Workplace Privacy Presentation

Prepared by Gordon D. Hamilton, BA, JD, LLM, LLM

McDougall Gauley LLP

Disclaimer: *The views and comments in this presentation are entirely my own, and do not reflect the views of McDougall Gauley LLP (unless you think they are absolutely great, in which case I am fine to give the credit to the firm).*

A Walk Through History – Humble Beginnings

- In 1972, *The Privacy Act* was adopted in Saskatchewan. Twenty-four years later, the Saskatchewan Court of Appeal pondered: "It is questionable whether such [a common law right of privacy] exists…and this likely accounts for enactment" of *The Privacy Act.*

  [Peters-Brown, 1996 CanLII 5076]

- During the same era, Manitoba and BC enacted comparable legislation that also attempted to deal with privacy in general, undefined terms. (BC has effectively replaced its privacy legislation)

A Walk Through History - Confusion

- In 2012, the Saskatchewan Law Reform Commission noted that *The Privacy Act* does not attempt to define privacy and that any definition of privacy must be elastic. This meant that the Courts would be left to define it.
- In 2007, BC Law Institute provided its thoughts on its comparable legislation:
  - *normal social interaction requires the interest in privacy to be balanced against the legal rights of others. The ultimate degree of privacy cannot be expected on all occasions and under all circumstances.*
  - *the degree of privacy to which a person is entitled for the purpose of the Act is greatest where the expectation of privacy is greatest.*

My First Exposure to Privacy Law

- *United Food and Commercial Workers, Local 1400 v. Saskatoon Cooperative Assoc. Ltd.*, 1992 CanLII 8000 (SK QB)

  Application involved two Questions alleging Privacy Breach (in injunction application):
  - Employees investigated for theft without union representation => *was this false imprisonment*?
  - Existence of security cameras in gas bars to monitoring employee safety => *was this unlawful surveillance*?

- With today's understanding, unlikely to have these questions presented to a Court… BUT read what is in the news now…

Recent Privacy Concerns in the News

- Privacy concerns over examining fecal matter in sewer systems, which could identify such things as Covid-19, use of opioids, and other private health-related details (CBC News article, May 29, 2022)
- Concern is that neighbourhoods and even apartment buildings could be identified and stigmatized (actually happened in Hong Kong and Singapore) (CBC News article, May 29, 2022)
- In Canada, health authorities are strictly controlled by privacy legislation, so minimal risk
- Bottom Line: If people think there might be a breach of privacy, they talk about it and raise concerns, regardless of how unlikely it is to be a privacy breach

Everyday Privacy Concern Examples

- Some parents of elementary school children (in SK) have refused to provide the school with the cell phone number for either parent on the basis of personal privacy. The same reason was given for refusing to fill out a school form asking where a parent works.
- Federal government's Covid-19 Exposure App, which included anonymized location data, was alleged to be a breach of privacy (technically, the app only provided proximity data to other app users, and was approved in advance of launch by federal OIPC)
- Covid-19 contact tracing of high school students – students not cooperating due to privacy concerns about who they have been hanging around during and after school

Privacy is a Balance of Rights

- BC Law Institute noted that “normal social interaction requires the interest in privacy to be balanced against the legal rights of others.”
- Both employers and employees frequently fail to properly recognize the requirement to balance the rights of others
- Society appears to misunderstand that individual rights only flourish when we protect the well-being of society as a whole [see CHRC: https://www.chrc-ccdp.gc.ca/en/resources/individual-rights-come-collective-responsibility]
  - e.g. does the right of an individual to refuse to wear a Covid mask trump the rights of others to collective safety from viral spread? - this question has led to significant friction in North American society recently

The Privacy Legislation Jungle

- Basic Premise – a Saskatchewan Employer
- Issues: private or public employer*
  - if a public employer, then will likely be subject to *The Freedom of Information and Protection of Privacy Act* (FOIP) e.g. PSC, or *The Local Authority Freedom of Information and Protection of Privacy Act* (LAFOIP) – e.g. universities
  - if a private employer engaged in commercial activities, then will likely be subject to *The Personal Information Protection and Electronic Documents Act* (PIPEDA)
  - if a private employer engaged in non-profit activities, PIPEDA does not generally apply

