



LESSON PLAN

Level: Grades 4 to 6

About the Author: Thierry Plante, Media Education Specialist,
MediaSmarts

This lesson was made possible by financial contributions from the Office of the Privacy Commissioner of Canada.

Data Defenders: Understanding data collection online



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

Overview

In this lesson, students explore the concepts relating to data collection that are introduced in the educational game [Data Defenders](#). The lesson will underscore for students the idea that their data is valuable and worthy of careful management by analyzing the platforms, applications and websites they use through the lens of the five privacy tools (which address the five principal ways data is collected online) introduced in *Data Defenders*. Finally, students consider how to apply these tools to their own online activities.

Learning Outcomes

Students will:

- Develop an understanding of
- the commercial objectives underlying the websites, services and applications they use
- the importance of managing their privacy online
- their rights as citizens and as children online in terms of privacy and data collection
- Identify the methods and purposes for data collection on most of the websites and applications they use
- Learn a variety of tools and techniques to help them manage their privacy online

This lesson plan also supports the development of several key privacy education competencies from the [Personal Data Protection Competency Framework for School Students](#), including:

- Understanding the concept of personal data
- Understanding the digital environment – technical aspects
- Understanding personal data regulations – economic aspects
- Managing my data: Learning to protect myself online



Preparation and Materials

- Review the *Data Defenders* game and *Data Defenders Teacher’s Guide* (available online at <https://mediasmarts.ca/digital-media-literacy/educational-games/data-defenders-grades-4-6>).
- Make any necessary technical arrangements for students to play the educational game *Data Defenders*. This game can be played on tablets, laptops or desktop computers. (If desired, the game could also be assigned as homework prior to the lesson. If this is the case, photocopy and distribute the handout *Data Defenders Homework Assignment* for students to complete as they play.)
- Ensure that Internet connections are available for the group activities.
- Photocopy enough of the following privacy tool handouts so that one-fifth of the class will get each one:
 - Private Browsing
 - Alter Ego
 - Total Control
 - Hide Me
 - Mighty Masks
- Review the activities within the handouts above, to ensure that you are familiar with what students will be asked to do.
- Photocopy the assignment sheet *Defending Your Data*.
- If students do not have Google accounts, create a dummy account at <https://accounts.google.com/SignUp?hl=en> for them to use during the group activities.
- Arrange for students who will be doing the “Hide Me” group activity to have at least one smartphone available for their group. This could be one they bring from home or one that you supply.

Notes:

The purpose of starting the lesson with the game is because the game is designed so that the first time students play (Round 1), they will most likely be unaware that their data is being collected (as they often are on the websites and applications they use). In Round 2, students are shown some tools and techniques they can use to manage their privacy. This lesson further explores these tools, techniques and concepts.

Depending on the ages and abilities of students, teachers may opt to conduct the investigation portions of the Private Browsing, Alter Ego, Total Control, Hide Me and Mighty Masks activities as a whole class activity using a whiteboard or data projector.

Procedure

Data Defenders

Tell students that they are going to play a game called “Data Defenders” and have them play through at least once (this should take approximately 20-25 minutes). Depending on how many Internet-connected devices are available, you may choose to have students play the game solo, in pairs, in small groups, or play as a class with a data projector or digital whiteboard. There’s no need to give them any more information about the game before they play.



If you decide to have students play the game at home, prior to the lesson, have them complete the *Data Defenders Homework Assignment* as they play.

Who’s Watching Me?

Once students have played through the game at least once, have them return to their regular seats. Write the word “Data” on the board and ask students the following questions.

