Speaking Notes for a General Audience

TITLE SLIDE: A guide to protecting your privacy

[SECTION 1 / SLIDE 2: Privacy 101]

SLIDE 3: What we're talking about today – and why

- Many people have multiple devices and accounts, including social media, email accounts and more. Plus, many of us pay for products and services with cards, or even our phones.
- As we increasingly conduct our day-to-day lives online and using technology, it often means we're sharing our personal information, which can put us at risk.
- Today, we're going to talk about how to protect that information. The goal of this presentation is to help you know more about your privacy rights and how the government and businesses have a responsibility to protect your information.

SLIDE 4: Know your privacy rights

- How many of you trust businesses to protect your privacy? What about government?
- The good news is that in Canada, government and business both have a responsibility to protect your privacy.
- The right to privacy is actually rooted in the *Canadian Charter of Rights and Freedoms*. Plus, there are provincial and territorial laws designed to protect your privacy rights.
- The Office of the Privacy Commissioner of Canada (OPC) is responsible for overseeing two federal privacy laws: The *Personal Information Protection and Electronic Documents Act* (PIPEDA), which applies to some businesses in Canada, and the *Privacy Act*, which applies to federal government departments and agencies.
- These laws set out how the government and some businesses need to handle your personal information. As an example, businesses need to disclose how they're collecting and using your information, usually through your consent. They also must store and dispose of this information responsibly.
- Resource: Your privacy rights

SLIDE 5: What counts as personal information?

- PIPEDA protects information that is identifiable to an individual.
- What is personal information?
- Think of the things that make you unique, like your fingerprints. In the same way, there is data specific to your life, like your credit card information and tax returns.

SLIDE 6: Things like

- Personal information includes your:
    - Name, race, ethnic origin, religion, marital status, educational level;
    - Email address and messages, IP (Internet protocol) address
    - Age, height, weight, medical records, blood type, DNA code, fingerprints, voiceprint (the characteristics of your voice);

SLIDE 7: Things like (cont.)

- Income, purchases, spending habits, banking information, credit/debit card data, loan or credit reports, tax returns;
- Social Insurance Number (SIN) or other identification numbers.
- Personal information can also include the words you type, the websites you visit and the photos you post.

SLIDE 8: Businesses have an obligation to protect you

- From buying groceries at the store to shopping for clothes online to paying for a service like a renovation, modern commerce often involves personal information. But sharing your personal information with businesses doesn't mean giving up control over it.
- PIPEDA sets the ground rules for handling personal information in the course of commercial activities.
- It applies equally to small and big businesses, whether they operate out of an actual building or only online.
- PIPEDA requires businesses to collect, use or disclose your information by fair and lawful means, with your consent, and only for purposes that are stated and reasonable. Basically, they can only collect personal information that’s essential to their product or service. If they want more, you can ask why, and you’re entitled to decline to provide it, while still being able to complete your transaction.
- There are also three provinces (Quebec, British Columbia and Alberta) that each have their own very similar privacy legislation.
- Any time something does not appear to be required for the product or service to function, say “no” or ask the organization about it.
- Resource: Businesses and your personal information

[SECTION 2 / SLIDE 9: Exercising your rights]

SLIDE 10: Accessing your personal information

- If you want to know what personal information the federal government or a private business has about you, you have the right to have access to it.
- It should cost you little or nothing to access this information.
- The process should be fast. The organization is suppose to provide the information you've requested within 30 days. If they don't have it, they must advise you of that fact within 30 days.
- There are some circumstances in which that timeframe could be longer. For example, a federal institution may extend the response deadline by a maximum of 30 days if:
    - meeting the original time limit would unreasonably interfere with the institution's operations; or
    - consultations are necessary to comply with the request and cannot reasonably be completed within the original time limit.
    - The deadline may also be extended for a reasonable length of time if the personal information has to be translated or converted into an alternative format.
- The OPC has resources online to walk you through the process of requesting your information, and how to correct any factual errors you spot in your information, once you receive it.
- Resources:
    - Accessing your personal information – federal government
    - Accessing your personal information – businesses

SLIDE 11: Why privacy policies are worth your time

- Reviewing privacy policies are worth your time because they can help you make informed decisions about whether you want to share your information. It's tempting to skip ahead but make time to read through the information before clicking "Accept" or "I agree." If you don't like what you read, don't use the product or service.
- As we've talked about, organizations collecting personal information are required by law to inform users about their privacy practices.
- Good privacy policies should tell you clearly, specifically and in plain language how an organization is handling your personal information. That includes:
    - what information is being collected
    - with whom it will be shared
    - why it's being collected, used or shared, and
    - any risks of harm

- The OPC has tips online to help you know what to look for. In a nutshell, look out for details on how your information is collected, what the organization is using it for and how long they'll keep it.
- Resource: What to consider when reading a privacy policy

SLIDE 12: Have a privacy concern? Here's what to do.

