Protecting Yourself from Online Schemes and Scams

March 13, 2024 **Jasmine Samra & Brent J. Arnold**

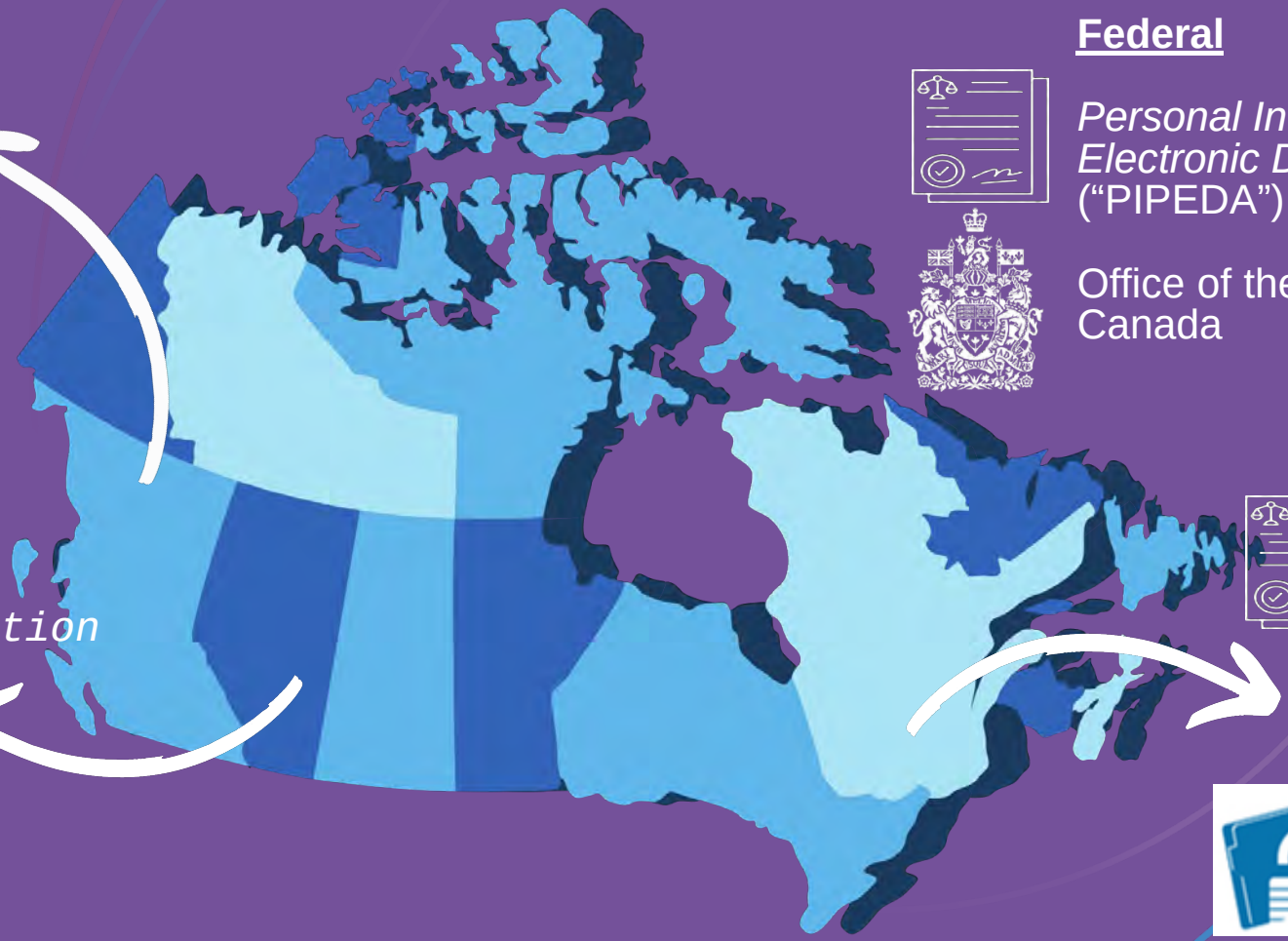
GOWLING WLG

Agenda

Topic
Privacy Laws
Your Rights under Privacy Law
Privacy Settings
Online Scams to Look For
Protecting Yourself Online
Questions?