**will not be examining public sector legislation in presentation*

Going Deeper into the Jungle

- A private or public employer in Saskatchewan who receives medical information from a sick / disabled employee, whether solicited or not, would be subject to the *Health Information Protection Act,* regarding the handling of the employee's personal health information
- A private employer in Saskatchewan that has customers in other countries may fall under certain international privacy laws. For example, if a company does business with an EU company, the *General Data Protection Regulations* (GDPR) apply. The GDPR contains 173 Recitals within 99 Articles, organized in 11 chapters, contained in 88 pages.

The Canadian Landscape

- The Canadian landscape continues to change.
- BC, Ontario and Quebec are the only provinces with privacy legislation comparable to PIPEDA. PIPEDA does not generally apply in those provinces because of their provincial privacy legislation.
- Impact on a Saskatchewan employer can be significant if it has employees in one of these provinces, which will require different privacy standards and protocols.

Quebec is Leading the Changes

- In 2021, Quebec significantly amended its privacy laws to align more closely with the GDPR standards. The changes include:
  - A mandatory privacy impact assessment for
    - any new or redesigned information system (e.g. HRIS)
    - the transfer of any personal information outside of Quebec (e.g. payroll data), and
    - The communication of personal information without consent (e.g. research, stats, etc)
  - Internal compliance processes must be re-evaluated for accountability and alignment with the new legislation
  - New regulations introduced for de-identified / anonymized information
  - Automatic decision-making processes (e.g. A.I.) modified to include GDPR-like rights in Quebec's privacy law (i.e. right to be informed, right of access, right to rectification, right to be forgotten, right to object, etc).

Future Impact on Employers

- Employees acquiring right to examine, comment on (e.g. object to), correct and/or delete personal information held by an employer in its paper and electronic files
- Example: supervisor notes about employee's excuse for absence might include personal information (e.g. alcohol addiction, family issue, medical test, etc.) and may be subject to legislative compliance
- Example: senior employee who was listed on the company website quits (the right to be forgotten may require the employer to scrub the internet of the employment reference)

Employer Policy Recommendations

- Have a workplace privacy policy, to establish expectations and procedures to deal with privacy complaints from employees
- Have an information and data privacy policy, to deal with
  - standards of control over information and data,
  - pre-breach preparedness,
  - mitigation measures,
  - risk management, and
  - post-breach protocols
- Both policies should be integrated to other workplace policies, such as discipline policies, whistleblower policies, etc.

Re-evaluation of Practices?

- Depending on which legislation applies and when future legislation changes occur, certain practices may require substantial changes (e.g. explicit employee consent). Examples could include:
  - the sharing of personal information with a group benefits insurer;
  - the sharing of personal information with a certified trade union;
  - type and extent of data obtained and retained on HRIS;

Costs of Infractions

- Canada has been catching up to other jurisdictions, such as EU, when it comes to penalties for privacy breaches
- Ontario (PHIPA – health privacy): individual fines up to $200K and organizations up to $1M (by comparison, maximum fines in Saskatchewan under HIPA are $50K for individuals and $500 K for corporations)
- A review of BC cases where a privacy breach was established outside of employment revealed damages awards ranging from $2500 to $50,000. The upper end of damages involved malicious and reprehensible conduct (a peeping voyeur case, and a case where phone calls were intercepted and given to an employer to try and get someone fired).

The Quebec Approach to Costs

- The Quebec legislation continues to mirror the GDPR regulations in the damages/costs area, and the legislative penalties confirm that approach.
- Administrative penalties are set at $50,000 per individual and 2% of global revenues for corporations up to $10M (revenue). Criminal penalties are roughly twice those amounts.
- The trend is to expect penalties and damages awards in privacy cases to dramatically escalate over the next decade.

First Quebec – But Who is Next?

