YOUNG CANADIANS SPEAK OUT:

A QUALITATIVE RESEARCH PROJECT ON PRIVACY AND CONSENT

MediaSmarts

Young Canadians Speak Out:
A Qualitative Research Project on Privacy and Consent

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

Cite as: McAleese, Samantha, Matthew Johnson, Marc Ladouceur. (2020). “Young Canadians Speak Out: A Qualitative Research Project on Privacy and Consent.” MediaSmarts. Ottawa.

Written for MediaSmarts by:
Samantha McAleese
Matthew Johnson
Marc Ladouceur

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

Introduction

The current digital information and literacy landscape offers accessible educational resources on privacy and online consent. Many of these resources aim to help young people understand the economics of personal information online and empower them to make informed, mindful choices about whether to consent to data collection. However, there are limits to what can be achieved by adults telling youth how they should manage their data profiles – especially as companies "are confronting the practical difficulties of trying to explain their personal information management practices."[1] The research project on which this report is based, *Young Canadians Speak Out: A Qualitative Research Project on Privacy and Consent*, **gave youth the chance to consider, discuss and design ways of obtaining consent online that are clear and meaningful to them.** Such opportunities for creative and critical engagement with youth are essential as researchers, educators, policymakers and representatives from the technological sector work to develop new policies and practices that impact how young people navigate the online world.

This project focused specifically on youth ages 13-16: an age group that is extremely active online, particularly in spaces such as social networks that rely heavily on data collection and behavioural advertising for revenue.[2,3] Although children under 13 might be considered the *most* vulnerable, there are significantly more protections in place for them due to legislation such as the *Children's Online Privacy Protection Act* (COPPA) in the United States and the *General Data Protection Regulation* (GDPR) in the European Union. Generally, youth aged 13 and over are considered capable of giving meaningful consent even though there is "little evidence of a magic switch in maturity when children turn 13."[4] As a result, the Office of the Privacy Commissioner (OPC) has stated that "consent processes must take into account the consumer's perspective"[5] and that consent "can only be considered meaningful if organizations

[1] Office of the Privacy Commissioner. (2016). *Consent and Privacy: A Discussion Paper Exploring Potential Enhancements to Consent Under the* Personal Information Protection and Electronic Documents Act. Office of the Privacy Commissioner. Ottawa.
[2] Steeves, Valerie, Samantha McAleese, Kara Brisson-Boivin. (2020). Young Canadians in a Wireless World, Phase IV: Talking to Youth and Parents about Online Resiliency. MediaSmarts. Ottawa.
[3] Steeves, Valerie. (2014). Young Canadians in a Wired World, Phase III: Online Privacy, Online Publicity. MediaSmarts. Ottawa.
[4] Livingstone, Sonia. (2018). Children: a special case for privacy? *Intermedia, 46* (2), 18-23.
[5] Office of the Privacy Commissioner. (2018). *Guidelines for Obtaining Meaningful Consent*. Ottawa: Office of the Privacy Commissioner. Ottawa.

have taken into account their level of maturity in developing their consent processes and adapted them accordingly."[6]

Other research demonstrates that how youth imagine online consent **does not match** with current processes – and that youth often do not see themselves as having given consent to businesses or online platforms at all, despite having agreed to their privacy policies and terms of service. For example, youth interviewed for MediaSmarts' research project *To Share or Not to Share: How Teens Make Privacy Decisions on Social Media*[7] mostly imagined consent in a corporate context in the same ways as they sought or gave it to their peers. Participants stated that they would like to be informed of the **precise uses** to which their data or content will be put, and to be able to **agree or disagree** to individual uses. Additionally, if someone opts to make their account private youth feel it should be taken to mean that they do not want the platform to share their profile or data with other users or businesses via data brokers. In other words, youth expect businesses to respect their choices. Finally, because so much of young people's social lives now takes place at least partly on online social networks, they **do not want to give blanket consent** to all of the terms and conditions in order to use a platform or service. Perhaps as a consequence of feeling unable to meaningfully consent, the participants in this study largely did not have any sense of themselves as having privacy rights. Indeed, almost none of the youth were aware of any of the rights they hold under *the Personal Information Protection and Electronic Documents Act*'s (PIPEDA) fair information principles or could imagine making use of them in any way.

While our previous research demonstrates a difference between young people's views on privacy and consent and the ways in which the various online platforms they use obtain it, a crucial piece of the puzzle was still missing: **young people themselves must be involved** in "the design of online child-friendly consent and privacy settings."[8] Therefore, with this project we offered youth an opportunity to develop concrete, actionable ways in which these two views of consent can be better aligned and gave participants space to understand and assert their rights and to present their solutions for obtaining meaningful consent online. Moreover, there is evidence that online privacy and consent solutions designed by and for youth will be of benefit to other segments of the population as well. Research by the Office of the Privacy Commissioner has identified attitudes towards consent among Canadian adults that

[6] Office of the Privacy Commissioner. (2018) *Draft OPC Position on Online Reputation*. Ottawa: Office of the Privacy Commissioner. Ottawa.

[7] 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.

[8] Berman, Gabrielle, and Kerry Albright. (2017). Children and the Data Cycle: Rights and Ethics in a Big Data World,
Innocenti Working Paper 2017-05. Florence: UNICEF Office of Research.

are similar to those our research found among youth, such as wishing for more granular choices when giving consent and seeing it as "not a one-time thing" but something that "can be revisited periodically."[9]

The key findings from three focus groups conducted with 22 youth aged 13-16 in Ottawa, including the products of a paper prototype design activity, are highlighted in this final report. Once again, we at MediaSmarts were reminded about the importance of engaging with youth on issues surrounding digital technology and the online world, and we are thankful to all participants who shared their insights, experiences and, perhaps most importantly, visions for how online platforms can better obtain meaningful online consent.

[9] Office of the Privacy Commissioner. (2017) *Qualitative Public Opinion Research with Canadians on Consent*. Ottawa: Office of the Privacy Commissioner. Ottawa.

Key Terms

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 for the purpose of establishing *data profiles*.

Data Profile: Your online data profile is the sum of all of the personal data a platform or data broker has collected about you. This profile is typically used to inform algorithmic decision-making, which may range from a platform's decision of what content to show or recommend to you, to an employer's decision of whether to interview or hire you.[10]

Office of the Privacy Commissioner of Canada: Established in 1983, the Office of the Privacy Commissioner (OPC) protects and promotes the privacy rights of individuals and oversees compliance with the *Privacy Act* and PIPEDA.

Meaningful Online Consent: In May 2018, the OPC provided guidelines for obtaining meaningful consent. These guiding principles help organizations develop "a consent process that respects their specific regulator obligations as well as the nature of their relationship with their customers."[11] When meaningful consent is obtained it confirms that a person has a comprehensive understanding of what will happen with the personal information, or data, they provide to online platforms.

Online Privacy: When we talk about online privacy, we are drawing attention to how your data and personal information is handled and protected online. This includes, but is not limited to: creating and managing passwords, understanding and adjusting privacy settings, protecting yourself against identity theft, scams and fraud, and being mindful of the content you share in online spaces such as social media and cloud storage.

PIPEDA: The Personal Information Protection and Electronic Documents Act (PIPEDA) is the law that requires private-sector organizations across Canada to "obtain an individual's consent when they collect, use or disclose that individual's personal information."[12] The Act provides safeguards for our personal information.

The Privacy Act: "The law that sets out your privacy rights in your interactions with the federal government. It applies to how the government collects, uses and discloses your personal information. The *Privacy Act* protects your personal information that government institutions hold. The Act also gives you the right to access your personal information held by the federal government."[13]

Terms of Service: The legal agreement between an online business (platforms, apps, websites, social networks) and the person who uses their service.

[10] Donovan, J., Matthews, J., Caplan, R., & Hanson, L. (2018). *Algorithmic Accountability: A Primer*. Data & Society. Retrieved from: https://datasociety.net/wp-content/uploads/2018/04/Data_Society_Algorithmic_Accountability_Primer_FINAL-4.pdf

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

[12] Office of the Privacy Commissioner. (2020). *PIPEDA in Brief.* Retrieved from: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/

[13] Office of the Privacy Commissioner. (2020). *The Privacy Act in Brief.* Retrieved from: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/pa_brief/

Online Privacy and Consent: What We Already Knew

Previous research tells us that "the presence of privacy policies [online] does not always correlate with a better understanding of [a platform's] information practices."[14,15] This, alongside the fact that most of us click '*I Agree'* without carefully reading privacy and consent documents, is what some have referred to as '**the biggest lie on the internet**.'[16] Additionally, while children and youth are concerned about privacy online,[17] and want to make "informed choices" about the information, data and content they share, scrolling through pages and pages of "long and boring" text is not a sufficient or meaningful way to make such choices.[18] **'I never read those things'** or **'nobody reads them'** are common reactions to terms of service agreements and/or privacy policies.[19, 20]

Given that more youth are participating in online spaces without direct parental supervision or guidance[21], it is very important that we encourage the development of processes that **enhance understanding** of online privacy and consent. Currently, most terms of service documents "are literally designed to discourage you from reading them" and offer far more protections to businesses and platforms, not to customers or users.[22] This is particularly concerning as we learn more about how our data profiles are increasingly mobilized and monetized by various data brokers, in ways which can have an impact on many aspects of our lives for years after the data is collected.[23]

[14] Burkell, J., Steeves, V., & Micheti, A. (2007). Broken doors: Strategies for drafting privacy policies kids can understand. Ottawa, ON.
[15] Obar, J. A., & Oeldorf-Hirsch, A. (2018). The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, 1–20.
[16] ibid
[17] 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.
[18] ibid
[19] Obar, J. A., & Oeldorf-Hirsch, A. (2018). The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, 1–20.
[20] Fernandes, C. N. (2019). *Big Tech must be held to account over user consent*. Retrieved May 19, 2019, from https://www.ft.com/content/40e558ce-158a-11e9-a168-d45595ad076d
[21] Brisson-Boivin, K. (2018) The Digital Well-Being of Canadian Families. Ottawa, ON.
[22] Pitts, D. (2018). *Can't understand clickable online contracts? It's time to legislate them away*. Retrieved from https://www.cbc.ca/news/business/clickable-agreements-contract-law-1.4634780
[23] Grauer, Y. (2018). *What are 'data brokers,' and why are they scooping up information about you?* Retrieved from: https://www.vice.com/en_us/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection

The Privacy Paradox

The opaque and inaccessible nature of privacy policies and online consent processes creates what is referred to in the literature as a **privacy paradox**. While people claim to care very much about their privacy and protecting their data in online spaces, their behaviours do not often match up. This is frequently presented as an individual problem, in that it is up to individual users to familiarize themselves with privacy policies and settings; as Sonia Livingstone points out, though, "we cannot teach what is unlearnable and people cannot learn to be literate in what is illegible."[24] Thanks to the work from the Office of the Privacy Commissioner of Canada – and specifically the guiding principles for obtaining meaningful online consent (see Appendix A for a summary) – there is, increasingly, an effort to shift the onus for privacy and data protection back onto corporations and online businesses.[25]

Youth and Online Privacy and Consent

When it comes to young people and how they manage content and data in online spaces, the stereotype remains that "youth are shameless and have no sense of privacy."[26] Conversations with youth serve to negate this assumption and demonstrate that young people "seem to change privacy settings more often than older people,"[27] though, perhaps due to a better understanding of how to navigate the interfaces of new apps and online platforms. That being said, the current standard online consent process, known as 'the clickwrap'[28], hides information, discourages engagement in the consent process and allows users to click *I Accept* or *I Agree* without having read the terms of service 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. Furthermore, a sense of powerlessness among youth about "the pervasiveness of online surveillance" [29] contributes to the pattern of quickly clicking through the consent processes and proceeding to participate in the online world. As Micheti, Burkell and Steeves[30] put it:

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

[25] Obar, J. A., & Oeldorf-Hirsch, A. (2018). The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, 1–20.

[26] 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.

[27] 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.

[28] Obar, J. A., & Oeldorf-Hirsch, A. (2018). The clickwrap: A political economic mechanism for manufacturing consent on social media. *Social Media + Society*, 1–18.

[29] Burkell, J., Steeves, V., & Micheti, A. (2007). Broken doors: Strategies for drafting privacy policies kids can understand. Ottawa, ON.

[30] Micheti, A., Burkell, J., & Steeves, V. (2010). Fixing broken doors: Strategies for drafting privacy policies young people can understand. *Bulletin of Science, Technology & Science, 30*(2), 130–143.