- Generally, what does the word “data” mean? *(Basically, data means “information,” and any kind of information can be data – how much an ant weighs, how hot the sun is, etc. Personal data, or personal information, which is the focus of the game, is information about a specific person, like you or me.)*
- Write “personal data” on the board and ask students: we know from the game that we sometimes give away our personal data when we do things online, can anyone think of other ways we produce personal data? *(Any time something we do is recorded somewhere we are producing personal data – our grades at school, things we buy at stores, our medical records, when we walk in front of a security camera, when we fill out a form, etc.)*
- What did you learn in the game about the reasons why apps and sites collect personal information about you? *(They use it to build a profile, which they can then sell to advertisers or use to advertise directly to you. This is why most social networks and search engines don’t charge you anything to use them.)*
- What are some of the kinds of personal data that are collected about you online? *(Things you do online, like what games you play; where you are; your likes and interests; information about you, like your gender and age; and information about your device and browser.)*
- What are some of the ways your data is collected online? *(Answers should reflect the ways that are introduced in the game: forms, quizzes, surveys, browser cookies, search engines, stuff they post, etc.)*

Powering Up Privacy

Tell students that while most of the places they go and things they do when they’re online collect data about them, there are things they can do to stop or reduce it.

Write the names of the five privacy tools from *Data Defenders* on the board:

- Mighty Masks
- Alter Ego
- Hide Me
- Total Control
- Private Browsing

Explain that each of these represent tools and strategies that can be used to stop or reduce the five most common ways personal data is collected online: through smartphone settings and applications; through quizzes, contests and surveys; through cookies and other browser-based technologies; through geolocation; and through the personal information we submit online, such as photos or registration information.



Divide the class into ten expert groups, assigning the privacy tools handouts so that there are two groups for each privacy tool. Ask each expert group to read the handout and answer the questions, then they will present what they've learned about their privacy tool to the whole class. Before the expert groups share their answers, distribute the assignment sheet *Defending Your Data* and tell students that they will need to pay attention and take notes during the other groups' presentations so that they will be able to apply all five of the tools for this assignment.

For younger classes, you may wish to skip the expert group activity and simply go through the different activities with the whole class.

Defending Your Data

Give students a chance to make sure they have gotten all the information they need for the *Defending Your Data* assignment sheet from the expert groups, then have them complete the "Action Plan" sections either in class or as homework.



Data Defenders Homework Assignment

As you play the Data Defenders game, answer the following questions.

1. Name three types of personal data mentioned in the game.
 - a)
 - b)
 - c)
2. What is an ad broker?
3. What's the best way to do an online search without giving up your personal data?
4. How does your phone know where in the world you are?
5. Who owns the pictures and other things that you post online?
6. What should you always keep in mind before using a public Wi-Fi (wireless internet) connection?
7. How can you avoid being shown ads based on the things you've searched for or videos you've watched?



Data Defenders Homework Assignment: Answer Sheet

Answer the following questions.

1. Name three types of personal data mentioned in the game.

Three of the following: What you do online, where you are, your personal information, stuff on your phone and stuff you like.

2. What is an ad broker?

Ad brokers collect and buy personal data and then sell it to advertisers.

3. What's the best way to do an online search without giving up your personal data?

Use a non-tracking search engine like DuckDuckGo.

4. How does your phone know where in the world you are?

Your phone's GPS (Global Positioning System).

5. Who owns the pictures and other things that you post online?

It depends on the Terms of Service of the app or platform you used to post it.

6. What should you always keep in mind before using a public Wi-Fi (wireless internet) connection?

Other people might see where you go online.

7. How can you avoid being shown ads based on the things you've searched for or videos you've watched?

Opt out of personalized ads.



Our privacy tool: Private Browsing



What does this privacy tool protect you against?

Advertisers LOVE to know where you go online so they can show you ads, improve their services and sometimes make money by selling your data. They can do this in many ways: looking at what you search for in a search engine, putting little tracker files called “cookies” in your computer, and by identifying you and following you online based on things that you have installed on your device.

How can you apply your private browsing skills?

1. Use search engines that don't keep track of what you search for, like DuckDuckGo.
2. Install browser plugins (sometimes called “Add-ons” or “Extensions”) like Privacy Badger and Ghostery to block trackers and make it harder for data collectors to recognize your device when you're online.

Time to do a little investigation of your own!

Go to My Activity <https://myactivity.google.com/myactivity> and see what it says about what you've done, watched and searched with Google products.

Open a new tab or window and do a search, look at a map, send an email or watch a video on Google or YouTube. Go back to the My Activity page and see what's new.