- Ontario has already prepared and published a White Paper in an effort to modernize its privacy law system. Many of its proposals reflect the changes already embodied in the Quebec legislation.
- Employers operating in other provincial jurisdictions, which previously only worried about PIPEDA, must now comply with Quebec law if the information was collected in Quebec. So, a Saskatchewan company with a branch office in Quebec must ensure that it is fully complaint with the Quebec legislation. Practically, this forces the Saskatchewan company to convert all of its policies to the most restrictive / prescriptive jurisdiction in which it operates, such as Quebec.
- And don't forget about the expanding impact of the GDPR in Canada (e.g. McDougall Gauley LLP asked to take steps regarding specific policies to be compliant with GDPR because of a client's head office in the EU)

The Common Law and Privacy

- In Saskatchewan, the Saskatchewan Court of Appeal in *Bigstone v St. Pierre* 2011 SKCA 34 has confirmed that there is a statutory tort for breach of privacy. As noted above, the Court doubted whether there was a common law right of privacy in 1996.
- The BC Court of Appeal (*Ari v ICBC*, 2015 BCCA 468) has refused to recognize a common law duty of care regarding privacy, limiting parties to the statutory regime.
- Ontario has taken a different approach, with its “intrusion upon seclusion” tort.

The Basics of *The Privacy Act (Saskatchewan)*

According to Section 2, a breach of privacy must be:

a) wilful,

b) without claim of right.

Without explicitly stating it as a factor in the legislation, there must also be a reasonable expectation of privacy.

Wilful Breach of Privacy / Claim of Right

- Must be “done intentionally, knowingly and purposely without justifiable excuse”
- Wilfulness is not satisfied if the actions are done “carelessly, thoughtlessly, heedlessly or inadvertently”
- “Private” information must be within some sphere of allowable access (hence the claim of right)

Source: *Privacy Law in Canada* (LexisNexis-Butterworths: Markham, 2001), Chapter 3: The Tort of Invasion of Privacy. pp. 76-77

The Privacy Act versus The Charter

- We are all familiar with the limitations of the strict applicability of the Charter to employers. However, Courts have been willing to allow the interpretation of non-Charter rights (such as privacy rights) to reflect Charter values (see *Law Society of British Columbia v. Trinity Western University*, 2018 SCC 32 par 46).
- In *Bigstone*, the Court of Appeal noted in par 21: *This suggests that the privacy [which] the Act protects may be more extensive, and different in some respects, than privacy under the Charter.*
- Bottom Line*:* The full impact of *The Privacy Act* could include Charter values to further expand its broader scope of protection.

What is Personal Information?

- One of the challenges from the legislation jungle is that personal information is defined differently (if at all).
- For example, PIPEDA defines personal information as:
  - Age, name, ID numbers, income, ethnic origin, or blood type;
  - Opinions, evaluations, comments, social status or disciplinary actions;
  - Employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions.
- *The Privacy Act* is completely silent and does not even contain the words “personal information”. However, it is reasonable for the Courts to look to comparable provincial legislation for guidance.

Personal Information in Saskatchewan

- For example, FOIP defines personal information under 10 subheadings, which include:
  - “information that relates to the education or the criminal or employment history of the individual…”
  - “any identifying number, symbol or other particular assigned to the individual, other than the individual’s health services number…”
  - “the personal opinions or views of the individual except where they are about another individual”
  - “correspondence sent to [the employer]…by the individual that is implicitly or explicitly of a private or confidential nature, and replies to the correspondence…”
  - “information that describes an individual’s finances, assets, liabilities, net worth, bank balance, financial history or activities or credit worthiness…”

GDPR Protects ‘Personal Data’

- Under the GDPR, ‘personal data’ is defined under Article 4 as:
  - any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- In an employment context, personal data would include such things as employment evaluations, employment history, employee medical information, employee email address (in some cases), employee photo on company directory, workplace videos (e.g. where employee works in environment under regular or constant video surveillance) – in certain contexts relating to employee identification

Employment Aspects – Some Examples

- Actual RM Minutes posted on public website:
  - “That Jim H. has passed his probation effective April 16, 2017.”
  - “That John H. be dismissed for cause effective April 16, 2017.”
  - “That James H. have his probation extended for 60 days due to his role in causing the recent damage to the grader.”
  - “That Jeff H. be offered employment at $31 per hour, subject to no sick time or paid leave to be paid out, 13 weeks probation, 3 weeks annual vacation, and $250 for reimbursement of safety equipment upon providing receipt for purchase.”

