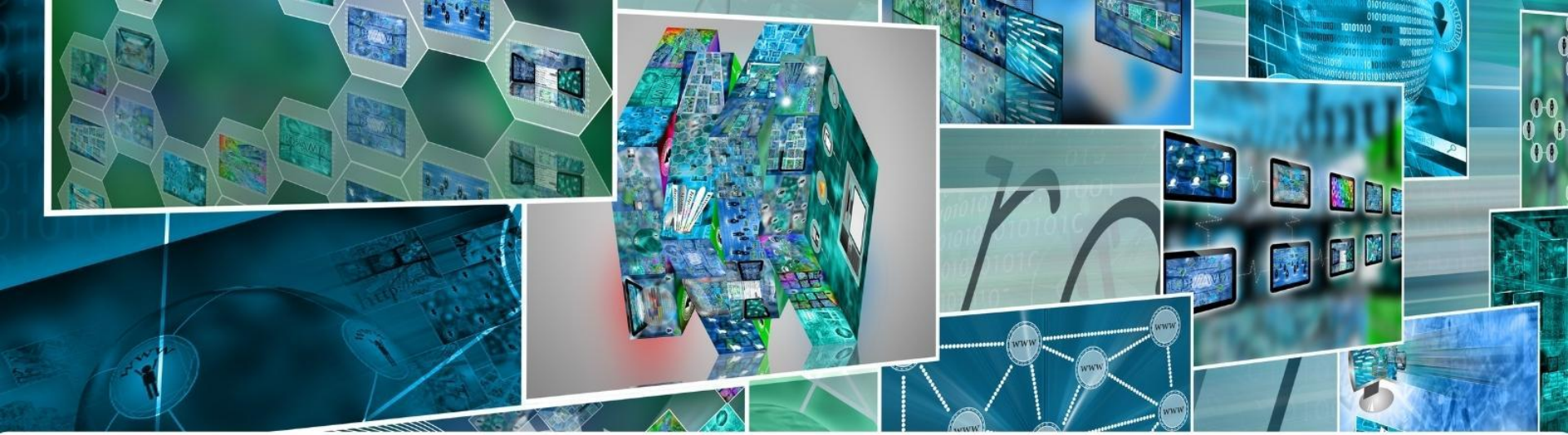


WATCHING THE WATCHERS

Better Late Than Never! Bill 88's Electronic Monitoring Policy Requirements

Join an Employment Lawyer, Privacy Lawyer & Privacy Consultant for a Free Webinar, Followed by a Q&A

spring LAW

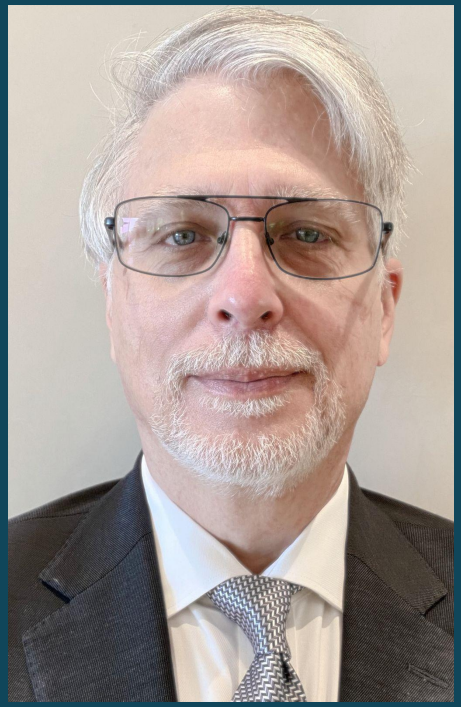
NNovation LLP

THE PRIVACY PRO

October 19 | 10:30 am - 11:30 EST

Lisa Stam

Spring LAW



Constantine Karbaliotis

NNovation LLP

Lauren Reid

THE PRIVACY PRO

Land Acknowledgement

We acknowledge that we are on the traditional territory of many nations including the Mississaugas of the Credit, the Anishnabeg, the Chippewa, the Haudenosaunee and the Wendat peoples and that this territory is now home to many diverse First Nations, Inuit and Métis peoples.

Legal Disclaimers

Timmy doesn't need a disclaimer but we do...

Even when it seems obvious

Legal Disclaimers

1) The content of this webinar should not be relied upon as legal advice.
2) Attending, accessing or viewing this webinar does not create a client relationship with anyone at SpringLaw, nNovation or The Privacy Pro.
3) You should apply your own judgement in making any use of any content from this webinar, including the use of the information as the basis for any conclusions. Every case and set of facts is different and unique to you - our videos are informational only.
4) The law changes quickly in Canada. We do not guarantee that the content of our recorded webinar video is accurate, complete or up-to-date given how quickly the law can change. SpringLaw, nNovation and The Privacy Pro assume no obligation to update the content. We assume no responsibility for errors or omissions in the content or other documents that are referenced by or linked to in the video. The content of this webinar may be changed without notice to you.

Please contact us if you have any questions about any of our content or your legal matter generally.

Presentation Roadmap

- Background
- Implications
- Your Gameplan
- Questions?

Background of Bill 88

Background of Bill 88

- The “Working for Workers Act 2022” amends the Employment Standards Act on Ontario
- Applies to organizations employing more than 25 employees
- Requires employers to, by October 11, 2022:
  - Provide a written policy that outlines workplace monitoring
  - Keep it up to date when changes are made

What does Bill 88 require?

