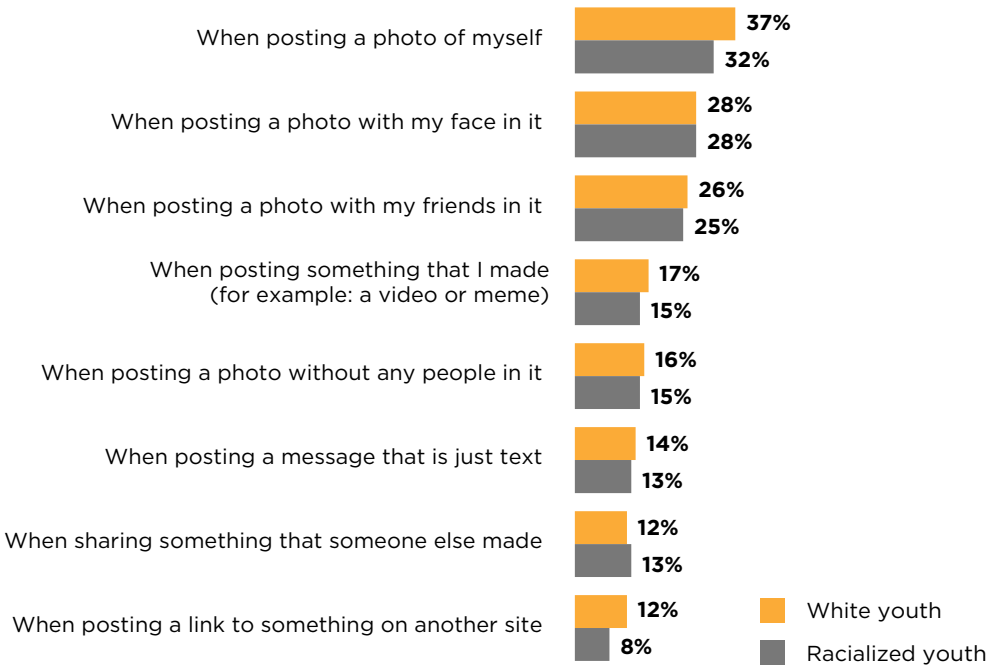
Specific Use of Privacy Settings – Grade



Specific Use of Privacy Settings – Sexual Orientation



Specific Use of Privacy Settings – Race



Specific Use of Privacy Settings – Disability