

# Peer Privacy Protectors Project

## A PRIVACY GUIDE BY TEENS, FOR TEENS

### TABLE OF CONTENTS:

**2**    *Introduction*

**4**    *Privacy 101*

**10**   *Five Eyes on You*

**18**   *Dollars for Data*

**25**   *When Your Watch Tells More than the Time*

**34**   *Online Reputation = Offline Impact*

# about the Peer Privacy Protectors Project (PPPP)

## — FOR TEENS —

A group of teens aged 13-19, from across the greater Toronto area, farther afield in Ontario, and even remotely from BC, worked for a year to learn more about privacy and how to protect it. They listened to experts speak about privacy research in an orientation talk and four workshops that focused on the priority privacy areas identified by the Office of the Privacy Commissioner of Canada: Economics of Personal Information; State Surveillance; Reputation and Privacy; and The Body as Information. Then they all wrote about what they learned, and what they thought about it. Young people in high school today are some of the first to have lived their whole lives with the internet. The reality is, adults haven't figured out what the rules should be or how to assess the benefits and risks of living lives where physical and online spaces are intertwined, but teens know it is equally essential to navigate both successfully to get through daily life. This book is by teens and for teens. We hope you like what the Peer Privacy Protectors have put together.

## — FOR TEACHERS AND PARENTS —

Young people are perhaps the most intensive technology users in Canada; recent research from the MediaSmarts Young Canadians in a Wired World Project (funded by the Office of the Privacy Commissioner of Canada) found that “virtually all of the students” surveyed in their most recent youth survey had access to the internet, “inside and outside of school” (MediaSmarts 2015, p. 3). Young people are also one of the most surveilled segments of the population. In September 2015, The Global Privacy Enforcement Network, in its third annual privacy sweep, found that most apps and websites for children and youth collect personal information, and many share information with third parties, probably for advertising purposes. Troublingly, at the same time, the OPC 2014 Privacy Survey states that “Canadians under 25 years of age stand out as having the lowest self-assessed concern for and understanding of their privacy rights.” Clearly, youth are vulnerable to privacy risks, and there is a compelling need for improved communication and education about privacy rights for young people.

The PPPP addresses that need. We used a connected learning approach to engage teen participants in a series of workshops to enhance their knowledge of privacy risks and rights and help them develop this

# Peer Privacy Protectors

guidebook based on these workshops to educate their peers. We also consulted with Canadian educators in a series of interviews to identify classroom needs for privacy education generally, and obtained informed feedback on the project's student-developed materials prior to preparing them for wider circulation. This book, and the accompanying [website](#), is the result. We hope it proves informative and helpful in classrooms across Canada.

## — ABOUT THE CCLA AND CCLET —

The Canadian Civil Liberties Association and Education Trust (CCLA and CCLET) is a non-partisan, independent, national, non-profit organization that has been at the forefront of protecting fundamental rights, freedoms and democratic life in Canada since 1964. CCLET has long experience talking with Canadian youth (and their teachers) about their rights. In 2014 alone, our education programs were presented to 9,477 students from elementary to university level, in 345 classes across 113 institutions. We engage students and provide current and future teachers with the knowledge and skills to develop critical thinking about rights and freedoms in the classroom.

We want to thank all of our amazing teen Peer Privacy Protectors who stuck with the project across two different school years, to the researchers who travelled to Toronto and gave up a Saturday afternoon to share their expertise and inspire us, to the teachers who shared their ideas and feedback, and to the Office of the Privacy Commissioner of Canada.

## — OPC —

This project has been funded by the Office of the Privacy Commissioner of Canada (OPC); the views expressed herein are those of the authors and do not necessarily reflect those of the OPC.

SHIVANI BALA  
RAPHAEL BRUK  
VIVIAN CHU  
RAVNEET DHALIWAL  
HARKIRAN GILL  
ABEER HASAN  
ERUM HASAN  
TANIA KENGATHARAN  
SHREYA KUMAR  
MAGGIE LIN  
WARREN LIU  
NATELA MAKARASHVILI  
SOHAM MEHTA  
AFREEN MOHAMED  
SAMENA RASHID-MOHAMED  
B. SANDHU  
SAYINCRAFT  
MIRAJ UMAR  
ASHWINI YOGARAJAH

# 1. Privacy 101

## — WHAT IS PRIVACY? —

Privacy can mean different things to different people — sometimes, it can even mean different things at different times to a single person. There are many definitions of privacy. A very famous definition, from 1890, comes from a law review article by Warren and Brandeis, who said that privacy is the right to be let alone (“The Right to Privacy” (4 Harvard L.R. 193 Dec. 15, 1890). In this conception of privacy, people need privacy to allow them to develop independently, to explore their own identity and humanity. Privacy can also be about control, the right to choose which parts of our lives or personal information we want to share with others and which parts we wish to keep secret. Privacy is not just an individual value, however, it is a public value, that helps people exercise other rights, including freedom of expression, freedom of religion, freedom of association, and democratic participation. It is also a social value — something we negotiate with others in relationships (both online and off). When we think about privacy as something that primarily benefits individuals, it can encourage us to think in terms of trade-offs. This is the kind of argument you might hear when people talk about national security—how important is one person’s privacy versus the security and safety of many people? But when we think about it as a social and public good, it changes the conversations we may want to have.

## — WHY SHOULD I CARE ABOUT PRIVACY? —

Everyone has information about themselves that they would never want to share with the world. Revealing personal information can be really embarrassing! Also, those who have access to your personal information may interpret or use it in a way that you never intended, which may disadvantage or harm you in the future. And even if you think you have “nothing to hide,” is the same true for everyone you care about? Will it always be true for you?



## What Does Privacy Mean To Me?



**THE KEY TO PRIVACY IS TO RESPECT  
EACH OTHERS INFORMATION**



**PROTECT MYSELF FROM FRAUDS AND HACKERS**



**BEING ABLE TO CONTROL WHO VIEWS MY POSTS ONLINE**



**PROTECT THE THINGS ONLY I NEED TO KNOW ABOUT**



**BEING ABLE TO KEEP SECRETS ON THE WEB**



**FREEDOM OF SPEECH**



**BEING ABLE TO CONTROL THE THINGS THAT HAPPEN TO ME**



*This desire for privacy is why most people close doors, why individuals do not post things such as social security numbers on social media, and why people sometimes turn off their cell phones and computers. It is not an attempt to be antisocial, but rather simply not wanting to share parts of our lives and time with others.*

*Privacy to me means an innate need for my information to be kept confidential and only to be shared when I have given consent. Having privacy also means that I have control over my information, as well as the knowledge of where it is going and how it is going to be handled. When smartphones are able to track everything from our home address to little intimate details like our heartbeats, it is really important to ask ourselves whether or not our individuality, privacy, and freedoms are being respected and kept confidential.*

*It's also important to know how policymakers interpret my data and whether or not in the long run my data will be used to my benefit or disadvantage. Lastly privacy is having confidence in the people with whom I choose to share my information, that they will not misuse it. Although privacy is something that is often taken for granted because it cannot be touched, bought or seen, it should not be taken lightly because without privacy, is there really anything that we can call our own?"*

NOTHING TO HIDE

BY TANIA KENGATHARAN



WWW.BITSTRIPS.COM

# Some laws that protect your privacy in Canada

## 1

### THE CANADIAN CHARTER OF RIGHTS AND FREEDOMS (CHARTER)


The Canadian *Charter of Rights and Freedoms* does not explicitly include a right to privacy.

However, several *Charter* provisions, such as Section 7 (the right to life, liberty and the security of the person) and Section 8 (the right to be secure against unreasonable search or seizure), do protect privacy. Section 8 is the most commonly discussed section when courts talk about privacy. It limits the government's power to search a person, including a person's residence or belongings, when that individual has a reasonable expectation of privacy. For example, it's reasonable for a person to expect privacy in their own home. If the police wanted to enter a home to search for evidence of a crime, they would generally need to obtain legal authorization (a warrant) before they can enter and intrude on the private lives of the people who live there. By contrast, your expectation of privacy in your luggage is greatly reduced when you choose to travel via airplane (a means of travel with very important security concerns), so in general, it is reasonable for airport security to require an x-ray scan of the contents of your luggage before you are permitted to board. *Charter* violations are usually dealt with in court.

