LESSON PLAN

Online Marketing to Kids: Protecting Your Privacy

This lesson is part of *USE, UNDERSTAND & ENGAGE: A Digital Media Literacy Framework for Canadian Schools*: http://mediasmarts.ca/teacher-resources/digital-literacy-framework.

$ 🔒

LEVEL: Grade 6 to 9

ABOUT THE AUTHOR: MediaSmarts

Overview

This lesson introduces students to the ways in which commercial apps and websites collect personal information from kids and to the issues surrounding children and privacy on the Internet. Students begin by considering how comfortable they would be with people knowing various things about them, and then watch and discuss a video which explains how targeted advertising works. They then explore the idea of targeted advertising through a class exercise in which Prince Charming tries to target Cinderella with an ad for glass slippers, and then analyze how their own personal information might be used to target them with ads. In the second part of the lesson, students are introduced to privacy policies and how they are rated by the website *Terms of Service, Didn't Read*. They read and analyze the site's rating for a popular app and then learn ways to limit data collection. In an extension activity, students are introduced to the idea of "dark patterns" and imagine how the Wicked Queen might use them to convince Snow White to accept "poison" cookies.

Learning Outcomes

Know: Students will learn...

- Privacy & security:
  - How personal information is used an ad targeting
  - Some possible impacts of data collection
  - What privacy policies are
  - Technical measures to limit data collection, including where and how to turn off ad targeting and tracking on popular apps
- Consumer awareness:
  - How apps and other online platforms make money
  - How and why online platforms use targeted advertising

Key vocabulary: Data, personal information, targeted advertising, privacy policy, dark pattern

Understand: Students will understand the following key concepts/big ideas:

- Media have commercial considerations: Personal information is valuable to the companies that own apps and websites
- Digital media have unanticipated audiences: You may be giving away more of your personal information than you are aware of when using apps
- Digital media experiences are shaped by the tools we use: Features and defaults of apps' design and interface can lead us to share more than we otherwise would.

Common misunderstandings to correct: The presence of a privacy policy does *not* mean that a service does not collect data, it only lays out how the service may collect and use your data

Do: Students will be able to...

- Identify how advertisers might target them using their personal information
- Evaluate a privacy policy
- Take steps to limit data collection when using apps and websites

PREPARATION AND MATERIALS

Review the teacher backgrounder *Most Popular Kids' Apps*

Prepare to distribute student handouts:

- *What Would People Know About You If They Knew...*
- *Finding Cinderella*
- *The Target is You*
- *Terms of Service and Privacy Policies*
- *Privacy Audit*
- *Hiding Cinderella*
- *Protecting Your Privacy on Apps and Websites*

If you are doing the extension activity, distribute the handout *Dark Arts and Dark Patterns*

Procedure

PART ONE: UNDERSTANDING TARGETED ADVERTISING

Begin by distributing the handout W*hat Would People Know About You If They Knew…* and asking students to imagine how much people would know about them if they knew…:

- Where they lived
- What videos they watched online
- What they did on social media (what they posted, viewed, commented on, Liked, etc.)
- What they bought online
- What they bought in person
- What they searched for online

Have students write at least two things in each category, with the reassurance that they won't have to share any of what they write. (This can be assigned as homework the day before if you prefer.)

When students have finished, ask them:

- Would you feel comfortable with people knowing these things?
- Are there some that feel more private or sensitive than others? (They don't need to give specific examples, though they can share which categories feel more or less sensitive, e.g. what they buy vs, what they've searched for)
- Are there some you would be willing to let some people (like close friends or family) know?
- Are there some you wouldn't want *anyone* to know?

HOW TARGETED ADVERTISING WORKS

If no students have mentioned it, point out that there are people who know *all* those things: the companies who own digital apps, websites and devices. All of these are examples of *personal information* or *personal data* that companies collect.

Ask students if they know *why* companies collect so much personal information.

When students have discussed the question for a few minutes, show them the video *How Targeted Ads Work*.

After the video, ask the following consolidation questions:

How do apps like social networks (Instagram, Snapchat, etc.) or video sites (YouTube, etc.) make money?

> By showing you ads.

How might knowing more about you help them make money?

