

Privacy – 2023 Year in Review



FEDERAL

LAWS & ANNOUNCEMENTS

Mar 7: The Privacy Commissioner revised its [guidelines](#) on the privacy risks of faxing personal information. Tips:

- Choose a machine that encrypts transmissions and requires users to key in a password to access and print the fax.
- Keep fax machines used to send or receive personal information in a secure area so unauthorized people don't see faxed documents.
- Before sending a fax, check that the receiver's number is correct, then verify in the machine's display window that you've keyed it in correctly.
- Only fax personal information that you'd feel comfortable discussing over the phone.

Action Point: [Avoid privacy violations](#) when using digital technology to monitor employees

May 29: The Office of the Privacy Commissioner published [new guidelines](#) on workplace privacy, including with regard to the use of software and other electronic solutions to monitor employees without violating PIPEDA and other personal privacy laws.

Action Point: [Avoid privacy violations](#) when using digital technology to monitor employees

Jun 29: The Office of the Privacy Commission offered [new instructions](#) to help businesses and individuals protect privacy on mobile apps. Many organizations that use apps to improve their customer interactions collect clients' personal information to do so, the Commission notes.

Aug 24: The federal Office of the Privacy Commission joined its global counterparts in issuing a [joint statement](#) calling on social media companies and other operators of websites that host publicly accessible personal information to take stronger measures to protect the private personal information of their users from illegal AI data scraping programs.

Action Point: Find out the 12 things you should do to [prevent data breaches](#) at your workplace

ALBERTA

LAWS & ANNOUNCEMENTS

May 25: The privacy commissioners of Canada, Alberta, BC and Quebec will jointly investigate OpenAI, the artificial intelligence company that operates ChatGPT, to ensure that it's secured "valid and meaningful consent" to collect, use and disclose personal information of individuals in Canada via the new app, which has gained over 100 million worldwide users since its release last November.

Action Point: Guard against ChatGPT risks by implementing a legally sound [workplace artificial intelligence use policy](#)

CASES

Privacy: Lunchroom Security Cameras Can Stay but Workers Must Be Notified

The union objected when a grocery store unilaterally installed surveillance cameras in the small lunchroom of a remote area warehouse in which all workers had no realistic alternative but to take their breaks. The company contended that the cameras were there to monitor security not productivity, which is far more problematic under privacy laws. Moreover, the cameras were in plain view and not monitored in real time. While ruling that the cameras could stay given the history of security incidents at the site, the Alberta arbitrator ordered the employer to post signs and add language to its theft policy making it clear to workers that:

- The cameras are there;
- The video recordings aren't accessible remotely;
- Only limited personnel have access to the recordings and only as needed to investigate a security incident; and
- The recordings are deleted within 6 months after they're made

[[Teamsters Local Union No. 987 of Alberta v Sobeys Capital Incorporated \(Rocky View\)](#), 2023 CanLII 4464 (AB GAA), January 16, 2023].

Action Point: Implement a legally sound [video surveillance policy](#) at your workplace

BRITISH COLUMBIA

LAWS & ANNOUNCEMENTS

Jan 27: The BC Privacy Commissioner called on the province to beef up privacy law protections to prevent data breaches in the private sector the way it has for the public sector.

Action Point: Find out the 12 things you should do to [prevent data breaches](#) at your workplace.

Mar 6: Newly tabled [Bill 12](#), the *Intimate Images Protection Act*, would make it easier for victims whose intimate photos or images have been published without consent to get the postings taken down and sue the person(s) who posted them for money damages.

May 4: BC sent letters to Twitter, Tinder, Meta, Grindr, Pornhub and other social media companies of their duties to immediately stop distribution or remove intimate images that were posted without the subject's consent from their platform or face court orders, fines and other penalties under newly passed [Bill 12](#), the *Intimate Images Protection Act*.

Action Point: Protect your organization from [revenge porn and cyberbullying liability](#)

Sep 13: A new BC Office of Information and Privacy Commission report finds that the Provincial Health Services Authority has taken "meaningful steps" to bolster the security of the Provincial Public Health Information System (System) used to track the spread of COVID-19 and other infectious diseases.

MANITOBA

LAWS & ANNOUNCEMENTS

Mar 13: First Reading for [Bill 27](#), which would make it easier for victims whose intimate images are published without consent to collect money damages by establishing the presumption that published images were nonconsensual. The accused would then have the burden of proving that they had reasonable grounds to believe that the accuser did consent to the publication.

Mar 30: Newly passed [Bill 12](#), the *Intimate Images Protection Act*, makes it easier for victims whose intimate photos or images have been published without consent to get the postings taken down and sue the person(s) who posted them for money damages.

Apr 12: Second Reading for [Bill 27](#), which would make it easier for victims whose intimate images are published without consent to collect money damages by establishing the presumption that published images were nonconsensual. The accused would then have the burden of proving that they had reasonable grounds to believe that the accuser did consent to the publication.

May 16: Third Reading for [Bill 27](#), which will make it easier for victims whose intimate images are published without consent to collect money damages by establishing the presumption that published images were nonconsensual. The accused will then have the burden of proving that they had reasonable grounds to believe that the accuser did consent to the publication.