## 3

### PRIVACY ACT

The *Privacy Act* provides rules for federal government institutions that collect, use and disclose the personal information of individuals in Canada. The *Privacy Act* also gives individuals the right to request access to and change personal information held by federal government organizations. For example, Statistics Canada is a federal institution. If you or a family member has ever responded to a census survey from Statistics Canada, your information would be protected by the *Privacy Act*.

The *Privacy Act* has "quasi-constitutional status" because privacy rights have been recognised by the Supreme Court of Canada as being "necessary to a free and democratic society: (*Lavigne v. Canada (Office of the Commissioner of Official Languages* 2002  C 53 at paras. 24-25). The Act was first passed in 1985.

*The Office of the Privacy Commissioner of Canada (OPC) is responsible for ensuring that the government complies with the Privacy Act and that businesses comply with PIPEDA, and has the power to investigate complaints from individuals about how their personal information was handled.*

## 2

## PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA)

Businesses will often need to collect personal information about you, such as name, age, income, telephone number, and more, to provide services or products.

PIPEDA is a federal law which sets out rules for how private sector businesses involved in commercial activities can gather, use and reveal an individual's personal information. It also applies to federally-regulated organisations such as banks and telecommunications companies. The purpose of PIPEDA is to protect you from businesses using your information without your knowledge or consent. It requires organizations to tell you that they are collecting personal data and what they will do with that information, and it gives you the right to retrieve and request correction of your information held by the organization. PIPEDA was first passed in 2000 and most recently amended in 2015.

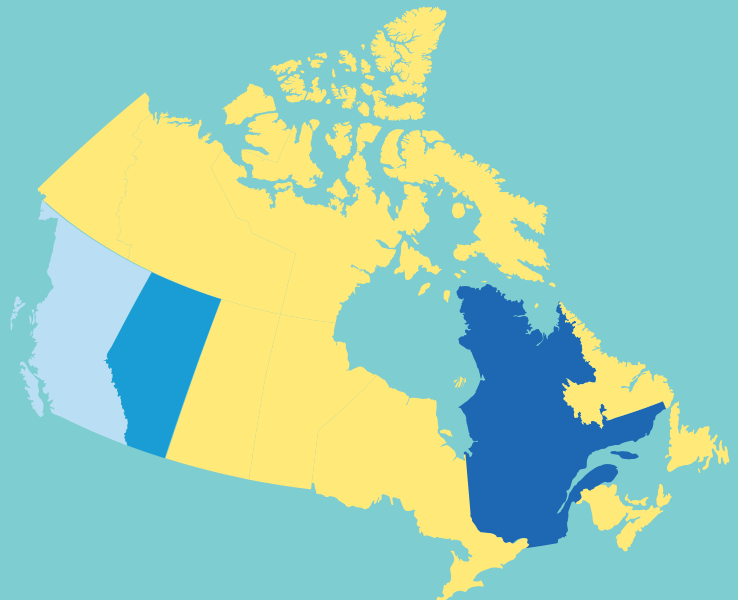
### — QUICK FACTS ABOUT PIPEDA —

#### THREE PROVINCES HAVE PRIVACY LEGISLATION SIMILAR TO PIPEDA.

Alberta, BC and Quebec have provincial private-sector legislation that applies to businesses in those provinces. PIPEDA applies in the rest of the provinces and territories.

#### PIPEDA IS BASED ON 10 FAIR INFORMATION PRINCIPLES:

- accountability • purpose specification
- informed consent • limiting collection
- limiting use, disclosure and retention
- accuracy • appropriate safeguards
- openness about information policies
- individual access • providing recourse



PIPEDA DOES NOT APPLY TO CHARITIES AND NON-PROFIT ORGANISATIONS.

## 2. Five Eyes on You: Government Surveillance



### — WHAT IS SURVEILLANCE? —

Professor David Lyon defines surveillance as “the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction” (*Surveillance Studies: An Overview*. Oxford: Polity Press, 2007, p. 14). Surveillance can be for our benefit, such as when a lifeguard watches a pool full of swimmers, or it can be for security purposes, such as when a store uses a camera to keep an eye on shoppers. It can also be to collect information about us to influence our behaviour — this happens a lot when we browse online. When we think about surveillance, we shouldn’t assume it is a bad thing, but it is very important to think about why it is being done, who is doing it, and whether we feel that the reason for the surveillance fits with the values we have as a democratic society.

In this section, the PPPP team will share some information about how surveillance takes place, and what privacy concerns are raised. We are going to talk mostly about surveillance by state agencies here, and you will learn more about private sector surveillance in the section on “Economics of Information.” Government surveillance is particularly important to learn about because of the power governments and their law enforcement and public safety agencies have over people within a country: they can deny services, arrest individuals and put them in jail, or even, in very extreme circumstances, deport non-citizens out of Canada.



*There are advantages and disadvantages of surveillance cameras such as solving unsolved crimes that have been caught on camera. The disadvantages consist of loss of privacy and being monitored at all times.”*

# Methods of conducting surveillance

There are lots of ways that targeted surveillance can be conducted, by police, by companies, or by national security agencies. These are some of the most common:

-  **Telephones** (landline wiretaps, cellphone tracking)
-  **Computers**
-  **Cameras:**
  -  **Security surveillance cameras**
  -  **Red light cameras**
  -  **Government monitoring cameras** (cameras such as those in the United Kingdom, operated by the government, monitored by police, i.e. CCTV)
  -  **Cell phone / digital cameras**
-  **Social media**
-  **Biometric surveillance** (human physical and/or behavioral characteristics for authentication, identification, or screening purposes; for example, fingerprints and DNA)
-  **Capturing aerial images and diagrams**
-  **GPS tracking**
-  **Agents who follow the target and keep detailed observations**
-  **Devices connected to a high risk individual on probation that maintain detailed logs and report back to a supervising officer.**

## — MASS SURVEILLANCE —

Sometimes surveillance isn't targeted. We call this "mass surveillance" or "bulk interception." Privacy International defines it like this:

Mass surveillance is the subjection of a population or significant component of a group to indiscriminate monitoring. It involves a systematic interference with people's right to privacy. Any system that generates and collects data on individuals without attempting to limit the dataset to well-defined targeted individuals is a form of mass surveillance. (<https://www.privacyinternational.org/node/52>)

A major problem with mass surveillance is that it happens in secret with no way for people to understand how their information is going to be used, if it is going to be used, or who is going to possibly use it. Mass surveillance is usually conducted by states.

## — NATIONAL SECURITY SURVEILLANCE —

When we think about surveillance, we often think about national security agencies that have the difficult job of protecting the country. There can be conflicts between national security goals and people's privacy rights; it is important to talk about those conflicts and make decisions about where we draw the lines, because we need both security and privacy to have a strong, safe and democratic society.

The Office of the Privacy Commissioner of Canada says:

Canadians want to be and feel secure, but not at any and all costs to their privacy — particularly when it comes to their own privacy. What they want is a balanced, well-measured and proportionate approach. It has become far too naive to believe that only "bad people's" privacy is at stake or "if we have nothing to hide, we have nothing to fear." (*Strategic Priorities*, <http://bit.ly/2mQ3PuC>)

# Canada's National Security Agencies



## — CSIS —

The **Canadian Security and Intelligence Service (CSIS)** is the organization in Canada with primary responsibility for the collection and analysis of

human intelligence. Its mandate and actions are governed by the Canadian Security and Intelligence Agency Act. Human intelligence is what we probably think of when we think of spies — people watching other people.