> *Young Canadians are resigned to the notion that they must 'pay to play,' and the currency is personal information. The choice they see in front of them is simple: give marketers what they want, or give up access.*

Doing Things Differently

All in all, it seems that it is not always clear "how consent actually works" online.[31] If that is the case, what steps can we take to help people (specifically youth) reclaim their agency and allow for more control over, and better protection of, their data? Organizations from England, Germany and Canada have re-imagined privacy and consent documents with this question in mind:

- The Children's Commissioner for England[32] recognized that "[c]hildren often don't know what they're signing up to when they join Facebook, YouTube, SnapChat, WhatsApp or Instagram" and worked with legal professionals "to create simplified versions of Terms and Conditions" for several popular online platforms.[33] These guides (example in Appendix B) are an invaluable resource for children and youth (as well as parents and teachers) and provide an example for how online businesses can ameliorate how they provide customers and users with clear information about how data is collected and what is done with it.

- Another initiative – *Terms of Service; Didn't Read* – from Berlin also addresses the fact that no one reads terms of service agreements or privacy policies. Tos;DR is a rating system that provides more transparency about current online privacy and consent practices from online platforms like Google, Amazon, Twitter, YouTube, Netflix and Wikipedia.[34] The visual components of the rating system (examples in Appendix C) are very user friendly.

- Finally, Canada's Association for Media Literacy has worked with law students to develop plain-language versions of terms of service agreements, and then collaborated with graphic arts students to communicate them as infographics.[35]

[31] 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.

[32] The Children's Commissioner in England (currently Anne Longfield) is responsible for promoting and protecting the rights of children. More information available here: https://www.childrenscommissioner.gov.uk/about-us/

[33] Children's Commissioner. (2017). *Simplified Social Media Terms and Conditions for Facebook, Instagram, Snapchat, YouTube and WhatsApp*. Retrieved from: https://www.childrenscommissioner.gov.uk/publication/simplified-social-media-terms-and-conditions-for-facebook-instagram-snapchat-youtube-and-whatsapp/

[34] Terms of Service; Didn't Read. (n.d.). *About*. Retrieved from: https://tosdr.org/about.html

[35] Association for Media Literacy. (2020). *End User License Agreements in Plain Language*. Retrieved from: https://aml.ca/resources/end-user-license-agreements/

Seventeen of these (example in Appendix D) have been done to date, with a particular emphasis on Canadian companies such as Rogers and Bell Media.

These examples demonstrate that clarifying online privacy and consent processes – especially for children and youth – is a priority in many jurisdictions for both government and civil society organizations. They also validate the need for new and innovative processes for obtaining meaningful online consent and reveal how the guiding principles developed by the Office of the Privacy Commissioner can be taken up by online businesses and platforms.

Summary

Current research and literature on online privacy and consent, including MediaSmarts' past research, consistently shows that:

1. **While youth do care about online privacy, they conceptualize it in ways that are different from adults and, in particular, ways that do not fit with many online platforms.**

2. **People generally do not take the time to read terms of service agreements or privacy policies because they are too long, difficult to find and hard to understand.**

These findings helped shape the research for this project and guided conversations and interactive activities about online privacy and consent with youth in Ottawa.

Research Method

From September 2019 to January 2020, we conducted three focus groups with 22 young people ages 13 to 16 in Ottawa. Participants were recruited with the help of community organizations such as Girl Guides of Canada, Youth Ottawa, local libraries and community resource centres.[36]

The focus groups, which ran for approximately two hours each, gave participants an opportunity to share their thoughts on, and experiences with current online consent processes. Each session began with a primer video that provided participants with essential knowledge about the meaning of consent in a data collection context, the economics of personal information online, an overview of the existing mechanisms of obtaining consent online, and their rights to privacy under federal legislation. Participants were also given a written summary of the primer video which they referred to during the prototype design activity.

The primer was followed by a brief discussion of participants' knowledge of, and experience with processes for obtaining meaningful consent online. We asked youth:

- **Do you think it is important for online platforms to obtain meaningful consent from users? Why or why not?**

- **What do you think would make it easier for you to consent online? What types of formats, designs, processes and/or explanations would be helpful?**

Following the discussion, participants were asked to develop 'paper prototypes' aimed at providing concrete solutions to help people (particularly youth) understand and navigate their consent choices. After reflecting on the information provided in the primer – including an overview of the OPC guiding principles for meaningful consent – and collaborating with their peers, youth participants developed new processes that may provide users with more consistent and meaningful privacy settings, and suggested ways for platforms to obtain "just in time" consent without creating "consent desensitization." [37] Examples of the prototype designs are presented throughout this final report.

[36] This project received ethics approval from Carleton University's Office of Research Ethics. Project #111338.
[37] Buitelaar, JC. (2016). Child's Best Interest and Informational Self-Determination: What the GDPR Can Learn from Children's Rights. *International Data Privacy Law.* doi: 10.1093/idpl/ipy006

With participant permission, the focus group discussions were audio recorded and transcribed for analysis. All identifying information was removed from the transcripts to safeguard participant anonymity. For the same reason, participants are identified only by pseudonym and age in this report.[38]

The focus group discussions and paper prototypes revealed the following:

- observations and concerns from youth about current online consent processes;
- suggestions from youth about how to fix or improve online consent processes; and
- reflections from youth about their online data sharing practices and their privacy rights.

[38] See Appendix E for more information about participants and focus groups.

Current Online Consent Processes: Experiences, Attitudes and Concerns

Before youth participants developed the paper prototypes for their re-imagined online consent processes, they engaged in a discussion with facilitators about *current* online consent processes. We wanted participants to think more intently about their experiences, attitudes and concerns with the ways in which online platforms are handling privacy, consent, data collection and data brokerage. What follows is a summary of what youth shared throughout the focus group discussions.

Too Long; Never Read

According to a 2008 study, the average internet user would have to spend an average of forty minutes every day (or 244 hours per year) in order to actually read the privacy policies of the sites they use.[39] This factor alone – the time it takes to read and understand online privacy and consent documents – was a big concern among the youth who participated in the focus groups. Most described scrolling past all of the text to get to the *I Agree* button, indicating that the text was boring, too long, and hard to understand. Erica (16) disclosed that if the policy is "more than one page…then I'm just going to click agree," but suggested that if the Terms of Service was summarized in one page then more people would pay attention. Others agreed with the concerns about length and complexity:

Natasha (15) *"I get it, I scroll to the bottom, I click accept, and say ok! It's 13 pages long. No one wants to read 13 pages of lawyer stuff."*

Leah (15) *"Yeah, it's boring."*

James (16) *"I feel like people would read it if it was worded better and to the point instead of all these words that no one understands."*

Some participants said that they try to read the policies, but tend to only focus on text that is bolded or underlined:

[39] McDonald, A.M. (2008). The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society*, *4*(3), 543-568.

> *I started to read it, but then I just started to read stuff that was in bold or stuff that was underlined because otherwise you just scroll and scroll and scroll."*
> *(Dana, 14)*

One participant, Melissa (13), said that she had to read the privacy and consent policies for Instagram because her dad insisted upon it. She acknowledged that it took her 'a while' and that she doesn't even recall the specifics of the document:

> *"I had to read it with my dad because he made me read it with him… for Instagram… [It took me] a while [to read]. I don't even remember it though."*

Overall, participants seemed very concerned with the 'just press once and then you're done' (James 16) approach to online consent as the process does not provide users with enough information about data collection and use. This echoes findings from previous MediaSmarts' research, *To Share or Not to Share: How Teens Name Privacy Decisions on Social Media*, in which youth expressed a lack of control over their personal information as a result of not fully reading and/or understanding the privacy and consent policies.[40] Discussions in all three focus groups for this current research project highlighted a frustration with 'the clickwrap' method for online consent, especially since it does not give users a chance to consider the potential unanticipated consequences of sharing content and data with online platforms.

Unanticipated Audiences and Consequences

As a result of not reading online privacy and consent documents, or not fully understanding what they read when they did so, some participants were shocked by the possible consequences of online data collection. Of particular concern was the potential impact that their data profile might have on future employment opportunities:

[40] 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.

> *One thing that specifically stood out to me in that video we just watched is that it mentioned whether or not you would be accepted into a job or not based on the data that's collected. And all of those things are very important, like what kind of stuff gets advertised to you, but I really think that whether or not you get a job is a really big deal! And I think I can safely say that barely anyone in this room actually knew that whether or not they got a job would be based on the websites we visit. So especially that point should be advertised more. (Andrew 16)*

Andrew felt betrayed after learning about this unanticipated consequence of being online and sharing personal information. He described it as 'a breach of privacy' or 'blackmail' and was disturbed by the idea that something someone does online when they are young can follow them for the rest of their life. Andrew understood that his data could be used for things like targeted advertising or suggesting friends on social media, but he felt as though having all his information shared with employers was 'crossing the line':

> **“** ***Obviously, you change as a person and everyone has something that they posted [online] that they are not proud of, or that they've commented, or even a private message that you've sent someone, or a post you've saved. And I think on that level it's sort of a breach of privacy.***

While none of them used the specific terms, many participants who shared Andrew's concerns about the permanence of the information contained within one's data profile, and the contexts in which it can be used, expressed a wish for a 'right to be forgotten' or 'right to erasure'.[41]

Another participant, Bianca (16) recounted a similar story of shock experienced by one of her peers who assumed that the information they shared with friends on SnapChat was also private and protected:

[41] The General Data Protection Regulation (GDPR) in the European Union "gives individuals the right to ask organizations to delete their personal data" in specific circumstances. More about 'the right to be forgotten' can be found here: https://gdpr.eu/right-to-be-forgotten/.

> *"There's a lot of kids I know who don't realize what they're posting is gonna have a big impact someday… There was something that happened a couple of weeks ago. Somebody got in trouble for possession of drugs and he was like, 'Well I never told anyone!' But he posted it on SnapChat! 'Well, how are the police able to get that?' And I'm like, 'It's on the internet, it's public information, you should have been aware that it's on the internet [and] anybody can get access to that!' So, it's things like that where kids really need to know what's going on because they can get themselves into trouble."*

Some participants expressed concern for peers who don't understand how data is accessed and used – even after it is deleted. Most acknowledged that they were not aware of what happens to all the data, information and content that they share online, reinforcing the need for more meaningful online consent processes:

> *Even the fact that after maybe it deletes, maybe it doesn't delete - it doesn't go away. You know there is a software that captures all that stuff, so I don't think people understand that and that's where the problems come in. (Shannon 16)*

> *I find this hard to answer because the truth is, I don't know what they do with the information. (Erica 16)*

This lack of information and understanding about data collection, storage and use contributes to youth feeling 'weird' or 'sketchy' about online business and their policies and practices.

'Sketchy' and 'Weird' Consent Policies and Practices

In a recent MediaSmarts' study, *Young Canadians in a Wireless World, Phase IV: Talking to Youth and Parents about Online Resiliency*, some youth used descriptors like 'creepy' and 'weird' to describe the presence of digital technology in the classroom and how data is collected and used in the online world.[42] These descriptors appeared once again throughout the focus groups for this research project as youth participants discussed how data is collected and brokered online. In some instances, it was the 'sketchiness' of open access Wi-Fi that encouraged youth to actually read privacy and consent policies:

[42] Steeves, Valerie, Samantha McAleese, Kara Brisson-Boivin. (2020). Young Canadians in a Wireless World, Phase IV: Talking to Youth and Parents about Online Resiliency. MediaSmarts. Ottawa.

> *If it's anything that's like, sketchy, I usually read a little bit into it... Like joining a random company's Wi-Fi network. If it's an open Wi-Fi network I always make sure to read a little bit so if they are like, 'Oh, by the way we're stealing all the information out of your phone,' that would really not be any fun. (Bianca 16)*

In contrast to the opacity of privacy policies, some participants thought it was 'weird' how simple the process of obtaining consent is on most websites, apps, and platforms. Gina (14) even questioned why companies don't have a mechanism to ensure that you've read the policies:

> *It's weird that you have to click the 'I agree to the Terms of Service' button when most of the time you haven't read them... [Platforms] could probably easily find out if you had opened the link or not to the Terms of Service because it's on a separate page and it's linked to you. They can tell if you've been on it or not. So, I just find that a little weird that they wouldn't not let you click it until you've actually clicked on it.*

These concerns about online consent processes led into discussions about algorithms and how data is collected and used by online platforms, like Instagram. Most participants had some knowledge about how platforms make money by selling data to advertisers, and while some were sanguine about this – as it allows for a more personalized online experience – others expressed 'mixed feelings' about how easily data from one app, platform, or website makes it over to another. Andrew (16) described this uncertainty:

> *I remember a while ago I was on eBay or something and I was buying clothes and I didn't end up buying anything – oh, it was Amazon! And it's the only time I've ever been on Amazon with my e-mail account. And for the next week, on YouTube, the little ads that would show up were all for that one article of clothing on the same website and it was different sellers posting it with different prices. And it wasn't even a minute since I was on Amazon! I went straight from that to YouTube and clicked on a different video and there it was this jacket... I had mixed feelings about it. I think... I kinda felt like it was sort of a breach of privacy. At the same time, at least they know what clothing I like so they are advertising properly.*

Finally, there were specific functions of devices and apps that made participants feel 'weird' – namely, location tracking.