Action Point: Protect your organization from [revenge porn and cyberbullying liability](#)

May 30: Royal Assent for [Bill 27](#), which makes it easier for victims whose intimate images are published without consent to collect money damages by establishing the presumption that published images were nonconsensual. The accused will then have the burden of proving that they had reasonable grounds to believe that the accuser did consent to the publication.

Action Point: Protect your organization from [revenge porn and cyberbullying liability](#)

NEW BRUNSWICK

LAWS & ANNOUNCEMENTS

Jun 22: That's the deadline to comment on a proposed *Personal Health Information Privacy and Access Act* [regulation change](#) that would allow a public body to collect and use an individual's Medicare number for purposes of identifying and verifying the identity of an individual in the health care system.

Action Point: [Avoid privacy violations](#) when using digital technology to monitor employees

NEWFOUNDLAND & LABRADOR

LAWS & ANNOUNCEMENTS

Feb 8: The Newfoundland Privacy Commissioner began public review of the *Personal Health Information Act* limiting the collection, use and disclosure of private medical information without the individual's written consent. To participate, email phicareview@gov.nl.ca before March 1.

Action Point: [Avoid privacy violations](#) when using digital technology to monitor employees.

May 24: Newfoundland completed legally required 5-year review of its personal health

information and privacy laws and what, if anything, should be done to improve and modernize them.

Action Point: [Avoid privacy violations](#) when using digital technology to monitor employees

NOVA SCOTIA

LAWS & ANNOUNCEMENTS

Jun 20: According to the Nova Scotia Office of Information Privacy [2022 Annual Report](#), there were 678 privacy breaches reported by provincial agencies under the *Personal Health and Information Act* during the past year, affecting protected health information of 12,188 individuals. Nova Scotia Health reported the most breaches by far, with 507, followed by IWK Health Centre with 102.

Action Point: Find out the 12 things you should do to [prevent data breaches](#) at your workplace

NORTHWEST TERRITORIES

LAWS & ANNOUNCEMENTS

Apr 18: The GNWT announced that a break-in at the department of Education, Culture and Employment's headquarters in Yellowknife might have compromised the personal data of approximately 3,000 individuals. The data was contained on Income Assistance Program files kept on computer hard drives that were stolen.

Action Point: Find out the 12 things you should do to [prevent data breaches](#) at your workplace

NUNAVUT

LAWS & ANNOUNCEMENTS

Sep 13: A new Department of Community and Government Services' Consumer Affairs Section [bulletin](#) cautions Nunavut residents to beware of identity theft, while offering tips on how to avoid it and what to do if you've been victimized.

Action Point: Find out about the 12 things you should do to [prevent data breaches](#) at your workplace

ONTARIO

LAWS & ANNOUNCEMENTS

Jan 25: The Ontario Privacy Commissioner sent a [letter](#) asking the Ministers of Labour and Public and Business Service Delivery to work together to create new laws to limit employer surveillance over and strengthen workplace privacy protections of workers. Employer "surveillance can invade an employee's home and capture intimate details of family life that are not relevant to an employee's professional capacity," the letter notes.

Action Point: Find out the 12 things you should do to [prevent data breaches](#) at your workplace

May 25: Ontario's Privacy and Human Rights Commissioners issued a joint statement calling on the government to develop "robust and granular rules" on the use of artificial intelligence technologies in the public sector. While AI technologies can greatly benefit society, they also rely on immense volumes of personal information that may not be properly protected, the Commissioners warn.

Action Point: Find out how to implement a legally sound [workplace artificial](#)

[intelligence use policy](#)

QUÉBEC

LAWS & ANNOUNCEMENTS

May 25: The Québec Information Access and Privacy Commission will join its federal, Alberta and BC counterparts in jointly investigating OpenAI, the artificial intelligence company that operates ChatGPT, to ensure that it's secured "valid and meaningful consent" to collect, use and disclose personal information of individuals in Canada via the new app, which has gained over 100 million worldwide users since its release last November.

Action Point: Guard against ChatGPT risks by implementing a legally sound [workplace artificial intelligence use policy](#)

SASKATCHEWAN

LAWS & ANNOUNCEMENTS

Aug 1: Updated *Health Information Protection Act* regulations took effect in Saskatchewan. [Key changes](#) include new privacy protections for genetic information and limits on trustees' collection, use and disclosure of personal health information.

Action Point: Find out about the 12 things you should do to [prevent data breaches](#) at your workplace

YUKON TERRITORY

LAWS & ANNOUNCEMENTS

Sep 14: The government had to shut down from noon to 4 pm as a result of a cyberattack targeting the Yukon.ca website. While the threat continued, the government was effective in responding to the attack and was able to restore 90% of the disrupted services by the morning of Sept. 15.

Action Point: Find out about the 12 things you should do to [prevent data breaches](#) at your workplace

Nov 2: [Bill 32](#), the *Victims of Crime Act*, making it harder for those convicted or accused of a crime to access personal information about victims that might compromise the latter's privacy and safety received Royal Assent and officially took effect. The law won't impact access to employment records by current or former employees nor to victims' access to their own records.

Action Point: Find out about the 12 things you should do to [prevent data breaches](#) at your workplace