LESSON PLAN

Level: Grades 9 to 12

Duration : 1.5 — 2 hours

This lesson was created by MediaSmarts for Canada's federal, provincial and territorial privacy protection authorities.

Privacy Rights of Children and Teens

Overview

In this lesson, students are introduced to the privacy principles that inform the Alberta and BC *Personal Information Protection Acts*, Québec's *An Act Respecting the Protection of Personal Information in the Private Sector* and the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) relating to personal information collection online. They learn ways to find out what personal information may or has been collected by platforms that they use, how to limit data collection about themselves, and the various forms of recourse that are available to them if they feel an organization is not respecting their rights.

Learning Outcomes

Students will learn:

- that they have legal and consumer rights with regards to personal information
- to evaluate how well the online platforms and services they use live up to those rights
- which federal, provincial and territorial laws and offices oversee privacy concerns
- how to make a privacy complaint
- how to create a media product in the context of language arts and/or media literacy and related subject areas

Preparation and Materials

- Arrange access to a computer lab or ensure that at least seven students have devices able to access the Internet (preferably laptops or tablets, as students will be reviewing Terms of Service and Privacy Policies)
- Photocopy the following handouts:
  - *Privacy Protection Principles*
  - *Protecting Your Privacy*
  - *Fair Information Principle Group Activity*: *Close Reading Table*
- Photocopy the assignment sheet *Your Privacy, Your Rights*

- If you are doing the extension activity, photocopy the handout *Making a Complaint* and prepare to project the document *Personal Information Protection and Electronic Documents Act (PIPEDA)* Complaint Form, or the equivalent forms from the Alberta, B.C. or Québec Commissioners:
  - https://www.oipc.ab.ca/media/794360/form_request_review_privacy_complaint_mar2017.docx
  - https://www.oipc.bc.ca/media/15566/howtofilecomplaintorganization.pdf
  - http://www.cai.gouv.qc.ca/documents/CAI_FO_plainte.doc
- The first and third link above are direct download links. If you are unable to access them by clicking, find them on the organizations' respective pages here:
  - https://www.oipc.ab.ca/forms.aspx
  - http://www.cai.gouv.qc.ca/diffusion-de-linformation/services-et-formulaires/

Procedure

What Are Rights?

1) Ask the class what they know about the term "rights."
   - When we talk about having the right to do something, what does it mean? (*That you can't be prevented from doing that thing.*)
   - Do rights sometimes protect you, as well as let you do things? (*Some rights protect your ability to do things – like expressing your opinion – while others guarantee your protection and freedom from certain things, like having your reputation damaged by false statements about you.*) Your rights to do things are limited by other people's rights to be protected, and other people's rights are limited in the same way.
   - Where do rights come from? (*Rights are guaranteed by the laws or constitutions of different nations. In Canada, your rights are guaranteed by different laws and by the Charter of Rights and Freedoms.*)
   - Do children have rights? (*Yes, though children often do not have certain rights such as the right to vote, while others are limited until they reach the age of majority, which in Canada is 18, such as the right to agree to contracts.*)
2) Now that they know more about the idea of rights, what examples of rights can students think of? (*Some examples: right to freedom of thought/expression; right to life, liberty and security of the person; right to the equal protection and equal benefit of the law without discrimination.*)

3) Is there such a thing as a right to privacy? (*Yes! Privacy is not specifically named as a right in the Charter of Rights, but the federal government and some provinces and territories have established privacy commissioners to advocate for Canadians' privacy rights and to investigate complaints under Canada's two privacy laws, the Privacy Act and the Personal Information Protection and Electronic Documents Act, as well as equivalent laws in Alberta, British Columbia, New Brunswick, Newfoundland and Labrador, Ontario and Quebec, which give you specific rights to privacy when dealing with governments and private businesses respectively. The Supreme Court of Canada has stated that the privacy laws have "quasi-constitutional status", and that the values and rights set out in the Act are closely linked to those set out in the Constitution as being necessary to a free and democratic society.*)

Why Do We Need Privacy Rights?