> *I find location...it's weird because I'll be at work and then I'll be working with a co-worker and the next day I'll get a notification from Facebook saying, 'You have a new friend suggestion,' [and it's] that co-worker I worked with last night. And I find that very weird. I don't know if it's a coincidence or if it's an actual location thing. (Shannon 16)*

However, youth participants also acknowledged what they considered to be legitimate uses of data. For example, after hearing Andrew share his story about the link between his eBay browsing habits and his Amazon ads, James (16) indicated that this particular use of data (and result of data brokering) didn't really bother him:

> *I feel like if I have to see ads anyway, I prefer for them to be something that I'm interested in. So, I don't really care about that part too much.*

Similarly, Natasha (15), was less concerned about how location and contacts might inform future friend and follow recommendations:

> *I guess who you follow? Say you follow a friend and it recommends you a friend that you didn't follow or like a celebrity related to them, that would be helpful.*

Throughout the discussions in all three focus groups there was a line that appeared between 'legitimate' and 'creepy' when it comes to how data is collected, used and brokered. Location, for example, was identified as a data point that can be useful in identifying general things such as recommendations for where to shop and what to buy. But most participants agreed that there should be a limit on how granular the data is and that users should have to opt-in to the location settings rather than discover that they are being tracked unknowingly by their phone or an app:

> *Even Apple, and I didn't know this until today, but there's a feature on your phone that it says where you've been, what mode of transportation you've been on, how long you were there for… But it's on your phone but I don't remember singing up for that. You know what I mean? I don't remember agreeing to say, "Yeah, you can know where I am at all times and how I got here." (Shannon 16)*

Generally, participants were not necessarily opposed to data collection, but they did express wanting more clarity and control (to reduce 'creepiness') and for corporations to not take and use data without their explicit consent.

Fixes and Features: Suggestions for New Online Consent Processes

In each of the three focus groups, opening discussions about experiences, attitudes and concerns towards current online consent processes fed nicely into the paper prototype design activity. Before splitting off into groups and working on the prototypes, participants already had some ideas about what they didn't like about the common 'clickwrap' method and other processes that serve to 'impede dissent'.[43] What came from this was a plethora of fixes and features that youth felt would greatly improve online consent processes and make them far more meaningful.

Text

Many of the fixes suggested within the prototype designs are about text. There was a consensus among participants that 'scrolling through a long black and white text is not fun,' and so their re-imaginings address this problematic standard to make the privacy and consent policies 'easier to read'.

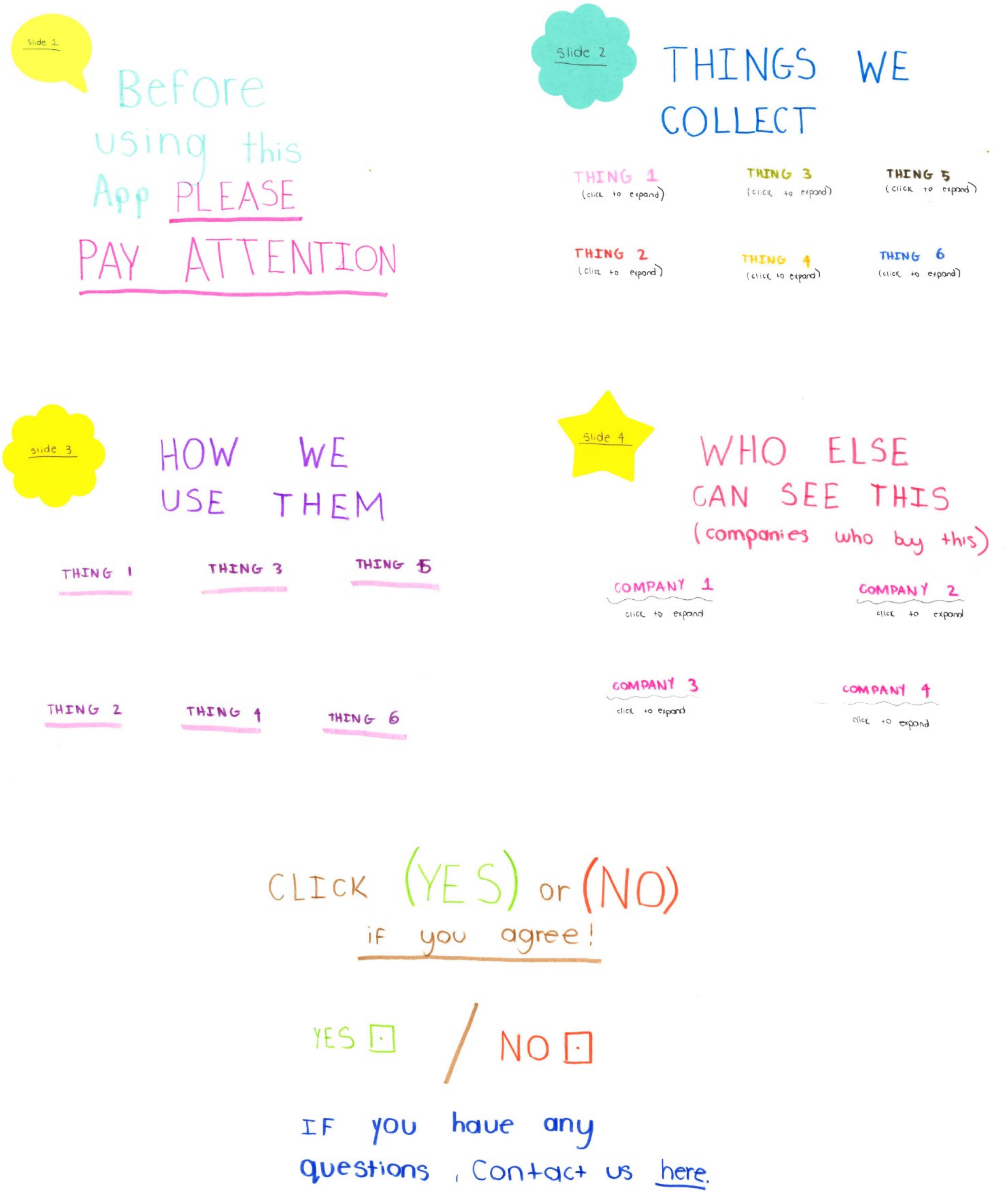
First, **simplicity** is an important factor:

- 'simple phrases'
- 'simple sentences'
- 'simple words'
- 'simple language'

Making the text simpler also involved using 'subtitles' and 'bullet points' and not showing too much content or text on the screen at once. In fact, many of the

[43] Obar, J. A., & Oeldorf-Hirsch, A. (2018). The clickwrap: A political economic mechanism for manufacturing consent on social media. *Social Media + Society*, 1–18.

prototypes involve a multi-step process with several ‘screens’ or ‘slides’ with a mixture of content including text, images, and videos.



Slide 1

Before using this App PLEASE PAY ATTENTION

Slide 2

THINGS WE COLLECT

THING 1 (click to expand)
THING 3 (click to expand)
THING 5 (click to expand)
THING 2 (click to expand)
THING 4 (click to expand)
THING 6 (click to expand)

slide 3

HOW WE USE THEM

THING 1
THING 3
THING 5
THING 2
THING 4
THING 6

Slide 4

WHO ELSE CAN SEE THIS (companies who buy this)

COMPANY 1 click to expand
COMPANY 2 click to expand
COMPANY 3 click to expand
COMPANY 4 click to expand

CLICK (YES) or (NO) if you agree!

YES □ / NO □

IF you have any questions, Contact us here.

Second, the youth-designed prototypes added **focus** to the text within online consent documents. Most commonly, this looked like bold, underlined and brightly coloured text. Participants suggested that if the text is 'all in bright colours as opposed to black and white [then] you are going to pay attention.' Ensuring that 'all of the important words are underlined' or bold increases the likelihood that people will read and understand. . One group added a feature that would show you the complete definition for terms that appeared in bold, ensuring that users understand the vocabulary used throughout the privacy and consent documents.

Next, **comprehension** of the text was a significant concern for participants. They understood that privacy and consent documents are 'meant for lawyers' and therefore proposed that platforms 'dumb it down so it makes more sense' for the everyday user. One group proposed various versions of the privacy and consent policies to match age and reading comprehension levels:

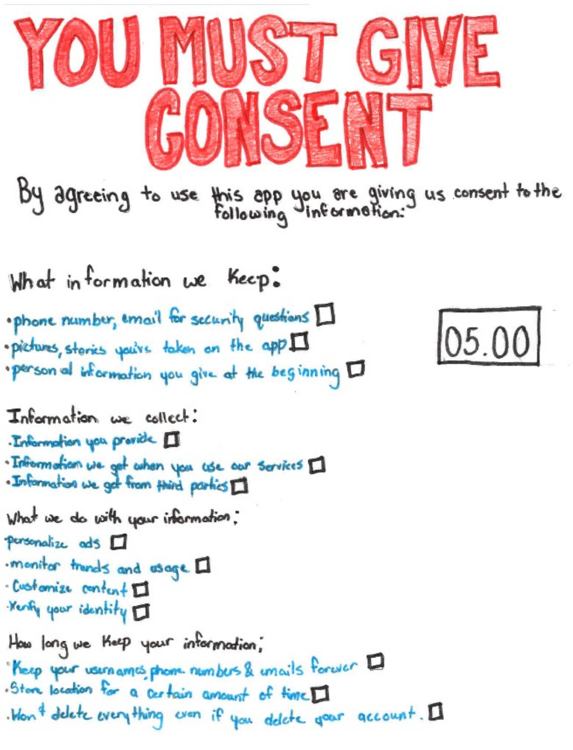
> *We want them to click their age so when they are reading the consent it's in easier words for them.*

This group (like others) clarified that the full consent policies would still be **accessible** in the app or platform if users were interested in accessing the original, but more complicated, text. The use of 'general wording' that 'everyone can read and understand' was an important feature for youth.

Verification

Another important feature suggested by youth participants was about verifying that users are *actually* reading, listening to, or watching the privacy and consent content. These verification fixes appeared in different formats throughout the various prototypes. Some groups used 'checkmark boxes' that users would have to click after reading a line-by-line consent document. Others incorporated timers (ranging from three seconds to five minutes) to ensure that the content remained on the user's screen long enough to be read. One group created a 'sandwich method' for consent which involved reading the documents *before* filling out personal information within the application and then confirming again before completing the sign-up process that the user understands the privacy and consent policies. Other participants really enjoyed this prototype feature:

> *I like what she said about how they have theirs at the beginning because I feel that by the time it comes around to the consent you have already downloaded the app and you don't have more time. (Melissa 13)*



YOU MUST GIVE CONSENT

By agreeing to use this app you are giving us consent to the following information:

05.00

What information we Keep:

- phone number, email for security questions □
- pictures, stories you're taken on the app □
- personal information you give at the beginning □

Information we collect:

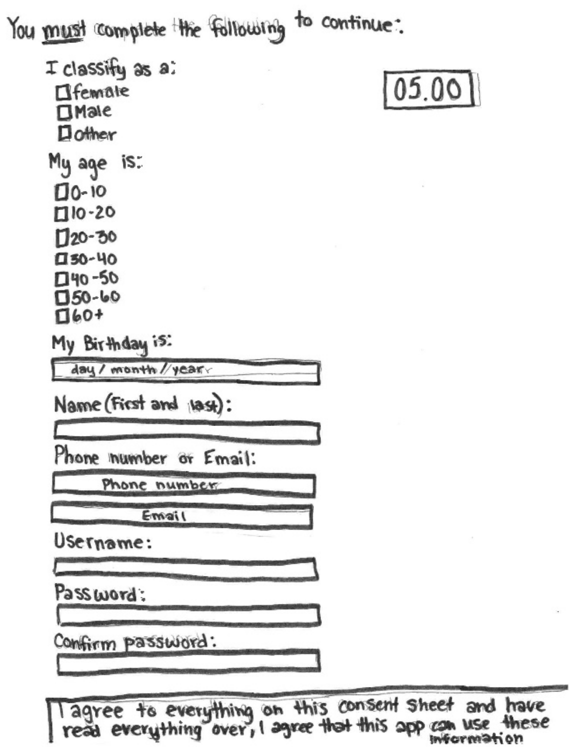
- Information you provide □
- Information we get when you use our Services □
- Information we get from third parties □