- From time to time, you might be concerned about how an organization is handling your personal information.
- A good place to start is to bring up your concerns directly with the business. Often, they can resolve the issue quickly.
- If you're not satisfied with how the organization responds, you have every right to issue a complaint through the OPC. You don't need a lawyer or consultant to do it. Online, the Office of the Privacy Commissioner has a guide to the complaint process. It also has an information phone line staffed with officers to help answer specific questions you may have about privacy-related issues.
- Resource: Report a concern

SLIDE 13: Ask questions – and speak up!

- While reviewing privacy policies, keep an eye out for contact information, in case you have more specific questions. Sometimes there is a privacy officer listed. It never hurts to ask the organization questions if you're unclear.
- Remember, you're also well within your rights to speak up if you think your information isn't being handled right. Bring it up with the organization directly or launch a formal complaint through the OPC.
- You may be nervous about bringing up your concerns with an organization, but there's no need. It's your right. The OPC also has plenty of resources designed to help you engage the right person, have a productive conversation and protect yourself.
- Resource: Tips for raising your privacy concern with a business.

SLIDE 14: Ready to share? Think twice!

- Online and in person, we're constantly being asked for our personal information.
- Don't just give it up.
- Think about why the organization needs it, who will use it, and how. If you're not sure, ask.
- If you're not comfortable with the answers you receive, let the organization know, and don't give out your personal information. That might mean not using the product or service the organization provides.
- Resource: 10 tips for protecting personal information

[SECTION 3 / SLIDE 15: More ways to protect yourself]

SLIDE 16: Protecting yourself with privacy settings

- Before you sign up for a service or download an app, learn about what personal information is collected and the privacy controls available. If you're not comfortable, don't sign up for it!
- The best way to control your personal information online is not to hand it over in the first place.
- Obviously, it's not always practical or possible to withhold information, one way to try to contain potential privacy implications is to use privacy settings.
- Privacy settings aren't a silver bullet, but they can definitely give you more control over your information. It's important to know that default settings can leave you exposed.
- Settings help you indicate whether or not you give consent for the collection, use and disclosure of your personal information. That's why it's important to choose privacy settings that you are comfortable with on all social media accounts, online services, devices and browsers.
- You should know that you have a right to say "no" to providing personal information that isn't integral to the product or service. Look for options to turn off actions like accessing your microphone or tracking your location if those actions are not required to use the service.
- It's important not to "set it and forget it" with your privacy settings. A lot of sites change their privacy settings frequently, so check back often to make sure you're still comfortable with what you're sharing.
- Resource: Tips for using privacy settings

SLIDE 17: Don't forget your devices

- Set device passwords that are difficult to guess. That way, if you leave your phone somewhere by mistake, it's much more difficult for someone to access your personal information.
- You can also install anti-virus and security software on your devices. Be sure to keep this software updated.
- Be sure to delete all personal information from your old devices (like your phone, laptop or tablet) before discarding, recycling or selling them. It's worth noting that even restoring electronics to factory settings doesn't permanently delete the data. Check with the device manufacturer.
- The OPC has information specific to managing privacy on your mobile devices.

SLIDE 18: Safe surfing

- The good news is that your internet browser has built-in tools to help protect your personal information. Take some time to learn about the security and privacy settings in your browser and keep them up to date. If you use different browsers (such as Chrome and Safari), check the settings in each one.
- While not foolproof, look for the lock icon, HTTPS protocol or green highlighting in the address bar. These are all signs the site is likely secure.
- When surfing on public Wi-Fi, avoid sensitive transactions such as online banking as the connection is not secure and others may be able to capture the data you are sending.
- You should also disable Wi-Fi and Bluetooth when you are not using it – when you leave your device open by default, you leave your data vulnerable to access by others without your knowledge or consent whenever you pass through cafés and other places offering open, public wireless networks.

SLIDE 19: What about passwords?

- Passwords are essential to keeping your personal information safe. Weak passwords and default passwords can leave you at risk.
- It's tempting to stick with one password for everything, but that's not the best way to protect your information. If one password gets compromised, you may risk access to dozens of your other accounts.
- When choosing a password, avoid obvious choices such as your mother's maiden name, child's name, pet's name, or other references that someone may be able to guess through information you have posted elsewhere.

SLIDE 20: Here's a tip

- Choose a strong password that is easy for you to remember but hard for others to guess. Make your password length 15 or more characters.
  - Passphrases should contain at least four unique words strung together—an easy way to select words is to use associations, like four items that you may find in your living room such as "Lamp Computer Toys Curtains."
  - Or, use a complex password if you cannot use a passphrase or if the password must be shorter than 15 characters. Complex passwords should contain a mix of letters (lowercase and upper case), numbers, and symbols, for example "L@mp*c0mput3r!".
- If you need to write passwords down to remember them, keep them offline in a secure place, such as a locked cabinet. Don't post a password in plain sight or where someone might find it.
- Don't use the "remember password" feature on your browser or device. Automatic logins can be convenient, but are not a good idea if you are sharing a computer.
- Be sure to always change default passwords that come with new devices or accounts. You should also use the automatic lock feature on your devices (meaning, set your phone to lock after a certain amount of time has elapsed and require you to log back in).