> Point out that as well as targeting you with ads, apps use your data to target you with content that will make you spend more time using them.

Do targeted ads always work?

> They don't always work well because the data they collect might be inaccurate (for instance, if you share a device or an account) or the guesses they make based on that data might be wrong.

What are some of the risks or downsides of targeted ads?

- you may be targeted based on characteristics that aren't supposed to be used;
- if the profile of you is inaccurate, you might not see ads or other content that you'd be interested in seeing;
- people at vulnerable times in their lives, like when they've just been diagnosed with a serious disease, might be targeted by scam ads;
- the data collected about you might be used for other purposes for years afterwards.

FINDING CINDERELLA

Now distribute the handout *Finding Cinderella*.

Ask students if they know the story of Cinderella, and tell (or have a student tell) the essentials:

- Cinderella lived with a wicked stepmother and two wicked stepsisters.
- Her Fairy Godmother magically gave her a dress, a carriage, and glass slippers so she could go to the royal ball.

- Cinderella met Prince Charming at the ball but had to leave before midnight.
- She left one of her glass slippers behind.
- Prince Charming went to every house looking for whoever's feet fit the shoe, and eventually found Cinderella.

Tell students to imagine that instead of going house-to-house, Prince Charming now can use targeted advertising to target Cinderella with an ad for glass slippers. How would he do that?

Have them consider:

What does he already know about his "target audience," Cinderella?

- Her apparent gender
- Her approximate age
- Her general location
- Her shoe size

What information might he have about her that is *inaccurate*?

Prompting questions:

Why might he have a mistaken idea about her income? (Because of the dress and carriage her Fairy Godmother gave her)

Do you think she has her own phone? How might sharing a phone with her stepsisters or stepmother

What could he learn about her from:

- Her search history?
- Her viewing history on YouTube or Netflix
  - Does she watch how-to videos about cleaning? Romance movies about princes?
- Her activity (viewing, posting, commenting, Liking, sharing) on social media such as Instagram, Snapchat or TikTok
  - Has she posted anything about the party? About her Fairy Godmother? Complaining about her stepmother or stepsisters? Trying to replace a single shoe?
  - Has she Liked any of his photos from the party?

- Her online purchases
  - If she's ever bought shoes online, he could match her shoe size!

THE TARGET IS YOU

Now distribute the handout *The Target Is You* and have students complete it for themselves. Ask each student to consider:

- What might online advertisers know or guess about you?
- What data would they know that from or base those guesses on?
- What might they think they know about you that is inaccurate? Why would they think that?
- What might they show you ads for, based on what they know or guess about you?
- What are some possible "side effects" of the things they know about you being shared?

Have each student share how doing this exercise made them feel about ad targeting and data collection. (They do *not* have to share any of their specific answers.) Use this to check their understanding of the big ideas and essential subject knowledge so far.

If you wish, you may have them write a reflection following this activity, with this prompt: I used to think about privacy… And now I think…

PART TWO: PROTECTING YOUR PRIVACY

GRADING PRIVACY POLICIES

Now ask students if they know what an app's **privacy policy** is, and what it does. Explain that it is not true, as many people think, that if an app has a privacy policy it will not collect *any* information about you. What a privacy policy does is tell you:

- What information they collect;
- What they are allowed to do with it;
- Who they can share it with; and
- How long they can keep it, among other things.

Now ask: How long do you think it would take to read the Terms of Service and Privacy Policy for:

- Instagram? (Approximately nine and a half hours.)
- YouTube? (Thirteen and three-quarters hours.)
- Amazon? (Fourteen hours.)
- TikTok? (Thirty-one and a half hours.)

(Estimates from https://www.socialmediatoday.com/news/how-long-does-it-take-to-read-the-terms-of-service-for-each-app-infograph/577235/.)

Distribute the handout *Terms of Service and Privacy Policies* and go through it with the class. Then distribute the *Privacy Audit* activity sheet.

> If possible, use a data projector or digital whiteboard to show students the *Terms of Service, Didn't Read* website (tosdr.org) and search for Google. Go to the Google listing and show students the terms marked in red, yellow, green and grey.