1) Ask students to think about why "privacy" would be considered as important to defend as rights like safety or freedom of expression.

2) Explain to students that for this lesson, you'll be looking specifically at your rights to privacy when it comes to personal information. To ensure that students are clear on the meaning of the term, read to them the following definition of personal information, or write it on the board:

   Personal information *is information about an identifiable individual. It can include your name, birthday, email address, and phone number. It can also include your opinions, your spending habits, your IP address, photos and digital images, and your email and text messages.*

3) Now ask why *personal information privacy* deserves to be protected. Point out that social networks, search engines, and e-commerce sites collect all sorts of personal information – photos, messages, what they've searched and bought, who they've interacted with. How confident are they that they know what these companies do with that data, why they collect it, and how long they keep it?

4) Distribute the handout *Protecting Your Privacy* and go through it with the class. Explain that these are ways of *limiting* how much of your information organizations collect, but that they also have privacy rights that govern how organizations can collect and handle their personal information.

Privacy Protection Principles: Your Right to Privacy

1) Distribute the handout *Fair Information Principles* and explain that these describe their **privacy rights** when it comes to what companies can do with personal information. Have the students read through the principles and make sure to identify and explain any vocabulary that is unfamiliar to them.

2) As a class, choose three online services, apps or platforms that collect user data, such as social networks, search engines and e-commerce sites. Write the names of these three websites on the board.

3) Divide the class into seven groups and assign each group one of the first seven principles on the handout. (If students are using their own Internet access devices, ensure that each group has at least one such device.) Tell each group that they are going to find out how well each of these three services respect the rights laid out in the Fair Information Principles by searching the services Terms of Service and Privacy Policy.

4) Ask students how many of them have ever read a Terms of Service or Privacy Policy before agreeing to it. Explain that because these documents are often very hard to read, once they've found the section that addresses the Fair Information Principle their group is focusing on, they will do a special "close reading" exercise to help them make sense of it.

5) Give each group three copies of the *Fair Information Principle Group Activity: Close Reading Table* handout and explain how to use it:

   a) Use the keywords listed below their group's Fair Information Principle to help find the relevant section.

   b) In the first column of the table, write down any words they don't understand and find the definition.

   c) In the second column, write down three—six *key phrases* that they think are central to the meaning of the section.

   d) In the third column, paraphrase in their own words what the section says about their principle.

   e) Give the service a ranking from one to five based on how well it lives up to their principle, where a zero is "there is no information given" and a five is "the service's terms of service and/or privacy policy meet all of the points given in the definition of the principle."

   Circulate as the groups are working and help them find the relevant sections if they need it. In a small number of cases the information may not be there at all, but in general at least two of the platforms chosen should have it.

6) Once the groups have completed the table, have them also give each service a ranking on Fair Information Principle number eight (Openness): How easy was it to find out how well this service lives up to your group's principle? How easy was the language to read and understand? Rank this from zero (completely incomprehensible or impossible to find) to five (you had no problems at all finding and reading it).

7) Now have groups share with the rest of the class what they found and the ranking they gave each site. Keep a tally on the board for the ranking of each website by principle. Once all the rankings are in, do a total ranking for each service.

If there were any services that got a zero on any principle, ask students whether they think that service is doing enough to respect their rights. What options do they have if a company isn't living up to its legal obligations?

Assessment/Evaluation Task: Your Privacy, Your Rights

Distribute the assignment sheet *Your Privacy, Your Rights* and tell students that they are going to create a poster or pamphlet that will **educate** and **inform** other students about **one** of the Fair Information Principles.

This poster/pamphlet will include the following information:

- Everyone has rights to privacy
- These rights include being treated by online businesses according to established privacy principles
- What a business must do to live up to the Fair Information Principle you have focused on
- What you can do if you feel a business is not living up to that Fair Information Principle

Privacy Protection Principles

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) and the Model Code for the Protection of Personal Information set out 10 principles of fair information practices, which set up the basic privacy obligations of private businesses under the law. These principles also inform the Alberta and B.C. *Personal Information Protection Acts* and Québec's *An Act Respecting the Protection of Personal Information in the Private Sector* applies. These principles are **your privacy rights** when it comes to what organizations can do with your personal information, and each organization's Privacy Policy and Terms of Service should show how they respect them.

