

LESSON PLAN

The Privacy Dilemma

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 9 to 12

ABOUT THE AUTHOR: Matthew Johnson, Director of Education, MediaSmarts

This lesson was made possible with financial support from the Office of the Privacy Commissioner of Canada.

Overview

In this lesson students learn the ways that the apps they use are designed to encourage them to share more information—both with other users and with the apps themselves. They are then introduced to the idea of persuasive design or “dark patterns” and investigate whether these are used to make it more difficult to opt out of data collection on popular apps. Finally, the class creates a “rogues’ gallery” to help them identify dark patterns when they encounter them.

Learning Outcomes

Know: Students will learn...

- Reading media: Types and characteristics of “dark patterns” that influence sharing of personal information
- Privacy & security: Technical measures to limit data collection, including where and how to turn off ad targeting and tracking on popular apps

Key vocabulary: Data, default, 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.

Do: Students will be able to...

- Identify ways that apps encourage us to share personal information
- Recognize and identify “dark patterns” that can influence how much personal information we share
- Limit or turn off data collection and ad tracking on popular apps

Preparation and Materials

Ensure that students are able to access the following websites:

- 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>

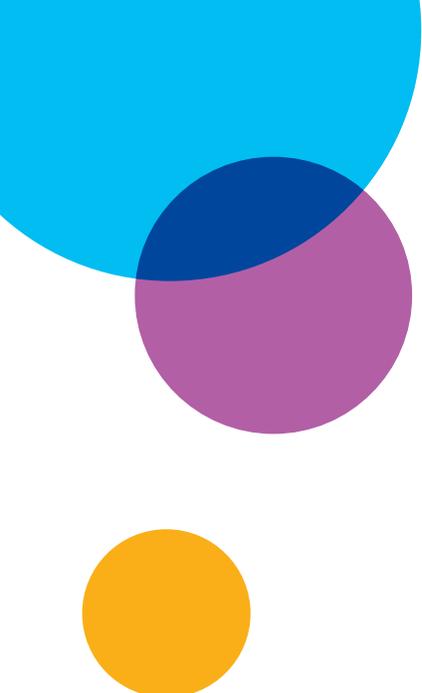
Prepare to distribute these handouts:

- *Made for Sharing*
- *Dark Patterns*
- *Dark Pattern Audit*
- *Rogues' Gallery*
- *Protecting Your Privacy on Apps and Websites*

Procedure

PERCEPTIONS OF PRIVACY

Begin by asking students how important their privacy is to them. (You may ask them to rate it on a scale of one to five, with one being a very low priority and five being a very high priority.) Ask those who say it is unimportant why they are not concerned. (They may feel that they have nothing to hide, that nobody is interested in violating their privacy, or that privacy is over-rated.) Ask students to give specific examples of real or feared violations of their privacy, which you may compile on the blackboard.



Using the examples raised by students, have the class try to define what is meant by “privacy.” Is it an absolute (you either have privacy or you don’t) or a relative thing (you can have more or less privacy)? Is privacy more important in some contexts than others (online vs. offline, at home vs. at school, etc.)?

MADE FOR SHARING

Explain to students that many apps are designed to encourage you to share personal information. This can mean consciously sharing something (like posting a photo or video) or interacting with something like a photo or video – this helps them learn (or guess) things like your interests, your age, your gender, et cetera.

Distribute the handout *Made for Sharing*. Divide students into groups or pairs and assign each group to do an analysis of either YouTube, Instagram or TikTok.