## — CSE —

The **Communications Security Establishment (CSE)** is the primary Canadian agency responsible for collecting foreign signals intelligence and for protecting the Canadian

government's information and communication networks. It is administered under the Department of National Defence, and its mandate is explained in the National Defence Act. CSE is the agency that monitors computer traffic. They are not supposed to collect information inside Canada about Canadians, but they are allowed to assist CSIS, the Canadian Border Services Agency, or the Royal Canadian Mounted Police if they receive a request that is authorised by a legal authority (i.e. a warrant from a judge).



## — RCMP —

The **Royal Canadian Mounted Police (RCMP)** is Canada's national law enforcement service, and operates under the Ministry of Public Safety Canada. The RCMP is unique in

that it is a national, federal, provincial and municipal policing body. RCMP have a role in national security. It is responsible for conducting investigations to allow for criminal prosecution of suspected terrorists in Canada, and has a mandate to reduce the threat of terrorist criminal activity in Canada and elsewhere through prevention, detection, investigation and gathering evidence.



## — CBSA —

**Canada Border Services Agency (CBSA)** collects information at the border through the Immigration Security Screening program. Working

with CSIS, CBSA monitors the movement of persons of interest as they enter or exit Canada, and when they apply for temporary or permanent residence or refugee status. CSIS, in turn, assists Citizenship and Immigration Canada and CBSA in their efforts to assess the admissibility of these individuals under the *Immigration and Refugee Protection Act*.

## Canada's Partners: The 5 Eyes

The **Five Eyes** is a secretive, global surveillance arrangement made up of the **United States National Security Agency (NSA)**, the United Kingdom's **Government Communications Headquarters (GCHQ)**, Canada's **Communications Security Establishment (CSE)**, New Zealand's **Government Communications Security Bureau (GCSB)** and the **Australian Signals Directorate (ASD)**. These agencies have worked together since 1946 to share intelligence, but even though the agreement between them has existed for a long time, we know very little about how it actually works.

THE FIVE EYES HAVE DEVELOPED THESE PROGRAMS:

CANADA



UNITED KINGDOM



**PRISM:** COLLECTS INFORMATION FROM AT LEAST 9 MAIN US INTERNET COMPANIES

**STATEROOM:** DATA COLLECTION PROGRAM INVOLVING INTERNATIONAL TELECOMMUNICATIONS, RADIO, AND INTERNET TRAFFIC



AUSTRALIA

**TEMPORA:** COMPUTER SYSTEM USED TO INTERCEPT ONLINE AND TELEPHONE TRAFFIC

**MUSCULAR:** SURVEILLANCE PROGRAM SIMILAR TO PRISM

**XKEYSCORE:** COMPUTER PROGRAM USED TO SEARCH AND ANALYSE GLOBAL INTERNET DATA



NEW ZEALAND




UNITED STATES OF AMERICA

## — WHY SHOULD YOU CARE ABOUT SURVEILLANCE? —

There are a number reasons teens (and everyone else) should care about surveillance. Different kinds of surveillance carry different potential risks and benefits (but people might disagree about who benefits and whether benefits are worth the risks).

### *State surveillance:*

*Unchecked surveillance can be harmful, as it can ‘chill  the freedom of expression’ as well as our personal privacy. It also has the potential of creating a variety of other harms, such as discrimination. It subjects us to state control and prevents us from progressing as a society.”*

### *Family life:*

*Research states that surveillance decreases opportunities for children to exercise self regulation and independence — if you know someone is always watching, you behave differently. It might also give you a false sense of security and raise your expectation that whoever is watching will be around to help when you get into trouble, rather than teaching you to make good choices for yourself.”*

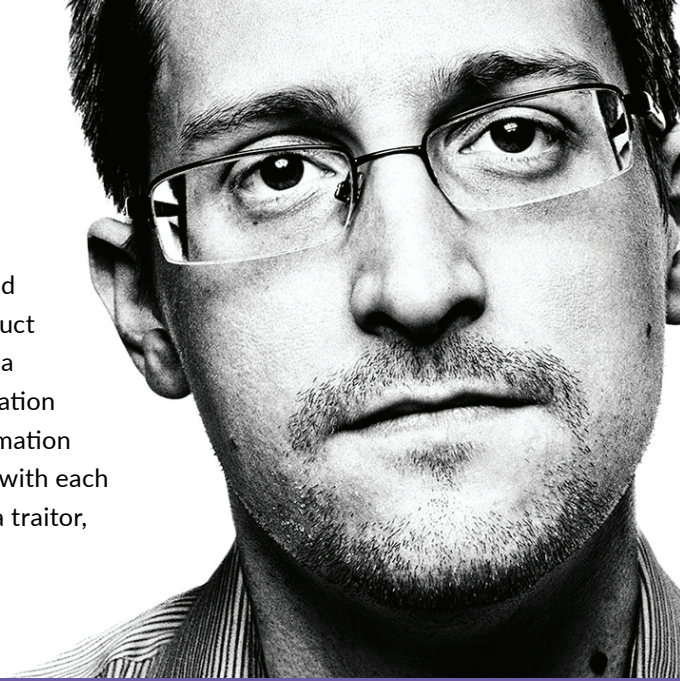


*Most teens are eventually forced to read George Orwell's 1984 for literacy circles. If you are one of the many students who have had the privilege, you will understand the dangers of governmental oppression. The book depicts a dystopian tale of how mass surveillance has led to the demise of freedom as we know it. The same concept applies in modern day. If we allow our governments to continue to increase surveillance measures in the name of national security, we are giving them permission to watch our every move. How safe are people when someone is constantly keeping tabs on us: Following us? Stalking us? In the Canadian Charter of Rights and Freedoms we have the right to privacy as well as the right to safety and security. Both are important, thus finding a balance between the two concepts in Canadian law is necessary to achieve optimal protection for citizens.*

*Currently, privacy is a controversial issue and what happens in the next few years is critical in determining the future of privacy law. Teens can't simply rely on adults to fight this because this isn't going to impact their lives nearly as much as it will shape ours. As technology becomes increasingly integrated into the fibres of society, so will the software that tracks us. Since the government feels that it is able to keep eyes on us at all time, we must also refuse to turn a blind eye to how there are bills being passed that strip us of our right to privacy. Teens today have shown their dedication to fighting issues of social injustices such as racism, homophobia, sexism and so much more. Many teens have taken it upon themselves to speak out against these injustices as leaders to have a better future and we are discovering that together we can affect change in society. Why should teens care about privacy? Because it's our future."*

## — WHISTLEBLOWERS —

Everyone has probably heard about **Edward Snowden**. He was a contractor with the US National Security Agency who was so concerned by the many government programs that were secretly being used to conduct mass surveillance by the US and international partners that he became a whistleblower. A whistleblower is someone who releases secret information to the public. The Snowden revelations have given us much more information about the way that governments spy on people, and share information with each other than we have ever had before. Some people believe Snowden is a traitor, and others think he is a hero.



## Peer Privacy Protectors Share:

### 10 things to know about state surveillance

1

THE PREVALENCE AND USE OF MASS STATE SURVEILLANCE INCREASED AFTER THE 9/11 ATTACKS IN THE UNITED STATES.

2

WHISTLEBLOWER WILLIAM BINNIE ESTIMATES THAT THE NSA IN THE USA COLLECTS DATA ON 3 BILLION PHONE CALLS A DAY (<http://bit.ly/2ndNRvx>)

3

MASS SURVEILLANCE CAN INCLUDE STORING AND ANALYZING OUR BROWSER HISTORY, INTERNET SEARCHES, EMAILS, INSTANT MESSAGES, WEBCAM CONVERSATIONS, AND PHONE CALLS. It also includes METADATA ("data about data") that can include email recipients, call times, and location records but not content information.

4

THE NSA HAS DEVELOPED A TOOL NAMED PRISM, which means they can tap into the servers of companies such as APPLE, FACEBOOK, GOOGLE and others without needing express permissions from the corporations themselves. MOST CANADIANS have accounts with at least one of these big companies.

