LESSON PLAN

Level:	Grades 7-8
About the Author:	Matthew Johnson, Director of Education, MediaSmarts
Duration:	75 minutes

Playing With Privacy

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 are introduced to the idea that their gaming experiences may compromise their personal information. Students consider the ways in which games may gather or solicit information about them and learn about tools which they can use to control their personal privacy, and then discuss the trade-offs between protecting their privacy and enjoying a full game experience. As a class, the students explore short scenarios designed to highlight the complexity of these trade-offs. Finally, in an optional evaluation task students assess a game on the basis of how much it compromises players' personal information and how well it permits them to take control of their personal privacy.

Preparation and Materials

- Read the backgrounders *Gaming consoles and personal information: playing with privacy* (https://www.priv.gc.ca/en/privacy-topics/technology/mobile-and-digital-devices/digital-devices/gd_gc_201905/), *Gaming Privacy Trade-Off Grid: Teacher's Version* and *Gaming Privacy Scenarios: Teacher's Version*
- Photocopy the student handouts *Gaming Privacy Trade-Off Grid*, *Gaming Privacy Scenarios* and (if doing the optional evaluation task) *Privacy Scorecard*
- Prepare an overhead or data projection of the *Personal Information Avatar*.
- Prepare to project the video *How to Stay Safe When Online Gaming* (https://www.youtube.com/watch?v=x6qlRaAC8S8)

Learning Outcomes

Students will:

- Identify the ways in which playing video games can compromise personal privacy
- Identify tools, habits and best practices that allow them to take greater control of their personal privacy
- Consider the tension between protecting personal privacy and enjoying a full gaming experience, and come to reasoned decisions on the topic
- Evaluate a game on the basis of how much it compromises players' personal privacy and how well it allows them to take control of their personal privacy

Procedure

Begin by asking students how many of them play video or computer games. (Make sure to include “social” or “casual” games such as *Candy Crush* and *Pokémon Go*.) Next, ask students to name some of their favourite computer games. Once you’ve collected some examples, ask students to name the main characters of the games they play. Ask students which games allow them to *create* or *modify* their characters before playing (for example, role-playing games such as *Skyrim* or online games like *Minecraft, Fortnite* or *Overwatch*).

Now project the *Personal Information Avatar* for the class and explain that you will be creating a character together. Ask students to contribute possible answers to fill in the spaces; show just one item at a time (if you're using a data projector or digital whiteboard, you can click through the slideshow version to reveal the different items; if you're using an overhead projector, you can cover the lower part of the page with a piece of paper and uncover the questions two at a time). Students will likely find the first two questions (name and age) unremarkable, then express a bit of puzzlement at the next three (address, phone number and email address). By the time you uncover "friends' names" and "credit card number," it will be clear to students that they are not making a regular character for a game; explain to them that they are, instead, contributing some of the information that video game companies gather about them when they play or register for games.

Ask students why they think computer game companies gather personal information. Record all suggestions but make sure the following are included:

- To set up a unique user account (name, address, etc.)
- To let users pay subscription fees or buy in-game content (name, address, credit card, etc.)
- To establish if a user is old enough to agree to the Terms of Service or to access certain kinds of content (age)
- To let users find other people to play with/against on the same server (address)
- To provide ads that are tailored to the player's interests (age, hobbies, etc.)

Point out that not every gaming company gathers all of this data, and that in many cases when users give up personal information it is part of a **trade-off** that improves their gaming experience – for example, knowing where a user allows the company to connect them to the nearest server (reducing "lag time" and making the game play more quick and smooth). Explain that it's important that users know when they're making these trade-offs, as well as exactly what they're trading and why.