Now divide the class into pairs or small groups. Assign each pair or group one of the apps listed in the backgrounder *Most Popular Kids' Apps* and then have them access the *Terms of Service, Didn't Read* website to compete the privacy audit activity.

When students have finished, have them share their findings with the rest of the class:

- What rating did their app get?
- Were they surprised? Why or why not?
- Do they think the rating was fair? Why or why not?
- If more than one group audited the same app:
  - Did they identify the same red and yellow terms as being most concerning?
  - Did they identify the same green terms as being most reassuring?
  - If there were differences between teams' ratings, ask the teams to explain their thinking.
- Does knowing the rating make them more or less likely to use the app? Why or why not?

PROTECTING YOUR PRIVACY

If none of the students raised this point during the last discussion, ask them:

- Do you sometimes feel like you *have* to use an app or service, even if you're uncomfortable with its effect on your privacy, because your friends are using it?
- Because your parents use it to contact you?
- Are you sometimes *required* to use one of these services to participate in school or an activity?

PROTECTING YOUR PRIVACY

Tell students that using an app or other online service doesn't have to be an all-or-nothing decision: there are ways of limiting how much of your information is collected and how it is used.

Distribute the handout *Protecting Your Privacy on Apps and Websites*.

When you have gone through it with the class, ask:

- Do you already do any of these things?
- Are there any things here that you want to start doing?
- Are there things here that you want to talk to your parents about doing?

Ask them to think back to the privacy audit they did earlier, in particular things about the app's privacy policy that made them uncomfortable. Now have them choose **three** tips from the *Protecting Your Privacy on Apps and Websites* handout that would make them more comfortable using the app, and write a short explanation (2-3 sentences apiece) explaining how that particular tip would help protect their privacy.

EXTENSION ACTIVITY: DARK ARTS AND DARK PATTERNS

Point out to students that although we may *want* to do these things to protect our privacy, apps don't always make it easy. The ways that they nudge us to do things we might not want to do—or to *not* do things that we *do* want to do—are called *dark patterns*.

Distribute the handout *Dark Patterns* and go through it with the class. Ask students how each of the examples on the second page illustrates each category:

- *Obstruction:* the option to accept data collection (“Accept and continue”) is a single step, while “Manage data settings” sounds like a lot of work.
- *Obfuscation:* “Select all” is big, green, and easy to find. As well, there is no easy “Reject All” button.
- *Pressure:* this warns you about bad things that will happen if you turn off customization, using exclamation marks to make its point, and makes the button to do so red.

Ask students if they know the story of Snow White. Make sure they recall the part where the Wicked Queen convinces Snow White to eat a poisoned apple, and tell them that they are going to imagine she is using dark patterns to convince Snow White to accept “poison” cookies instead.

Tell students to come up with one example of each type of dark pattern that she might use to do so. They can draw a cookie consent box in the smartphone screen in the handout or use a full sheet of blank paper, or draw it digitally.

STUDENT HANDOUT

ONLINE MARKETING TO KIDS: PROTECTING YOUR PRIVACY

What Would People Know About You If They Knew...

List at least two things that someone might know (or think they know) about you based on each of these:

What videos you watch online?

What you do on social media (things you've posted, viewed, commented on, Liked, etc.)?

What you buy online?

What you buy in person?

What you search for online?

STUDENT HANDOUT

ONLINE MARKETING TO KIDS: PROTECTING YOUR PRIVACY

Finding Cinderella

For this exercise we are going to imagine that Prince Charming is using targeted ads to find Cinderella after she ran away from the ball.

What does he already know about his "target audience"?

What might he *think* he knows that is inaccurate?

What could he learn about her from:

- Her search history?
- Her viewing history on YouTube or Netflix?
- Her activity (viewing, posting, commenting, Liking, sharing) on social media such as Instagram, Snapchat or TikTok?
- Her online purchases?

STUDENT HANDOUT

ONLINE MARKETING TO KIDS: PROTECTING YOUR PRIVACY

The Target Is You

Now you're going to imagine how apps, websites, and data brokers target *you*.

Think about what you've learned about targeted advertising and think of **at least two answers** to each of these questions:

- What might online advertisers know or guess about you?