GOWLING WLG

Canadian Private Sector Privacy Laws*



British Columbia

Personal Information Protection Act ("PIPA BC")

Office of the Information & Privacy Commissioner for British Columbia

Alberta

Personal Information Protection Act ("PIPA AB")

Office of the Privacy Alberta

Federal

Personal Information Protection and Electronic Documents Act ("PIPEDA")

Office of the Privacy Commissioner of Canada

Québec

Act respecting the protection of personal information in the private sector ("Québec Act")

Commission d'Accès à l'Information

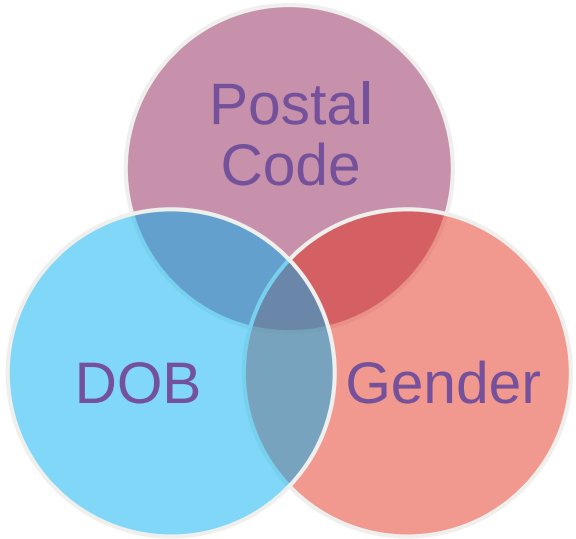
* Canada also has federal and provincial legislation governing the public sector, and sector-specific legislation governing personal health information held by "health information custodians".

GOWLING WLG

Personal Information

- “Personal information” is “information about an identifiable individual”.
- “Information will be about an “identifiable individual” where there is a serious possibility that an individual could be identified through the use of that information, either alone or in combination with other information”.

Personal Information



Source: Office of the Privacy Commissioner of Canada, https://www.priv.gc.ca/en/about-the-opc/publications/illustrations/#h20

GOWLING WLG

Obligations on Companies Collecting Your Data

Business Must:	
1. Obtain Valid, Informed Consent	6. Be Accurate about your Information
2. Be Accountable	7. Use Appropriate Safeguards
3. Identifying Purposes of Collection	8. Be Open with you
4. Limit Scope of Collection	9. Give you Access to your information
5. Limit Use, Disclosure and Retention	10. Provide a method to Complain or Challenging Compliance

Source: Office of the Privacy Commissioner of Canada, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/guide_org/

Your Rights Under Privacy Law

- Canadian privacy legislation ensures that:

1. You have the right to access and correct any information a company has about you.
2. Companies can't post your personal info unless you consent, and they are required to keep it up-to-date
   - Problem: you may have given consent without even knowing it
3. You *don't* have a "right to be forgotten"—e.g. can't demand that search engines drop you from search results (available in EU and Quebec.)

Protecting Yourself Online

Before You Sign Up:

- Learn what personal information a service or app collects.

Explore Privacy Settings:

- Default settings might not offer enough protection, so explore and adjust privacy settings.
- Does the app really need access to your location, contacts, calendar, photos, cameras and microphone?
- Look for options to disable location-based settings or limit tracking to when you're actively using the service.

Source: Office of the Privacy Commissioner of Canada, https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/online-privacy/gd_ps_201903/

Protecting Yourself Online

Coordinate Settings Across Devices:

- Keep your privacy settings consistent across different devices for added security and control.