Now show students the video *How to Stay Safe When Online Gaming*. Organize students into pairs and distribute the handout *Gaming Privacy Trade-Off Grid*. Have one partner in each pair read the section *Risks to Privacy* and the other read the section *Tools for Controlling Your Privacy*. Have each pair work together to match risks with tools in the grid and then discuss the trade-offs in each case. When each pair has had a chance to do this, take up the *Gaming Privacy Trade-Off Grid* with the whole class. Once you've matched risks and tools (see *Gaming Privacy Trade-Off Grid: Teacher's Version* for the right answers) have students discuss possible privacy trade-offs in gaming. For example:

- To be able to have a persistent online presence (either to maintain an online character or to record your scores, achievements, etc.) you need to create an account, which usually means giving up some personal information
- To be profitable, most commercial games need players to either subscribe to or buy in-game content, typically using a credit card

- To reduce lag time, game companies may collect geolocation data (where you're playing from) so they can connect you to the nearest server
- Chat systems and other features that let you talk to other players can be a privacy risk, but they can also make the game more fun

Distribute the handout *Gaming Privacy Scenarios* and go through the scenarios with the class. After reading each scenario, ask students to identify the privacy trade-offs (what losses or risks to privacy are involved, and what is gained) and discuss whether and why they would accept them. (The decisions the students come to are less important than their being aware of the factors that go into those decisions.)

Evaluation (Optional):

Distribute the *Privacy Score* handout and instruct students to use it to evaluate a game of their choice in terms of how it treats their privacy. If you wish to avoid more than one student evaluating a game, have students make a list of games and then allow each student to select one from that list.

Gaming Privacy Trade-Off Grid

Playing video games may mean giving up personal information, either by providing information to the game company or while chatting with other players. This is often part of a **trade-off** where giving up your information results in a better game experience. That doesn't mean, though, that you should always give up personal information when you're asked to – or that you can't take steps to limit how much personal information you give out. With a partner, take a look at the *Privacy Risks* and *Privacy Tools* below and then match them on the *Trade-Off Grid*; then you can decide which risks you think are worth taking and how you can keep risks to your privacy to a minimum.

Privacy Risks

Identity spoofing: Playing games often means setting up an online identity. If other people are able to get (or guess) your login information (including your name and your password) they could access your account and pretend to be you or even delete your identity. If your game account is connected to a social networking profile, they might be able to impersonate you there as well.

Identity theft: If someone has access to important information about you (in particular, your full name, your full date of birth and your Social Insurance Number) they may be able to use it to commit fraud by buying things or taking out credit cards in your name.

Credit card fraud or mistaken charges: You may need to give credit card information (yours or a parent's) to either subscribe to a game or get access to some game content. (For instance, many games use the "freemium" model: the basic game is free but there will be some content – types of characters, areas in the game, etc. – that you have to pay to access.) If someone other than the game company gets your credit card information they can use it to make purchases that will be charged to you. It's also possible for charges to appear on your credit card statement for things you didn't mean to buy.

Behavioural tracking: Websites of all kinds, including games, often track what you do when you're on them. They may do this for many different reasons, such as figuring out what kinds of ads you're most likely to respond to. In some cases websites will even track what you do after you leave the site.

Protect your friends and contacts: If you allow a game to connect to your social network account this will often be used to advertise the game to your friends ("friendvertising"). This is done both by having you post things like achievements or high scores to your own profile and also by targeting your friends for advertising, since they know your friends are likely to be interested in many of the same things as you. This may also give the game company access to some or all of the information on your profile.

Locational privacy issues: Many games find out your location (based either on your IP address or GPS information on a mobile device) to connect you to the nearest server or put you in touch with other nearby players.

Sharing with third parties: There's no guarantee that any information you give to a gaming company will stay with them. Companies may share some information with third parties including advertisers and marketers; financial institutions like banks, credit card companies and credit agencies; freelance programmers; call centres providing technical support; Internet Service Providers; researchers; and law enforcement or other government agents.

Cyberbullying and griefing: Some people enjoy picking on other players, especially new ones. Sometimes people will target other players if they know they're kids. Even though you can see who you're playing with, it's common for girls, LGBTQ people, people with disabilities and visible minorities to be targeted too.

Privacy Tools

Use a pseudonym: If the game allows it make sure that it only displays a nickname rather than your real name; if that's not possible make sure that your full legal name is not displayed (if your name is Michael, for instance, register as Mike).

Share minimal personal information: The best approach to avoiding privacy risks is simply to limit how much personal information you give out. When you're registering a user account only give out required information (there will usually be some indicator, like an asterisk or a different font colour, to show you what information is required and what's optional). When you're communicating with other players avoid sharing personal information such as your age, where you go to school and your home address.