Open a new tab or window and do a search on DuckDuckGo (www.duckduckgo.com) or Startpage (www.startpage.com). Go back to the My Activity page and see what's new.



Our privacy tool: Alter Ego



What does this privacy tool protect you against?

Apps and advertisers like to know what YOU like. This helps them show you ads, improve their services and sometimes make money by selling your data. They can do this in many ways: by looking at what ads you click on; by asking you in sneaky ways such as quizzes, surveys or contests; and by the videos you watch.

How can you apply Alter Ego privacy tools?

1. Use browsers and websites that let you opt out of getting personalized ads. (A browser is an app or program you use to visit websites, such as Chrome or Firefox.) While you'll still see advertisements, they won't be based on what they know about you and there will be limits on how much data about you can be collected.
2. Recognize all of the sneaky ways that companies might try to collect personal data about you – and know what information you have to give out to do something online, and what you can skip, are all examples of using your Alter Ego privacy tool in real life.

Time to do a little investigation of your own!

Go to My Activity <https://myactivity.google.com/myactivity> and see what it says about what you've done, watched and searched with Google products.

Click on Activity Controls on the left side of the page.

Scroll down the page. Which activities are being tracked (the blue slider on the right) and which are being paused (the grey slider on the left)? Are there any activities that are being tracked that you would prefer to pause, so that data isn't collected?



Our privacy tool: Total Control



What does this privacy tool protect you against?

Our phones usually contain a LOT of our personal information: where we are, where we've been, who our friends are (from your contact list and from your social media apps), who we talk to the most, who we texted this morning, what we and our friends look like (from our photos), and much more! Until you take total control, a lot of people can have access to all that data. But you can put a stop to that!

How can you apply Total Control privacy tools?

1. Get to know your phone's privacy and security settings. You can turn off a lot of things on your phone that either collect or share your data. It can take some digging, and some settings are more obvious than others, but once you make the effort to find out, you can lock down your phone and call the shots!
2. Understand how applications on your phone work and talk to each other. Have you ever noticed that when you install a new app, it asks you for a bunch of permissions? Have you ever wondered why a game would need to have access to your photos? In most cases, there's no reason to give a game or app access to everything on your phone. You can remove those permissions once the app is installed and it works just fine.

Time to do a little investigation of your own!

Go to the Family Section of the Google Play store (go to <https://play.google.com/store/apps/category/FAMILY> if you're using a computer).

Pick an app that you think you might want to download and click on it.

Scroll down to where it says "Additional Information" near the bottom of the page. Find "Permissions" under that heading and click on "View details" below that.

Scroll through the list that pops up of things that the app will ask other apps, or the device, to do or to tell it. Write them down and discuss what each one means together. Which seem like they're really important for the app and which do you think might not be necessary?



Our privacy tool: Hide Me



What does this privacy tool protect you against?

Your phone needs to know where it is so that it can make and receive calls and help some apps work better (like maps, or tagging your photos with a location). You may have heard of GPS (global positioning system), which most smartphones use. There are other ways that your phone can figure out where you are, too.

How can you apply Hide Me privacy tools?

1. Know how to turn off the ways that your phone knows where you are when it doesn't need to know: this means turning off the GPS, Bluetooth and Wi-Fi when you aren't using them. If your phone doesn't know where you are, neither will the apps installed on your phone.
2. Know which apps share your location with others. For example, it's very possible that the photos you take with your phone say when and where you took them.

Time to do a little investigation of your own!

Read these articles:

<http://sciencewithkids.com/science-facts/Bluetooth.html>

<http://www.funkidslive.com/learn/techno-mum/wifi-wonders/>

<https://spaceplace.nasa.gov/gps/en/>

Using a smartphone (your own or one your teacher provided), find the icons (pictures) that stand for Wi-Fi, GPS and Bluetooth.

How do you turn WiFi, GPS and Bluetooth off and on? When would you want to have those turned on, and when would you want them turned off?



Our privacy tool: Mighty Masks



What does this privacy tool protect you against?