5

AN AGENCY IN THE UNITED KINGDOM CALLED THE GOVERNMENT COMMUNICATIONS HEADQUARTERS (GCHQ) TRACKS THE IP ADDRESS OF PEOPLE WHO HAVE VISITED THE WIKILEAKS WEBSITE, NO MATTER WHERE THEY LIVE IN THE WORLD. (<http://bit.ly/2ntMrc9>)

While Snowden is the whistleblower that most people have heard of, there are other important ones as well. One whose experience is said to have influenced Snowden is **Thomas Andrews Drake**. Drake is also from the United States, and he worked at the NSA. In 2006, he leaked unclassified information about waste and unconstitutional activities within the NSA to a reporter, including information about a program for domestic mass surveillance called Trailblazer. Drake was charged under the American Espionage Act, but charges were later dropped in a deal that ended with him pleading guilty to misusing the agency's computer system and receiving a year of probation. However, he paid a very high price for his effort to warn people about the NSA's transgressions; his life was shattered and his ability to work in his field was destroyed.

6

**DESPITE ALL THE MASS SURVEILLANCE, THERE IS NO STRONG PUBLIC EVIDENCE THAT IT HAS DIRECTLY PREVENTED A SINGLE TERRORIST ATTACK.**

7

**EMAILS AND MESSAGES YOU SEND FROM CANADA TO SOMEONE ELSE IN CANADA SOMETIMES GET ROUTED THROUGH THE USA BEFORE REACHING THE OTHER PERSON. THIS OPENS THEM UP TO SURVEILLANCE IN THE UNITED STATES.**

8

**INFORMATION SOMETIMES GETS SHARED BETWEEN INTELLIGENCE AGENCIES WHEN IT SHOULDN'T BE.** Jean-Pierre Plouffe who acts as CSE watchdog commissioner said in his 2014–15 annual report that the CSE has indeed broken the rules by passing metadata involving the communications of Canada's citizens to the Five Eyes. (<http://bit.ly/2ntNA3F>)

9

**GOOGLE, FACEBOOK, YAHOO AND OTHER SOCIAL MEDIA SITES OFTEN COOPERATE WITH NATIONAL SECURITY AGENCIES AND LAW ENFORCEMENT.** Between January to June 2016, Facebook had requests for information on about 1,205 Canadian users and almost 83% of those requests produced some data in response. (<http://bit.ly/2njJvjc>)

10

**IT ISN'T JUST PEOPLE WHO HAVE SOMETHING TO HIDE WHO SHOULD BE CONCERNED ABOUT PRIVACY.** Everyone requires a certain amount of privacy at some point, and **EVERYONE DESERVES THE RIGHT TO PRIVACY.**

## 3. Dollars for Data

### — THE ECONOMICS OF INFORMATION —

When you use the internet, information is being collected about you, often without your knowledge. In the previous section, you learned about how and why governments may want to access your online information for public safety and national security purposes. Businesses and other individuals also have an interest in your online activities, primarily for their own profit. This section of the guide will talk about how information about your online behaviours, interests, and habits is collected by businesses, and the privacy risks involved. While it's unlikely that any of us will stop using the internet any time soon, knowing how our information is being collected and used by businesses allows us understand the tradeoffs of using their online services. We can then make informed decisions about the websites and applications (apps) that we use and be more careful about the information that we share online. Knowing which companies put our privacy at risk also allows us to hold them more accountable for protecting our private information.

### — HOW ARE YOU TRACKED? —

Behavioural tracking is a technique used by website publishers and advertisers to collect information about your online activities, including: the pages you have visited; the amount of time you spend on each page; your search history; and your online purchases. Using this information, marketers are able to increase the effectiveness of their advertising by targeting specific people who are likely to buy from them.

A data broker is a business that engages in behavioural tracking to collect and analyze a web-user's personal online information, and sells that information to make a profit. Data brokers may share information such as your name, address, and age with businesses who may use that information for marketing purposes. Some data brokers advertise that they can provide hundreds of data points about individuals, and have collections of data that include information about millions of people. Most of the time your information is being sold without your permission.

## Tracking Cookies

Cookies are little bits of information that a website can store on your computer to make your experience on that website more convenient the next time you visit. For example, cookies can remember your preferences, help with automatic logins, and save your shopping cart items. While cookies are generally harmless text files on your computer from a single website, tracking cookies collect and use your information across multiple websites and sends that information to a remote database for analysis. Tracking cookies can be a privacy concern because they can create a record of your activities from all the sites you have visited, and send that information along with personal identifiers such as your name and address to a third party without your knowledge and consent. Many online services provide an opt-out option for targeted advertising, so you may want to look for that option.

*Both video surveillance and facial recognition technologies have privacy implications because they reduce our ability to go about our daily business without a record of our activities or whereabouts, and to do so anonymously. Imagine the possible consequences of a stranger being able to connect an image of you to your identity and your social media profile!*

HERE ARE A FEW EXAMPLES HOW DATA BROKERS, COMPANIES OR HACKERS CAN COLLECT YOUR ONLINE INFORMATION.

## Video Surveillance

Video surveillance is a monitoring system using cameras to record activity in a physical location. You may see video surveillance cameras used in stores to prevent theft, but it can also be used to help companies make business decisions. For example, by recording the behaviour of shoppers, a store can determine what areas shoppers visit most, and relocate merchandise accordingly. Stores are supposed to notify you about cameras, including why they use them. Do you remember seeing any signs notifying you of video surveillance in your favourite place to shop?

## Facial Recognition

Using facial recognition software, images of individuals can be analysed and compared with other images in order to identify that individual. Companies like Facebook use facial recognition software to help you tag photos. The problem is, with vast quantities of images uploaded and tagged on Facebook on a daily basis, it is becoming easier for companies, government authorities, and individuals to use social media and facial recognition software to identify individuals with high degree of accuracy.

# Cloud storage

## — IS THERE A COST FOR ‘FREE’ SERVICES? —

When we talk about data being stored “in the cloud” what we really mean is that it is stored remotely, on a server that may be located anywhere in the world. Services like Dropbox, Google Drive, iCloud and others are examples of cloud storage. Often these services allow you to store quite a lot of information for free. However, there are a few different kinds of privacy risks to think about when you are using cloud storage.

### FIRST: WHERE IS YOUR DATA STORED?

If it is in Canada, it is covered by Canadian privacy law. If it is not in Canada, it is covered by the law of the country where it is stored, which means the privacy protections you have will be different.

### SECOND: WHAT ARE THE RULES ABOUT WHO GETS TO ACCESS YOUR DATA?

Can the company see it? What kind of policies do they have about when, or if, they can look at it?

### FINALLY, WHAT KIND OF SECURITY DOES THE CLOUD SITE MAINTAIN?

In other words, what are they doing to make sure your data is safe? It’s also becoming common for schools to partner with service providers to give free storage to students, to create spaces to store and share assignments. What kind of questions might you want to ask about this “free” storage? Are there any privacy risks when your school requires you to use cloud storage connected to a school account? What rights does the school board or your school administrators have to look at your information?

## Marketers love teens!

Data collected from the online activities of young people are particularly valuable not just because young people are consumers, but also because they influence the purchasing decisions of people around them. Young people may influence their family's decision to shop at a certain store, or choose a specific place for vacation. They also influence their peers through their social networks at school or online. Information spreads quickly among youth, and a new product or brand deemed as "cool" soon becomes the "it" item that everyone wants.

Adults are the present, but young people are the future. Young people will be the consumers who are beginning to shape the economy for many years to come. The information of adults is valuable for short-term business goals and trends but by learning and understanding the identities and fiscal habits of youth, an organization is able to better adapt its practices for the future by creating ideas that will prove to be sustainable as opposed to temporary.

In the past, the media has always found children and teens to be easy targets as they blindly observe everything that is advertised to them. However, this generation of young people are more critical and aware of the antics used by the media and advertisers than ever before. Media literacy has been improving in schools, which has led to more alert youth who passively consume less than previous generations.