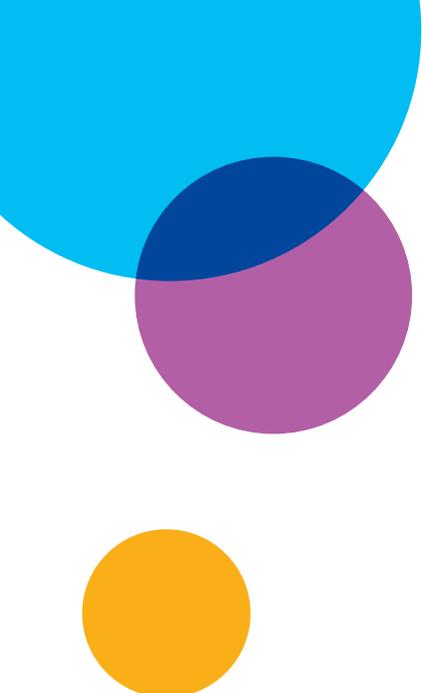
Have each group analyze the app they were assigned and identify how its design encourages you to share personal information. When they have finished, have the groups share their findings with the class and compare their answers.

DARK PATTERNS

Tell students that when platforms use design features interface to nudge us to do things we might not want to do—or to *not* do things that we do want to do—these 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.



Distribute the assignment sheet *Dark Patterns Audit* and go through it with the class.

Have students form groups and choose one app (Google/YouTube, Facebook/Instagram, or TikTok) where at least one group member has an account.

If no students in a group have an account on any of those three apps, have them use this Google account:

ExampleID1996@google.com Password: **i:N9HuCVnHTjY6**

Now have students follow the instructions on the exercise sheet.

After students have been working for about ten minutes, check in to confirm that they have been able to find how to change their data collection settings or turn off ad targeting. If they have not, give them the appropriate link:

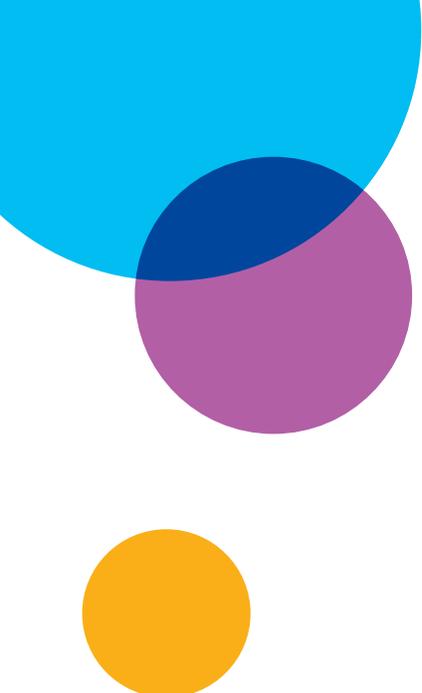
- Google and YouTube: <https://myaccount.google.com/data-and-privacy>
- Facebook, WhatsApp and Instagram: <https://www.facebook.com/privacy/checkup/>
- TikTok: <https://support.tiktok.com/en/account-and-privacy/personalized-ads-and-data>

ROGUES' GALLERY

Distribute the assignment sheet *Dark Patterns Rogues' Gallery* and go through it with the class. Have each student (or, if you prefer, each pair or group) choose one dark pattern that they identified in either the *Made for Sharing* or *Dark Patterns Audit* activities and create a “wanted” poster that will help other people recognize it.

When students have completed their posters, hang them around the room. Distribute sticky notes or paper clips to students, then have them view all the posters and attach a note or clip to each one if they have ever seen that dark pattern on an app or website.

When students have finished viewing all of the posters, see which ones have the most notes or clips. Ask students why they think those dark patterns might be most common in apps aimed at kids/teens and what they could do to avoid or recognize them.

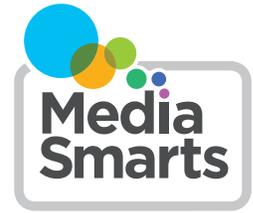


REFLECTION

Distribute the handout *Protecting Your Privacy on Apps and Websites*. As a reflection or exit ticket, ask students to read through it and consider:

- 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?

THE PRIVACY DILEMMA



Made for Sharing

.....

Choose either YouTube, Instagram or Tiktok and use this handout to identify this app's features and how those encourage you to share more personal information. We've given examples from Snapchat of the different kinds of features you should think about. Your job is to find similar examples from Instagram.