Regularly Review and Adjust:

- Review your privacy settings often as they can change regularly.

Source: Office of the Privacy Commissioner of Canada, https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/online-privacy/gd_ps_201903/

Protecting Yourself Online

Passwords:

- Use strong, unique passwords for each account to prevent unauthorized access
- Avoid using easily guessable information like family names or birthdates in passwords
- Consider creating passwords using acronyms or phrases
  to make them memorable but difficult to guess
- Where available enable MFA
- Consider using a password manager

Source: Office of the Privacy Commissioner of Canada, https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/online-privacy/tips_pw/, https://www.priv.gc.ca/en/about-the-opc/publications/illustrations/#h20

GOWLING WLG

Online scams to watch out for: Tax season

- Tax season scammers pose as representatives of the CRA to try and trick you into sending money for fake debts or providing sensitive personal information they can use to commit fraud.
- **NEVER CLICK LINKS FROM UNFAMILIAR PHONE NUMBERS**
- **Example of scam texts:**

1. Your tax refund is now available. Click here to receive your payment
2. You owe money to the CRA. We will send your file to a collection agency, contact us now
3. You have a refund of $3,000 this year. Click here to initiate the claim process.

Online scams to watch out for: Tax season

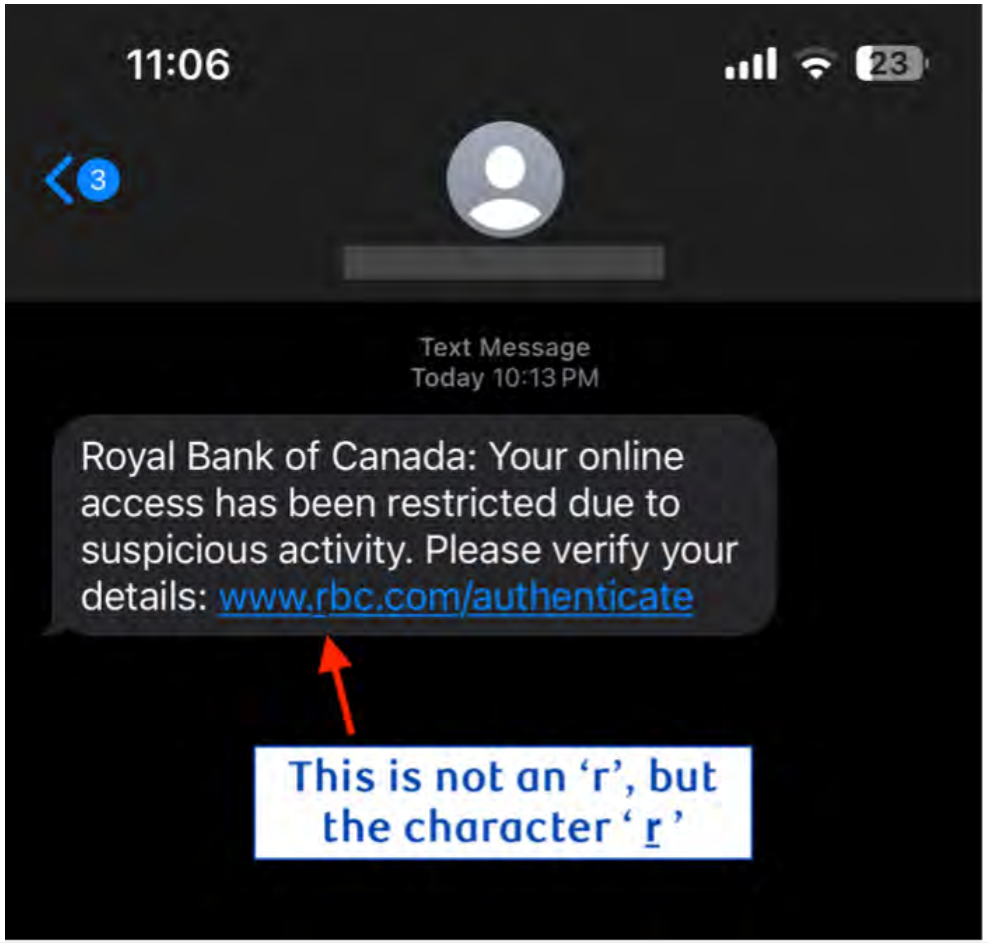
Latest scam alerts

- **Text message scams containing personal information**
  Scammers are sending text messages claiming to be from the CRA that may contain personal information.
- **Canada Carbon Rebate (formerly known as Climate action incentive payment) scam by text message**
  Scammers are sending text messages claiming to be from the CRA about the Canada Carbon Rebate.
- **Emergency or disaster benefit scams by text message or email**
  Scammers are sending text messages or emails to those impacted by emergencies or disasters.
- **Grocery Rebate scam by email or text message**
  Scammers are sending emails or text messages claiming to be from the CRA about the Grocery Rebate.
- **Cryptocurrency scam by phone**
  Scammers targeting individuals by phone, requesting money be transferred via cryptocurrency to cancel an RCMP warrant for their arrest.
- **GST/HST tax refund/credit scam**
  Scammers are targeting individuals by text message or email, claiming that the CRA is sending them a GST/HST tax refund or credit, and are requesting personal information to proceed.
- **Text message scam to access your CRA accounts**