Governments are covered by a different set of privacy rules: the federal government and its agencies are covered under the *Privacy Act,* the provincial and territorial governments and their agencies are subject to their own protection of privacy acts. The laws that apply to governments are based upon the same principles as PIPEDA, but one major difference is that governments do not generally require your consent to collect your personal information.

For this exercise we will be looking at eight of the principles:

1) **Accountability** - An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

(In other words, organizations should take good care of your personal information and it should be easy to find out what their privacy policy is and who you can talk to if you have a question or a problem.)

Search keywords: accountability, responsible, responsibility, liability, contact, "contact person"

2) **Identifying purposes** - Organizations must identify the reasons for collecting your personal information before or at the time of collection.

(In other words, they should clearly tell you why they're collecting any piece of personal information, either before they collect it or when they collect it.)

Search keywords: reason, why, "how we use", collect, purpose

3) **Consent** - Where it is appropriate, an individual must have knowledge of and give consent to the collection, use or disclosure of personal information. An organization should make a reasonable effort to inform individuals of the purposes for collecting information. Consent should be meaningful; the purposes should be explained in such a way that the individual can reasonably understand the use and disclosure of their personal information. Individuals are entitled to withdraw consent at any time.

(In other words, they should make sure you understand what they're going to do with your information and make sure you've agreed to it before they collect it.)

Search keywords: consent, permission, authorize, allow

4) **Limiting Collection** - The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

(In other words, they should only collect what they actually need, and only collect it in ways that are fair and legal.)

Search keywords: manage, "what kind", delete, necessary, collection, limit

5) **Limiting use, disclosure and retention** - In general, organizations should use or disclose your personal information only for the purpose for which it was collected, unless you consent. They should keep your personal information only as long as necessary.

(In other words, they should only use or share your personal information for the reason they said they were collecting it, and not keep it longer than they need to.)

Search keywords: disclosure, share, "how we share", use, keep, store

6) **Accuracy** - Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

(In other words, they should make sure that any information they have about you is correct and up-to-date.)

Search keywords: necessary, update, updating, correction, "user content"

7) **Safeguards** - Organizations need to protect your personal information against loss or theft by using appropriate security safeguards.

(In other words, they should take steps to keep your personal information from being hacked or stolen.)

Search keywords: protect, safeguard, security, theft

8) **Individual access** - Generally speaking, you have a right to access the personal information that an organization holds about you.

(In other words, you should be able to find out everything they've collected about you.)

Search keywords: access, request, control, "your data", "your information"

9) **Recourse (Challenging compliance)** - Organizations must develop simple and easily accessible complaint procedures. When you contact an organization about a privacy concern, you should be informed about avenues of recourse.

(In other words, it should be easy to make a complaint if you think they haven't respected your privacy rights, and they should tell you what they can do to make things right.)

Search keywords: recourse, complaint, remediation, dispute, arbitration

10) **Openness** - An organization's privacy policies and practices must be understandable and easily available.

(In other words, you should be able to easily find and understand what they do with your personal information and what you can do if you have a problem.)

To determine openness, you will be basing your judgment on how easy it was to find and read the sections relating to the other Fair Information Principles.

Protecting Your Privacy

Ask questions: Get in the habit of reading privacy policies associated with the websites and apps you use. Companies should be able to answer any questions you have about what personal information they are collecting, and how your information will be used and protected. If they can't, or you don't like what you hear, this should raise red flags. Some platforms, like the search engine DuckDuckGo, don't track you at all, and others track less than their competitors. Keep data collection in mind when you're choosing search engines, shopping sites, social networks, and so on.

