cenera people • strategy • solutions

Top 10 Privacy Issues for HR

OR “how I learned to accept that privacy isn’t going away, especially in HR”

Access and Privacy Legislation

Legislation	Applies to	Information Scope
Freedom of Information and Protection of Privacy Act (FOIP)	**Public Bodies** Municipalities, Universities, Schools, Health Regions, Lodges, Nursing Homes.	All records, including personal information.
Health Information Act (HIA)	**Custodians/Trustees** Health professionals, health regions, Ministry.	Identifiable information about health, health care history and provision and/or payment of health services.
Personal Information Protection Act (PIPA)	**Organizations** Private sector organizations not covered by other privacy legislation.	Personal information, including employee information.
Privacy Act, Access to Information Act (ATIP)	**Federal Agencies** Government of Canada departments, Crown Corporations, First Nations services.	All records, including personal information.
Personal Information Protection and Electronic Documents Act (PIPEDA)	**Canadian Private Sector** Private sector organizations throughout Canada, except in provinces with similar legislation.	Only personal information as part of “commercial activities”, which does not include employment information. All personal information held by Federal Works and Undertakings (FWUBs), including banks, telecoms, transportation companies, some pipelines.

Who are Your Employees?

- Full time
- Part time
- Casual
- Temporary
- Contracted service providers
- Volunteers
- Board members
- Council members

#1 Employee Surveillance

- ALL ‘surveillance’ is considered a collection of personal information.
  - Have policy and notices
  - ONLY for ‘authorized’ (valid work alone/safety or QA) purposes in areas where there is no ‘reasonable expectation’ of privacy (not locker rooms, washrooms).
- Types of Surveillance:
  - Emails, computers and telephones including:
    - Keystroke and ‘idle time’ monitoring, auditing email, blocking website access
    - GPS tracking for company owned vehicles and equipment ‘work-alone’ location for safety
  - Video
    - Establish the business reason for conducting video surveillance and use only for that reason.
    - Have clear notices in all camera locations
    - Securely store any recorded images, limit access appropriately and retain according to your policies.
    - Provide individuals access to the video upon request, and information about who has access, and why, what information is being captured, and what is being done with recorded images.

#2 Drug Testing

- Problem: Drug and Alcohol use/impairment in the workplace. Cannabis legalization adds another dimension.
- Privacy issue: over-collection of personal medical information of majority of employees involved – a kind of surveillance issue.
- Privacy law: “reasonableness”
  - PIPA IR 2005-04
    - Are there legitimate issues that an organization needs to address through surveillance?
    - Is the surveillance likely to be effective in addressing these issues?
    - Was the surveillance conducted in a reasonable (i.e., least intrusive) manner?
- Testing types
  - Post-Incident or Reasonable Cause: identifiable issue, effective response
  - Pre-employment or pre-access: effectiveness in question
  - As a condition of employment/monitoring agreement after a policy violation: Duty to accommodate drug abuse problems
  - Random: As a general practice for all employees, problematic. Effectiveness for prevention? Deterrence? Immediate detection due to randomness?
- Suncor Case
  - Random drug and alcohol testing for safety sensitive positions at specific worksites.
  - 2012: challenged by Union, subject to a series of arbitration decisions that have been overruled and appealed.
  - 2018: agreement between Suncor and Union to implement random drug testing under specific conditions.

#3 Investigations

- Collect, use and disclose type and amount of information necessary to gather information required for the investigation
- Hold all records related to the investigation in a secure manner, separate and apart from other HR records.
- Restrict access on a “need to know” basis.
- Who is notified about an investigation?
  - Parties and witnesses of value; supervisors/managers only if workplace changes are required
  - C-suite only if there are matters of liability or risk requiring their attention
- Who gets to see the report and the records?
  - Report is circulated only among the final decision-makers because it contains sensitive personal information, and widely circulating may negate any future claim of privilege
  - Inform Complainant of the outcome and of decisions that directly affect his/her work
  - Inform the Respondent of the outcome and any action to that is directly applicable to him or her
  - Upon request provide access to records under legislation, applying provisions to protect third party personal information, and your organization’s decision-making processes
  - Provide records when compelled by police, for court or quasi-judicial proceedings