  A text message scam impersonating the CRA to gain access to your CRA accounts.
- **Text or instant message offering a refund**
  A text message scam impersonating the CRA to offer fake refunds to Canadians. This is known as phishing.
- **Fraudulent tax returns - identity theft**
  Scammers acquire personal information (such as user ID and passwords), and file fake tax returns in your name. This is referred to as identity theft and targets all Canadians.

Source: CRA website: https://www.canada.ca/en/revenue-agency/corporate/security/protect-yourself-against-fraud/scam-alerts.html

GOWLING WLG

Online scams to watch out for: Punycodes



Current Scam Alerts - RBC

GOWLING WLG

Online Scams To Watch Out For: AI Scams

- Be cautious of hyper-realistic fake videos and images (deepfakes)
- Watch for highly personalized phishing emails, often too good to be true
- Common AI scam tactics:
    1. Fake AI chatbots mimicking real customer support to steal information.
    2. Scammers using AI to create convincing fake social media profiles.
    3. Voice cloning used in phone scams pretending to be trusted individuals.

Online scams to watch out for: AI Scams

Scammers can easily use voice-cloning AI to con family members: expert

Regina woman believed her grandson was on the line asking for help

Aishwarya Dudha · CBC News · Posted: Jun 18, 2023 6:00 AM EDT | Last Updated: June 19, 2023

A 75-year-old woman in Regina is a victims of the grandparent scam. She and her family believe voice cloning technology was used to impersonate her grandson to scam her for over $7000. (CBC News)

Source: CBC News
Scammers can easily use voice-cloning AI to con family members: expert | CBC News

GOWLING WLG

Protecting Yourself Online

- Don’t click unfamiliar links / attachments
- Update your OS, apps
- Encrypt your computer
- Backup your data on cloud or external storage
- Don’t repeat passwords -- be random
- Two-factor ID
- Cover your webcam with tape
- Stay informed about the latest online scams

Source: New York Times, Nov. 16, 2016, https://www.nytimes.com/2016/11/17/technology/personaltech/encryption-privacy.html?emc=eta1&_r=0

Protecting Yourself Online

- Watch out for fake websites asking you for info:
  1. Domain name (url)—does it look like the real site?
     - Secure websites use https instead of http – this isn't fool proof the absence of https on a website requesting personal information is a red flag.
  2. Spelling / grammar mistakes
  3. How long has it been online?
  4. Who owns the domain? (https://ca.godaddy.com/whois)
  5. Err on the side of caution, if something feels off about a website, avoid providing any personal or financial information.