In the table on the other side of the page, list the app's features in the left-hand column. Features are the things that you are able to do with the app. Some features describe a general action you can take (like sharing a photo) and others describe something more specific to that app (like sending a disappearing photo with Snapchat).

Make sure you think about:

- Filling in your profile
- Sharing posts, photos and videos
- Controlling who sees what
- Responding to and sharing other people's posts, photos and videos
- How other people respond to what you post (Likes, shares, etc.)
- How the app responds to what you and/or your friends post (Snapchat streaks, for example)

For each of the features, write in the middle whether it is a default feature (something that happens automatically, or unless you tell it not to), whether it is easy to do, or whether it is hard to do. (In general, something that takes just one or two taps or clicks is easy to do; something that takes three or more is hard to do.)

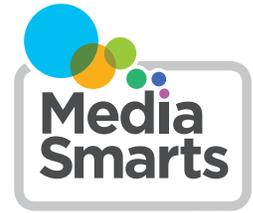
For instance, Friends see your Story *by default* on Snapchat. It is easy to send a Snap and hard to change your default privacy settings.

In the right-hand column, write down how you think those features – and whether they are default, easy, or hard to do – affect how much of personal information you share. Don't think just about your own personal information, but your friends' as well!

WHICH APP ARE YOU ANALYZING?

FEATURE	DEFAULT, EASY OR HARD?	EFFECT ON PRIVACY

THE PRIVACY DILEMMA



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

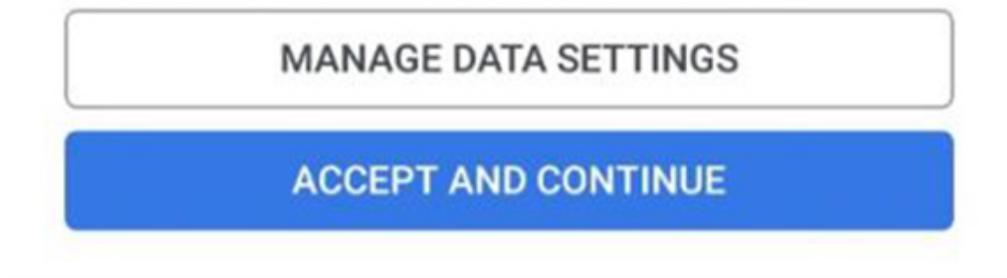
Obfuscation: Making it harder to find the tools we can use to protect our privacy.

- 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)

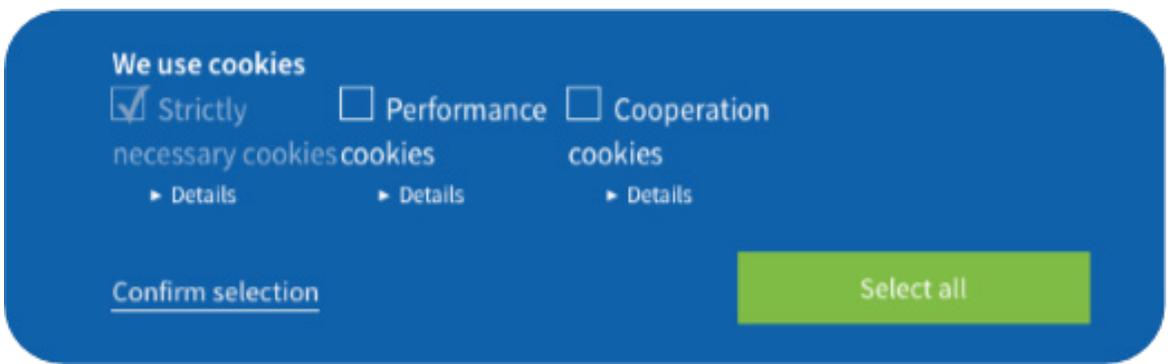
Pressuring: Making you feel that it’s good to accept data collection or making you feel bad about protecting your privacy.

- 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

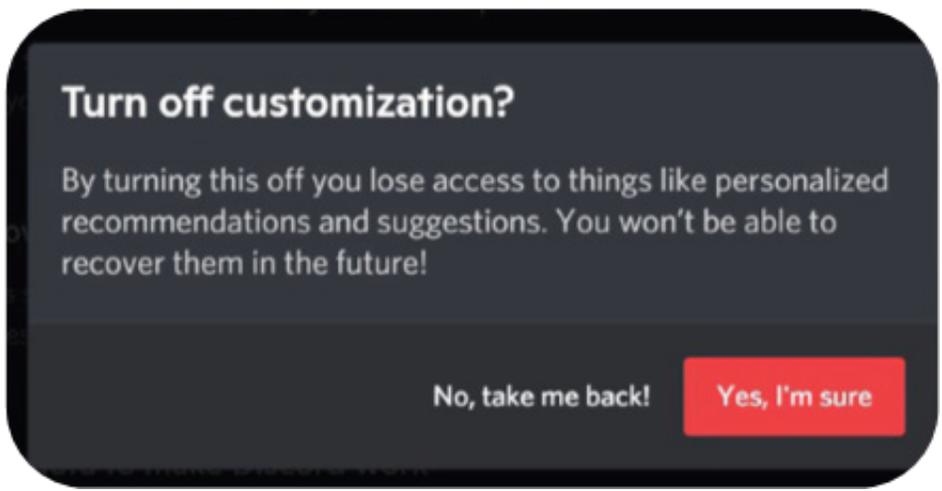
OBSTRUCTION:



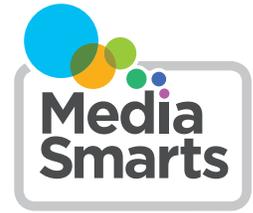
OBFUSCATION:



PRESSURING:



THE PRIVACY DILEMMA



Dark Pattern Audit

.....

How hard do different apps make it to turn off data collection and ad targeting?

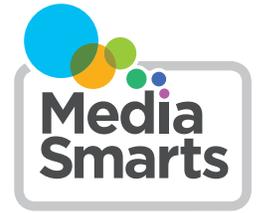
Answer the questions below on separate paper.

1. Start by logging into Google, Instagram or TikTok. Write down which one here:
 - Were you able to find it?
 - If so, how hard was it to find?
 - How many clicks or taps did it take?
2. Now try to find the page for changing your data collection settings or turning off tracking and targeted ads.
 - Were you able to find it?
 - If so, how hard was it to find?
 - How many clicks or taps did it take?
3. Now try turn off data collection and ad targeting.
 - How easy or hard do they make it to do?
 - How sure are you that you know what you've agreed to?
4. Did the app use any *dark patterns*...
 - When you were trying to find the page?
 - When you were trying to turn off data collection or ad targeting?

Describe examples you found of each type of dark pattern:

- *Obstruction*
- *Obfuscation*
- *Pressuring*

THE PRIVACY DILEMMA



Rogues' Gallery

.....

Choose one of the three types of dark patterns:

Obstruction (making it harder to do things that give away less privacy);

Obfuscation (Making it harder to find the tools we can use to protect our privacy); or

Pressuring (making you feel that it's better to accept data collection or making you feel bad about protecting your privacy)

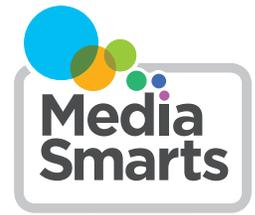
(Review the *Dark Patterns* handout to help you remember the definition and examples of each one.)

Now you will make a “wanted” poster that will help people recognize this dark pattern when they see it. It should include:

- The name of the pattern
- A graphic or drawing illustrating it
- What it's “wanted” for (why is it dangerous?)
- Its distinguishing characteristics (how will you recognize it?)
- What you should do when you see it

Your final product must be printable so that we can display the posters in the classroom.

THE PRIVACY DILEMMA



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."