#4 Occupational Health Privacy

- Health assessments for leave, disability management
  - Only medical providers view health information.
- Accommodation programs
  - Health treatment program needs to be confirmed by HR.
- Safety and OHS injury tracking
  - Injury records required but limited in access according to OHS Act.
- Referred benefits providers
  - Supplemental medical benefits
  - EFAP
  - Wellness programs
- HIA jurisdiction confusion
  - Health information generated by health providers, but not employment health assessments.

#5 Workplace ‘Reach’

What is “the workplace” these days?

- To determine whether an employer has ‘reach’ for monitoring, investigation, discipline:
  - employee’s out of hours conduct likely to cause serious damage to the relationship between the employer and employee; or damages the employer’s interests; or is incompatible with the employee’s duties as an employee (violation of policy)
- Employers should minimize their risk of harm to reputation and brand and risk of vicarious liability for an employee’s out of hours behaviour:
  - have a suitable workplace code of conduct and social media policy; and
  - inform employees of their rights and obligations and the circumstances under which they may be disciplined or terminated for their conduct beyond the workplace.
- Employees should be aware:
  - when using social media in a workplace context — including a social media account hosted by their employer —their personal information, including off-duty comments and postings on social media about workplace issues or that may otherwise reflect on the employer, can be collected, used and disclosed by the employer.

#5 Workplace ‘Reach’ - Examples

- An employee who, following a relationship breakup with a work colleague, posts intimate images or sexual videos on social media (an act known as “revenge porn”) was validly terminated because of the ongoing harm and violation the publication can cause to the victim and the effect it may have on her dealings with their other work colleagues.
- A Manitoba Judge retired early from the bench after her ex posted intimates photos of her. A disciplinary panel of the Canadian Judicial Council was to examine whether the photos are "inherently contrary to the image and concept of integrity" of the judiciary and undermine public confidence in the justice system. The inquiry suffered delays and legal challenges before the Judge agreed to retire and the case was stayed.
- An employee dismissed for social media posts calling his employer’s clients “spastics and junkies” was reinstated (despite his conduct being considered a valid reason for dismissal) because the dismissal was found to be harsh in light of a number of mitigating circumstances, including the employee’s long history of employment.
- An employee dismissed following sexually lewd behaviour at a hotel after a staff Christmas party was found to have been validly terminated, not only because of the lewd conduct as such, but she was not honest with the employer during its investigation, therefore the employer could not be assured of her honesty in the future.
- An employee stating where they worked on their Facebook page established the requisite link between employee and employer to justify dismissal for out of hours conduct in making derogatory posts, even though the posts did not relate to their employment.

#6 Privacy Breaches of Employee Information

- Real harm
  - financial: loss of funds, credit, employment, (fraud and ID theft)
  - humiliation and loss of status or reputation (disclosure to work colleagues, family)
  - physical damage to person or property (disclosure to potential perps)
- Persistent rationalizations by organizations
  - Hackers (not us): internal vs. external
  - “No risk to individuals”: not financial, no risk
- No need for intent – breach itself is harm
- Recent upswing in email phishing, social engineering, ransomware, network compromises
- Response as important as prevention