What we do with your information;

- personalize ads □
- monitor trends and usage □
- Customize content □
- Verify your identity □

How long we Keep your information;

- Keep your usernames, phone numbers & emails forever □
- Store location for a certain amount of time □
- Won't delete everything even if you delete your account. □



You must complete the following to continue:

05.00

I classify as a:

□ female
□ Male
□ other

My age is:

□ 0-10
□ 10-20
□ 20-30
□ 30-40
□ 40-50
□ 50-60
□ 60+

My Birthday is:

day / month // year

Name (First and last):

Phone number or Email:

Phone number

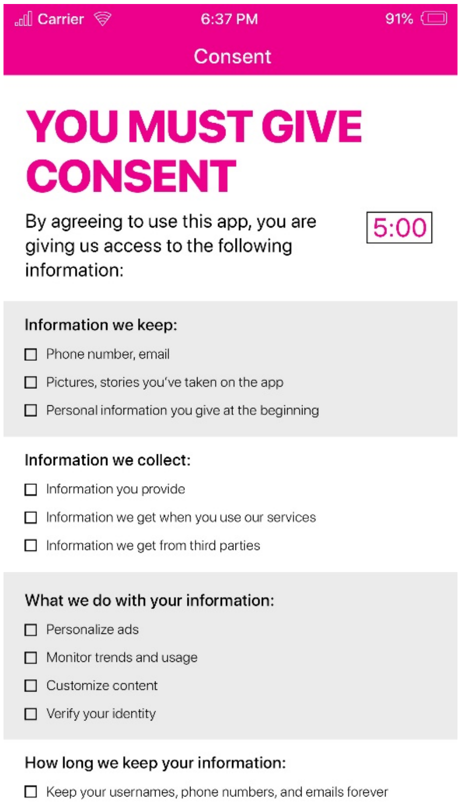
Email

Username:

Password:

Confirm password:

I agree to everything on this consent sheet and have read everything over, I agree that this app can use these information



Consent

YOU MUST GIVE CONSENT

By agreeing to use this app, you are giving us access to the following information:

5:00

Information we keep:

□ Phone number, email
□ Pictures, stories you've taken on the app
□ Personal information you give at the beginning

Information we collect:

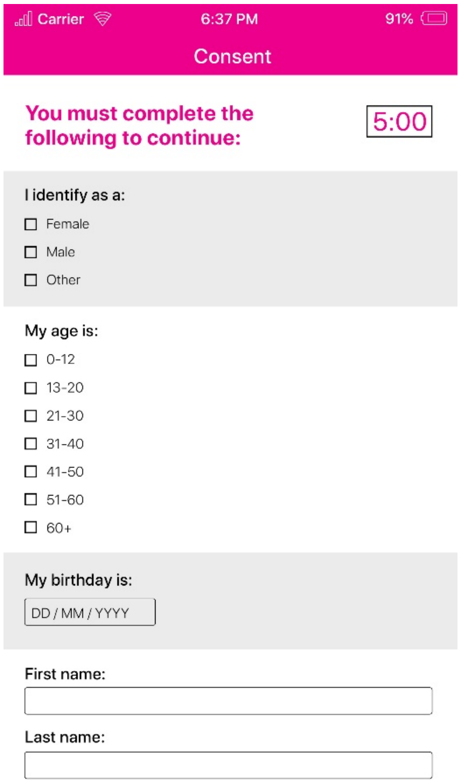
□ Information you provide
□ Information we get when you use our services
□ Information we get from third parties

What we do with your information:

□ Personalize ads
□ Monitor trends and usage
□ Customize content
□ Verify your identity

How long we keep your information:

□ Keep your usernames, phone numbers, and emails forever



Consent

You must complete the following to continue:

5:00

I identify as a:

□ Female
□ Male
□ Other

My age is:

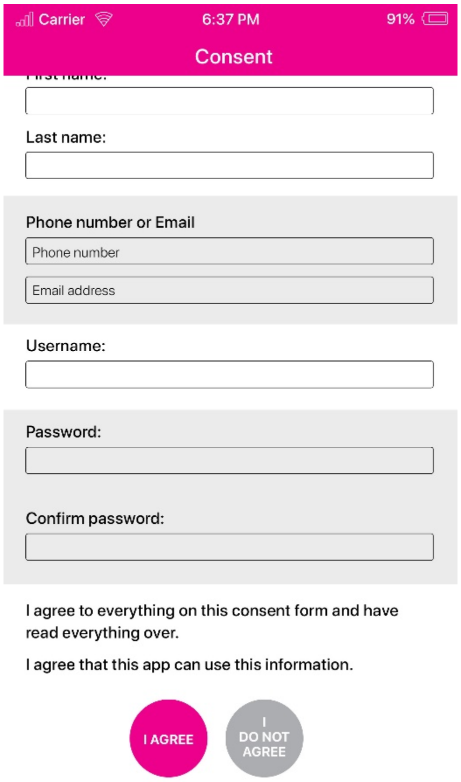
□ 0-12
□ 13-20
□ 21-30
□ 31-40
□ 41-50
□ 51-60
□ 60+

My birthday is:

DD / MM / YYYY

First name:

Last name:



Consent

First name:

Last name:

Phone number or Email

Phone number

Email address

Username:

Password:

Confirm password:

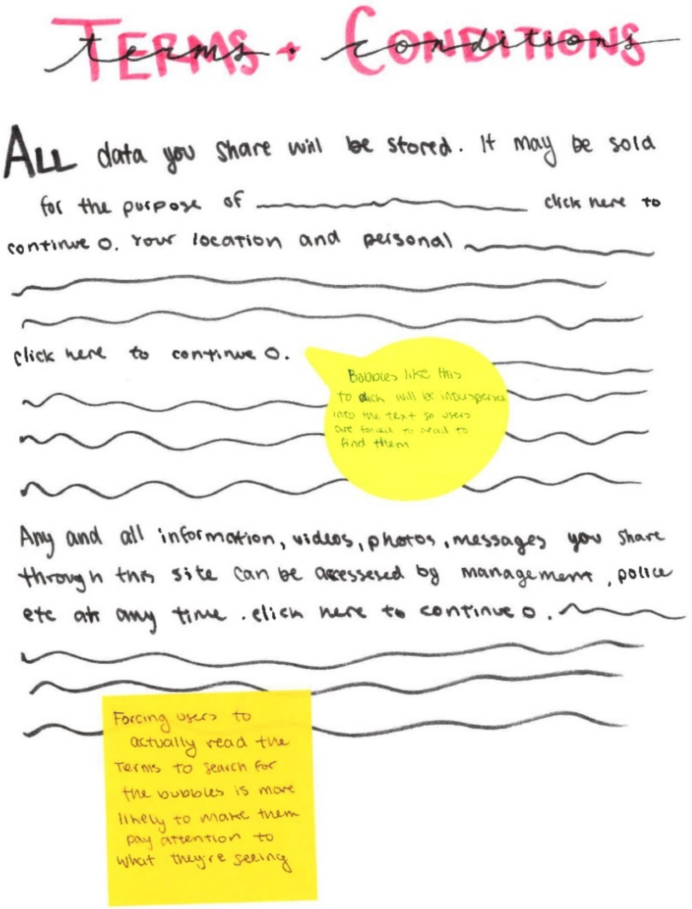
I agree to everything on this consent form and have read everything over.

I agree that this app can use this information.

Another part of verification was the ability to 'go back at any time' to review privacy and consent content. Whether in the form of videos, images or text – youth were insistent that the information be easy to find within the app. This idea of ongoing consent was very important to the youth participants.

Finally, during the third focus group Bianca (16) recalled a story about Van Halen's brown M&Ms clause in their venue and performance contracts[44]:

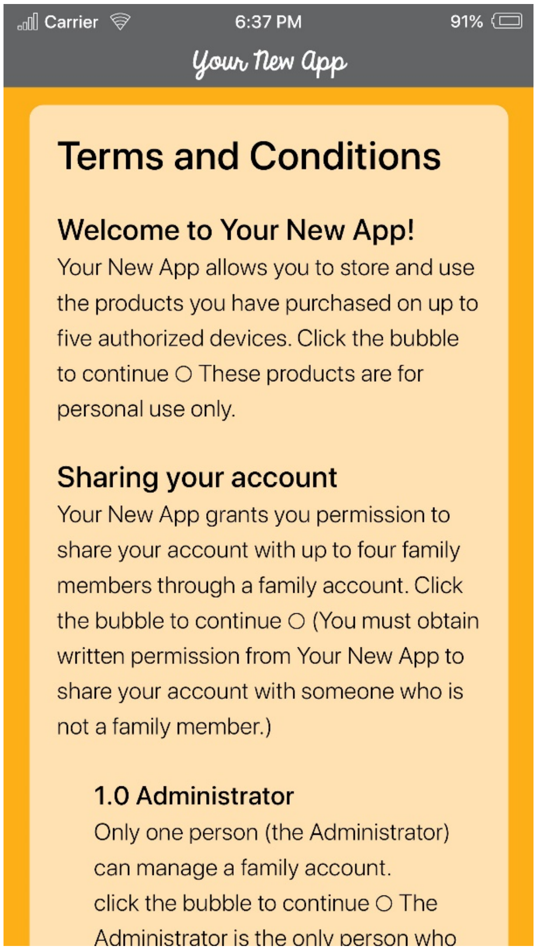
> *So, they made this thing so that any venue they played at they had this contract and deep in the contract they had something like a large bowl of M&Ms has to be in the room – with the brown ones sorted out. If they [got there] and saw there wasn't an M&M bowl, or the brown one's weren't sorted out, they knew that [the venue] didn't fully read the conditions [of the contract] properly.*


Terms + Conditions
All data you share will be stored. It may be sold for the purpose of
click here to continue ○. Your location and personal
click here to continue ○.
Bubbles like this to click will be interspersed into the text so users are forced to read to find them
Any and all information, videos, photos, messages you share through this site can be accessed by management, police etc at any time. click here to continue ○.
Forcing users to actually read the Terms to search for the bubbles is more likely to make them pay attention to what they're seeing

[44] Mikkelson, D., & Mikkelson, D. (2001). Did Van Halen's Concert Contract Require the Removal of Brown M&Ms? Retrieved from https://www.snopes.com/fact-check/brown-out/

Bianca incorporated this verification feature into her own online consent process prototype and said she had seen a similar process in another online platform that she signed up for recently:

> *...there was a whole section that I had to read, and it was like, in the text there was a spot you had to click and you have to make sure you're reading it to be able to, I don't know how to describe it, but you wouldn't know where to click unless you actually read the whole thing... So that really forces me to read all of the information before I can continue.*



Terms and Conditions

Welcome to Your New App!

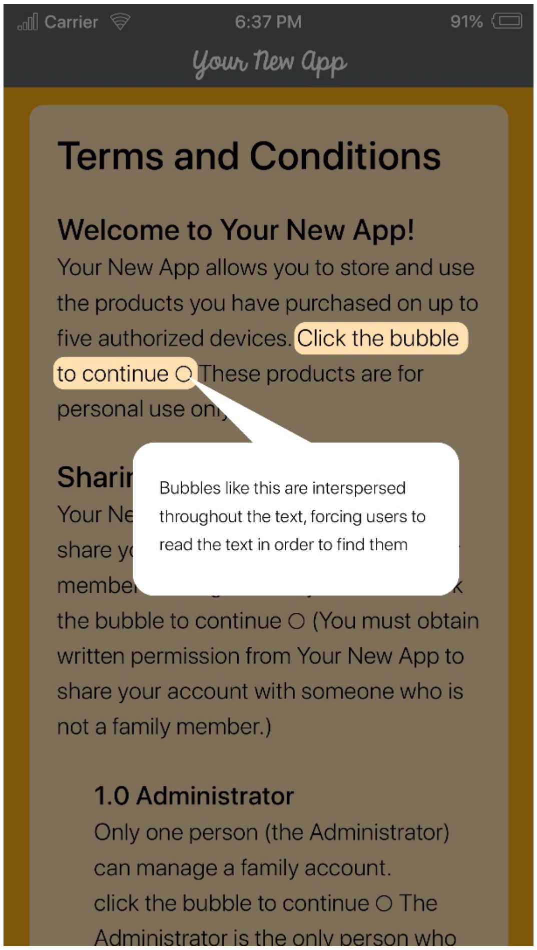
Your New App allows you to store and use the products you have purchased on up to five authorized devices. Click the bubble to continue ○ These products are for personal use only.

