



Privacy, the Internet and that Phone in your Pocket

Subject(s): History, Civics, Social Science, Law, Politics

Grade Levels: 9-12

Specific Student Learning Objectives:

- Students will develop an understanding of privacy rights and why a guarantee of privacy is necessary in free and democratic societies (Students will consider the question, if you have nothing to hide, why should you care about privacy?);
- Students will demonstrate an ability to identify and consider competing interests when determining the reasonableness of a search of private information;

*This lesson plan fulfills multiple provincial curriculum expectations. For a list of Overall and Specific curriculum expectations as outlined by the Ontario Ministry of Education, please refer to the accompanying document, *CCLET Privacy Lesson, Curriculum Links.pdf*.

Enduring Understanding(s)/Big Idea/Essential Questions

- What is private information?
- Who needs privacy and why?
- Who should be allowed to have access to/collect/retain our private information?
- Under what circumstances, if any, should someone be allowed to have access to our private information without our consent?
- If we share our own private information with another person, government actor, or private company, what should they be allowed to do with it?

Context: This lesson is intended to introduce students to the concept of privacy rights as guaranteed in section 8 of the *Canadian Charter of Rights and Freedoms*, which provides that everyone has the right to be secure against unreasonable search and seizure. In light of society's ever increasing reliance on electronic devices to store and share personal information, this lesson will focus on privacy rights as they relate to information on cell phones, computers, and social media in a variety of contexts.

PREAMBLE:

In order for this lesson – or, really, *any* critical-thinking lesson – to be effective, students must be given clear *permission to disagree*. Divergent points of view must be encouraged throughout the lesson so that the issues raised can be fully and meaningfully explored. There are no right answers to these questions, and part of the lesson is to help students understand how challenging and interesting issues of fairness, citizenship and justice can be. Quite aside from adding to the debate, encouraging diversity of opinion and point of view is vital to fostering democratic habits and active citizenship.

Introduction:

What is private information and who needs privacy anyway?

In order to have a better understanding of privacy rights, students must first challenge the belief that the only people who want privacy are those who are doing “bad things”.



1. Consider the following individuals and identify what kind of information they might need to keep private: Doctors; Lawyers; Entrepreneurs; Activists/Protesters;
 - a. How would a lack of privacy prevent these individuals from performing important social functions?
2. What about teenagers? Even if you are not breaking any rules, consider why you may want:
 - a. personal privacy (i.e. protection from things like strip searches or collecting your DNA);
 - b. Territorial privacy (i.e. privacy in your bedroom, your school locker, your car)
 - c. Informational privacy (i.e. information about you such as your address, your emails and text messages)

Why be concerned about keeping information private if you have nothing to hide?

Present students with the following scenarios for discussion:

Scenario 1: There's a new principal at your school and he's keen to get to know the students better. One day while you are standing in line in the cafeteria, he sparks conversation and asks about your friends and family, do you have siblings in the school, whether you walk or take the school bus etc. When you mention you have a sister and a new baby brother, he enthusiastically asks if you have any pictures.

Scenario 2: There is a new principal at the school and he's keen to get to know the students better. You are among a select group of students that the principal has chosen for an interview. When you arrive for your interview, you are simply told to write down your home address, the first and last names of your friends and family members, and instructed to submit pictures of all your "associates" by the end of the week.

Discussion Questions:

- 1) In both scenarios, you are essentially being asked for the same information. Is your reaction to the first scenario different from your reaction to the second? Why or why not?
- 2) Would you be more or less willing to provide the requested information in scenario 1 or scenario 2? Explain your reasoning.
- 3) Would you feel differently, if instead of your school principal, it was a police officer asking you questions in scenario 2? Why or why not?
- 4) What questions, if any, would you want to ask/consider in either scenario? (e.g. Why was I chosen for this interview? Why does the principal/police officer want to know this information? What will he/she do with this information? Will he/she be sharing this information with others? Are there potential consequences if I provide this information – could it be misused in some way?)
- 5) What if all this information was available to your friends on your Facebook page? Should the fact that you have shared this information with your Facebook friends mean that you no longer have a right to keep the same information private from your principal or the police?
- 6) What kinds of conclusions, both accurate and inaccurate, could be drawn about you by collecting this kind of information? What kinds of consequences could result from these conclusions? (e.g. if some of my friends or family are considered "trouble-makers," will the principal/police officer assume I am too? Will I be treated differently because of the conclusions drawn from my personal information?)