#6 Privacy Breaches of Employee Information

Selected Alberta Breaches Involving Employee Information, 2017

Total of 18 reported in 2017

- **IHS Global Canada Ltd.**
  Date: March 2017
  Impact: 352 employee records taken by terminated employee.
- **Centerfire Contracting Limited**
  Date: March 2017
  Impact: 120 employee T4 slips emailed to other employees.
- **McDonald's Restaurants of Canada Limited**
  Date: March 2017
  Impact: 94,556 job applications
- **Open Text Corporation**
  Date: June 2017
  Impact: Storage device containing 300 employee records stolen
- **CBI Home Health (AB) Limited Partnership**
  Date: December 2014
  Impact: Unauthorized disclosure of PI of 530 employees to Union
- **FPInnovations**
  Date: August 2016
  Impact: Unauthorized internal and union access to and disclosure of employee information spreadsheet.
- **Trailer Wizards Ltd.**
  Date: February 2017
  Impact: Unauthorized internal and union access to and disclosure of employee information spreadsheet.
- **Marin Software Incorporated**
  Date: February 2017
  Impact: Spear phishing incident. Unauthorized external disclosure of 795 employee payroll records.
- **Wood Law Office**
  Date: May 2016
  Impact: 2 hard drives stolen by ex-volunteer and firm database accessed remotely affecting 1000 clients and staff.
- **eScreen Canada ULC**
  Date: February 2016
  Impact: occupational health screenings of employees stolen and kept by a former disgruntled employee.

#6 Major Data Breaches of Employee Information

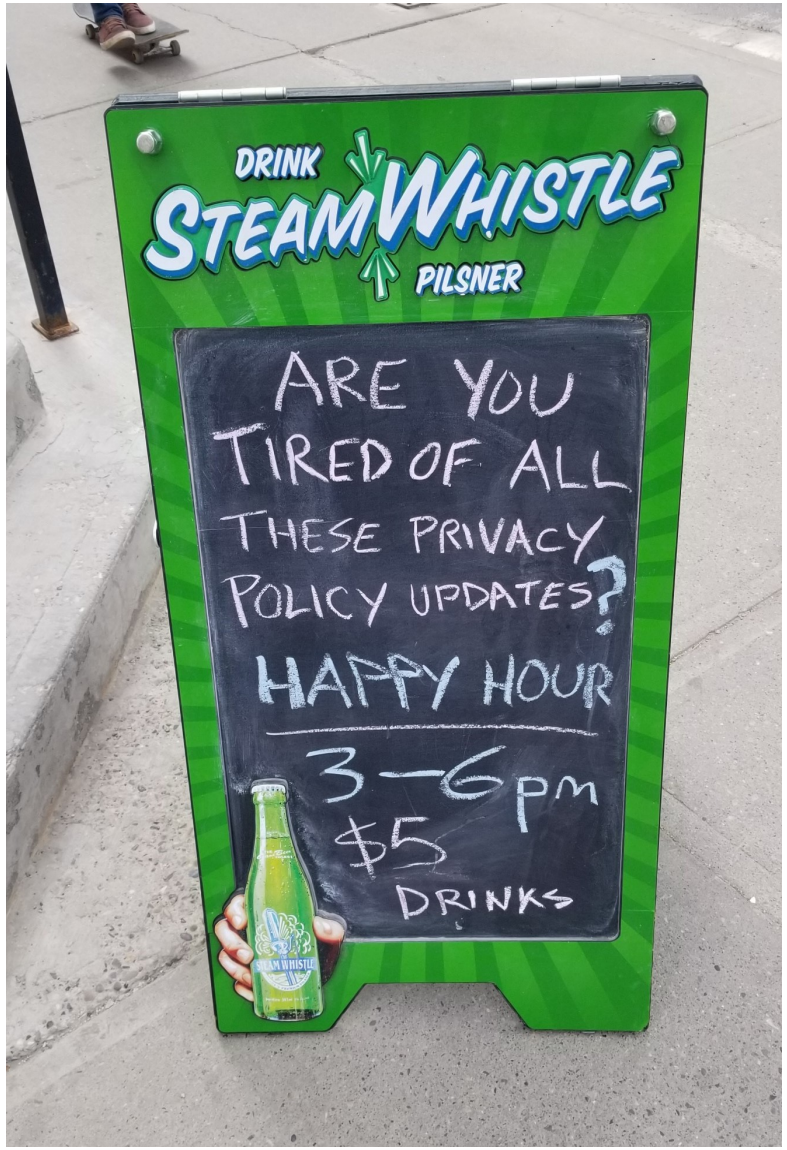
- **US Office of Personnel Management (OPM)**
  Date: 2012-14
  Impact: Personal information of 22 million current and former federal employees
- **RSA Security**
  Date: March 2011
  Impact: Possibly 40 million employee records stolen.
- **Revenue Quebec**
  Date: June 2019
  Impact: 23,000 current, former and contractual employees at Revenue Quebec