Employment Aspects – More Examples

- Paramedic tells his union president about the circumstances from the last shift yesterday, involving transportation of heart attack patient from Spiritwood to Prince Albert, including details about patient's condition while waiting for hospital to receive patient
- Employer announcing in an email to staff that an employee will be on a *medical* leave of absence for the next 4 weeks
- Human resources staff sharing HRIS screen with a manager to discuss employee absences, when screen contains other personal information
- Harassment complaint investigation report includes details about employee's mental health, which is then provided to both the complainant and the respondent

Employment Aspects – More Examples

- Employer announcing that all employees must now return to work in the office, even those who are unvaccinated – after previous announcement that said unvaccinated employees cannot return to work yet (everyone knows who didn't return before in their department).
- Company laptop with payroll data stolen from backseat of manager's locked car – direct deposit information, employee names, hourly rates of pay, home addresses, etc. on spreadsheet for uploading to payroll processing company.
- Employer notifying insurer of employee on sick leave so that it can adjudicate whether current medical information will satisfy anticipated LTD claim (since LTD date approaching) – insurer calls employee to gather additional medical information

Latest Federal Government Example

- On May 3, 2022, the federal government sent out an email to about 200 employees who had claims in relation to the Phoenix pay system.
- By mistake, everyone's names were put in the "CC" field rather than the "BCC" field of the email, so all claimants now know who else has filed a claim.
- This is in addition to a previous screw-up in February 2020 when another mass email was sent containing "full names, personal identifiers, home addresses and Phoenix overpayment amounts to officials in 62 departments and agencies" rather than to the employees' department heads. [Source: CBC News article, June 1/22]

Responding to Privacy Data Breach

- These happen more frequently than many realize. The standard response includes the following steps:

  - Stop & Contain the Privacy Data Breach
  - Enact the Privacy Breach Protocols (should be set out in a privacy policy)
  - Notify Those Impacted by the Privacy Data Breach
  - Investigate the Breach and Enact Steps to Remediate

Review of Key Saskatchewan Cases

- Leading Saskatchewan case: *Bigstone v St Pierre*, 2011 SKCA 34
  - Sets out role of *The Privacy Act* in Saskatchewan
- Other Saskatchewan cases:
  - *Ratt v Tournier*, 2014 SKQB 353, which follows *Bigstone* and provides additional analysis of *The Privacy Act*
  - *Bierman v Haidash*, 2021 SKQB 44 (CanLII) is the latest review by the Courts of *The Privacy Act* and highlights that proof of damages is not a requirement in the legislation (nominal damages of $7500 were awarded)
- Common Law Privacy Tort in Saskatchewan:
  - *Peters-Brown,* 1996 CanLII 5076 suggests that no such tort exists in Saskatchewan

Other Relevant Privacy Cases

- Manitoba has very similar privacy legislation
  - See *Zeliony v. Dunn et al.*, 2021 MBQB 136 (CanLII), which adopted *Bierman v Haidash* in rejecting a summary judgment application on the basis of breach of the statutory privacy tort.
  - In *Heckert v. 5470 Investments Ltd.*, 2008 BCSC 1298, the Court said that a contextual approach is required when assessing claims of privacy breaches
- Ontario's common law tort of intrusion upon seclusion
  - See *Jones v. Tsige*, 2012 ONCA 32 which stated that "damages for intrusion upon seclusion will ordinarily be measured by a modest conventional sum".

Relevant BC Privacy Case

- BC: *Ari v. Insurance Corporation of British Columbia*, 2015 BCCA 468 (CanLII) confirmed that there is a statutory tort for breach of privacy and that the statutory regime (which includes a general privacy law similar to Saskatchewan's *The Privacy Act* and comparable legislation to FOIP and LAFOIP) "constitutes a comprehensive statutory framework for dealing with conduct" that would be considered as a breach of privacy.

Questions????

Questions????

Questions????