*"We are being categorized and our information is being exploited for the sole purpose of someone else making a profit, which is not fair. Organizations everywhere are putting a price tag on your identity and the characteristics that you should have based on trivial facts, which is why being careful of what information you share online is extremely important."*

*"The issue with this is would we want advertisers to follow our daily searches and activities and keep a track of what we like or dislike to advertise relevant products that might be of interest to us? Or would we rather see irrelevant ads without having the advertisers invade our privacy? This question would be for us as individuals to decide."*



## Social media quizzes

Did you recently take that quiz called “Who is your true soulmate?” I know right, it was so intriguing. Social media quizzes are designed to look really fun and they look like a great way to pass time. Next time you take that quiz on Facebook, think twice. Your answers can provide valuable information making it easier for hackers to hack into your private accounts. Quizzes commonly ask questions that can reveal answers to your security questions for resetting passwords to your bank account or email! Keep in mind that anyone can make a quiz so be super careful when deciding to take one!

Don't ignore those terms and conditions!


One of the ways to be informed of the privacy risks of your favourite apps, is to read the terms and conditions or privacy policies associated with an app before installing it. By understanding what privacy risks are involved, you can decide whether or not the services provided by the app are worth it. Even if you don't have time to read about every app (and really, no one does) you probably have the 30 seconds it takes to skim the list of permissions that come up on your phone screen when you do a download, and make a choice about whether they seem reasonable or weird. Does that bubble-popping game really need to access your contacts? Maybe it would be better to find a different game.

## Do a privacy audit of your favourite app!

*Here are two examples of privacy audits of popular apps conducted by students. Do you have these installed on your phone? Would you consider deleting either app now that you have a better understanding of the privacy risks involved with using those services? Consider auditing another one of your favourite apps to get a better understanding of how your privacy may be at risk.*

### — INSTAGRAM —



- Instagram can collect your email and share it with other companies connected with Instagram. Say hello to junk mail, my friend.
- Instagram has a function that allows you to “find friends”  giving Instagram access to contact lists or your other social media accounts, like Facebook.
- Instagram provides your information, including web pages you have visited outside of Instagram, to third-party analytics companies. This helps Instagram do things like measure user traffic and trends and send you targeted advertising.
- Instagram uses cookies that record information about your activities on Instagram. The cookies can also collect information about your browsing history on sites and services other than Instagram. All this information can be shared with companies outside of Instagram.
- When sharing your information with Instagram’s affiliates or third-party service providers, Instagram can decide whether or not to also include data that can identify you.
- If Instagram goes broke, your data is sold along with the company.
- Instagram does not knowingly collect info about kids under 13.
- Instagram may transfer your information, including personal information, to other countries where you don’t reside. That means that your data may be sent to be stored or processed in a country that has different laws about protecting your data than the country in which you live.
- Now for the big downer: even if you cancel your account, Instagram gets to keep your data!

## Do a privacy audit of your favourite app!

*Teens feel much too comfortable with Snapchat because of the unique “disappearing” photo messaging service they offer. The PPPP did a selective privacy audit of the new Snapchat privacy policy and there are some areas of concern to highlight.*

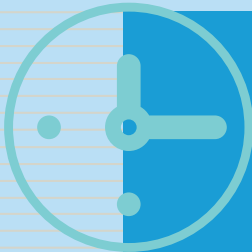
### — SNAPCHAT —



- The company says in its terms of service that users give it a “worldwide, royalty-free, sublicensable, and transferable license to host, store, use, display, reproduce, modify, adapt, edit, publish, and distribute that content for as long as you use the service.”\*
- What does this mean? It means Snapchat is reserving the right to do what it wants to with things you create and send. This works along with the privacy policy, which limits what it stores about you. Some kinds of chats get deleted quickly from its servers and won’t be available for use (like Snaps and Chats) and others get kept longer, like Live Stories and Memories. What is available also depends on how you set your privacy settings. Complicated, right?
- When you use Live or Local Stories, you are agreeing to let Snap Group and its affiliates and business partners “the unrestricted, worldwide right and license to use your name, likeness and voice” in “any and all media or distribution methods (now known or later developed).”\*
- This means that Snapchat is essentially getting permission to hold onto your information and publicly use it, even in ways you can’t imagine because they haven’t been invented yet. Again, you can control who can see your stories using your privacy settings, but the default is to share widely.
- Snapchat is allowed to share your information with other snapchatters, with its business partners and affiliates, and the public. It can also share with third parties, such as people who sell services to them or who provide functionality.
- There is a lot of information collected about you that Snapchat can potentially share, including your device information, which consists of the browser you use, the language it is set in, your wireless network, and your mobile network that includes your phonebook. Snapchat also gathers your location information. Of course filters about the city you are in would be impossible to use without gathering your physical location, but it is important to know that Snapchat does, in fact, gather your location services assessing for trends.
- Snapchat records the amount of times you use a certain filter and shares user data with the third parties that make the filters. Maybe you are very fond of the “flower crown” or perhaps the dog filter. Either way, Snapchat records the number of times a user uses specific filter.
- Of course Snapchat must have access to certain information so it knows which filters are most in demand, but remember the list of information it collects about you is quite extensive, and that gets shared too.
- Snapchat may process your data in the UK and US, where different privacy laws apply than in Canada.

\* <https://www.snap.com/en-US/terms/#terms-row>

## 4. When Your Watch Tells More than the Time



### — PRIVACY AND SECURITY IN MOBILE TECHNOLOGIES —

Wearable and mobile technologies are increasingly collecting personal information about location, health and fitness, and interactions across a range of our daily activities. Then, they make the information they collect accessible to a wide range of potential audiences. When you use these technologies (and let's face it, who leaves home without a cell phone most days?) you need to know the way these technologies work and the range of privacy risks inherent in producing and sharing this highly personal information. Many of the risks you face on mobile technologies are the same as those in the online world more generally, and then there are some, like location tracking, that are more specific to things like cell phones that you carry around on a daily basis. This section talks about a range of risks that occur online, whether you are using a desktop or laptop computer, a cell phone, or other mobile technologies.



### — WHAT IS WEARABLE TECHNOLOGY? —

Things like smart watches and fitness trackers are called “wearables”: technology that you put on and use to make life more convenient. It can be super useful to be able to see a text message flash on your watch without having to pull out your phone. It can be motivating to have a fitness tracker counting your steps and sending encouraging messages — “good job, you’ve reached your goal of 10,000 steps today!” But these devices also need to collect information about you in order to work, and sometimes they may collect more information than they need to work, or they might share information with the company that makes the product or other companies they partner with. There are some concerns, for example, that information from fitness trackers could be used by insurance companies to assess whether you are eligible for health insurance. There are also known security risks with some of these devices that can compromise the privacy of your information. It's always important to make informed choices when you decide to use these devices. Think about the benefits and risks, and decide your priorities.



## — WHAT IS LOCATION TRACKING AND HOW MIGHT IT BE USED? —

You might be aware that it is possible to track the location of your cellphone through GPS technology — you have probably noticed apps like Google Maps or Waze ask for this information. However, location tracking involves more than just GPS signals — your phone's Wi-fi capabilities can also be used to determine its location. In fact, locating your phone using Wi-fi signals is much more precise than GPS, and works even in places where GPS cannot, like in the subway.

Locating your phone using Wi-fi is somewhat technical and there are several different ways to do it. However, broadly, it is possible to determine your phone's location using Wi-fi signals because as you move through the world with your phone, it is constantly emitting signals searching for Wi-fi networks to connect to. It is possible to determine your phone's location by measuring how long it takes those signals to reach a Wi-fi router.

This method can also be used by third parties to figure out your location. This information is really valuable to stores, that want detailed information about their customers. Retail establishments can use your phone's Wi-fi signals to find out when you go into a store, and when you pass them by. Within the store, they can figure out what displays you stop in front of or what aisles you linger in. They may use this information to inform how they organize their stores or even to strategically send you advertising based on your location in the store. The data they collect could also be combined with information collected by other retailers. For example, a number of stores in a mall could develop a detailed profile of where you went on a shopping trip by combining together the information each collected about you individually. Of course, stores aren't the only ones who might want to track someone — this kind of information could be used in law enforcement, on one side, or by criminals, on the other.

### — WHAT IS ENCRYPTION AND WHY MIGHT YOU CARE? —

Encryption is essentially a technological method of changing information to make it unreadable, unless you have the key to put it back into its original form. It is a way of keeping information away from prying eyes, and making sure that even if it is intercepted, no one can read it. There are tools that encrypt information you send by default, such as some messaging services. There are also tools you can add to your email to encrypt messages. And places that have a duty to keep your information safe, like banks, use encryption to help them do so. Encryption isn't always foolproof, and usually it is only content, not metadata (remember metadata from the surveillance section?) that gets encrypted. But it is an important protection.

There has been public debate recently about whether there should be limits on the ability of people to use encryption, or limits to how strong encryption should be, because there have been situations where police or national security agents say it is affecting their ability to collect evidence from devices or through interceptions. This is sometimes called “going dark.” There are some really important things to consider in this debate. First, weakening encryption weakens privacy and security for everyone, everywhere, who use encrypted services in their daily lives. Second, reading information from devices is probably not the only way of collecting evidence, even though it can be an important one. And third, we need to be careful pitting privacy against security in conversations about encryption. It's really more about conflicts between data security and investigative needs, which are both important to public safety.

# Online security threats

When we use our computers and mobile devices to access the internet, we are also putting ourselves at risk of attack from a number of online security threats that can have really damaging consequences not just to our electronic devices but our lives. Below are some examples of the most common security threats so you know what to look out

for as you use the internet on all of your devices, followed by some practical tips on how to minimize your risk.

Malware is a term to describe any kind of software that is intended to harm a user or do damage to their computer systems. The following are some specific types of malware.

**SCAREWARE** scares users into purchasing a fake or harmful product to protect them from something terrible happening to their computer.

**How does it attack?** You may see a false internet advertisement or pop-up on your screen claiming it has found dozens of potential threats on your computer. In reality, these “threats” are either nonexistent or not a threat to your machine, but the scareware tries to convince you to purchase software like an anti-virus to eliminate the so-called threats.

**How can it harm you?** Not only does scareware trick you into making a purchase with your credit card, the software you download is often designed specifically to damage or **disrupt your computer**.

**What are the symptoms?** Generally any pop-ups or warnings that are designed to instil fear and panic are likely scareware.

**How to protect yourself:** Don't click any ads or download software from companies you don't trust or don't know. If you have a real security threat on your computer, do some research about which products are best to treat those threats before making any purchases.

**A VIRUS** is a program that is designed to attach itself to a file or program in your computer so that it can duplicate and infect other computers.

**How does it attack?** A computer can pick up viruses through normal web activities like sharing music, files or photos with other users; visiting an infected website; opening spam email or an infected email attachment from one of your contacts; downloading free games or software.

**How can it harm you?** Viruses can wreak havoc on your computer! They can damage programs; delete files; cause permanent damage to your hard disk; replicate themselves and infect other computers; flood networks with traffic and cause lagging with internet activity; use up computer memory; cause frequent computer crashes; send itself in emails to your entire contact list; steal your passwords and record your keystrokes to name a few!

**What are the symptoms?** Some signs your computer is infected with a virus are slow performance or odd erratic computer behavior; unexplained data loss; frequent computer crashes; or weird emails being sent to your contacts.

**How to protect yourself:** Use antivirus protection and a firewall and ensure that your protection and operating system is always up-to-date. Increase your browser security settings, avoid questionable web sites, evaluate free software and only download software from sites you trust. **Also practise safe email protocol:** don't open messages from unknown senders and immediately delete messages you suspect to be spam, even if the email is from someone you know.

**TROJAN HORSES** pretend to be programs that you want on your computer, but in reality they are a form of malware that harms your computer system and puts your personal information at risk.

**How does it attack?** Unlike viruses, trojan horses cannot replicate themselves. In order for Trojans to spread and infect a computer, the trojan horse program must be downloaded and installed by someone who has been fooled into thinking the trojan is actually a desirable program, like a game or screensaver.

**How does it harm you?** Trojan horses make your personal information very vulnerable to theft because it allows hackers to remotely access and control your computer. Not only can they steal the information stored in your computer, they can also delete important files or install other malware which can cause further damage to your computer and increase your privacy risks.

**What are the symptoms?** The most reliable way to determine if your computer is infected with a Trojan horse is to instal reliable and well-known malware protection software and run a scan for possible infections.

**How to protect yourself:** Be wary of downloading and running file attachments that are executables (i.e. files that end with .exe, .vbs, or .bat). Install malware protection and keep it up-to-date.

**RANSOMWARE** stops or limits a user from accessing their computer's operating system or files until they pay a ransom.

**How does it attack?** You may acquire ransomware by visiting certain websites, clicking on infected ad, opening emails or downloading content containing infected files.

**How does it harm you?** Ransomware is a way for criminals to extort money from you in exchange for allowing you access to your locked computer or critical files that have been encrypted. In some cases ransomware can also be used as blackmail where cyber criminals will threaten to send personal information, private videos or images to your contacts if you don't pay up. Even where a ransom is paid, full access to your computer and files may still not be restored.

**What are the symptoms?** Your computer will display a message or image to inform you that your data has been encrypted or locked, or threaten you with some other type of possible harm if you do not provide the required ransom. Ransom payments also have time limits in which you must comply or suffer consequences. Ransom threats may also be masked as a message from law enforcement agencies requiring you to pay a fine for engaging in your online activities.

**How to protect yourself:** Avoid opening unverified emails or clicking links embedded in them; regularly update software, programs, and applications to protect against security threats; and back up important files regularly using the 3-2-1 rule — create 3 backup copies on 2 different media with 1 backup in a separate location.

# Online security threats

**SPYWARE** gathers information about the user without his or her consent. Spyware falls into three general groups, domestic spyware, commercial spyware, and malicious spyware. Domestic spyware is usually purchased by an owner to help them monitor internet behaviours on their network systems. For example, your school may monitor students' use of school computers. Commercial spyware, on the other hand, is software that companies use to track your internet browsing activities, and this information is usually sold to marketers who then target you with advertisements. Malicious spyware is used by hackers to steal your information and use it to harm you.

**How does it attack?** You may be exposed to spyware by using a computer on which spyware was installed, visiting websites or clicking on ads or pop-ups that will download spyware to your computer without your knowledge. Sometimes spyware is downloaded to your computer as part of another program or app you have installed.

**How does it harm you?** Information about you is gathered without your consent, and even without you noticing. This can lead to serious risks for the security of important information that you would entrust in your devices. Domestic spyware could allow system administrators to look at your browsing history or emails. Commercial spyware could collect things like passwords, internet chats, and even your keystrokes and send them to individuals who wish to steal your identity.

**What are the symptoms?** Spyware can slow down your computer and has been known to increase the chances of computer crashes because it uses your computer's memory and system resources while it runs in the background. Since spyware will help download advertisements and send information to their "home base," this activity will use up a lot of your internet bandwidth that could be otherwise very valuable.

**How to protect yourself:** Be careful about what you download on your computer and resist clicking on pop-up ads. Install and regularly update malware protection software. Take the time to read the terms and conditions of free apps and programs that you install to flag anything that sounds like they are permitted to gather information about you, which could mean the information will be gathered through spyware.

**PHISHING** is not malware, but rather a method of scamming people for their money. People use emails, phone calls, and fake websites to pose as a real company, and trick the victim into providing their credit card, account logins, or other sensitive information. Some phishing scams may look and sound like the businesses they pretend to represent by copying actual images and logos from the real business' website.

**How to protect yourself:** Be very careful of anyone who asks you for personal information, particularly banking information, in an email, chat, or over the phone. Banks never contact customers to request your login information this way. When in doubt, visit your bank in person or research the company contacting you to determine if it is legitimate.

Generally, never send highly confidential information over email, or click on links from an email to sign on to your online accounts. Generally if an email, link or advertisement seems too good to be true, it's probably not real so avoid clicking or providing any information.

# Privacy protective technologies and tips

So, there are lots of ways for your information to be threatened. How can you protect yourself? Not all of these methods are right in every situation or for every person. The best thing you can do is to think about what risks exist in a situation and what you're willing to accept. It's OK to say, "I want to use a mapping app on my phone to help me find a place I'm looking for so I'm turning on location tracking." But you might want to turn it off if you don't need it. It's probably not smart to say, "I don't need anti-virus software on my computer." The PPPP team have put together some lists of pointers to help you protect your privacy and the security of your data on personal devices, with special attention to protecting your location and personal information.

## PROTECT YOUR LOCATION WHEN YOU'RE OUT IN THE WORLD

- If you're worried about location tracking, turn it off when you're not using it.
- Ensure your messages and picture messages do not tag your location. For example, you may not want to give your home address away by including location information with a photo of your cat.
- Be careful connecting to free Wi-fi networks. Most of them are safe, but they are probably all collecting information about you and may also facilitate tracking — if you have a few minutes, take the time to look at the terms of service for networks you might want to use often, such as at your favorite coffeeshop.

## PROTECT YOUR LOCATION WHEN YOU'RE BROWSING ONLINE

- There are tools you can use to shield your location.
- Proxy tools can hide your Internet Protocol address or assign a new, random IP number each time you use your computer. Using these proxies allows you to surf the internet with greater anonymity because it prevents websites from knowing your IP number. Do some research to see if one of these tools is right for you.
- A VPN (virtual private network) can provide a secure connection over the Internet between a user and the data they exchange or the websites they visit when connected. They encrypt the data that is exchanged across the connection. You can use a VPN on a computer or cell phone.

# Privacy protective technologies and tips

## THINK SECURITY! THERE ARE SEVERAL SIMPLE THINGS YOU CAN DO:

- Update your apps, computer, and phone software whenever you have the option. This is because almost all updates include things called security patches that close holes in the software that make it easier for someone to hack you. Make sure you keep your notifications on so you know when to update your software.
- Use two-factor authentication to access your accounts. This means that you have to go through another level of security beyond the simple username and password to get into your accounts. Some online services that offer this are Gmail, Evernote and Dropbox. A typical extra step of security is for your account to send a text message with a special code to enter after you try to login online. So if anyone other than you tries to log into an account and you have two-factor authentication via text message set up, you'll get a text message notifying you that someone is trying to hack into your account.
- Clear your cache. Now we already know that almost every teenager in the whole world already does this! Clearing your cache is extremely important to protect your privacy on your computer. Saved cookies, saved searches, and Web history could point to home address, family information and other personal data.
- Use strong passwords and keep them secret. There are tools, like password safes, that you can use to help you remember really complex passwords. There are also strategies you can use to make memorable passwords, such as using the first letter from every word of a wacky sentence. It can be hard to balance making passwords tough to guess but easy to remember, and really hard once you have 20 of them! One approach is to group together the accounts you have that require passwords based on the level of risk. For accounts where the consequences of a hack are low, have one password. Have another for medium risk things, and then have individual passwords for things that need very high security.
- Turn off "save password" feature in browsers. Even though it saves you the hassle of typing in your username and password every time you are logging into an account, it is not good to put that much trust into your browser where it might be accessible by malicious software, or even the next person who uses your computer without your knowledge.
- Put a sticky note on your camera. This might make you seem super paranoid; however, whistleblowers in the past have revealed that many organizations like the NSA can "spy" on American citizens through the front face camera on their computers and phones. The sticky note prevents any hacker or organization from spying on you and invading your privacy through your camera. Even though you might not have anything to hide, it's better to not have someone watching you!
- Use a firewall, which creates a barrier between your computer and the internet and only allows certain types of data to pass. For instance, a firewall may allow email exchange and web browsing but may disallow things like Windows file sharing. This way it helps stop any exchange of data from happening between your computer and the internet without you knowing it!
- Think about encrypting your data, and using services that have end-to-end encryption. There are great ones out there: do your research and make choices based on your needs and priorities.
- Think before leaving private data in the cloud! Online file-syncing services are very convenient services but are not the safest in terms of protecting your private information. Depending which service you use, data that you put in these services may be sitting unencrypted or protected with a layer of encryption beyond your control. Do some research to find more encrypted storage services with great privacy policies that will make sure your private data is safe.

“

*Passwords! If you don't want a hacker coming in to leak all your ... pics, you don't want to have a weak password. Trust me, I had a guy hack into my Facebook when FB wasn't dead and show everyone a video of me doing the chicken dance in Grade 4. Well, and also once a guy tried to hack into my World of Tanks profile and sold all my tanks! I realized that my password was something along the lines of :imanidiot. Well ... that certainly made me really pissed, as my accounts were vulnerable to attack at anytime.”*

## CELL PHONES NEED EXTRA PRIVACY PROTECTION. HERE ARE THE PPPP'S TOP 10 THINGS YOU CAN DO TO PROTECT YOUR PHONE.

- 1 **ALWAYS HAVE A PASSWORD FOR YOUR LOCK SCREEN** (The longer, the better, and never anything too obvious!)
- 2 **TURN YOUR LOCATION SERVICES OFF WHEN YOU DON'T NEED IT** 
- 3 **DON'T ALLOW AUTOMATIC CONNECTIONS** (Things like unknown Wi-fi servers can seriously put your phone and your information into potential danger.)
- 4 **ALWAYS CHECK THE PRIVACY SETTINGS FOR YOUR APPS AND CONSIDER WHETHER OR NOT THEY ARE WORTH KEEPING/INSTALLING** (Some apps ask a lot about your personal information- location, passwords etc.)
- 5 **DON'T STORE PASSWORDS AND IMPORTANT INFORMATION ON YOUR PHONE** (Store them in a device that you don't bring around with you, e.g. computer, tablet.)
- 6 **INSTALL ANTIVIRUS SOFTWARE ON YOUR PHONE** (Most data leaks are from virus problems!)
- 7 **DO NOT DOWNLOAD ANYTHING FROM AN UNKNOWN OR NOT TRUSTED SOURCE** (Chances are, they aren't safe!)
- 8 **TURN YOUR BLUETOOTH OFF WHEN YOU DON'T NEED IT** (You can be tracked from your bluetooth.)
- 9 **NEVER LEND YOUR PHONE TO ANYONE YOU DON'T KNOW** (risky!)
- 10 **BE AWARE OF YOUR SURROUNDINGS, AND STORE YOUR PHONE IN A SAFE PLACE** (To protect both the security and safety of your phone)

## 5. Online Reputation = Offline Impact

### — ‘STAYING WOKE’ ABOUT YOUR REPUTATION AND PRIVACY —

Teens need to ‘stay woke’ and be alert to privacy risks to reputation. But what do we mean when we talk about reputation online? What kinds of protections might assist in protecting reputation and privacy online? What are the risks, particularly for young people living their lives online? What rights do people have, or should they have, to protect their online reputations? What role do governments and corporations currently play in protecting people online, and what role should they play?

### — WHAT IS ‘ONLINE REPUTATION’? —

When you put something online, it can stay there for a long time, possibly forever. And, you can’t take it back — once you put something online, it can be almost impossible to remove it completely. When someone else puts something online about you, it’s exactly the same except you have even less control. People in high school now are the first generation of Canadians who have lived all of their life with access to the internet, and our society is still trying to work through how to develop rules, laws, and norms about how the huge amounts of information increasingly available about people can be used — or should be used — to affect their lives. Is it fair for potential employers to look at Facebook? Is it fair for police to monitor Twitter? Is it fair that anyone should be able to collect a whole bunch of information about us, analyze it, lump it in with the information of others, and make decisions about what to try to sell us or what services we deserve (this is one way big data works)? Who should be responsible for making the rules and enforcing them — governments? Companies? There are a lot of questions here, and the answers are going to have a serious effect on how people get judged and treated in the future, in both professional and personal relationships.

“

*Without knowing you,  
people often judge you  
based on what you post.”*

## — WHAT DOES ONLINE REPUTATION MEAN TO ME? —

*To me, online reputation means how other people view you when they look for you online. Online reputation matters because it is a literal way of knowing how someone is as a person, without physically knowing them. I always keep my posts clean and appropriate because I would like to get a good job in the future. Nowadays, employers check our social media accounts to get a feeling of how we are as a person, and it is best to make sure whatever posted online is appropriate, because once something inappropriate is posted on the Internet, it never goes away.”*

*“In my opinion online reputation means the digital footprints you leave online. As in real life, a footprint can be traced, so can one’s digital counterpart. Our online reputation will follow us everywhere we go. However through all this it is not to say that online activity is bad. If you were able to maintain a positive online reputation that could put you a step ahead of other peers and colleagues. It is important to not abstain from online activity as we live in a new and digital age where everything revolves around the internet, but to be able to maintain a positive online reputation. Instead of trying to hide ourselves from the world, we could portray our best versions of ourselves to the world.”*

*“I personally sense that more individuals are able to base their impression of me due to my social media use in comparison to those people who set their impression on me solely based face to face meetings. On social media, I have a larger amount of audience and it is important that the message that I send benefits me and doesn’t impact me negatively. I am aware of situations where individuals make a mistake that ruins their online reputation and they have no control over it because it is nearly impossible to completely take something back once it is posted. I am cautious of what I post, the posts I like, the requests I accept and the people I add because all of them have a contribution to provide a reflection on the type of person I am. Whenever I post anything online, I wish that only friends that I permit will view it; however, I am aware that can never be true. There will always be additional viewers who will obtain access that I may not have control over.”*

# Peer Privacy Protectors Share:

## Tips to protect your online reputation


Controlling your reputation in the physical world is difficult enough as it is, but protecting it online can be even more challenging. The truth is that nothing you post online will ever be truly private or secure. And, you can't take it back — once you put something online, it can be almost impossible to remove it completely. However, if you want to take action to ensure that your online presence remains untarnished, here are a few helpful tips and tricks to help you stay on top of how people see you online.

Not all tips will apply or appeal to everyone, and some of them will probably raise questions in your mind. The tip about how to create a positive image for a potential employer, for example, might make you wonder if employers should be allowed to use social media to evaluate job candidates at all. But all of these tips, written by the PPPP teens, provide things to think about when you are putting yourself out there online. Your future self will thank you.

### MAINTAIN A POSITIVE AND PROFESSIONAL PRESENCE

- Avoid hiding behind the screen: people are often careless about what they post online because it feels more impersonal. Avoid completely disconnecting from reality and remember that you should be mindful of how you conduct yourself online similar to how you would in face-to-face encounters.
- Try to think before you act: Think before you click on any link, and consider what effects your post or picture will have in your future. And since nobody always remembers to think before every single post, check out our hints for curating your online reputation!
- Consider using a codename or alias: Use a variation, or an entirely different name when making a social media account to keep personal and professional lives separate, keeping in mind that some sites have rules about how you identify yourself.
- Share your personal side — strategically. Focus your efforts in the area you'd like to be known for whether it's your business or writing. By becoming more conscious and aware of the power of your reviews, images and personal interests virtually, it's possible to take control and harness the positive power and advantages of your online reputation.
- Never cyber-bully anyone on social media. If word spreads about you doing so, expect your follower count and your reputation to be on a roller coaster plunging straight down from hero to zero.
- Remember, you have freedom of speech. You decide what you post, but you also have to take full responsibility for all your posts. Make your posts worthy of your values and beliefs.

## CURATE AND MONITOR

- Search yourself: Use different search engines (remember, Google isn't the only one) to search for yourself and comb through whatever results pop up. Do both a text search and an image search! Also put your name through social media search engines and look through those results.
- You can also have a Google alert on your name to keep track of any new content that is posted about you.
- Take the time to hide or remove any problematic content or information you do not want associated with your online identity. This could include reporting any inappropriate photos and removing tags to deleting unbecoming tweets and photos.
- Ask others remove negative content about you too. If you see that someone has posted a negative photo, video or comment about you, you should politely ask them to delete it because you can't.
- Regularly review your contacts, circles, friends and followers.
- Stay fresh  instead of trying to bury the past, look to building a new future. Update your accounts with professional and clean looking posts and photos because Google brings up the latest information, so when you update your accounts, fresh updates show up first.
- You can use the power of social media to enhance your public image. For example, if you're looking for a part-time job, it's probably safe to assume your boss might search for you on Facebook. Send out posts or updates promoting your recent work and that share your opinions on world issues. Often employers like to see their candidate's Twitter page to get a sense of their opinions and what drives them in life.

## PROTECT YOUR PRIVACY

- Take control of your privacy settings on social media. Facebook, Twitter and many other social media platforms have a privacy option, where you can limit the audience of your posts and photos. Turn on all of these privacy options so only you and your current friends can view your posts, rather than anyone who searches for your name.
- Protect your password: Not only should you make a complex password that can't be easily guessed, you should not share passwords with friends as it is meant for you to access your information. Even when friends 'hack' your account as a joke, it can still be damaging to your online reputation.
- Assume that nothing is private: if something will be truly damaging to your online reputation and would create major problems, then DON'T POST IT!

## GET INFORMED, BE CAREFUL, AND STAY ON TOP OF CHANGES TO THE ONLINE WORLD

- Remember that service providers often change things like terms of service including privacy policies. It's not enough to look at them once, you need to check for changes regularly.
- Do not enter personal information online unless you've checked the credentials of the website. If you feel as though they're asking for too much information, or weird information, listen to your instincts and find another site that does the same thing, because you almost always have choices!
- Don't talk to strangers: if you don't know who you are speaking to on the internet, be careful when disclosing confidential information. Anonymity online can be helpful in situations like mental health chatrooms, however you must exercise discretion because you never know who you are speaking to/who they will share your information with.
- Delete dormant accounts. Are you so totally done with Twitter? If you're positive that you are not going to revisit that old questionable account from when you were 13, delete the account.



## — WHAT IS THE ROLE OF GOVERNMENT AND CORPORATIONS IN PROTECTING ONLINE REPUTATION? —

We've provided a lot of tips for managing your own reputation, but there's another side to the issue. Do governments have a role to play, by making laws or regulations, and enforcing them, to make sure that information we share online is treated fairly? How about the companies that ask for our information (or track us without asking) and use it to improve their products, target their advertisements, and make money? Remember, sometimes we share information willingly, because we want to communicate, connect with friends and family, but sometimes we have to share information in order to get services, to buy things, and generally just to participate in daily life in the 21st century.

There are many different opinions about where responsibility should rest for keeping our information and reputations safe, and for deciding who gets to use it, and for what. Policies are going to be developed and discussions need to happen at all sorts of levels. No one has all the answers to what a perfect balance would look like between personal, corporate, and state accountability but it's an important conversation to have. What do you think?

One right that you have right now, under current laws, is the right to complain. If you are worried that information has been collected from you that shouldn't have been, or that information about you is being used inappropriately, you can stand up for your rights. Most companies address your rights to ask for information to be corrected or removed in their privacy policies, or terms of service. You might have to look hard to find them, but they should be available. If it is information collected under the *Privacy Act* or PIPEDA, you can file a complaint with the OPC. If it is information that would be collected by a provincial government, provinces have their own Privacy Commissioners. You can find more information on the CCLA website at [pppp.ccla.org](http://pppp.ccla.org).

*Privacy is important.  
You deserve it!  
The PPPP team hope  
we have helped you think  
about ways to protect  
YOUR privacy.*