Use restrictive privacy settings: Many games have privacy settings that allow you to control how much information you share. In some cases the settings will be part of the platform (a gaming console, for example) rather than the game itself. By picking privacy settings you can decide things like who can see whether you're online, who can view your profile, who can contact you through chat, whether people can see your location and so on. Your device's privacy settings can also control whether or not the game can turn on the camera or know your location.

Strong passwords: One of the best ways to prevent identity spoofing is to have a strong password that is at least eight characters long and uses a mix of upper- and lower-case letters as well as numbers and non-letter characters (like punctuation marks). You can make custom passwords for each account by adding the first and last letter of the site the password is for. For example, by starting with the word "banana" you can make a master password of B@n4na, which would become FB@n4nae when you registered for Fortnite. If the game allows it, multi-factor authentication is also a good idea. This means that as well as putting in your password, you get a code sent to your email or mobile device that you have to enter to confirm it's you.

Get connected your way: Only send personal information, especially credit card information, to secure sites. You can tell a site is secure because its Web address begins with "https" instead of just "http". As well, avoid sending personal information over wireless connections and **never** send it over a public Internet hotspot. You can also use your device settings to set limits on how long you play and how much data you use.

Choose who plays the game with you and protect your friends and contacts: It's best to only play with people you know offline if possible. If not, turn off the game's chat function. If you need chat to play, be careful about what information you give out. If your gaming account is connected to a social networking profile make sure to set your privacy settings there, too: this lets you control things like whether the gaming company has access to your friends list.

Get to know the privacy policy: Most sites have a Privacy Policy that explains which personal information the site collects and what is done with it. Privacy policies will also often explain why this information is being collected, how it's stored, how it's disclosed and how it will be used, which can help you decide whether you think it's worth it.

Research before giving consent: Every site has a Terms of Service that define the rules you and the site will follow. Terms of Service will usually tell you whether and how you can delete your account and what will be done with any collected information once your account is deleted. These can be difficult to read but it's important to look through them so you can make an informed decision about what privacy trade-offs you're agreeing to and why. Who has access to your data? How is it shared? Who can see it once it's collected?

GAMING PRIVACY TRADE-OFF GRID

	Use a pseudonym	Share minimal personal information	Use restrictive privacy settings	Strong passwords	Get connect-ed your way	Choose who plays with you	Get to know the privacy policy	Research before giving consent
ID spoofing								
ID theft								
Credit card fraud								
Behavioural tracking								
Friendvertising								
Locational privacy								
Sharing with third parties								
Cyberbullying and griefing								

GAMING PRIVACY TRADE-OFF GRID: TEACHER'S VERSION

	Use a pseudonym	Share minimal personal information	Use restrictive privacy settings	Strong passwords	Get connect-ed your way	Choose who plays with you	Get to know the privacy policy	Research before giving consent
ID spoofing	✓	✓	✓	✓				
ID theft	✓	✓		✓	✓			
Credit card fraud	✓	✓	✓	✓	✓			
Behavioural tracking			✓		✓		✓	✓
Friendvertising			✓			✓	✓	
Locational privacy			✓				✓	
Sharing with third parties							✓	✓
Cyberbullying and griefing	✓	✓	✓			✓		

Gaming Privacy Scenarios

Scenario One. Jillian wants to get an account for *Planet Princess* so that she can play the same character each time and add items to her character's virtual castle. To do this she has to fill in a form that asks for information including her name, her email address and her hobbies.

Scenario Two. When Tony starts playing *World of Chivalry* he meets another player who uses the chat function to ask him if he'll help kill a dragon. Tony checks to see if he's turned on the chat function without realizing it and finds out that it's on unless you go into your settings and turn it off.

Scenario Three. Samir wants to sign up for a VIP account to play *Alien Legacy* so that he can have access to special weapons and armour. He's asked for his name, age and email address and told that if he's under 13 he needs to give one of his parents' email address as well.