- **Are there any parents here?** Here's a tip for you: if you decide to ask your children to share their passwords with you, make sure that they understand that this is a special exception, just between you. They should never share their passwords with anyone else, including their friends.
- The OPC has more great tips for choosing and using passwords effectively.
- Resource: Tips for creating and managing your passwords

SLIDE 21: Don't fall victim to identify theft

- Identity theft occurs when someone takes information about you and pretends to be you for fraudulent purposes.
- Every year, thousands of people are victims of identity theft. Your name, date of birth, address, credit card, Social Insurance Number (SIN) and other personal identification numbers can be used to open credit card and bank accounts, redirect mail, establish cellular phone service, rent vehicles, equipment, or accommodation, and even secure employment.
- If you are a victim, the consequences are serious. For example, you can be denied a driver's license or cell phone service and it can take years to undo the damage.
- There are several ways identity thieves gain access to information, but there are also plenty of ways to protect yourself.
- Online, use strong passwords and privacy settings.
- Review all credit card and bank statements to make sure there are no unauthorized purchases.
- Don't give out credit card numbers or other personal information over the phone unless it's to a trusted person or you initiated the call yourself.
- Carry only essential ID such as your driver's licence and health card. Leave your SIN card, passport and birth certificate in a safe place at home.
- When it comes to paperwork, discard your information securely. Shred old bills, statements or other paperwork that has your personal information on it.
- Resource: Identity theft and you

SLIDE 22: The spam threat – it's beyond your inbox

- Spam messages are annoying, but they also pose a threat to privacy. Spam emails or texts can actually include malware or spyware, used to gain access to your personal information.
- One simple way to avoid spam is not to post your email address online publicly. Spam starts with a practice called "address harvesting," where computer programs indiscriminately collect email addresses that are sold to spammers.
- You can also set up a separate email account only for joining online communities or filling out forms and using a different primary account for communications with trusted

contacts. That way you can easily change the extra accounts if they are harvested and you start receiving spam.
- Protecting yourself from spam goes beyond your inbox. Keep your devices – your computers, phones and tablets – all safe with security software (anti-virus and anti-malware software) that you download from a trusted source. Be sure to keep your software up-to-date.
- Resource: Top 10 tips for protecting your inbox, computer and mobile device

SLIDE 23: Tips to stay safe from spam

- Don’t open e-mails from an unfamiliar person or organization. Deleting mail from unknown senders can avoid a host of future problems.
- If you do open a message, don't reply to spam as that can confirm your address as being active and cause you to receive more spam. For the same reason, never click on a "remove" or "unsubscribe" link in a suspicious spam message. You may be unwittingly “subscribing” to receive even more spam.
- Never click on links or attachments in an email if the message is suspicious. They may be harbouring malware, which, if unleashed, can jeopardize your privacy or compromise your device.
- You can also report unsolicited e-mail containing suspicious attachments or content to the Spam Reporting Centre at www.fightspam.gc.ca.

SLIDE 24: Staying safe on social media

- How many of you use social media? Keep your hand up if you use social media more than once a day. Twice a day? Five times a day? More?
- Social media can be great for staying in touch with friends and family, sharing photos and videos. But it can also put your personal information at risk.
- Understand and manage the different privacy settings on all your social media accounts. Review privacy policies before signing up, and review settings regularly to make sure you’re still comfortable with the options you’ve chosen.
- Be sure to choose strong passwords that are unique to your different social media accounts.
- Log out of your accounts when you’re not using them. If you’re not using an account anymore, ask the company to delete your account and your data. Simply deactivating an account or deleting the app from your device isn’t the same, since all your data will remain on the company’s servers.
- Be mindful of the information you post, including photos that might show personal information. Be considerate, too. Ask others before you post photos, videos or information that they’re in whether they’re comfortable with what you’re sharing.

- Remember to also consider how the information you post online may impact the offline world. Think twice about comments or images you share that could harm your reputation or the reputation of others.
- Resource: Staying safe on social media

SLIDE 25: Summary

- Know your privacy rights.
- Ask questions when businesses ask for your information.
- Keep your information safe with strong passwords, privacy settings and security software.
- Surf safely. Make sure you're using a secure website when doing transactions online, and turn off Wi-Fi and Bluetooth when you're not using them.
- Protect yourself from identity theft by limiting what information you share and carry, using strong passwords, and shredding sensitive information.
- Be wary of spam messages – never reply or click on links in spam messages.
- Be cautious about the information you share on social media. Respect the privacy of other people.

SLIDE 26: Where to learn more

- This presentation was produced by the Office of the Privacy Commissioner of Canada (OPC). The OPC's job is to enforce federal privacy laws. Canadians can turn to the OPC for information on privacy, or bring forward privacy complaints and concerns to its office.
- The Office supports the Privacy Commissioner, who is an independent agent of Parliament.
- For more tips on how you can protect your privacy, please visit www.priv.gc.ca