- What data would they know that from, or base those guesses on?

- What might they think they know about you that is inaccurate? Why would they think that?

- What might they show you ads for, based on what they know or guess about you?

- What are some possible "side effects" of the things they know about you being shared?

STUDENT HANDOUT

ONLINE MARKETING TO KIDS: PROTECTING YOUR PRIVACY

Terms of Service and Privacy Policies

Privacy Policies outline the privacy terms and conditions of a particular site. However, many privacy policies are vague, misleading or non-existent, as well as being very long: that's why just half of Canadian kids have ever read one or had someone read one with them.

Luckily, you don't have to read the whole policy to understand how it will affect your privacy. When you read a Privacy Policy, you want to look or search for section titles like:

- "Personal information we collect" or "How we collect your personal data."
- "Geolocation" or "geotargeting": If an app wants to access your location for reasons that don't make sense to you, you may need to turn off GPS on your device.
- "How we use your personal information": Look for vague phrases like "business activities" or "business purposes."
- "Personalize," "enhance," "improve your services" or "interest-based advertising": If the policy contains any language like this, find out if you can turn off algorithmic sorting (such as by switching from the "For you" to the "Following" feed) and targeted advertising.
- "Your rights" or "your choices": This will usually lay out what options they have to give you under the laws where you live.

The website **Terms of Service, Didn't Read** (tosdr.org) grades different apps' and websites' terms of service and privacy policies from **A** to **E**:

A: These " they treat you fairly, respect your rights and will not abuse your data."

B: These "are fair towards the user but they could be improved."

C: These terms of service "are okay but some issues need your consideration."

D: These "are very uneven or there are some important issues that need your attention."

E: These terms of service "raise very serious concerns."

These grades are based on the opinions of the site's volunteers, but they give specific reasons for why each grade is assigned:

- **Red:** Terms that are seriously unfair to the user
- **Yellow:** Terms that raise some concerns
- **Green:** Terms that protect or empower the user
- **Grey:** Terms that have a neutral impact on the company and the user

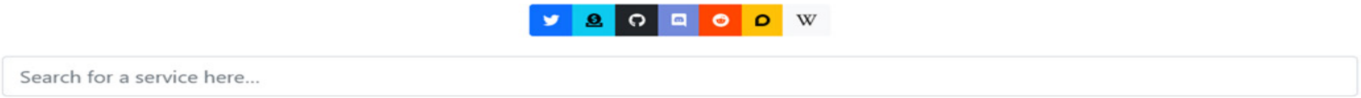
STUDENT HANDOUT

ONLINE MARKETING TO KIDS: PROTECTING YOUR PRIVACY

Privacy Audit

1. List the app that you are auditing:

2. Go to the Terms of Service, Don't Read home page (tosdr.org) and search for the app. **If it is not listed there, choose another.** The search box is at the top of the page, just above the featured rankings:



Search for a service here...

Write the app's score (A-E) below:

3. If there are any terms that are marked as **red**, list the **two** that you feel have the **worst** effect on your privacy.

4. 4. If there are any terms that are marked as **yellow**, list **two** that you feel have the **worst** effect on your privacy.

5. If there are any terms that are marked as **green**, list **two** that you feel do the most to **protect** your privacy.

Answer the following questions on separate paper:

6. Did the rating surprise you? Why or why not?
7. Do you think the rating was fair? Why or why not?
8. Does knowing the rating make you more or less likely to use the app? Why or why not?

STUDENT HANDOUT

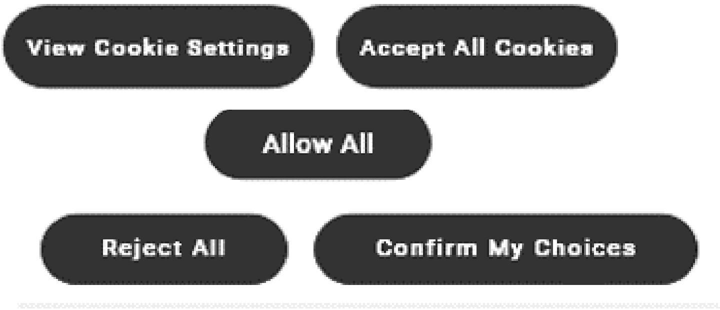
ONLINE MARKETING TO KIDS: PROTECTING YOUR PRIVACY

Protecting Your Privacy on Apps and Websites

Almost all of kids' favourite apps and websites make money from targeted advertising, which uses their personal information to choose which ads to show them. Many of them also sell the data they collect to data brokers, which use information from many sources to make detailed profiles of users. Some also share it with other apps that are owned by the same company, such as Google and YouTube or Instagram and Facebook.