Scenario Four. Zoe connects her gaming and social network accounts so that she can see when any of her friends are available to play against her in *Thrash Mountain*. A little while later some of her friends complain that she's spamming them with her high scores and others say that all the ads they're seeing are for skateboards and skate magazines.

Scenario Five. After several years of playing Lily decides to give up her *Alien Legacy* account. Even after her account is closed, though, one of her friends tells her that he can still access her profile, which includes her name, where she lives and information she had given about her hobbies and interests.

Scenario Six. Olivia is playing *Atlantis Adventures* with the chat function turned on. She joins a guild with several other players who all live in the same province. As they play together she gets to know some of them quite well and they often chat about their own lives as well as what's happening in the game.

Scenario Seven. *Alien Legacy* just added a button called "Post a highlight" that lets you capture your gameplay and post it on YouTube. If you click on it but don't have a YouTube account it goes to the YouTube "Register for an account" page.

Scenario Eight. All of Gabriel's friends seem to have more time to play *World of Chivalry* than he does because they all have castles and he's still a wandering knight. He notices that you can buy a castle for just five dollars in real money but you need a credit card to do it.

Gaming Privacy Scenarios (Teacher's Version)

Scenario One. Jillian wants to get an account for *Planet Castle* so that she can play the same character each time and add items to her character's virtual castle. To do this, she has to fill in a form that asks for information including her name, her email address and her hobbies.

*This is a very common trade-off where a player has to give up some personal information in order to set up a persistent character or account. Under Canadian law, companies have to get **meaningful consent** from players before collecting personal information; that means they have to make clear what information the player is giving up and what will be done with it (this should be in the Privacy Policy), including what information will be visible to other players or third parties like advertisers. The best practice when dealing with young gamers is for the company to get parents' permission before registering them and give parents access to the account. When asking for personal information, companies should clearly distinguish between **required** and **optional** information so that the player can avoid giving out more information than is absolutely necessary.*

Scenario Two. When Tony starts playing *World of Chivalry* he meets another player who uses the chat function to ask him if he'll help kill a dragon. Tony checks to see if he's turned on the chat function without realizing it and finds out that it's on unless you go into your settings and turn it off.

There are lots of reasons why chat and other communication functions should be "opt-in" instead of "opt-out," especially when many of the players are young people. Either way, the game should make the controls to turn chat on and off -- as well as to block specific players, in case of things like one player harassing another -- easy to find and to use. The best practice with young gamers is to give parents the ability to turn chat functions (and other ways of communicating with other players) on and off.

Scenario Three. Samir wants to visit the Casino Zone in *Alien Legacy* so that he can play gambling-themed minigames and win special weapons and armour. When he goes there, he's asked to click a box verifying that he's over 18 before he can go in.

A game should verify that someone is over 18 before allowing access to gambling content, but in this case the game has made it too easy for Samir to lie about his age. This is one good reason for games to find out how old players are when they register before they know whether the game's content will be restricted if they're under 18.

Scenario Four. Zoe connects her gaming and social network accounts so that she can see when any of her friends are available to play against her in *Thrash Mountain*. A little while later, some of her friends complain that she's spamming them with her high scores and others say that all the ads they're seeing are for skateboards and skate magazines.

Because many people have their social network accounts constantly on, linking them with a gaming account is a good way of finding out when your friends are available to play with you. However, this may give the game company access to everything on your profile, including your friends list and everything you post. It's important to read the Privacy Policy before agreeing to link two accounts so that you know what you're getting into; most social networks also have their own privacy controls that let you determine what information third parties like this can access.

Scenario Five. After several years of playing, Lily decides to give up her *Alien Legacy* account. Even after her account is closed, though, one of her friends tells her that he can still access her profile, which includes her name, where she lives and information she had given about her hobbies and interests.

Under Canadian law, companies must have procedures in place to delete personal information they don't need any more. A game's Terms of Service and/or its Privacy Policy should have information on how to fully delete an account but if it doesn't, a complaint can be lodged with the Office of the Privacy Commissioner.

Scenario Six. Olivia is playing *Atlantis Adventures* with the chat function turned on. She joins a guild with several other players who all live in the same province. As they play together she gets to know some of them quite well and they often chat about their own lives as well as what's happening in the game.