#7 Collection of Personal Information

- View and discuss the job application – stop over collecting.
- **Highlights**: keep “authorized’ and ‘business’ purpose of collection in mind
  - SIN number only at hire
  - Ask if ‘eligible to work in Canada’
  - Driver information – get abstracts on regular basis
  - Get Police Information Check or Vulnerable Sector Check only if necessary and do them regularly – at hire isn’t sufficient
  - Ask demographic information only if required for an established program or by law (to report to Gov of Canada hires who identify as indigenous)
  - Use literacy/numeracy testing

#8 Privacy/Security Programs

- Privacy Programs: employee practices and compliance
- Collecting, using, and disclosing PI: too much or unauthorized
- Right of access
- Security: unauthorized disclosure, loss, alteration or destruction
  - Social engineering, phishing
  - After work/employment compliance
  - Snooping
  - BYOD
  - HRMS and cloud
  - Mandatory breach reporting under PIPA, PIPEDA and HIA
- Policy knowledge, training, enforcement: Compliance or Engagement?


DRINK
STEAM WHISTLE
PILSNER
ARE YOU TIRED OF ALL THESE PRIVACY POLICY UPDATES?
HAPPY HOUR
3-6pm
$5 DRINKS

#9 Reference and Other Checks

- What the laws say?
  - Limit collection, use and disclosure to the type and amount of information for your ‘authorized’ and valid business purpose
  - Collect directly when possible, or indirectly according to the legislation
  - Collect without consent for “employee management purposes”
- If an applicant’s choice of references is inadequate for a proper assessment of past performance:
  - ask the applicant for more suitable references to collect information from specific individuals you deem necessary allowing the applicant to clarify or amend their choice of references and express agreement or disagreement to the collection of information from other individuals.

#9 Reference and Other Checks

Using Social Media for Staffing and Recruitment

- Employees should know:
  - that social media information may seem transitory and informal, but once personal information is posted online it gains permanence — and can be circulated and searched by others.
- Employers and recruiters should be aware:
  - social media pages, even if publicly available, can contain inaccurate, distorted or out of date personal information about job applicants, and should therefore be cautious about relying on that information.
- Employers and recruiters should also guard against:
  - using personal information gathered from social media, or any other online source, in a discriminatory manner against a job candidate or an existing employee.

#9 Reference and Other Checks

Police Information Checks

- Order of the Alberta Office of the Information and Privacy Commissioner (OIPC), upheld by the Alberta Court of Queen's Bench:
  - Determined that Edmonton Police Service's (EPS) use and disclosure of an individual's personal information contravened the Freedom of Information and Protection of Privacy Act (FOIP Act).
  - Illustrates many unresolved issues with PICs and VSCs, such as unfairness, exercise of discretion, consistency, over-disclosure, over-collection by employers, consent and accuracy.
  - Information and Privacy Commissioner Jill Clayton called for legislation to resolve these issues, similar to Ontario's recently passed law.
- Employers should assess the need for a criminal record check, considering:
  - When it will be requested, how it will be enforced and what information will be required.
  - Do not use as a 'routine' part of reference checking.
  - When required for a legitimate business purpose, have those checks repeated regularly to be effective.

#10 Third Party Service Providers

- Universal in privacy legislation – organization with “control” responsible for all service providers.
- External service providers for HR PI:
  - Payroll
  - Occupational health/disability
  - Lawyers
  - Workplace investigators
  - Coaches
  - Search experts
  - Career transition providers
- How do ensure compliance with privacy program standards?
  - Contracts
  - Inspections, audits
  - Provider provided solutions
- External referred HR service providers:
  - Benefits providers
  - EFAP

Joan Dunlop, Partner
Rick Klumpenhouwer, Partner

cenera people • strategy • solutions

Rick.Klumpenhouwer@cenera.ca

403.294.3799

Joan.Dunlop@cenera.ca

403.294.7243