Protecting Yourself Online

- **Watch out for phishing emails:***
    1. The message contains a mismatched URL
    2. URLs contain a misleading domain name or *punycode*
    3. The message contains poor spelling and grammar
    4. The message asks for personal information
    5. The offer seems too good to be true
    6. You didn't initiate the action
    7. You're asked to send money to cover expenses
    8. The message makes unrealistic threats

http://www.techrepublic.com/blog/10-things/10-tips-for-spotting-a-phishing-email/

Actions to Take for Identity Fraud/Theft

1. If the incident involved theft or crime, report it to the local police.
2. If the incident involved a scam or fraud, report it to the Canadian Anti-Fraud Centre at: https://antifraudcentre-centreantifraude.ca/report-signalez-eng.htm
3. Inform banks and credit card companies and request new cards with new numerical identifiers to prevent further unauthorized use.
4. Report any missing identity documents (e.g., driver's license, health card) to the appropriate organization.

Source: Office of the Privacy Commissioner of Canada, https://www.priv.gc.ca/en/privacy-topics/identities/identity-theft/guide_idt/

Questions?

GOWLING WLG

Who to contact

Brent J. Arnold is a partner practising in Gowling WLG's Advocacy department, specializing in cyber security and commercial litigation. He acts for plaintiffs and defendants in data breach-related litigation, and serves as breach coach / counsel for companies affected by cyber attacks. In 2019, he co-authored the Canada chapter of Chambers *Global Practice Guide: Data Protection & Cybersecurity*, 2nd ed. In 2022, he co-authored the Canada chapter of the Chambers *Fintech 2022: Trends and Developments* report.

Brent chairs the Steering Committee for the Cybersecurity and Data Privacy section of the U.S.-based Defence Research Institute (DRI), and is past chair of the Ontario Bar Association's Privacy and Access to Information Law Committee. He currently serves on the Ontario Bar Association Council.

He is a Director of the Canadian chapter of the Internet Society, a global organization devoted to improving the affordability, accessibility, fairness and security of the internet. He is also a member of The Advocates' Society's Artificial Intelligence & Automated Decision Making Task Force, and International Associationn of Privacy Professionals, and the International Association of Defense Counsel.

Brent J. Arnold
Partner & Data Breach Coach / Counsel,
Advocacy Department
Toronto

+1 416-369-4662
+1 416-347-2737
Brent.Arnold@gowlingwlg.com
www.linkedin.com/in/brent-arnold-cyberlawyeryyz
cyberlawyeryyz
@cyberlawyeryyz.bsky.social

GOWLING WLG

Who to contact

Jasmine Samra is recognized as a certified information privacy professional by the International Association of Privacy Professionals. Jasmine advises clients on a broad range of privacy and cyber security issues across a variety of industries. She advises companies on privacy compliance and data protection issues, and helps organizations develop privacy compliance programs, privacy and social media policies. Jasmine provides privacy advice in connection with corporate transactions, outsourcing arrangements and transborder data flows.

Jasmine has extensive experience in requests under Canada's Access to Information Act and provincial freedom of information legislation, and assists clients in protecting confidential third-party business information under these laws. She also helps clients manage and respond to data breaches and other privacy-related incidents.

She regularly advises on compliance with Canada’s Anti-Spam Legislation and has created anti-spam compliance policies and programs.

Prior to joining Gowling WLG, Jasmine served as senior counsel at one of Canada's largest financial institutions. In this role, she was responsible for providing legal advice with respect to a range of issues affecting the privacy, cyber security and social media for various lines of businesses.

Jasmine Samra

Counsel

Toronto

+1 416-369-6676

Jasmine.samra@gowlingwlg.com

www.linkedin.com/in/jasmine-samra-02aa2254

GOWLING WLG

GOWLING WLG