Sharing your account

Your New App grants you permission to share your account with up to four family members through a family account. Click the bubble to continue ○ (You must obtain written permission from Your New App to share your account with someone who is not a family member.)

1.0 Administrator

Only one person (the Administrator) can manage a family account. click the bubble to continue ○ The Administrator is the only person who



Terms and Conditions

Welcome to Your New App!

Your New App allows you to store and use the products you have purchased on up to five authorized devices. Click the bubble to continue ○ These products are for personal use onl

Bubbles like this are interspersed throughout the text, forcing users to read the text in order to find them

Sharin

Your Ne

share y

membe

the bubble to continue ○ (You must obtain written permission from Your New App to share your account with someone who is not a family member.)

1.0 Administrator

Only one person (the Administrator) can manage a family account. click the bubble to continue ○ The Administrator is the only person who

Overall, participants were eager to include fixes and features that encourage users to engage more with the content of privacy and consent documents – once again ensuring that people understand what they are signing up for.

Clarity and Control

Clarity and control were also very important elements that youth participants incorporated into their prototypes. The features that young people emphasized help users *truly* understand how data is being collected, what it can be used for, in particular if it is sold to or shared with a third party such as a data broker, and what privacy policies are in place to protect user rights. The most common fixes for ensuring clarity and control were:

- **Unbundling options**: allowing users to give or withhold consent to different forms of data collection and different uses of their data.

- **Line-by-line consent**: where the online platform makes clear what will be done with the collected data by encouraging users to read and click agree to the various components of the document.

- **Just-in-time notices**: giving users the information they require about data collection and data uses as they engage with various components of the app, platform, or website.

All these fixes serve to increase transparency and give users the opportunity to stop and reflect more regularly about their online data profiles and how they can better manage them. One participant noted the following:

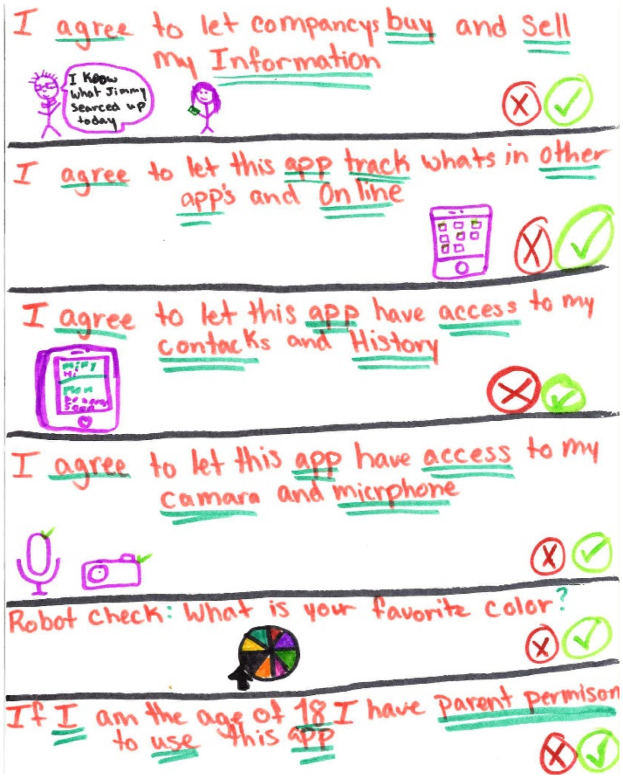
> *“The problem with how we consent to things right now, we noticed, is that you have to consent to too much at once. You don’t really get time to process or understand everything.*

The solution, then, is to ‘break things down’ or divide the privacy and consent documents into various chunks or screens so that the user is not faced with too much information all at once.

> *They would all be separate screens, so you could check and then go to the next one.*

This unbundling, as mentioned above, also involves the option to opt-in to certain features and to opt-out of others.

Instead of just one sentence that ***says I Agree****, it has a bunch of different sentences and you have to click* ***I Agree*** *to each one.*



I agree to let companys buy and Sell my Information ⊗ ✓

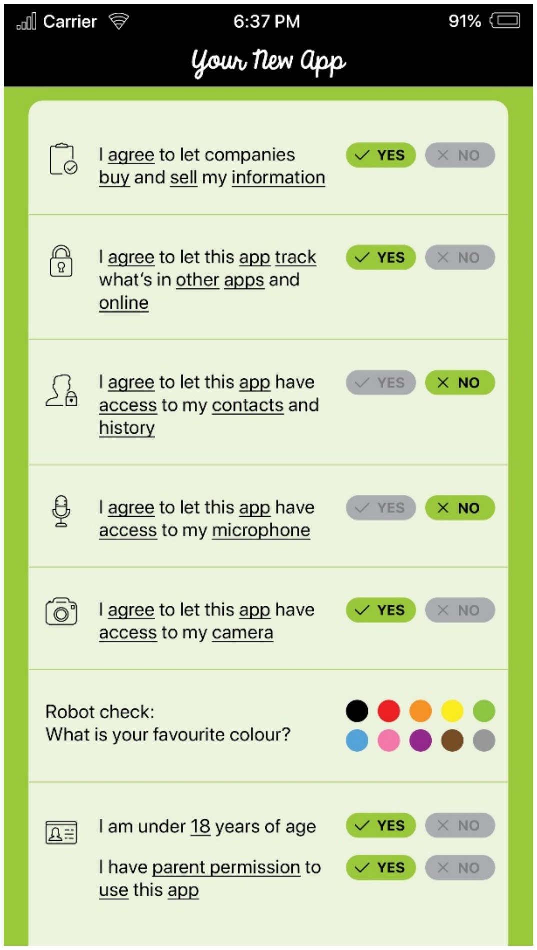
I agree to let this app track whats in other app's and On line ⊗ ✓

I agree to let this app have access to my contacks and History ⊗ ✓

I agree to let this app have access to my camara and micrphone ⊗ ✓

Robot check: What is your favorite color? ⊗ ✓

If I am the age of 18 I have parent permison to use this app ⊗ ✓



I agree to let companies buy and sell my information [✓ YES] ✕ NO

I agree to let this app track what's in other apps and online [✓ YES] ✕ NO

I agree to let this app have access to my contacts and history ✓ YES [✕ NO]

I agree to let this app have access to my microphone ✓ YES [✕ NO]

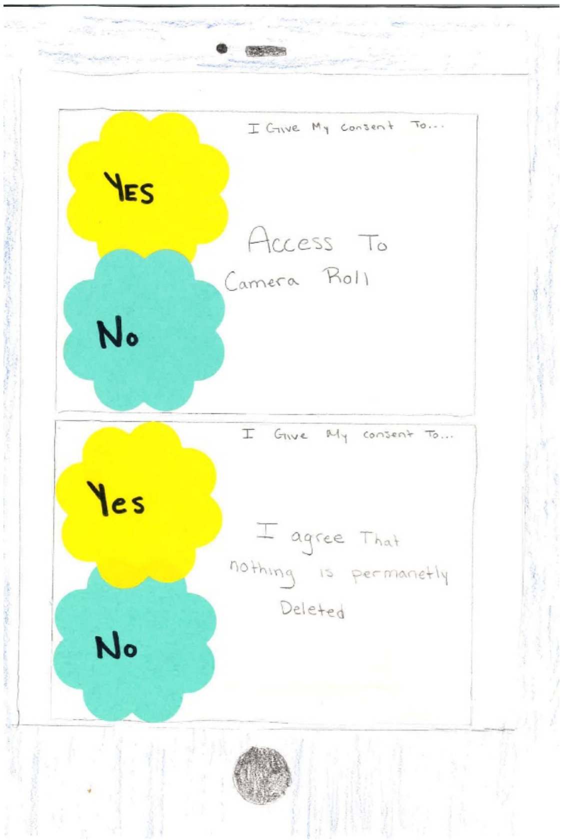
I agree to let this app have access to my camera [✓ YES] ✕ NO

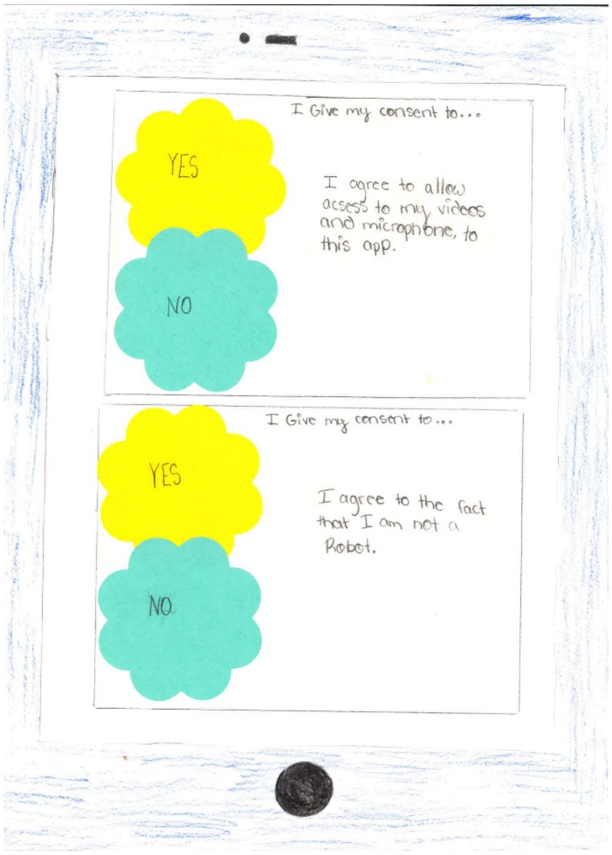
Robot check:
What is your favourite colour? ● ● ● ● ● ● ● ● ● ●

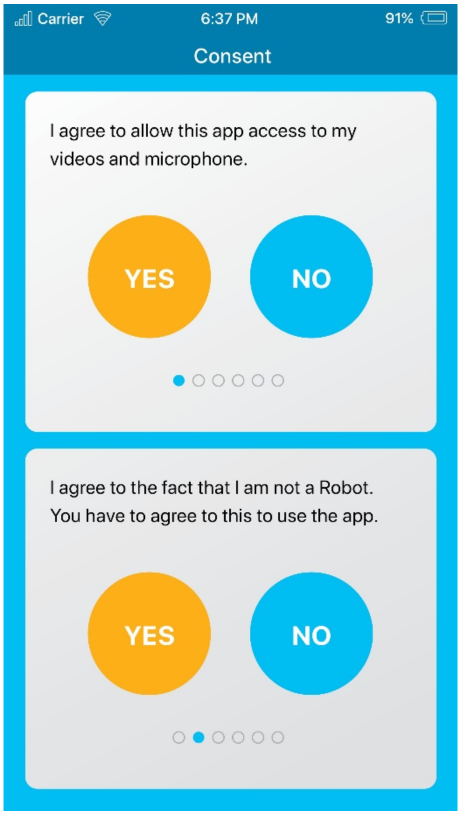
I am under 18 years of age [✓ YES] ✕ NO

I have parent permission to use this app [✓ YES] ✕ NO

One group made their prototype design look like Instagram's poll feature that users can incorporate into their Stories. They presented various elements of the consent policies and allowed users to click 'Yes' or 'No' depending on their data sharing preferences.



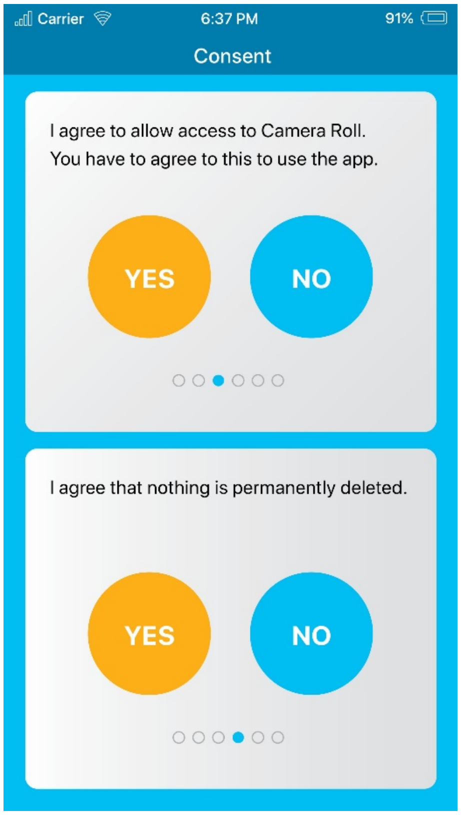

I Give my consent to...
YES
I agree to allow acsess to my videos and microphone, to this app.
NO
I Give my consent to...
YES
I agree to the fact that I am not a Robot.
NO



Consent

I agree to allow this app access to my videos and microphone.