Lots of services need to collect some of your personal information. For example, when you create an account somewhere, you usually have to give your name and a way you can be reached (a phone number or an email address for example). Other times, you may be giving away some personal information online without realizing it when you use a service or an app: for example, when you post a photo or text someone.

How can you apply Hide Me privacy tools?

1. Know what personal information you need to provide when you sign up for something, and what information you don't have to give.
2. Know what types of information about you companies want to collect: some of it is obvious, like your name, but some of it might surprise you, like a record of what you "liked" online.

Time to do a little investigation of your own!

As a group, make a list of every time you can remember that you have:

- Taken a quiz or survey on a computer or phone
- Filled out a form on a computer or phone
- Liked or shared something online, like a photo or video

Starting from this list, put together a "profile" of what advertisers know about you from the activities you've done online.



Defending Your Data – Assignment Sheet

For this assignment, you will learn from your classmates about different ways to control your privacy online, and come up with an action plan to help you decide who knows what about you.

For each of the privacy tools we've studied, list what you think are the three most important points. Then give an example of a program, website, app or device that you use where this privacy tool could help you manage your privacy and briefly explain (in complete sentences) your action plan for how you will use it.

1. Private Browsing

Key points:

a.

b.

c.

I could use this with...

Action Plan: To help manage my privacy, I will:

2. Alter Ego

Key points:

a.

b.

c.

I could use this with...

Action Plan: To help manage my privacy, I will:



3. Total Control

Key points:

a.

b.

c.

I could use this with...

Action Plan: To help manage my privacy, I will:

4. Hide Me

Key points:

a.

b.

c.

I could use this with...

Action Plan: To help manage my privacy, I will:

5. Mighty Masks

Key points:

a.

b.

c.

I could use this with...

Action Plan: To help manage my privacy, I will:



Task Assessment Rubric: Defending Your Data – Assignment Sheet

	Learning Expectations	Achievement
<p>Use</p> <p>Skills and competencies that fall under “use” range from basic technical know-how – using computer programs such as word processors, web browsers, email and other communication tools – to the more sophisticated abilities for accessing and using knowledge resources, such as search engines and online databases, and emerging technologies such as cloud computing.</p>	<p>Students will:</p> <ul style="list-style-type: none"> • demonstrate awareness that their activities on the Internet leave a permanent “digital footprint” or “trail” and behave accordingly • research and explain how different digital tools can be used to manage data privacy online 	<p>Insufficient (R)</p> <p>Beginning (1)</p> <p>Developing (2)</p> <p>Competent (3)</p> <p>Confident (4)</p>
<p>Understand</p> <p>“Understand” includes recognizing how networked technology affects our behaviour and our perceptions, beliefs and feelings about the world around us.</p> <p>“Understand” also prepares us for a knowledge economy as we develop information management skills for finding, evaluating and effectively using information to communicate, collaborate and solve problems.</p>	<p>Students will:</p> <ul style="list-style-type: none"> • demonstrate an understanding of the concepts of “data” and “personal information” • demonstrate an understanding that the purpose of many apps and websites is to collect and monetize data, and be aware of methods used to collect data in digital environments 	<p>Insufficient (R)</p> <p>Beginning (1)</p> <p>Developing (2)</p> <p>Competent (3)</p> <p>Confident (4)</p>
<p>Create</p> <p>“Create” is the ability to produce content and effectively communicate through a variety of digital media tools. It includes being able to adapt what we produce for various contexts and audiences; to create and communicate using rich media such as images, video and sound; and to effectively and responsibly engage with user-generated content such as blogs and discussion forums, video and photo sharing services, social gaming and other forms of social media.</p> <p>The ability to create using digital media ensures that Canadians are active contributors to digital society.</p>	<p>Students will:</p> <ul style="list-style-type: none"> • research a tool for managing their online privacy and share their findings with the class • develop an action plan for managing their online privacy 	<p>Insufficient (R)</p> <p>Beginning (1)</p> <p>Developing (2)</p> <p>Competent (3)</p> <p>Confident (4)</p>