But as William Budington of the Electronic Frontier Foundation says, "There are things you can do to protect your privacy by 85, 90, 95 per cent that will not add much friction to your life." Here are a few key ones:

- Install privacy-protecting plugins such as Privacy Badger on laptops and desktops and apps such as DuckDuckGo on mobile devices.
- Review what information different apps are collecting on mobile devices.
- Review and customize privacy settings. For example, here's how you can turn off tracking and targeted ads on:
    - Google and YouTube: https://myaccount.google.com/data-and-privacy
    - Facebook, WhatsApp and Instagram: https://www.facebook.com/privacy/checkup/
    - TikTok: https://support.tiktok.com/en/account-and-privacy/personalized-ads-and-data
- Don't sign in to any apps or websites using your social network logins. You can also make secure and disposable email addresses using SharkLasers or ProtonMail if you want to register for something without giving away your regular email address.
- Go into your devices' Settings and turn off apps' permission to access the camera, microphone and location.
- If you use iOS devices like iPhones or iPads, make sure to refuse data collection when installing new apps. If you use Android devices, install the DuckDuckGo app and turn on App Tracking Protection.
- Accept only the minimum required level of data collection on websites – first, by never clicking "Accept All," and then by looking for phrases like "Reject All" or "Only Necessary."



PRIVACY PLAN:

Think back to the privacy audit you did earlier.

Choose **three** of the tips above that would make you feel more comfortable using that app.

Write 2-3 sentences for **each** tip explaining why it would protect your privacy when using that app.

STUDENT HANDOUT

ONLINE MARKETING TO KIDS: PROTECTING YOUR PRIVACY

Dark Arts and Dark Patterns

“Dark patterns” are ways that apps nudge us to do things we might not want to do. They can also nudge us not to do things that we do want to do.

In this exercise we’ll look at how they nudge us to **give away more personal information** and make us less likely to **take steps to control our privacy**.

There are three main types of dark patterns relating to privacy:

Obstruction: Making it harder to do things that give away less privacy.

- Making data collection the default choice (so you have to do something not to have your personal information collected)
- Adding extra steps to make you confirm that you don’t want your data collected
- Making it easier to accept than to reject data collection

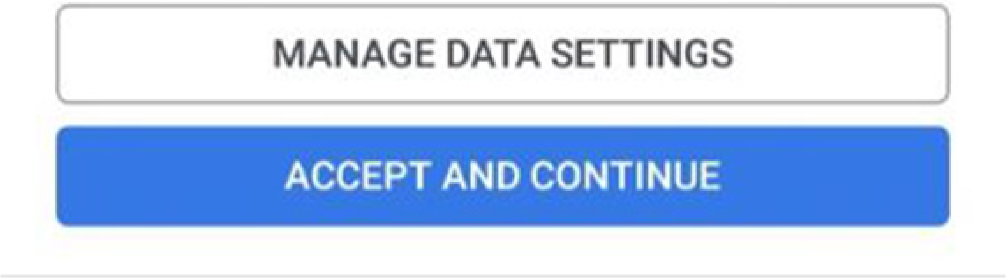
Obfuscation: Making it harder to find the tools we can use to protect our privacy.

- Making privacy options hard to find
- Making buttons or other features that allow data collection more obvious or more appealing
- Not being clear what data you have to give and what’s optional
- Making your choices confusing
- Suggesting that tools or choices protect your privacy more than they do (like “Incognito” mode)

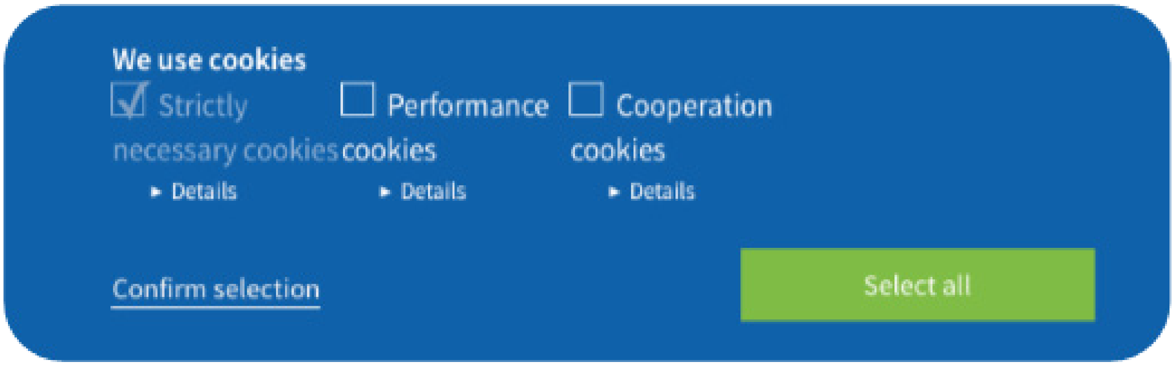
Pressuring: Making you feel that it’s good to accept data collection or making you feel bad about protecting your privacy.

- Making the app harder to use if you don’t share personal information
- Scaring you with what you will lose or not get if you don’t share your personal information
- Not letting you say “No” outright

OBSTRUCTION:

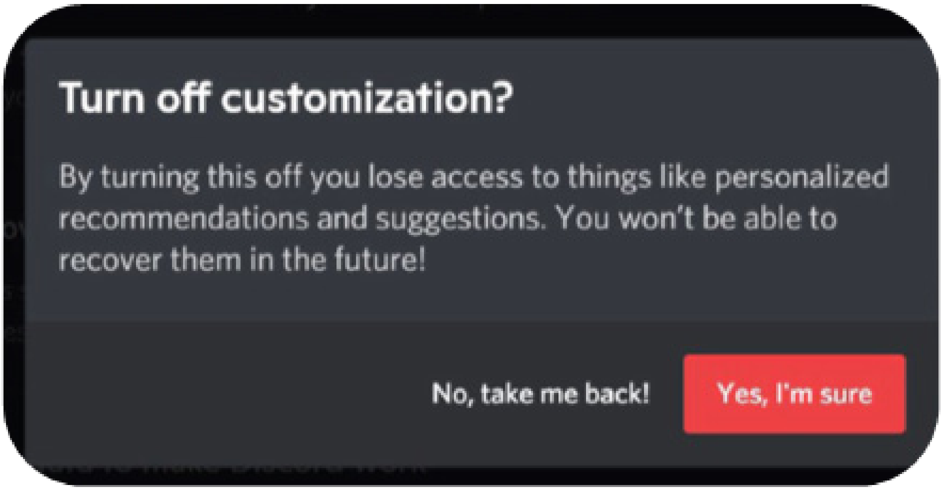


OBFUSCATION:


We use cookies

☑ Strictly necessary cookies ☐ Performance cookies ☐ Cooperation cookies

PRESSURING:


Turn off customization?

By turning this off you lose access to things like personalized recommendations and suggestions. You won't be able to recover them in the future!

How can the Wicked Queen convince Snow White to accept “poison” cookies?

Come up with one example of each type of dark pattern that she might use:

TEACHING BACKGROUNDER

ONLINE MARKETING TO KIDS: PROTECTING YOUR PRIVACY

Most Popular Kids' Apps

According to MediaSmarts' *Young Canadians in a Wireless World* survey, these are the apps where Canadian kids in grades 4 to 11 are most likely to have an account:

YouTube
(60% have accounts)

Facebook
(57% have accounts)

TikTok
(54% have accounts)

Instagram
(50% have accounts)

Snapchat
(41% have accounts)

X (formerly Twitter)
(29% have accounts)

Amazon
(28% have accounts)

WhatsApp
(27% have accounts)