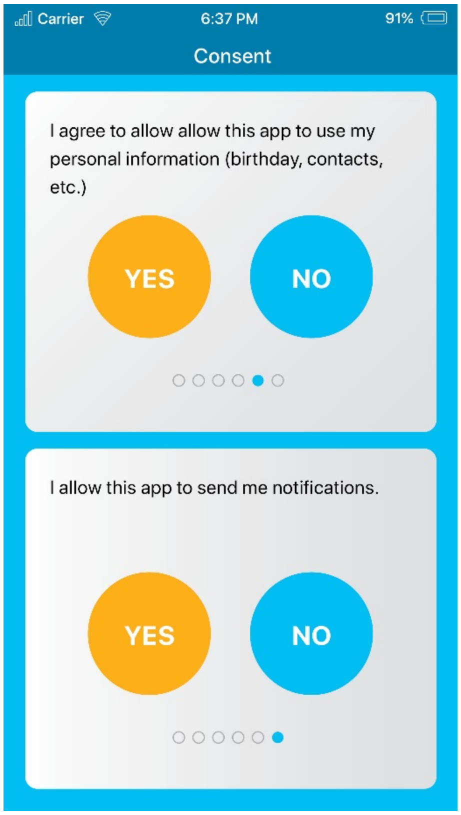
I agree to the fact that I am not a Robot. You have to agree to this to use the app.



Consent

I agree to allow access to Camera Roll. You have to agree to this to use the app.

I agree that nothing is permanently deleted.



Consent

I agree to allow allow this app to use my personal information (birthday, contacts, etc.)

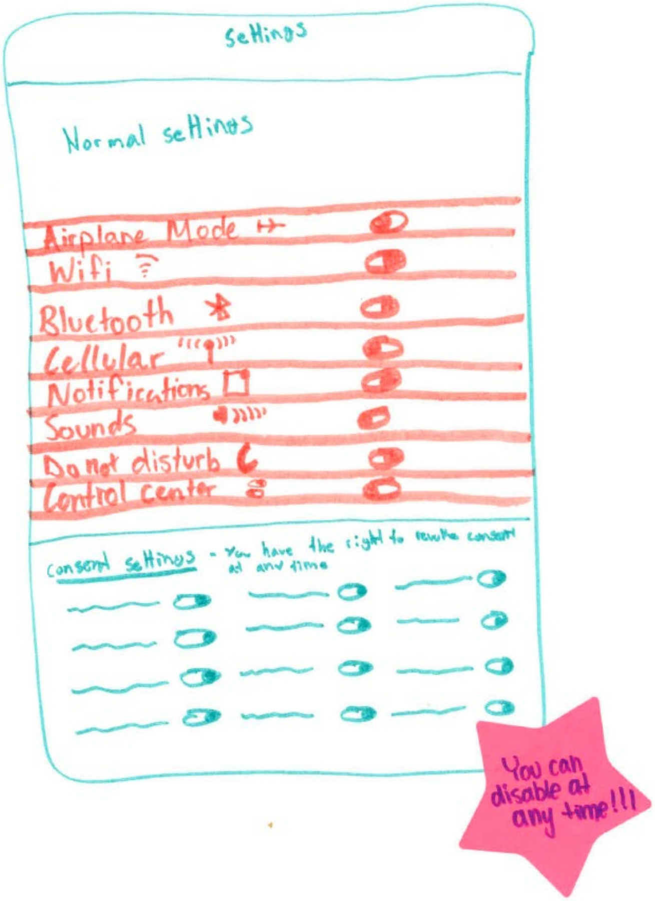
I allow this app to send me notifications.

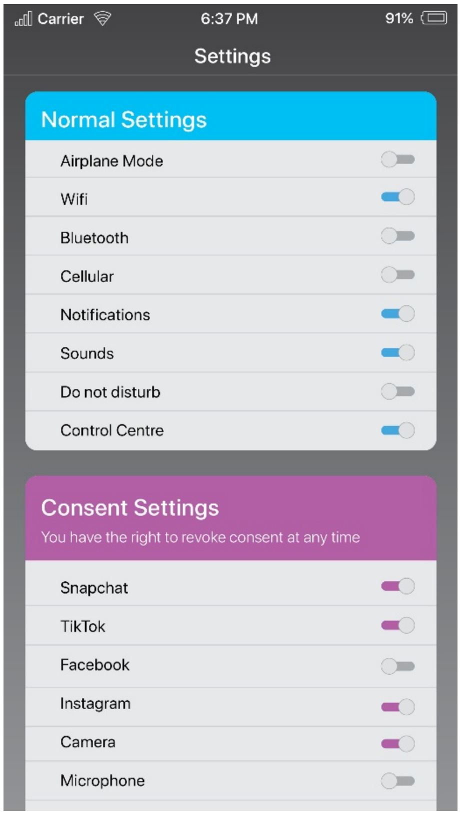
Other groups adopted a 'toggle' feature, similar to toggle switches in cell phone settings.

> *You would be able to toggle different things that you are consenting to rather than consenting to the whole terms of service.*

Lastly, one group included a pop-up feature in their prototype design to remind users of the privacy and consent policies as they are beginning to interact with the app or platform. For example, before a user first posted a photo on Instagram a pop-up would appear to remind them of the data implications of posting that content:

> *Pop-ups [will appear] as you are doing more things... The first time you post a picture the pop-up will say, 'By posting this picture, we will access your gallery.'*




Carrier 6:37 PM 91%

Settings

Normal Settings

Airplane Mode ○
Wifi ●
Bluetooth ○
Cellular ○
Notifications ●
Sounds ●
Do not disturb ○
Control Centre ●

Consent Settings

You have the right to revoke consent at any time

Snapchat ●
TikTok ●
Facebook ○
Instagram ●
Camera ●
Microphone ○

It is important to note that while youth are definitely interested in giving more clarity and control to users, they also understand that giving up some personal information is mandatory in order to properly and safely engage in (and benefit from) these online spaces. For example, providing your name, e-mail and location seemed reasonable to most participants:

> *Facilitator:* *What [data] would be reasonable for the platform to say, "You must agree to this or you can't use the service?*
>
> *Bianca (16):* *Email is reasonable. If you get locked out of your account email saves your butt, that makes sense… to have it, but not to sell it further.*
>
> *Erica (16):* *Your name I think should be ok.*
>
> *Shannon (16)* *Your name, not always your full name, but sort of a label to your account. And as well not your exact location, but your country so they can give you more specific shopping websites or products they can offer you.*
>
> *…*
>
> *Erica: I wouldn't say full birthday, but year… I kinda get it. Like, it's not crazy. Especially for making sure you are of age to use things like SnapChat and Instagram.*

One group (ages 13-14) noted that for certain apps some features were 'non-negotiable' and 'if you say no to the majority [of the privacy and consent documents] then you can't use the app':

> *So, you are signing up for Instagram, for example, and you are saying, "No, you can't have [access to] my camera roll or my videos," then there is no point in using the app because that's what it is mainly used for.*

Another group (ages 15-16) preferred the just-in-time notices in this regard, noting that you can use apps like Instagram without posting pictures, but if you *do* post a picture you will be prompted to read the section of the privacy and consent documents that pertain specifically to that function:

> *Really, you don't need to consent to everything as soon as you get the app because you haven't really done everything yet. Basically, if you go your whole life on Instagram and you never post a picture, you'll never see that little thing that says, "Oh, by the way, that picture will be used for this and that," because you don't need to see it... There is no need to consent to something that you aren't going to use... You consent to things that you do. If you don't do them, you don't need to worry about those things.*

Once again, participants felt strongly that a long, scrolling text, with no mechanism for verifying that you have read and understood it, is insufficient, and their prototypes were designed in ways to put the onus back onto online businesses and corporations to ensure that people (especially youth) understand their rights online. Unbundling, line-by-line consent, and just-in-time notices provide more clarity and control to users – even when sharing personal information and data is a mandatory requirement of the app, platform or website.

Thinking Differently About Privacy and Consent

After participants presented and explained their paper prototypes, facilitators checked-in for one last round of discussion. These discussions largely involved youth reflecting on their own data sharing practices and the long-term consequences of not fully understanding their privacy rights. Some youth indicated that they will be more 'mindful' and 'aware' about reading privacy and consent documents and understand that more information gives them more power and control over their data.

> ***"I wouldn't say it [will change my] behavior, but I would say more mindfulness, ... It's more awareness about how connected we are to everything. (Bianca 16)***

Youth were generally in agreement that platforms need to provide users with more information in a way that is clear and meaningful. While participants seem to enjoy receiving targeted advertisements and recommendations based on factors like age, gender, interests, internet searches and location, they want to know more about how their data is collected and have the option to share or not share certain data points with particular apps at specific times (ongoing consent).

> *I don't necessarily like it but I guess if I knew everything about different companies that my data was being sold to, and I kind of had a better understanding of it and I sort of knew… what kind of effects things that I post have and I was better informed of that I guess I'd be ok with that. (Jordan 16)*

The youth we spoke to confirmed the "perception that privacy policies primarily serve the purpose of protecting the website owners rather than the website users."[45] They were under no illusion about how online platforms benefit from current online consent processes and were bothered by their opacity and complexity. The concerns they shared with us, and the features they included in their prototype designs, tell us that youth want more information, more control, and more transparency from the online platforms they use. Finally, youth also have a desire to actively participate in, and be consulted about, the re-imagining and re-designing of the processes that determine how data collection will affect their lives.

[45] 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.

Summary and Recommendations

The findings from this qualitative research project demonstrate an urgent need for online platforms to re-design their privacy and consent processes. We heard clearly from participants that meaningful online consent – as conceptualized through the Office of the Privacy Commissioner's guiding principles – is practically non-existent. Youth shared repeatedly that they do not read the long and complicated terms of service documents, even though they are concerned about 'sketchy' and 'weird' data sharing practices. This confirms the 'illusion of consent'[46] or privacy paradox that is outlined in the literature at the beginning of the report. Unfortunately, it seems that many companies maintain a 'better to seek forgiveness rather than permission' approach to privacy[47] that leaves users with a lot of questions and concerns about the economics of personal information in the online world.

However, our conversations with youth ages 13 to 16 in Ottawa also indicate a shift "from resigned acceptance of [policy and consent] practices toward an engaged and critical analysis."[48] Young people are ready and willing to share their experiences, attitudes and concerns with how online platforms currently explain their data collection and sharing policies. Additionally, as demonstrated through their paper prototypes, youth have many ideas for fixes and features that can improve *everyone's* understanding of online privacy and consent so that we can all better avoid the risks and unanticipated consequences of sharing personal details on the internet. Finally, the OPC's guiding principles for meaningful consent resonated strongly with participants and the prototypes they designed offer important insight into how youth would like to see these principles taken-up through new and innovative online consent processes.

The results of this study are a call to action for educators, policymakers and online platforms to improve upon how we approach privacy and consent online. Participants consistently called out a lack of clarity and creativity in current approaches that contribute to a poor understanding of their privacy rights and were equally clear about wanting more information, more protection, more accessibility, more control, and more engagement. The recommendations that follow echo these calls for improvement.

[46] Frischmann, B. (2019). *Electronic contracts and the illusion of consent*. Retrieved May 19, 2019, from https://blogs.scientificamerican.com/observations/electronic-contracts-and-the-illusion-of-consent/?redirect=1
[47] Fernandes, C. N. (2019). Big Tech must be held to account over user consent. Retrieved May 19, 2019, from https://www.ft.com/content/40e558ce-158a-11e9-a168-d45595ad076d
[48] Burkell, J., Steeves, V., & Micheti, A. (2007). Broken doors: Strategies for drafting privacy policies kids can understand. Ottawa, ON.

More Information

Participants made it quite clear that youth need more information about how their data is collected and brokered:

> *…having more information about this in schools would probably improve a lot of cyber security stuff. You could come in and talk about like, 'Hey! People are taking all of your information, just a heads-up!' That's something that would probably open a lot of kid's eyes. (Bianca 16)*

Existing MediaSmarts' resources, such as *Data Defenders* and *Click if You Agree* (both created with support from the Office of the Privacy Commissioner), can assist with this educational component – but we recommend developing new educational resources that incorporate the findings from this report and reflect the OPC's guiding principles for meaningful consent. These resources would be of value both at school and at home.