Action:**Case Studies:**

Either as a class or in small groups, consider each of the attached case studies and questions (see handouts below). If working in small groups divide the cases among the groups and have them present their case and answers to the class.

To allow for a full debate and exploration of the competing interests at stake each scenario, be sure to encourage devil's advocate points of view throughout the class discussion.

Consolidation and Debrief:

Conclude the lesson by asking students to reflect on some or all of the following:

- What could be some consequences if government, police, or private companies had limitless access to anyone's cell phone, emails, or computer?
 - a) What types of perfectly legal activities might individuals be reluctant to engage in?
 - b) How might a lack of privacy impact an individual's self-expression; sense of independence; learning; creativity?
- What kinds of safeguards would I want in place to ensure that my privacy, and the privacy of others, is protected from unnecessary intrusion? What should government/police/private companies have to do before they are given access to personal information?
- If I do allow others to have access to my private information, what kinds of policies/guarantees would I want in place to ensure that my information is protected?

Case One: Cell Phones at School

Alex attends a high school in Alberta where the school administration has concerns about students using illegal drugs during their lunch breaks or after school. One day at lunchtime, Alex was getting sandwiches with a group of students, when they got involved in a fight. The students were not on school property at the time, and nobody was hurt.

School officials heard about the confrontation, and concluded that it might have been drug-related. The principal demanded that Alex turn over his smart phone and provide the password. The principal searched through the emails, text messages and pictures on Alex's phone. He found a text message from another student named Sarah, asking if Alex knew where she could score some marijuana.

The principal decided that this text message provided evidence that Alex was dealing drugs and selling them to other students. Alex was suspended from school and also faced an expulsion hearing. The principal also called police and asked them to investigate Alex for drug offences.

QUESTIONS TO CONSIDER:

- 1) Should the school get involved in incidents that occurred off school property? Why or why not?
- 2) What was the principal's goal in looking through Alex's smart phone? Do you think the principal's actions were fair? Why or why not?
- 3) After the principal found the incriminating text message, was it reasonable to accuse Alex of being a drug dealer?
- 4) When, if ever, should schools have the ability to look through a student's personal cell phone? When, if ever, should school officials be allowed to give police information they find on a student's personal cell phone?
- 5) Should the standard for searching a cell phone be different for police than for principals i.e. should police be required to get a search warrant first? Why or why not?

CASE TWO: FACEBOOK AND CYBERBULLYING

Mr. Douglas, a high-school principal in Ontario, announces to the school that a new policy is being introduced: from that day forward, personal electronics will be prohibited at school. Students are not to bring any personal electronics – including cell phones – into school.

Students at the school are upset about the principal's decision. That night at home, one student creates a Facebook group entitled "Mr. Douglas, the Grinch that stole school spirit." Eighteen students join the Facebook group and several of them begin to discuss Mr. Douglas and the rule about personal electronics in school. The following comments are made by five different students, all writing on the wall of the Facebook group:

- *Mr. Douglas is an idiot, he makes stupid rules and is the worst principal ever.*
- *Yeah, he's really a **#!*@@#\$. What a jerk.*
- *This cell phone ban is a complete joke. We should start a petition and hand it in to the school administration. I bet we could get 500 signatures in a day.*
- *If you think they're going to listen because we sign some petition you're dreaming. We should grab some rocks and smash some windows then we'd have a chance of getting their attention.*
- *Don't be stupid. Any violence is just going to make things way worse and is dangerous. But maybe we could do some kind of petition, plus a protest or walkout or something.*

The next day, an announcement is made over the school PA system. The names of all eighteen students who joined the Facebook group are read, and they are called into the principal's office. All eighteen students are suspended for "cyberbullying."