Privacy settings: Mobile devices, browsers, sites/apps and other web-enabled items such as video games and cameras often have adjustable privacy settings. For devices, this may include the ability to control everything from location tracking to screen locks. For browsers, users can often control things like cookies and pop-ups, while apps and websites such as social media sites generally allow users to control what personal information others can see about them. Be sure to review and adjust privacy settings regularly and never rely on default settings.

App permissions: During installation, verify that the permissions being sought by the app match not only what the privacy policy says but also what you would expect the app to require. (Permissions within mobile apps allow the app access to your device's data and capabilities in order to run. These permissions could include location, identity, email and contacts.) Also pay attention to the app description in the app store as well as any "in-app" notices which may explain the app's collection and use of personal information.

Private browsing: Some browsers have a "private browsing mode," but super and Flash cookies are not always covered by these settings.

Do Not Track: Some browsers allow you to send a message to websites asking them not to track your activities while you're using them. This is usually found in the "Privacy" section of the "Settings" menu (sometimes you have to click on "Advanced Settings".) You can also visit the http://donottrack.us website for more information on how you can prevent tracking. Here too you will have to keep in mind that this is a partial solution, since not all third parties respect the "do not track" header.

Don't give out more information than you have to: Avoid sharing too many personal details with large numbers of people, for example by allowing open access to your social media pages. Familiarize yourself with the privacy settings of your favourite social networks and adjust them according to your comfort level. When posting information online it's also worth thinking about who might see it apart from your intended audience—would the things you write or the pictures you post cause embarrassment in real life? How would you feel if your current or potential employer saw what you posted?

Turn off GPS when you don't need it: A lot of apps collect your GPS information, and it's also automatically included in photos you take with your phone. You can avoid this by turning off GPS when you're not using it. You can also go into your device's settings and turn off Geotagging, which means photos (but not other apps) don't have your GPS information.

Fair Information Principle Group Activity: Close Reading Table

Instructions:

1) Find the service's Terms of Use and Privacy Policy.

2) Use the keywords listed below your principle to help find the section in one or both of these that connects to your group's principle.

3) In the first column, write down any words you don't understand and find the definition.

4) In the second column, write down three-six *key phrases* that you think are central to the meaning of the section.

5) In the third column, paraphrase in your own words what the section says about your principle.

6) Rank this service on a scale of 0 to five, where 0 means the information is not there" and a five is "this service's clearly meets all of the points given in the definition of the principle."

7) Now rank the service on how well it meets Principle number eight (Openness): How easy was it to find out how well this service lives up to your group's principle? How easy was the language to read and understand?

   (You won't need to do a specific Keyword search for this, but base your judgment on the sections you read for steps one through six.)

   Rank this from zero (completely incomprehensible) to five (you had no problems at all reading it.)

Principle: _____

Service: _____

New vocabulary	Key phrases	Summary

Your Privacy, Your Rights

For this assignment you are going to create a poster or pamphlet that will **educate** and **inform** other students about **one** of the Fair Information Principles.

This poster/pamphlet will include the following information:

- Everyone has rights to privacy
- These rights include being treated by businesses according to the Fair Information Principles
- What a business must do to live up to the Fair Information Principle you have focused on
- What you can do if you feel a business is not living up to that Fair Information Principle.

Your Privacy, Your Rights—Rubric

	Learning Expectations	**Achievement**
Use 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.	*Privacy and Security:* • demonstrates awareness that his/her activities on the Internet leave a permanent "digital footprint" or "trail" and behaves accordingly • uses information technology-related vocabulary in context *Community Engagement:* • uses digital media to be part of a community *Making and Remixing:* • communicates information and ideas effectively to multiple audiences using a variety of media and formats • participates in society through online engagement in democratic actions (e.g. lobbying, petitions, parliament)	Insufficient (R) Beginning (1) Developing (2) Competent (3) Confident (4)
Understand "Understand" includes recognizing how networked technology affects our behaviour and our perceptions, beliefs, and feelings about the world around us. "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.	*Privacy and Security:* • understands the concept of privacy in their everyday lives, and as it relates to using the Internet • identifies and communicates values and beliefs that affect healthy choices *Consumer Awareness:* • understands the ways websites and companies influence consumers' privacy habits, as well as consider companies' motives in doing so • shows an understanding of the roles and responsibilities of different stakeholders in relation to online privacy *Community Engagement:* • shows awareness of the discourse on both the issues and the opportunities involved in new media • shows an understanding of the issues through their creative work	Insufficient (R) Beginning (1) Developing (2) Competent (3) Confident (4)