For many players, socializing is a big part of the game, sometimes even more important than the game itself. Like any online communication, though, this carries privacy risks. It's important for young people to know how to manage their privacy online in any setting and to be aware of the possible unexpected audiences of what they say. As well, many games use either IP addresses or GPS information to find out where players are. This may be done to match them to other nearby players or connect them to the nearest server, or to customize advertising based on location. Whatever the reason, the best practice for games is to either make it opt-in or easy to turn off if you want to.

Scenario Seven. *Alien Legacy* just added a button called "Post a highlight" that lets you capture your gameplay and post it on YouTube. If you click on it but don't have a YouTube account it goes to the YouTube "Register for an account" page.

This may sound like a fun idea, it makes it very easy to spread your personal info. As well, you need to be at least 13 to get a YouTube account. If Alien Legacy *wants to keep this feature they should make it opt-in and let parents of younger players turn it off permanently.*

Scenario Eight. All of Gabriel's friends seem to have more time to play *World of Chivalry* than he does because they all have castles and he's still a wandering knight. He notices that you can buy a castle for just five dollars in real money but you need a credit card to do it.

Before Gabriel submits his (or his parents') credit card information, he should make sure that World of Chivalry *is run by a reputable company and that the information will be sent over a secure connection. He should also find out if he can delete the credit card info from the company's servers after he's made the purchase: there have been several cases where game companies have had their servers hacked and player information, including credit card data, has been stolen.*

Privacy Scorecard

Name: _____

Select a video game (computer game, online game, mobile phone/table game or console game) and see how well it handles your personal information. Make sure to look at the Terms of Service and the Privacy Policy (if there is one).

The Game

What it the name of the game?

_____

What is the name of the company that makes the game?

_____

If it is an online game give the web address below; if it is a console game list which console it is for.

_____

Privacy Risks

Do you have to create an account to play the game?

_____

If not, do you have to create an account to access all the game's content?

_____

Does the game ever ask you if you need your parents' consent to register if you're under a certain age?

_____

Is it clear what information is **mandatory** (you **have** to give it to register) and which is **optional** (you're just **asked** to give it)?

_____

What information do you **have** to give to be able to register?

_____

What information are you **asked** to give when you register?

_____

Does the game create a profile for you that is visible to other players?

_____

If so, what information is included in the profile?

_____

Does the game ever ask you for credit card information?

_____

Does the game ever collect information about where you are playing from?

_____

Does the game company ever share any of the data it collects from you? If so, with whom does it share it?

_____

Does the game have any kind of chat or communication function (message boards, etc.)?

_____

If you answered *yes* to the question above, does the game start with that function automatically **on** or automatically **off**?

_____

Does the game have the option to connect to a social network account?

_____

If you answered *yes* to the question above, does the game start with that function automatically **on** or automatically **off**?

_____

Privacy Trade-Offs

For each privacy risk you have identified, list any benefits to you as a player that come from it.

1. _____
2. _____
3. _____

4. _____

5. _____

6. _____

7. _____

Privacy Tools

Is there a Privacy Policy listed that explains what information will be collected from you, what it will be used for and whether it will be shared with anyone?

_____

If so, how easy is it to find and to read?

_____

Does the site have privacy settings that allow you to control things like who can see your profile, who can contact you during the game, etc.?

_____

If so, what are the privacy settings able to control?

_____

If the game is a console game does the console have any privacy settings that apply to all of the games you play on it?

_____

If so, what do the privacy settings control?

_____

If you are ever required to send credit card information is it done over a secure connection?

_____

What will the company do with your personal information if you close your account?

_____

Final Evaluation

Now that you've identified the privacy risks, their potential benefits to players and the tools that are provided to manage your privacy, write a short paragraph explaining the following:

- Whether or not the privacy risks would keep you from playing the game and the reasons for your decision.
- The ways that you would minimize the risks to your privacy if you did decide to play.
- And, if you would not play this game, an explanation of things it would have to improve relating to its handling of your personal information in order for you to play it.

Personal Information Avatar

Name:

Age:

Address:

Hobbies:

Phone number:

Email address:

Friends' names:

Credit card number: