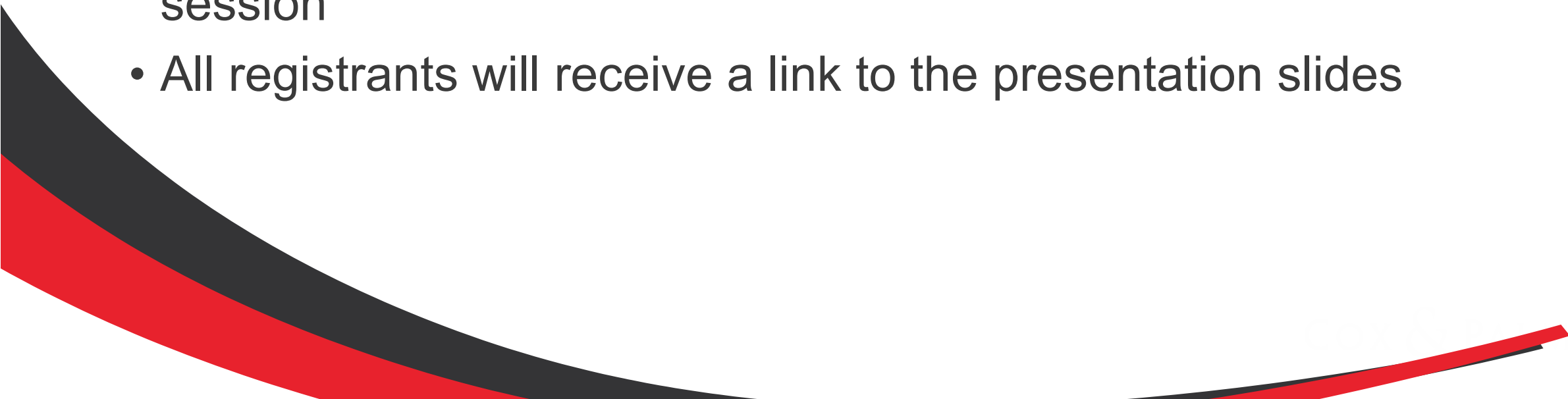


# Welcome to Cox & Palmer's Regional Employment & Labour Group Webinar

*Navigating Workplace Privacy*

Our presentation will begin shortly.

# Housekeeping Items

- For optimal viewing we highly recommend disconnecting from your VPN to ensure strong connectivity throughout the presentation
  - If you have any questions during the webinar, you can submit them through the Q&A button at the bottom, and our panel will respond to as many questions as possible at the end of the session
  - All registrants will receive a link to the presentation slides
- 

# Navigating Workplace Privacy

October 23<sup>rd</sup>, 2024



**Jessica Bungay**  
Partner, NB



**Matthew LeBlanc**  
Lawyer, NB



**Matthew Gough**  
Lawyer, NL



**Nicola Watson**  
Lawyer, NS



**Isabelle Keeler**  
Lawyer, PE

# Agenda

- Welcome & introduction
- Legislative Overview
- Electronic Monitoring of Employees
- Privacy & Social Media
- Secret Recordings in the Workplace
- Q&A
- Closing remarks

# Legislative Overview

Matthew LeBlanc (NB)

# Legal Framework

## 1. Federal rules

- Substantially similar: AB, BC, QC
- Otherwise, legislative void...

## 2. Health sector privacy legislation

- Limited application to workplace

## 3. Public sector privacy legislation

- More tools

## 4. Privacy torts

- Common law
- Statutory

## 5. Other considerations...

- Criminal
- Unionized
- Monitoring...



# 1. Federal rules

- Only applies to federally regulated industries
  - Banks
  - Interprovincial transportation
  - Broadcasting
  - Etc.
- Does not apply to provincially-regulated employers *vis-à-vis* their employees
  - Does apply to commercial activity

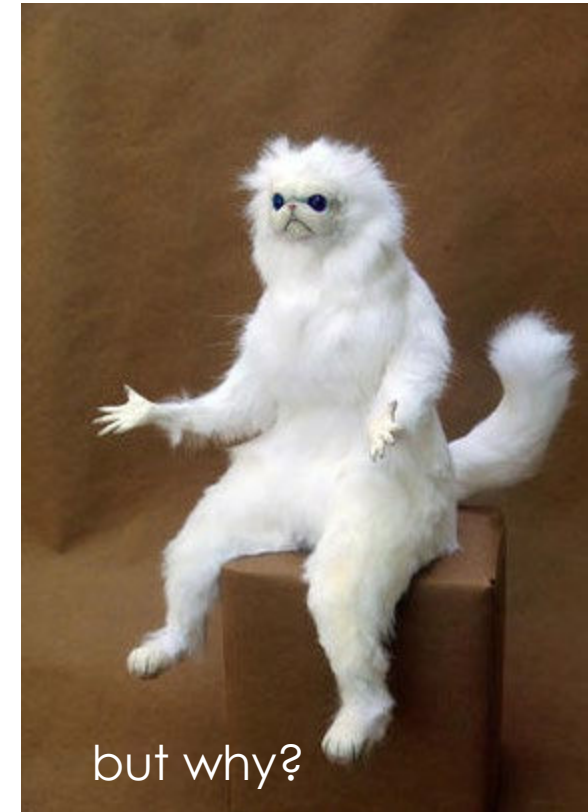
# PIPEDA

- *Personal Information Protection and Electronic Documents Act*
- 10 principles:
  1. Accountability
  2. **Identifying purposes**
  3. **Consent**
  4. Limiting collection
  5. Limiting use/disclosure/retention
  6. Accuracy
  7. Safeguards
  8. Openness
  9. Individual access
  10. Challenging compliance



# PIPEDA ctd.

- 2. Identifying purposes
  - What is the reason? Clear & narrow
  - Communicate reason – keep records
  - At or before time of collection
  - Examples
    - Providing benefits
    - Assessing accommodation
    - Opening account



# PIPEDA ctd.



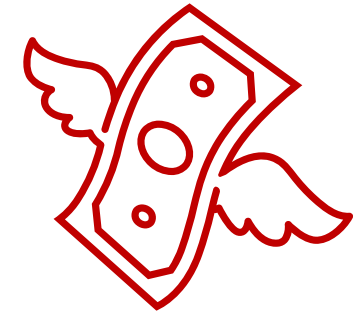
- 3. Consent
  - Knowledge & meaningful consent
  - Nature, purpose and consequences of the collection, use or disclosure
    - Necessary to fulfil an explicitly specified and legitimate purpose
    - Non-integral = choice
  - Each time!
  - Convey: what ; with who ; why ; risks
    - Consent should be express when info is sensitive, outside reasonable expectations or meaningful residual risk of significant harm

# Exceptions to consent (employment)

- Business and contact information
  - Name
  - Title
  - Work email
  - Business phone number and address
- Work product
- Information necessary to establish, manage or terminate employment relationship



# ... ByePEDA!



- *Digital Charter Implementation Act, 2022*
  - *Consumer Privacy Protection Act*
    - re: commercial activity; modernize/extend rules on private sector companies collecting personal information of consumers
  - *Personal Information and Data Protection Tribunal Act*
    - new Tribunal & consequences (greater of \$25m or 5% of global revenue)
  - *Artificial Intelligence and Data Act*
    - regulates interprovincial / international trade/commerce in AI



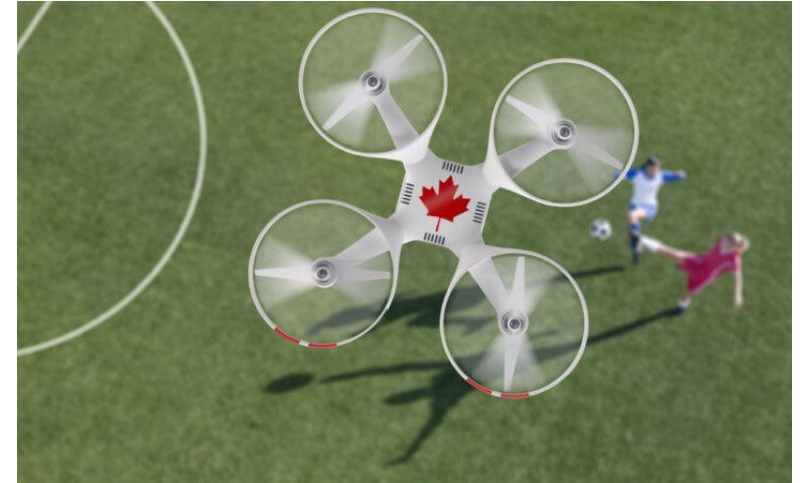
## 2. Health sector

- Each Atlantic province has specific legislation
- Limited application to employment
- Liability as custodian...



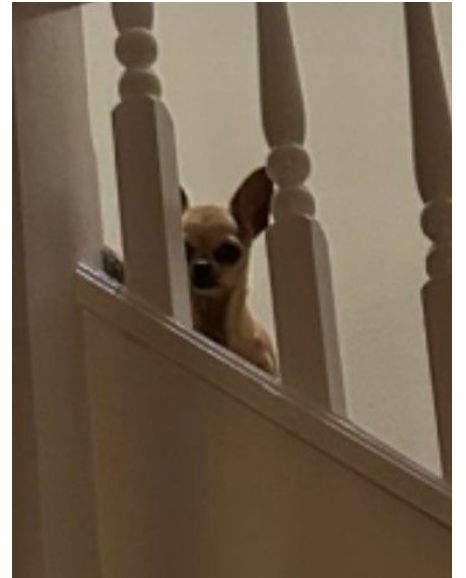
### 3. Public sector

- Employees have extra ammunition...
  - *Charter* protections
  - Freedom of information statutes
    - Includes information re: employment history
    - Note limited statutory exceptions  
(e.g. negotiations, ongoing legal proceedings...)



## 4. Torts

- Potential application to employment
- 4 recognized privacy torts
  1. **Intrusion upon seclusion**
    - highly invasive monitoring / social media checks?
  2. **Public disclosure of private facts**
    - publicity given to private life ...disclosure of confidential information...
    - actionable *per se* (without proof of damages)
  3. Publicity placing person in a false light
  4. Appropriation of a person's name or likeness





# ... and statutory torts!

- Only in NF (and MB, BC, SK)
- NF *Privacy Act* – section 3
  - willfully and without claim of right violate the privacy of an individual
  - also actionable *per se*
  - consent is a defence



## 5. Other considerations

- *Criminal Code*
  - Interception – s.184
  - Fraudulent interception – s. 342.1
- Unionized?
  - Look at collective agreement
    - Electronic monitoring / surveillance
    - Property searches
    - Disability management
    - D&A testing



# Example: monitoring...

- General test for actions/policy (esp. union)
  - Necessity
  - Effectiveness
  - Proportionality
  - Less intrusive option?
- Video monitoring vs GPS monitoring vs IT monitoring
- Constructive dismissal? *Colwell v Cornerstone Properties Inc*, 2008 CanLII 66139 (ON SC)
  - Subreption (surreptitious)



# Gaps? Fill them in!



**Legislative gaps**



**Company policies**

# Electronic Monitoring of Employees

Isabelle Keeler (PEI)

# The Rise of Electronic Monitoring Technologies

- Electronic monitoring is not a new practice. However, the increase in remote work as a result of the COVID-19 pandemic has accelerated the scope and use of electronic monitoring technologies by employers.
- According to a recent survey, **70%** of surveyed employees who use a digital device for work indicated that some aspect of their work is digitally monitored, with **32%** of employees reporting experiencing one of the following: location tracking, webcam/video recording, keyboard/keystroke monitoring, computer screen capture, or biometrics such as facial features, voice, or iris scan. (Future Skills Centre, July 2023).

# Why Engage in Electronic Monitoring?

- There are legitimate business reasons for engaging in electronic monitoring of employees. Examples include:
  - ensuring the protection of physical and data security;
  - verifying or assessing an employee's presence at work (i.e., time theft);
  - ensuring and tracking productivity;
  - determining the location of company vehicles/property; and
  - preventing leaks of confidential information.

# The Downside of Electronic Monitoring?

- Pervasive forms of electronic monitoring and surveillance can impact the trust that is integral to the employment relationship.
- Other potential impacts include the creation of a chilling effect on employees' creativity and sense of autonomy, loss of dignity, or adverse mental health effects.





# **Case Examples:**

## **Video/Audio Surveillance, Location/GPS Tracking & Time Tracking**

# PIPEDA Findings #2022-006

- A complaint was filed by an employee under PIPEDA regarding the Employer's decision to install a dash camera into a company vehicle that continued to record audio and video.
- The recording device was active when the truck was on or idling, which meant that it could be active when drivers were off duty and not working.
- The Employer took the position that the audio and video recording was installed for an appropriate purpose to improve the safety of its operations.

# PIPEDA Findings #2022-006

- The Commissioner investigated the complaint and found the following of relevance:
  - The continuous monitoring of employees resulted in a loss of privacy that was disproportionate to the benefits being gained.
  - The Employer could have achieved its objectives in a less privacy-intrusive manner (i.e., recording only when the driver was on duty/driving).
  - The Commissioner recommended for the Employer to limit the audio functionality capabilities to be active only when a driver is on duty and/or driving and technologically limit access of the personal information captured by the system to only those employees who “need to know” for the Employer’s purposes.

# PIPEDA Findings #2022-006

- **Key takeaways?**

- In this case, the purpose of the surveillance was safety. If an employee is off-duty on a break and not driving the truck, there is no reason for the employer's safety interests to be engaged.
- Underscores need (regardless of whether PIPEDA applies) to consider the stated objective and whether less intrusive measures on an employee's privacy exist to achieve the same objective.

# ***IUOE, Local 793 v Earth Boring Co.***

## **(2021)**

- The Employer introduced third-party software called ExakTime. The purpose of the software was to take the place of proper timesheets and records.
- The ExakTime software required employees to download an application on their personal cell phones. Employees were then required to use the application to clock in and clock out by taking a photo of themselves onsite and uploading it to ExakTime, which indicated the time and geolocation at the time the employee clocked in or out.
- The Union grieved the introduction of this software.

# ***IUOE, Local 793 v Earth Boring Co. (2021)***

- The arbitrator considered all of the surrounding circumstances to determine whether the Employer's policy requiring the use of ExakTime struck a reasonable balance.
- The arbitrator upheld the grievances and required the Employer to halt the use of the application in its current form.

# ***IUOE, Local 793 v Earth Boring Co. (2021)***

- In particular, the arbitrator was not swayed that the Employer actually had a problem that needed to be addressed due to the lack of evidence presented at arbitration.
- The arbitrator also had serious concerns about ExakTime retaining employee data (including facial images) indefinitely, storing data on third-party servers, sharing data with third-parties, and tracking employees' location outside of working hours.

# *IUOE, Local 793 v Earth Boring Co.* (2021)

- **Key takeaways?**

- An Employer must demonstrate the presence of a real security issue with appropriate evidence before implementing electronic monitoring.
- Security measures such as two-factor authentication and encryption of data in transit and in storage may reduce the severity of an application's intrusion into employee privacy.
- The length of time for which data is stored may either reduce or increase a software technology's intrusion into employee privacy.
- Whether or not the data is a) shared with third-parties and b) stored by third-parties may factor into how intrusive the technology is determined to be.



## ***Kone Inc. v IUOC, Local 82 (2022)***

- The Employer implemented an application on work-issued mobile devices of its construction employees.
- Among other things, the application used GPS technology to determine how far an employee's work device was from an identified work location on a job site during work hours.
- The Union grieved the implementation of this application, arguing that it was contrary to the parties' collective agreement, arbitral jurisprudence, and BC's privacy legislation.

## ***Kone Inc. v IUOC, Local 82 (2022)***

- The arbitrator found that the Employer's collection of GPS locations through the application was reasonable and dismissed the grievance. In particular, the arbitrator found the following:
  - Information about whether an employee is at work during work hours is “at the low end of sensitivity” from a privacy perspective. The more specific the information, and the more it intrudes on an employee's personal time, the greater the sensitivity.
  - The “geofence” used in the application to track GPS was specifically designed to gather non-specific data about attendance without tracking an employee's movements, which made it more reasonable.

## ***Kone Inc. v IUOC, Local 82 (2022)***

- While there was some evidence of attendance and time-theft issues, the arbitrator noted that even in the absence of any issues, the management of attendance is a proper purpose for collecting information from employees.
- An employer is not required to prove it has exhausted every other possible alternative before collecting location data. It must only show that less privacy-intrusive alternatives are not practicable. In this instance, the arbitrator rejected the Union's suggestion that the employer could hire more supervisors or work with clients to monitor employees.

# *Kone Inc. v IUOC, Local 82 (2022)*

- **Key takeaways?**

- Do your due diligence regarding third-party applications! In this case, the application was designed to collect only the information needed (i.e., whether the employee was at the workplace during working hours) and no more. No information was collected about employees' locations on their own time, which led the arbitrator to conclude the information collected was on the "low end" of the privacy spectrum.
- An Employer may not be required to prove the existence of a problem in the workplace to justify the collection of location information depending on the purpose. The Employer needs to demonstrate that it has a proper purpose linked to the management of employees.

# **Electronic Monitoring:** **Considerations for** **Employers**



# Key Considerations

1. Consider and ensure compliance with applicable legislation (i.e., PIPEDA or substantially similar legislation in AB, BC, QC, health information legislation, privacy legislation, Charter, ESA requirements for ON, etc.), common law, collective agreements, and applicable policies.



# Key Considerations

2. Identify a clear purpose for monitoring and gather evidence of the workplace issue requiring the use of electronic monitoring.
3. Consider whether a less intrusive solution exists to resolve the workplace issue that you are trying to fix. If you have determined that a less intrusive solution is insufficient, document the rationale.
4. Before investing in third-party electronic monitoring technology, understand the technology's data practices, including how long data may be stored for, where data is stored, who has access to the data, and what security measures are built into the technology.

# Key Considerations

5. Create a policy regarding the electronic monitoring that you are introducing. Policies are important for the following reasons:
  - The policy can be used to provide clear notification to employees.
  - It sets out the identified purpose for the applicable electronic monitoring.
  - It advises employees of if, how, and in what circumstances electronic monitoring occurs, who can access the information, the circumstances under which the information may be used, and how long the information will be kept for.
  - It warns employees to not expect absolute privacy in relation to their use of the Employer's resources and property.
  - It warns of consequences of non-compliance.
  - It helps to create a clear, transparent, consistent practice.



# Privacy & Social Media

Nicola Watson



# Overview

1. Social Media Use & Policies
2. Workplace Investigation Tips
3. Recent Social Media & Workplace Privacy Cases



# Social Media

Includes a variety of internet-based communication tools.

Enables users to interact and share information and opinions (by video, audio, photographs, and text) publicly or privately with one another.



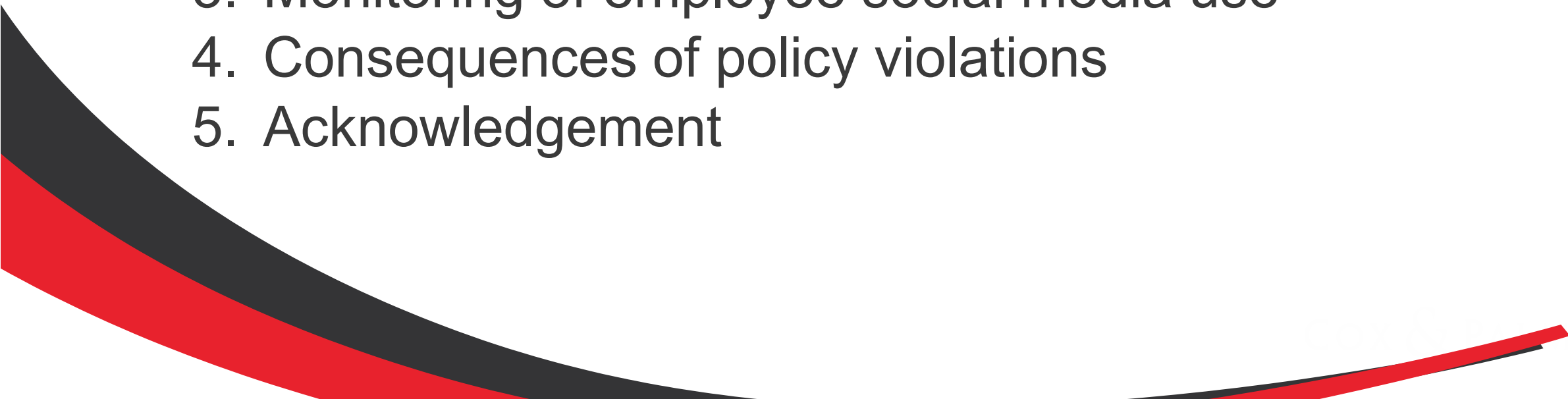
# Employee Privacy & Social Media

## Factors to consider:

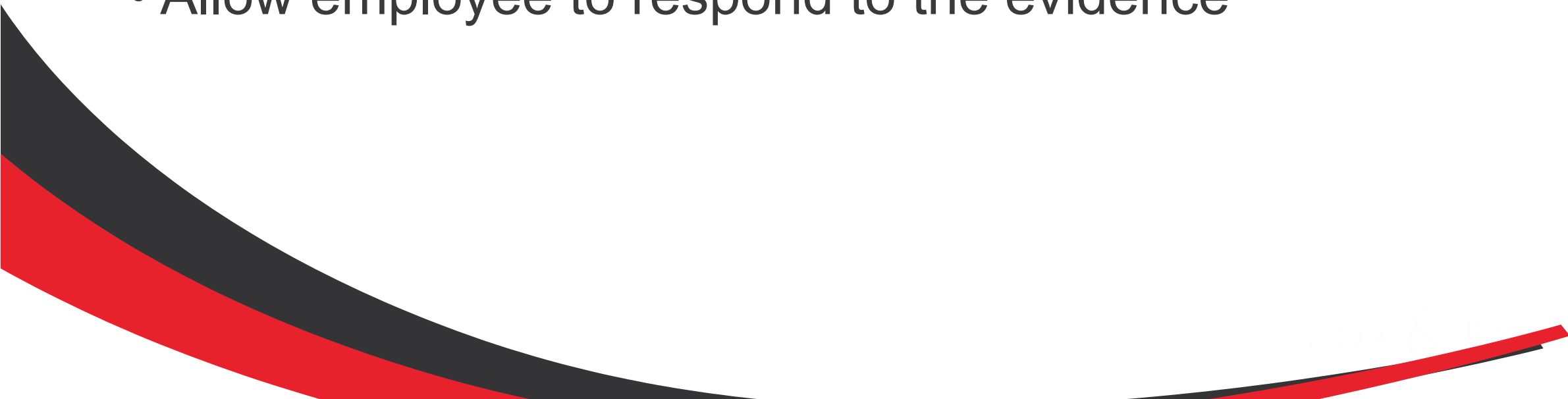
- Applicable privacy legislation, common law protections, and internal employer policies
- Balance between employer interest and employee privacy
  - Use of employer devices
  - Accessibility of information and privacy settings
  - Connection to the workplace

# Social Media Policies

## Key Elements:

1. Purpose and scope of policy
  2. Guidance on appropriate/ inappropriate use
  3. Monitoring of employee social media use
  4. Consequences of policy violations
  5. Acknowledgement
- 

# Workplace Investigations

- Always consider employee privacy interests
  - Do not use fake accounts to gain access accounts
  - Conduct a fulsome investigation
  - Allow employee to respond to the evidence
- 

# CASE EXAMPLES




# ***CBC v Canadian Media Guild***

- Alleged employee misconduct overshadowed by breach of employee's privacy in obtaining the information relied on






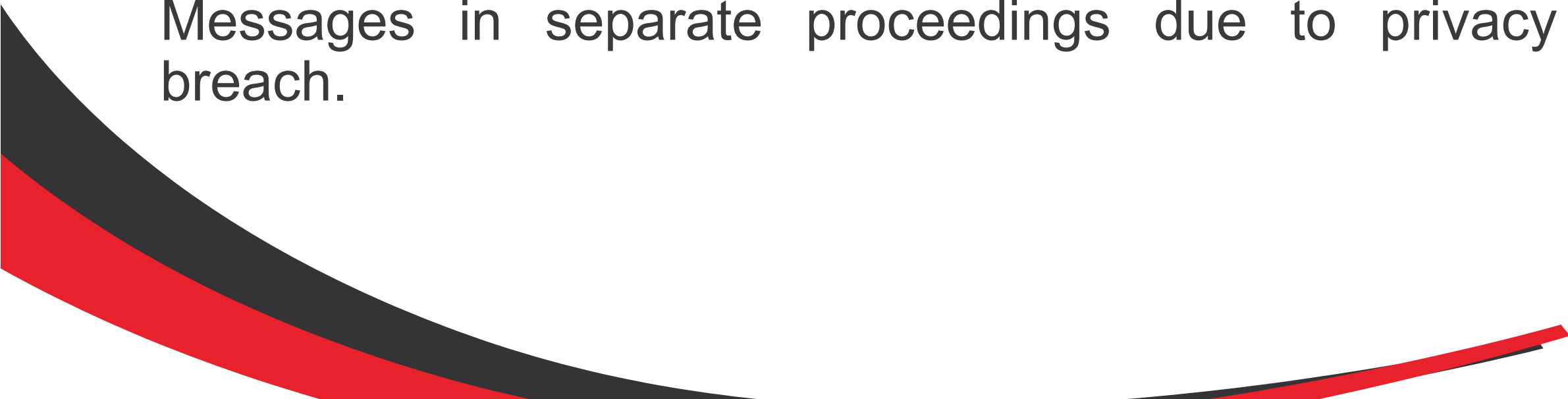
## ***Metrolinx v. ATU, Local 1587***

- Comments in WhatsApp group came to attention of co-worker and employer and became a workplace issue – employer had a duty to investigate harassment.
  - Arbitrator's original decision overturned – it was too focused on the Greivor's right to privacy.
- 

# ***Rancourt-Cairns v. Saint Croix Printing and Publishing Company Ltd.***

- Employee sued employer for wrongful dismissal and intrusion upon seclusion.
  - Court determined Facebook posts reviewed by employer were public, so there was no genuine issue for trial.
- 

# ***Power v. Mount Pearl (City)***

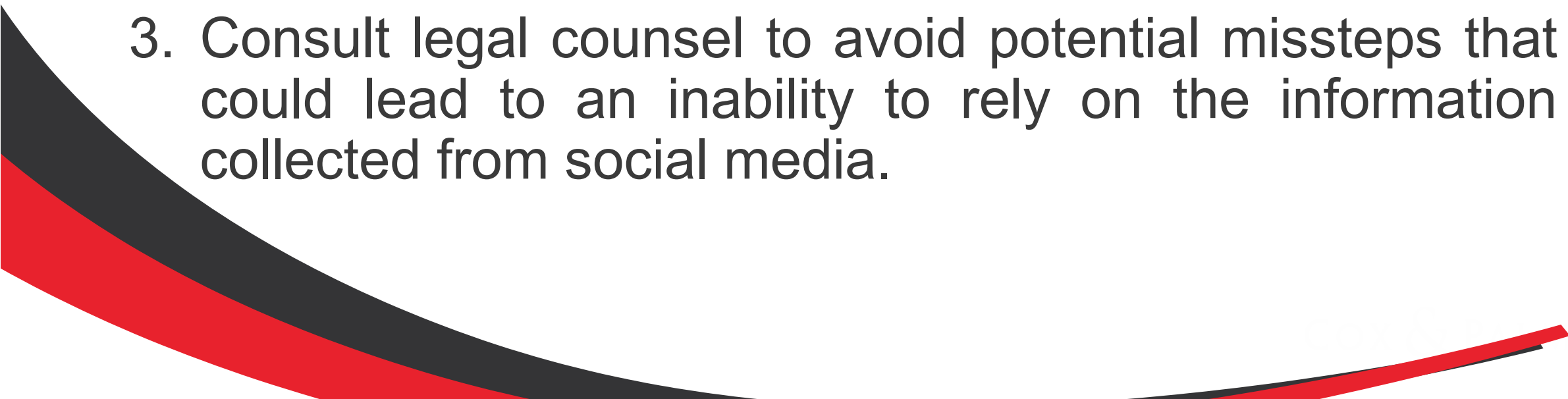
- Review of employee's Facebook Messenger by while he was on leave amounted to statutory tort and inclusion upon seclusion
  - Employer precluded from relying on Facebook Messages in separate proceedings due to privacy breach.
- 

## ***Unipco v. Mullin***

- Court relied on messages in granting employer injunction despite potential that employer engaged in intrusion upon seclusion in reviewing messages.



# Key Takeaways

1. Develop social media policies and train your employees on them.
  2. Consider employees' privacy expectations, even on work devices.
  3. Consult legal counsel to avoid potential missteps that could lead to an inability to rely on the information collected from social media.
- 

# Secret Recordings in the Workplace

Matthew Gough (NL)

Legal? Ethical? Good Idea? Bad Idea?

# Are Secret Recordings Legal in the Workplace?

- Section 184(1) of the *Criminal Code* states:  
Every person who, by means of any electro-magnetic, acoustic, mechanical or other device, knowingly intercepts a private communication is guilty of
  - (a) an indictable offence and liable to imprisonment for a term of not more than five years; or
  - (b) An offence punishable on summary conviction



# A Lawyer's Favourite Answer: It Depends...

- If an employee is part of the conversation, then that conversation would not be considered private under the *Criminal Code*, and therefore would be legal to record.
- This is sometimes referred to as the “one-party consent” exception, where if one party themselves consents to the recording of the conversation they are part of, they have not breached s. 184, regardless if the other party is aware of the recording or not.
- However, individuals secretly recording conversations which they are not part of would be a breach of s. 184 (and subject to the saving provision in s.184(2))

# If its not Illegal, is it Ethical? (Employee's Version)

- Even if an employee consents to recording their own conversation, should they?
- Employment relationships are built on and require trust between the Parties.
- Secret recordings of conversations does not *typically* build trust and can significantly harm the employment relationship if discovered after the fact.
- Secret recordings may also be violation of workplace policies, which could warrant discipline. Depending on the employee's role, it may also be a violation of their professional obligations.

# If its not Illegal, is it Ethical? (Employer's Version)

- If an employee can consent to record a conversation, then an employer or management employee could also consent and record conversations with an employee without the employee's knowledge or consent.
- But again, employment relationships are built on trust, and secretly recording employee meetings can backfire on employers.
- In the event of litigation over wrongful dismissal of an employee, these secret recordings may be required to be disclosed if at all relevant.
- Disclosure of secret recordings of employee's could have a significant negative impact on other employees (e.g. morale, trust, productivity, etc.)

# Case Law Examples

# *Shalagin v Mercer Celgar Limited,* **2022 BCSC 112**

- [1] “Is the surreptitious recording of one’s fellow employee’s a basis for dismissal? That is the core issue in this wrongful dismissal claim.”
- [24] “As part of his human right proceeding, the plaintiff produced certain documents, including information about surreptitious recordings he had taken while employed. Later, at his examination for discovery for this action, he disclosed further information about these secret recordings.”
- [50] “There is no dispute that the surreptitious recordings were made. The only question is whether the fact of the recordings go to the root of the plaintiff’s contract, and fundamentally struck at the plaintiff’s employment relationship.”
- [52] “[...] legality is not the sole barometer. The question is whether the employee’s actions fundamentally ruptured the relationship, such that the mutual trust between the parties is broken.”

# ***Shalagin v Mercer Celgar Limited,*** **2022 BCSC 112 (cont'd)**

- [55] “In *Fredrickson v Newtech Dental Laboratory Inc.* 2015 BCCA 357, the employer argued that the employee should have returned to work after termination when an offer to this effect was made. The employer argued that failing to take up this invitation was a breach of the duty to mitigate. The Court of Appeal disagreed in light of the fact that the plaintiff was by then aware that the employer had made surreptitious recordings of the plaintiff. The Court of Appeal stated:
  - ‘[29] ... I am of the view that the trial judge was clearly wrong in failing to reflect the mutuality of trust, in the context of this employment, inherent in the relationship between employer and employee.
- [72] “As such, I find that the plaintiff’s conduct in surreptitiously recording his colleagues constitutes just cause given the effect of the relationship of trust. As such, the claim must be dismissed on this basis alone.”

# ***Shalagin v Mercer Celgar Limited Partnership, 2023 BCCA***

- [14] “Mr. Shalagin testified that it was after these incidents in 2012 – 2013 that he began to record conversations with management personnel – not to improve his English, but ‘because I felt that maybe something like that would happen again and I would be able to do something about it and file a complaint or do something.’”
- [42] “I do not necessarily equate Mr. Shalagin’s surreptitious recording of his colleagues and supervisors with expressly misleading one’s employer or telling lie to someone in the course of one’s duties. However, the recording activity was underhanded and would be regarded by most employers as misconduct undermining the trust relationship between employer and employee. It also violated the privacy interests of persons who were recorded, as well as those who were discussed in the recordings.”

# ***Hart v Parrish & Heimbecker, Limited***

## **2017 MBQB 68**

- [34] “For the period from October 16, 2013 up to and including the date of his dismissal, the plaintiff surreptitiously recorded meetings with senior management of the defendant. He recorded the meetings by placing his cell phone on the table in the record mode and did not advise the parties that they were being recorded.”
- [58] “In addition to the unacceptable conduct known at the time of dismissal, the defendant relies upon acts of the plaintiff that were unknown at the time of dismissal. Specifically, the defendant relies upon the fact that the plaintiff began surreptitiously recording meetings that he with senior management which commenced with a recording on October 16, 2013 and ended with the final meeting the plaintiff had with Bill Parrish, Jr. on March 4, 2013.”



# *Hart v Parrish & Heimbecker, Limited*

## 2017 MBQB 68 (cont'd)

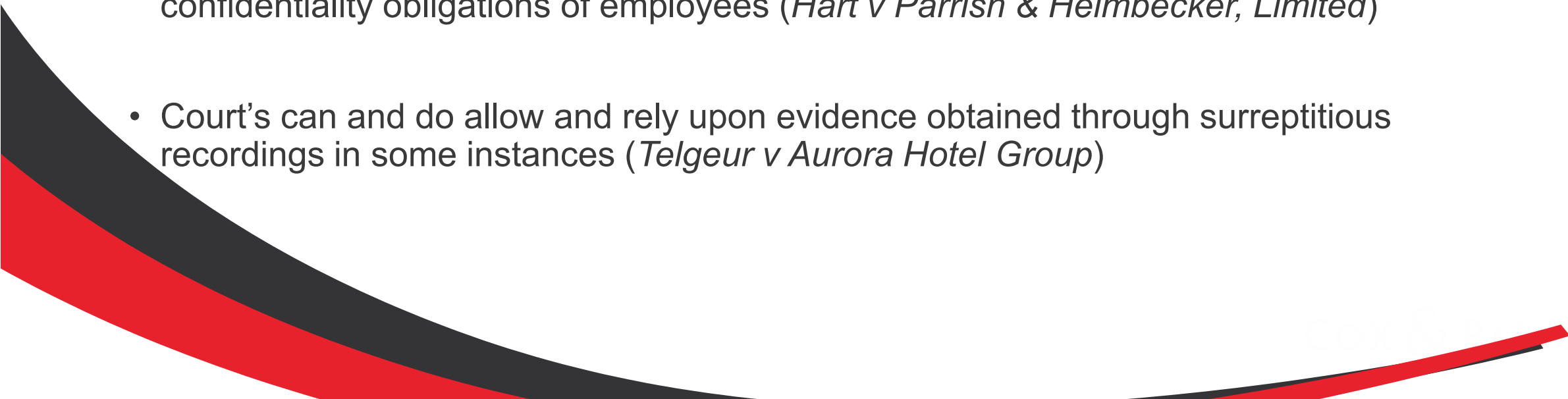
- [59] "...The defendant submits that the use of a company telephone for a purpose that was never intended was a deliberate violation of his duty of confidentiality and a breach of trust and loyalty to the defendant.
- [97] "The plaintiff's inappropriate use of his cell phone in secretly recording meetings with his superiors does amount to a breach of his confidentiality and privacy obligations to the defendant. The plaintiff admitted on examination for discovery that he knew a breach of the confidentiality obligations could result in termination."
- [98] "The misuse of cell phone was also a breach of his personal code of conduct that he prepared as a result of his meetings with Stone Ridge Consulting."



# ***Telgeur v Aurora Hotel Group,*** **2023 ONSC 1324**

- Plaintiff held position of General Manager with Employer and was terminated after 3 months.
- During the termination meeting, the Plaintiff surreptitiously recorded the discussions and later sought to rely upon the recording in his wrongful dismissal action.
- [47] “I have concluded that a claim for bad faith damages should be awarded in this case. As noted previously, the termination meeting was surreptitiously recorded by the plaintiff. This recording, however, highlights a number of disturbing aspects about the plaintiff’s termination.”

# Takeaways for Employers

- Employees can legally record conversations they are apart of without consent of the Employer (s. 184 of the *Criminal Code*)
  - Surreptitious recordings can amount to just-cause, even if discovered after the fact (*Shalagin v Mercer Celgar Limited Partnership*)
  - Surreptitious recordings may also result in breaches of workplace policies, privacy, and confidentiality obligations of employees (*Hart v Parrish & Heimbecker, Limited*)
  - Court's can and do allow and rely upon evidence obtained through surreptitious recordings in some instances (*Telgeur v Aurora Hotel Group*)
- 



# Takeaways for Employers (cont'd)

- Employment relationships rely on trust, which is a two-way street.
- Secretly recording meetings with employees can result in significant downside, with little upside.
- It is almost always better to inform employees they are being recorded in the normal course of business, with few exceptions.
- Employers and Managers should be counseled to be cognizant employee's may record their conversations without consent.



This presentation is provided as information only and is a summary of the issues discussed. It is not meant as legal advice or a legal opinion and you are cautioned to seek specific legal advice for your unique circumstances. © Cox & Palmer. All rights reserved. All intellectual property rights, including copyright, in this presentation are owned by Cox & Palmer, except as specifically noted.

This presentation may not be reproduced or distributed without the prior written consent of Cox & Palmer.

COX & PALMER

[coxandpalmerlaw.com](http://coxandpalmerlaw.com)