	Learning Expectations	**Achievement**
Create 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, social gaming and other forms of social media. The ability to create using digital media ensures that Canadians are active contributors to digital society.	*Privacy and Security:* • communicates ideas and information in a variety of oral, print and other media texts, such as short reports, talks and posters • uses privacy tools and settings to control who accesses the information collected about them online *Community Engagement:* • creates a practical implementation plan • interacts, collaborates, co-constructs content, and publishes with peers, experts, or others employing a variety of digital environments and media • makes valuable contributions to the public knowledge domain (e.g. wikis, public forums, reviews)	Insufficient (R) Beginning (1) Developing (2) Competent (3) Confident (4)

Extension Activity: Defending Your Rights

Ask the class what they would do if a website/service they use didn't seem to have any information about how they respect their user's rights in terms of their personal information. What would they do if a company actually did not respect some of their rights at all? (For example, they could complain to the company, organize a boycott or protest, switch to an alternative service, or complain to their provincial, territorial or federal privacy commissioner.) Make a list of the top three or four responses on the board.

1) Remind students that according to the principle of accountability, each service should have a person they can contact to ask a question or send a complaint. If they can't find one, they aren't satisfied with the response, tell them that they do have a right to privacy under the law and can make a complaint to a federal, provincial or territorial Privacy Commissioner.

   Distribute the handout *Making a Complaint* and go through items one and two with the class.

2) Project the document *Personal Information Protection and Electronic Documents Act (PIPEDA) Complaint Form*, or the equivalent forms from the Alberta, B.C. or Québec Commissioners. Review this with students, emphasizing the following key items:

   a) If using the PIPEDA form, you need to be a customer or an employee to make a complaint.

      ⇒ If you're not either of those, you can still tell the Office of the Privacy Commissioner of Canada about a bad practice by going to their website and clicking on "Report a Concern". They won't respond to this directly but may decide to investigate based on your information.

      ⇒ Mention to students that you do not need to be a customer or employee in BC or Alberta. If they have your personal information then the Personal Information Protection Act applies to protect the personal information.

   b) You are expected to have made some effort to resolve this with the company before you make a complaint.

   c) You are expected to provide some evidence to support your complaint.

Making a Complaint

Before you make a complaint about a privacy practice, ask the following questions:

1) Have I already brought my complaint to the organization whose practice I want to complain about?

Before bringing a complaint to a privacy commissioner, you should try to resolve the issue with the organization whose practice you object to.

2) Who should I direct my complaint to?

Take a look at the table on the other side of the page to decide if this is a complaint you can make under provincial, territorial or federal privacy legislation. In general, if it is a **business** that **operates in Canada** it will be subject to PIPEDA or to an equivalent provincial law.

3) How do I make a complaint?

Federal and provincial Privacy Commissioners have forms you can download and use to make a complaint. You do not need a lawyer or any kind of advisor, and it does not cost you any money to file a complaint.

4) What happens when I make a complaint?

The Commissioner's office will decide whether or not to investigate the complaint. Depending on what it finds, it may ask the organization to release your personal information, to correct inaccurate information, or to change their business practices.

At the end of the investigation the office will tell you and the organization that was investigated what they have decided. They may also publish their findings, but if they do, nothing that can identify you needs to be included.

Where do I make my complaint?

Type of organization	What law applies? Who do I contact?
Federally-regulated business operating in Canada, engaged in commercial activity Examples: bank, airline, telephone or broadcasting company	The *Personal Information Protection and Electronic Documents Act* (PIPEDA) applies. For more information, contact the Office of the Privacy Commissioner of Canada.
Private sector organization Examples: retail store, service, hotel, restaurant, insurance, entertainment	The Alberta or B.C. *Personal Information Protection Act* applies in Alberta or B.C.; in Québec *An Act Respecting the Protection of Personal Information in the Private Sector* applies; in all other provinces and territories the federal *Personal Information Protection and Electronic Documents Act* applies, For more information, contact the appropriate federal or provincial oversight office based on the location of the organization that has collected your personal information.
Individuals who collect, use or disclose personal information for non-commercial purposes	In Alberta, B.C., and Québec collection, use, or disclosure is covered by each province's privacy legislation regardless of whether it is for a commercial purpose. In all other provinces and territories, the conduct of individuals who are **not** collecting, using or disclosing personal information **for commercial purposes** is not covered under Canadian privacy laws. For more information, contact the appropriate federal or provincial oversight office based on the location of the organization that has collected your personal information.
Organizations carrying on business primarily outside of Canada	The Alberta, B.C., Québec or federal acts may apply (determined on a case-by-case basis). For more information, contact the appropriate federal or provincial oversight office based on the location of the organization that has collected your personal information.

Source: Office of the Privacy Commissioner of Canada https://www.priv.gc.ca/en/report-a-concern/leg_info_201405/

Personal Information Protection and Electronic Documents Act (PIPEDA) Complaint Form[1]

SECTION 1: Complainant / Representative Information

(*Here you give your name, contact information, etc.*)

SECTION 2: Details of Complaint

Please provide information about your complaint below.

You should also describe any efforts you made to resolve the issue with the organization concerned.

1) Which organization is your complaint against? (Please identify by specific name and location. Provide legal name of organization, if known.)

2) Are you submitting the complaint as a customer or as an employee of the organization?

3) Summarize your complaint. (Please describe the events or circumstances that led to your complaint. Include details such as the names or positions of people involved in the incident, the locations where the incident occurred, and any other factors you consider relevant. If the organization gave you a reference number in relation to this issue, please include it as well.)

4) Have you attempted to resolve the matter with the organization?
If 'Yes', please outline your efforts and describe the result, if any. If 'No', please specify the reason why not.

5) Have you complained about this incident to another body or organization?
If 'Yes', please provide details. (Indicate the name of the body, and include relevant details such as dates and a reference number.)

6) How can the Office of the Privacy Commissioner of Canada help address your concerns? (Please describe any steps or remedies that would resolve your issue.)

SECTION 3: Documentation

If you have documents relating to your complaint, please attach them to your complaint:

- Any correspondence between you and the organization on this matter.
- Any documentation that indicates that you are authorized to act for another person (authorization form).
- Other relevant documentation.

SECTION 4: Certification

By signing this form, you certify that the information you provided on this form, to the best of your knowledge, is true and complete.

[1] Adapted from the official complaint form found here: https://www.priv.gc.ca/en/report-a-concern/file-a-formal-privacy-complaint/file-a-complaint-about-a-business/file-a-complaint-under-pipeda/ps_pipeda_pdf-rtf

This lesson plan is available free of charge to educators and program facilitators. We encourage you to copy and share it. We invite your feedback to help us make improvements in the future. Email your comments to: Youth.Jeunes@priv.gc.ca.

Office of the Privacy Commissioner of Canada

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Commission d'accès à l'information du Québec

OIPC Office of the Information & Privacy Commissioner Nova Scotia

Office of the Access to Information and Privacy Commissioner New Brunswick
Commissariat à l'accès à l'information et à la protection de la vie privée Nouveau-Brunswick

Manitoba Ombudsman

Office of the Information & Privacy Commissioner for British Columbia
Protecting privacy. Promoting transparency.

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER for Prince Edward Island

Office of the Saskatchewan Information and Privacy Commissioner

Office of the Information and Privacy Commissioner of Alberta

OIPC OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER NEWFOUNDLAND AND LABRADOR

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER NORTHWEST TERRITORIES

Yukon Information and Privacy Commissioner

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER OF NUNAVUT

Media Smarts