Furthermore, participants' attitudes towards data collection depended in part on whether their data would be used *only* by the platform collecting it (which would affect only their experience with that platform) or if their personal information would be sold/shared with third parties (which would contribute to their overall data profile). Platforms, therefore, could benefit from being more forthcoming about data collection, storage and sharing practices: for example, if users know that their data will not be shared with third parties this could become a 'selling point' for the platform, app or service. More information about how data is collected, stored and brokered also offers protection to youth (and other users) who are concerned about the potential long-term (and unintended) consequences of sharing personal information online.

More Protection

During the focus group discussions youth expressed concern about the long-lasting nature of the things they share online.

> *It just made me realize how public my life really is. I really don't have any privacy… I know I'm going to start paying a lot more attention from now on. (Erica 16)*

Young people are worried about how their data profiles might influence future education and employment opportunities, among possible future consequences, and felt that this *permanence* was unfair. Therefore, we suggest that policymakers and platforms reflect on how they can provide additional protections to children and youth in this regard. For example, it might be worthwhile to consider a data erasure approach similar to what is outlined in the European Union's *General Data Protection Regulation* (GDPR). The 'right to be forgotten' article of the GDPR "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.[49]

Essentially, online platforms could offer users more clear options for how they can permanently delete their data and/or prohibit their personal information from being shared in ways and in places that they did not initially understand or agree to. Youth, especially, should be privy to such protections.

More Accessibility

There was a consensus (and frustration) among participants that terms of service agreements and privacy policies are *completely* inaccessible.

> *Maybe if they formatted it differently? [Changed] the way the whole consent form works? Like they said before, the form that they use is meant for lawyers, so you can't just gloss over it. Maybe if it sort of gives you information as you go, and maybe it can just be formatted differently – like a slide show? Or different tabs? Not just one long document that has all the information on what data is being collected. (Andrew 16)*

The paper prototypes that participants developed during the focus groups offer multiple strategies and features to improve accessibility, verification and comprehension. The fixes they suggest are:

- clear, plain and simple language
- short sentences and paragraphs to summarize important information
- headings and bullet points
- bold, underlined, and colourful text
- videos and graphics alongside text
- interactive components (such as multiple checkboxes)
- timers that keep the text on your screen (up to five minutes)
- page limits for privacy and consent documents

Online platforms should consider incorporating some (if not all) of these fixes. This would be a good start towards increasing engagement with, and a comprehensive understanding of, online privacy and consent documents. Adding simplicity and focus to these very complicated documents will bring platforms closer to a meaningful online consent process.

[49] GDPR.EU. (2020). *Everything you need to know about the "Right to be forgotten".* Retrieved from: https://gdpr.eu/right-to-be-forgotten/

More Control

Youth were very interested in features and options that give some control over data collection back to users. This re-balancing of the scales was important for youth who expressed feeling powerless in the face of complicated terms of service agreements.

> *...for the most part I often find myself just being like, 'Yeah ok, I agree. I agree to whatever is going on here.' (Bianca 16)*

The features they incorporated into their paper prototypes to address this lack of control are as follows:

- **Unbundling options**: allowing users to give or withhold consent to different forms of data collection and different uses of their data.
- **Line-by-line consent**: where the online platform makes clear what will be done with the collected data by encouraging users to read and click agree to the various components of the document.
- **Just-in-time notices**: giving users the information they require about data collection and data uses as they engage with various components of the app, platform, or website.

Participants felt strongly that these options give people more control over what data is collected and how it is used and linked these features directly to how meaningful consent is conceptualized within the OPC guidelines. Therefore, we recommend that online platforms consider these features (in addition to the fixes above that improve accessibility) when re-designing their online privacy and consent processes.

More Engagement

Finally, and perhaps most importantly, we recommend that researchers, policymakers and platforms continue to create space and opportunity to engage with youth about online privacy and consent. Participants were very excited to hear that the paper prototypes they developed during the focus groups would be shared with the Office of the Privacy Commissioner and online platforms. Youth bring a lot to the table when it comes to digital technology and the online world and their vision, innovation, creativity and enthusiasm should be recognized by those in decision-making positions.

MediaSmarts will continue to engage with young people across Canada in order to develop new resources, tools and supports that best address their experiences, attitudes and concerns about the online world.

Appendices

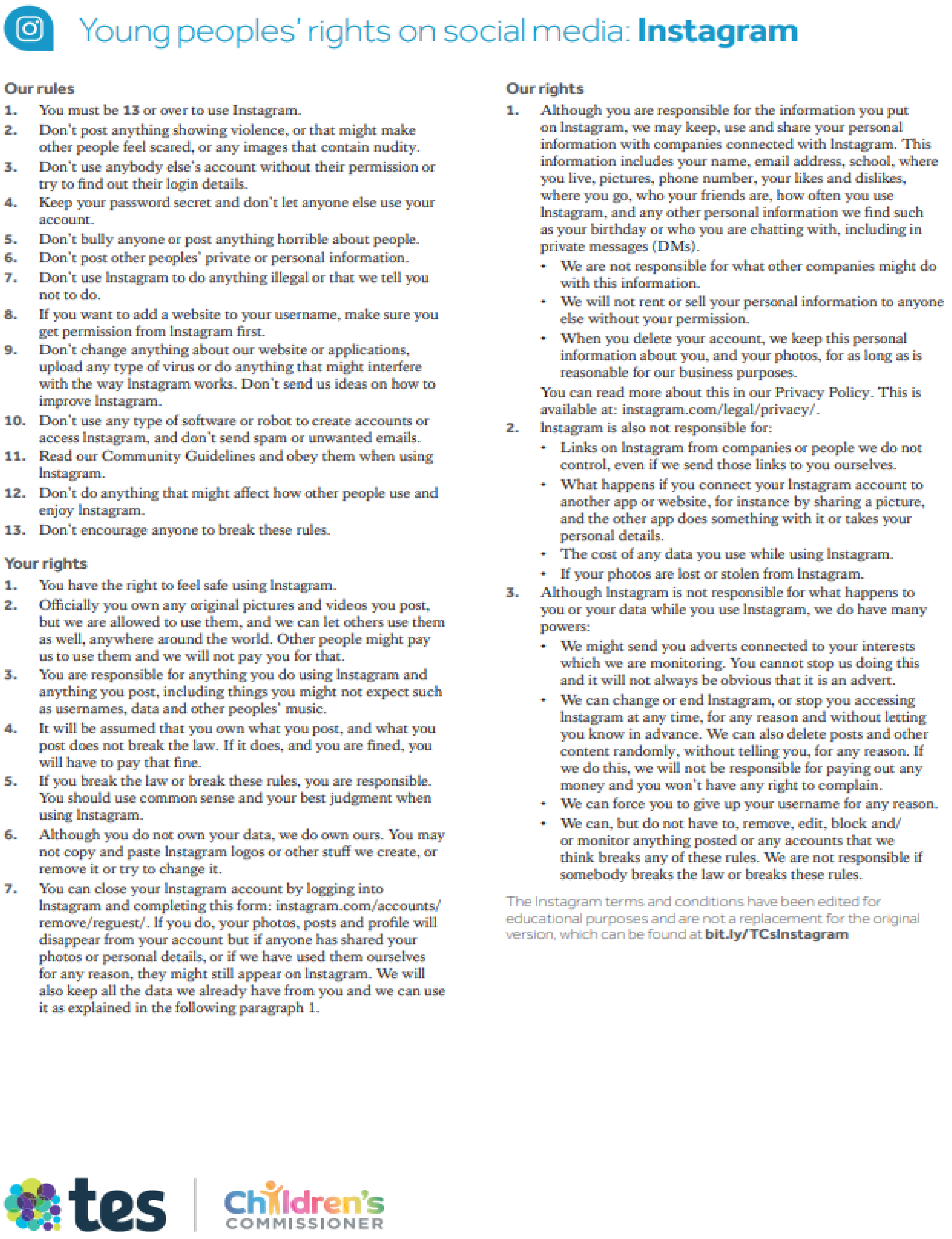
Appendix A: Summary of OPC's Guiding Principles for Meaningful Consent[50]

1. Emphasize key elements
    - Information provided about the collection, use and disclosure of individuals' personal information must be readily available in complete form – but to avoid information overload and facilitate understanding by individuals, certain elements warrant greater emphasis or attention in order to obtain meaningful consent.
        - What personal information is being collected
        - With which parties personal information is being shared
        - For what purposes personal information is collected, used or disclosed
        - Risk of harm and other consequences
2. Allow individuals to control the level of detail they get and when
    - Information must be provided to individuals in manageable and easily-accessible ways (potentially including layers) and individuals should be able to control how much more detail they wish to obtain, and when.
3. Provide individuals with clear options to say 'yes' or 'no'
    - Individuals cannot be required to consent to the collection, use or disclosure of personal information beyond what is necessary to provide the product or service – they must be given a choice. These choices must be explained clearly and made easily accessible. Whether each choice is most appropriately 'opt-in' or 'opt-out' will depend on factors discussed in the "Form of Consent" section of this document.
4. Be innovative and creative
    - Organizations should design and/or adopt innovative consent processes that can be implemented just-in-time, are specific to the context, and are appropriate to the type of interface used.
    - When seeking consent online, organizations should do more than simply transpose in digital form, their paper-based policies from the offline environment. Organizations are encouraged to use a variety of communications strategies – including "just-in-time" notices, interactive tools and customized mobile interfaces – to explain their privacy practices.

[50] Full version of the OPC Guidelines for Meaningful Consent are available here: https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/#_seven

5. Consider the consumer’s perspective
    - Consent processes must take into account the consumer’s perspective to ensure that they are user-friendly and that the information provided is generally understandable from the point of view of the organization’s target audience(s)
6. Make consent a dynamic and ongoing process
    - Informed consent is an ongoing process that changes as circumstances change; organizations should not rely on a static moment in time but rather treat consent as a dynamic and interactive process.
7. Be accountable: Stand ready to demonstrate compliance
    - Organizations, when asked, should be in a position to demonstrate compliance, and in particular that the consent process they have implemented is sufficiently understandable from the general perspective of their target audience(s) as to allow for valid and meaningful consent.

Appendix B: Example of Simplified Terms and Conditions from The Children's Commissioner in England[51]



Young peoples' rights on social media: **Instagram**

Our rules

1. You must be **13** or over to use Instagram.
2. Don't post anything showing violence, or that might make other people feel scared, or any images that contain nudity.
3. Don't use anybody else's account without their permission or try to find out their login details.
4. Keep your password secret and don't let anyone else use your account.
5. Don't bully anyone or post anything horrible about people.
6. Don't post other peoples' private or personal information.
7. Don't use Instagram to do anything illegal or that we tell you not to do.
8. If you want to add a website to your username, make sure you get permission from Instagram first.
9. Don't change anything about our website or applications, upload any type of virus or do anything that might interfere with the way Instagram works. Don't send us ideas on how to improve Instagram.
10. Don't use any type of software or robot to create accounts or access Instagram, and don't send spam or unwanted emails.
11. Read our Community Guidelines and obey them when using Instagram.
12. Don't do anything that might affect how other people use and enjoy Instagram.
13. Don't encourage anyone to break these rules.

Your rights

1. You have the right to feel safe using Instagram.
2. Officially you own any original pictures and videos you post, but we are allowed to use them, and we can let others use them as well, anywhere around the world. Other people might pay us to use them and we will not pay you for that.
3. You are responsible for anything you do using Instagram and anything you post, including things you might not expect such as usernames, data and other peoples' music.
4. It will be assumed that you own what you post, and what you post does not break the law. If it does, and you are fined, you will have to pay that fine.
5. If you break the law or break these rules, you are responsible. You should use common sense and your best judgment when using Instagram.
6. Although you do not own your data, we do own ours. You may not copy and paste Instagram logos or other stuff we create, or remove it or try to change it.
7. You can close your Instagram account by logging into Instagram and completing this form: instagram.com/accounts/remove/reguest/. If you do, your photos, posts and profile will disappear from your account but if anyone has shared your photos or personal details, or if we have used them ourselves for any reason, they might still appear on Instagram. We will also keep all the data we already have from you and we can use it as explained in the following paragraph 1.

Our rights

1. Although you are responsible for the information you put on Instagram, we may keep, use and share your personal information with companies connected with Instagram. This information includes your name, email address, school, where you live, pictures, phone number, your likes and dislikes, where you go, who your friends are, how often you use Instagram, and any other personal information we find such as your birthday or who you are chatting with, including in private messages (DMs).
   - We are not responsible for what other companies might do with this information.
   - We will not rent or sell your personal information to anyone else without your permission.
   - When you delete your account, we keep this personal information about you, and your photos, for as long as is reasonable for our business purposes.

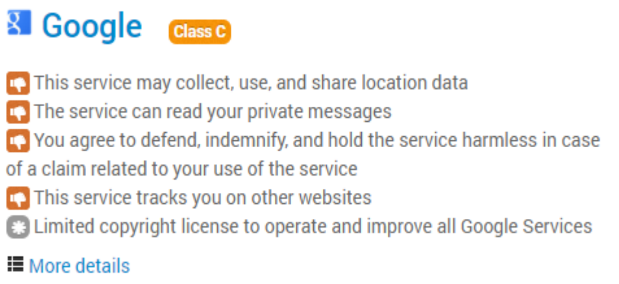
   You can read more about this in our Privacy Policy. This is available at: instagram.com/legal/privacy/.
2. Instagram is also not responsible for:
   - Links on Instagram from companies or people we do not control, even if we send those links to you ourselves.
   - What happens if you connect your Instagram account to another app or website, for instance by sharing a picture, and the other app does something with it or takes your personal details.
   - The cost of any data you use while using Instagram.
   - If your photos are lost or stolen from Instagram.
3. Although Instagram is not responsible for what happens to you or your data while you use Instagram, we do have many powers:
   - We might send you adverts connected to your interests which we are monitoring. You cannot stop us doing this and it will not always be obvious that it is an advert.
   - We can change or end Instagram, or stop you accessing Instagram at any time, for any reason and without letting you know in advance. We can also delete posts and other content randomly, without telling you, for any reason. If we do this, we will not be responsible for paying out any money and you won't have any right to complain.
   - We can force you to give up your username for any reason.
   - We can, but do not have to, remove, edit, block and/or monitor anything posted or any accounts that we think breaks any of these rules. We are not responsible if somebody breaks the law or breaks these rules.

The Instagram terms and conditions have been edited for educational purposes and are not a replacement for the original version, which can be found at **bit.ly/TCsInstagram**

tes | Children's COMMISSIONER

[51] More examples of simplified terms and conditions from the Children's Commissioner are available here: https://www.childrenscommissioner.gov.uk/publication/simplified-social-media-terms-and-conditions-for-facebook-instagram-snapchat-youtube-and-whatsapp/

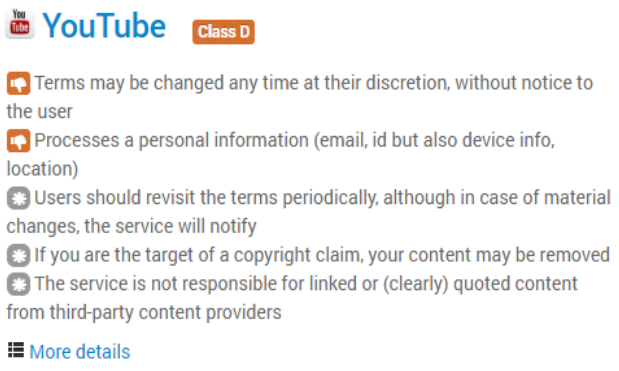
Appendix C: Terms of Service; Didn't Read – Examples of Rating System[52]



Google Class C

👎 This service may collect, use, and share location data
👎 The service can read your private messages
👎 You agree to defend, indemnify, and hold the service harmless in case of a claim related to your use of the service
👎 This service tracks you on other websites
✱ Limited copyright license to operate and improve all Google Services

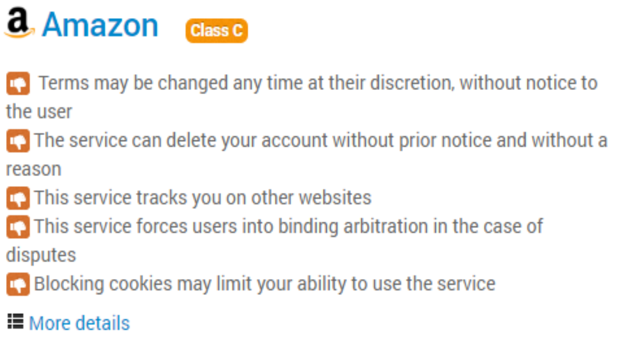
More details



YouTube Class D

👎 Terms may be changed any time at their discretion, without notice to the user
👎 Processes a personal information (email, id but also device info, location)
✱ Users should revisit the terms periodically, although in case of material changes, the service will notify
✱ If you are the target of a copyright claim, your content may be removed
✱ The service is not responsible for linked or (clearly) quoted content from third-party content providers

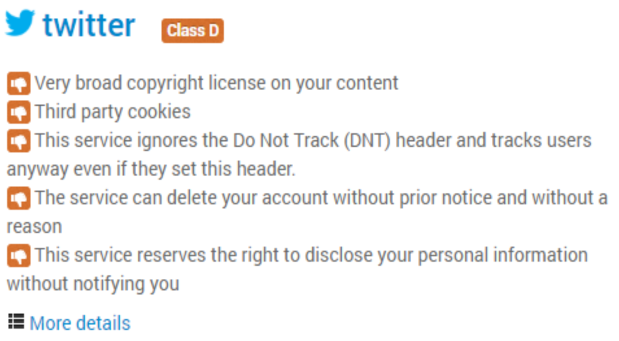
More details



Amazon Class C

👎 Terms may be changed any time at their discretion, without notice to the user
👎 The service can delete your account without prior notice and without a reason
👎 This service tracks you on other websites
👎 This service forces users into binding arbitration in the case of disputes
👎 Blocking cookies may limit your ability to use the service

More details



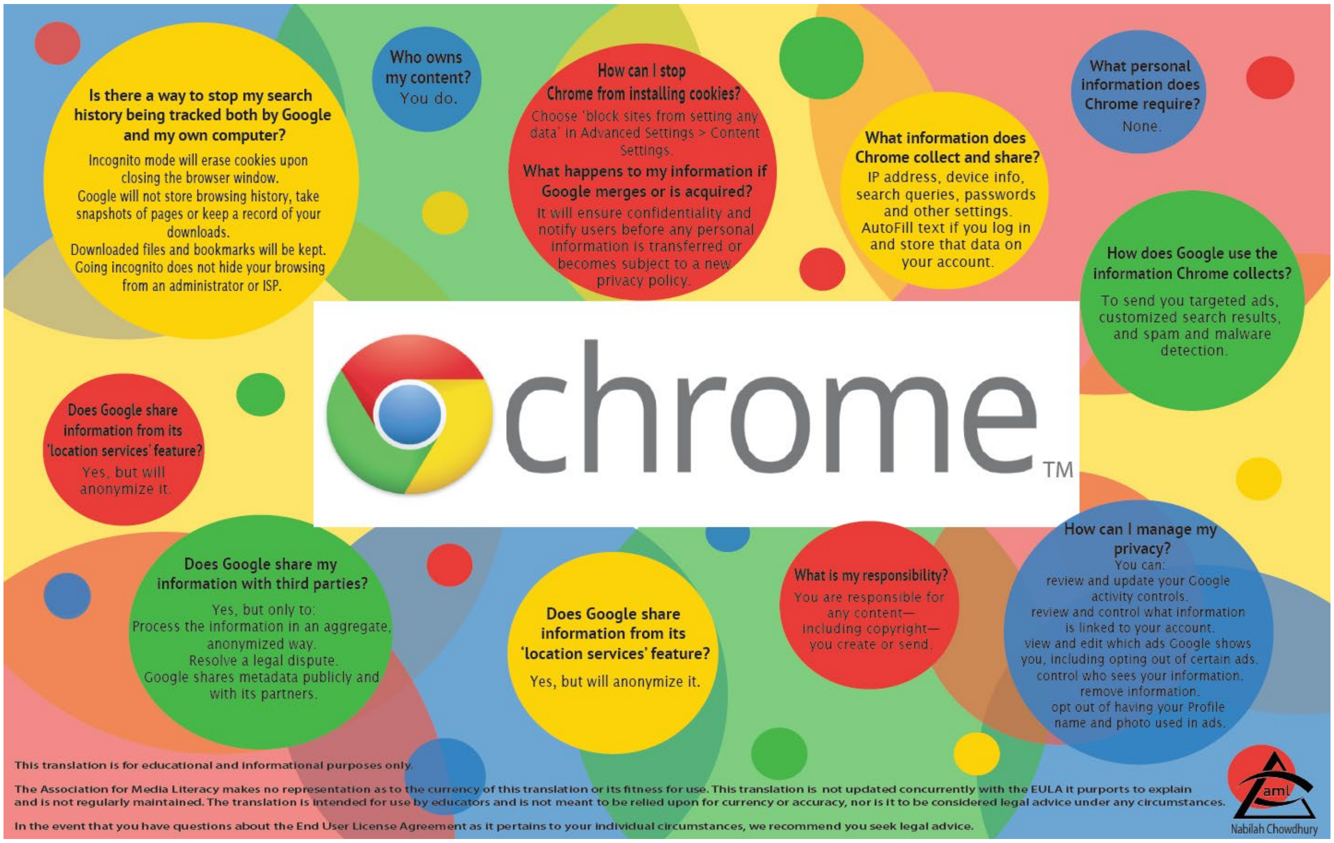
twitter Class D

👎 Very broad copyright license on your content
👎 Third party cookies
👎 This service ignores the Do Not Track (DNT) header and tracks users anyway even if they set this header.
👎 The service can delete your account without prior notice and without a reason
👎 This service reserves the right to disclose your personal information without notifying you

More details

[52] More details about the ToS;DR rating system available here: https://tosdr.org/

Appendix D: Plain Language End User Licence Agreements[53]



chrome™

Is there a way to stop my search history being tracked both by Google and my own computer?

Incognito mode will erase cookies upon closing the browser window.
Google will not store browsing history, take snapshots of pages or keep a record of your downloads.
Downloaded files and bookmarks will be kept.
Going incognito does not hide your browsing from an administrator or ISP.

Who owns my content?

You do.

How can I stop Chrome from installing cookies?

Choose 'block sites from setting any data' in Advanced Settings > Content Settings.

What happens to my information if Google merges or is acquired?

It will ensure confidentiality and notify users before any personal information is transferred or becomes subject to a new privacy policy.

What information does Chrome collect and share?

IP address, device info, search queries, passwords and other settings.
AutoFill text if you log in and store that data on your account.

What personal information does Chrome require?

None.

How does Google use the information Chrome collects?

To send you targeted ads, customized search results, and spam and malware detection.

Does Google share information from its 'location services' feature?

Yes, but will anonymize it.

Does Google share my information with third parties?

Yes, but only to:
Process the information in an aggregate, anonymized way.
Resolve a legal dispute.
Google shares metadata publicly and with its partners.

Does Google share information from its 'location services' feature?

Yes, but will anonymize it.

What is my responsibility?

You are responsible for any content—including copyright—you create or send.

How can I manage my privacy?

You can:
review and update your Google activity controls.
review and control what information is linked to your account.
view and edit which ads Google shows you, including opting out of certain ads.
control who sees your information.
remove information.
opt out of having your Profile name and photo used in ads.

This translation is for educational and informational purposes only.

The Association for Media Literacy makes no representation as to the currency of this translation or its fitness for use. This translation is not updated concurrently with the EULA it purports to explain and is not regularly maintained. The translation is intended for use by educators and is not meant to be relied upon for currency or accuracy, nor is it to be considered legal advice under any circumstances.

In the event that you have questions about the End User License Agreement as it pertains to your individual circumstances, we recommend you seek legal advice.

aml

Nabilah Chowdhury

[53] More examples of the plain language end user license agreements from Canada's Association for Media Literacy are available here: https://aml.ca/resources/end-user-license-agreements/

Appendix E: Participants and Focus Groups

Focus Group	Pseudonym	Age	Gender
#1	James	16	Boy
	Andrew	16	Boy
	Natasha	15	Girl
	Leah	15	Girl
	Amélie	15	Girl
	Kaitlin	15	Girl
	Jordan	16	Boy
	Claire	15	Girl
	Tara	16	Girl
	Charlotte	15	Girl
#2	Elise	13	Girl
	Faye	13	Girl
	Sarah	13	Girl
	Cassie	13	Girl
	Dana	14	Girl
	Morgan	13	Girl
	Melissa	13	Girl
	Gina	14	Girl
	April	13	Girl
#3	Shannon	16	Girl
	Bianca	16	Girl
	Erica	16	Girl