QUESTIONS TO CONSIDER:

- 1) Do you think the principal's actions were fair? Why or why not?
- 2) Should schools ever have the ability to censor students for their activities on Facebook? If you answered "yes," under what circumstances should this be allowed? If no, why not?
- 3) Looking at each of the comments the students made, which ones – if any – should have been punished? Should the student who started the group have been punished?
- 4) The principal suspended the students using the Ontario Safe Schools Act, which prohibits "cyberbullying." Do you think this was an appropriate use of the law? Why or why not?
- 5) What if there were a group of citizens posting complaints and negative comments about a politician on Facebook? Should a politician be able to censor those comments or have the commenters punished for "cyberbullying?" What could be the consequences of the law being used in this way?

CASE THREE: SEARCHING A TEACHER'S LAPTOP

Mr. Cole was a high-school English teacher in Ontario. The school where he worked provided him with a laptop, which he was allowed to use for personal purposes (e.g. browsing the Internet or storing personal photos) in addition to work.

The school's IT technicians were doing some routine maintenance on Mr. Cole's laptop when they found a hidden folder. When they looked inside the folder, they found nude photographs of an underage female student.

The school administration confiscated the laptop and handed it over to police, who searched Mr. Cole's files and Internet browsing history without obtaining a warrant. Mr. Cole was charged with child pornography.

QUESTIONS TO CONSIDER:

- 1) Did Mr. Cole have reason to expect that the images on his laptop would remain private? Why or why not?
- 2) Typically, the police need to obtain a warrant before entering your home or searching through your purse (although there are exceptions). In this case, should the police have obtained a warrant before searching through Mr. Cole's laptop? Why or why not?
- 3) Is there information on your laptop you would consider private? Would you feel comfortable if your parents, your best friend, a teacher or your boss looked through all your folders?
- 4) Mr. Cole's laptop contained evidence that he had committed a serious crime. But consider the situation of his colleague, Ms. Lee, who teaches chemistry and who also uses a school laptop. IT technicians were working on Ms. Lee's laptop when they found emails and photos from May 3, 2012. On that day, Ms. Lee called in sick – but the emails and photos reveal that she actually spent the day shopping and attending a concert.
 - Based on this evidence, should the school principal be allowed to discipline Ms. Lee for lying and claiming a sick day? Why or why not?

CASE FOUR: FACEBOOK PRIVACY

In October, Facebook announced that it had nearly 1.2 billion monthly users. Seven hundred and fifty million people log into Facebook each and every day. Users can choose privacy settings that limit the amount of information that is disclosed to difference Facebook users and the general public over the Internet.

When Facebook users sign up for the service, they all agree to a contract saying that Facebook owns their data. Everything users do is tracked by Facebook, retained, and can be used for commercial purposes. Facebook stores private messages and chats sent over the site on its database, regardless of whether these private conversations have been deleted by Facebook users.

In order to make money, Facebook sells the personal information of its users to other companies. Most of this information is sold in a general, aggregated, anonymous format.

Recently, an executive at Facebook said the company is considering collecting data on cursor movements and “hovering.” Every time a user’s cursor “hovers” over a certain image or link, this information would be tracked. That way, Facebook could track your interest in a certain item – even if you don’t actually click the link. This information would then be sold to advertisers, to help them target customers more efficiently.

QUESTIONS TO CONSIDER:

- 1) Do you think it’s fair that Facebook sells your personal data and private messages to advertisers in exchange for allowing you to use the social media site? Do you think Facebook’s policies are problematic? Why or why not?
- 2) Facebook is a private company, not a government actor like a police officer or public school official. Do you think private companies should be allowed to act differently from government actors when collecting or sharing your personal information? Explain.
- 3) What might be some of the risks/consequences associated with posting your personal information on Facebook?
- 4) There are reports that potential employers and even universities are looking at applicants’ Facebook pages to see whether they have posted inappropriate content. Does that seem fair to you? If you were hiring an employee, would you check out their Facebook page?