- A policy must be provided in writing, either on the organization's intranet, or posted
- Must define the purposes for which employees are monitored:
  - Ensure that employees understand whether it applies to general or specific monitoring
  - Inform employees if their devices are being monitored

Nuances

- This year, applies to organizations that have 25 or more employees as at January 1, 2022
- For future years, employers having 25 or more employees on January 1st of any year, must have a policy in place by March 1st of each year
- Employees includes probationary employees, trainees, officers, employees on lay-off/leave
- Count must include all Ontario locations, as well as temporary staff; part-time/casual each count as ‘one’

Temporary staff

- Where an employer is obliged to provide notice, it must also be made to ‘assignment employees’ (temporary staff) and notice must include their roles
- Temporary staffing agencies must also provide a notice if they exceed 25 employees

What the policy has to say

- Policy must state that the employer may electronically monitor employees
  - What are the circumstances of monitoring, and the purposes for which the data might be used
  - The policy has to include all forms of electronic monitoring; if no monitoring is done, the policy must say this
  - The date the policy was prepared and the data any changes were made

Implications of Bill 88

Application

- This is not limited to devices provided or issued by the employer, or to work being done at home or remote locations
- Includes many forms of monitoring:
  - GPS/geolocation
  - CCTV
  - Performance monitoring
  - Monitoring electronic communications (email, chat, web usage)

Consequences?

- The Bill does not limit the kinds of monitoring, nor does it restrict the potential uses of monitoring (whether or not a use may not be detailed in the policy)
  - Complaints under the *Employment Standards Act* are limited to whether the policy is provided
  - Could presumably include they actually disclose the monitoring
- *Quaere*: Does this have implications outside the Employment Standards Act?

Disciplining Employees

- Can you rely on data gathered for disciplining employees?
  - Is purpose of collection capturing discipline?
  - If unionized, does CBA permit this?
  - What formal notice requirements are in place?
- *Should* you rely on data gathered?

HR Law & Data

- Evidence rules may exclude the info gathered:
  - Was the measure used necessary?
  - Was the measure likely to be effective?
  - Was loss of employee privacy proportional to the benefit gained?
- Guiding best practice - *is there a less intrusive way to gather the information?*

Relying on Data to Discipline Employees

- More likely YES can rely on evidence if:
  - Improve customer service
  - Protect assets and network security
  - Enhance employee safety (e.g. missing persons case, high crime storefront area)
  - For GPS in vehicles, for dispatch efficiency and track stolen vehicles
  - In investigations to determine potential breach of law or contract

- More likely NO cannot rely on evidence if:
  - Performance managing employees where employee privacy interests outweigh business needs
  - No advance notice was given nor consent provided
  - A less intrusive option was available
  - In unionized workforces without express CBA permission

HR Law Risks

- Constructive Dismissal claim in all provinces
- Invasion of privacy tort claims in all provinces
- Grievance in unionized workplaces in all provinces
- Claims under privacy acts in applicable provinces (not Ontario)
- **Attrition & business reputation** (← biggest risk)

Key takeaways

- Doubtful whether the high-level, generic statements in most employee privacy notices/policies meet the specificity requirements of Bill 88
- Most organizations are only dimly aware of the monitoring they are doing
- You may need have a discussion with staff you didn't have before about what is reasonable to monitor
- If you don't disclose your monitoring (adequately), consider whether you can rely on the evidence

Your Gameplan

Game Plan

- Find out what monitoring is currently taking place
- Decide what to do (you have options)
- Publish a policy
- Communicate thoughtfully, and be prepared for questions from employees

October 11
is 20 calendar days and
15 business days away

What is monitoring?

- Loss prevention
  - Using cameras and sensors to detect and deter theft
  - Using GPS devices to track the location of vehicles
- Security
  - Using Data Loss Prevention (DLP) tools to detect and prevent unauthorized activity
  - Monitoring employees' home environment to identify non-compliant behaviour such as others in the home, presence of mobile cameras
- Compliance
  - Monitoring communication of investment advisors to detect insider trading
- Productivity
  - Monitoring idle time, website and app usage
  - Automatically tracking attendance using badge access, computer logon
- Performance
  - Recording calls and meetings for quality and training purposes
- Operations
  - Fleet management tools to optimize routes


GONG
cloudtalk
TERAMIND
allego
JustCall
ActivTrak
KICKidler
Salesloft.
Hubstaff
mindtickle
Chorus
by zoominfo
WORKTIME®
INVOCA
(Veriato)
WING MAN PARTNERS
WE'VE GOT YOUR BACK
MeetRecord
apploye
Insightful
AVOMA
HubSpot
ptimus Hive
DeskTrack
CallRail
CallMiner
Time Champ
(Interguard)
Office 365
CONTROLIO
DeskTime
EKRAN
hexnode
Time Doctor
Prodoscore™
Revenue
Backlsh
Till one of kind
traqq
fireflies.ai


Groups Filter
All
Support
0 Notifications
user@company.com
myGEOTAB
Getting Started & Help
Dashboard
Map
Vehicles
Activity
Maps BI
Engine & Maintenance
Zones & Messages
Rules & Groups
Driver Safety Scorecard
Average Score
75.25
14%
14%
43%
29%
Low Risk
Mild Risk
Medium Risk
High Risk
Fleet Mileage (last week)
Sun 881
Mon 786
Tue 824
Wed 1,031
Thu 549
Fri 629
Sat 1,145
0
500
1000
1500
Last 3 Months Fuel Trend
Fuel Burned
1600
1400
1200
1000
800
600
400
200
0
March 2017
April 2017
May 2017
Month
Top 5 Aggressive Drivers
45
40
Driver 11
Driver 6
Driver 1
Driver 21
Driver 18
Harsh Braking
Harsh Cornering
Hard Acceleration
Top 5 Seatbelt Violations
Incident Count
450
400
350
300
250
200
150
100
50
0
Vehicle 8
Vehicle 11
Vehicle 4
Vehicle 23

take a guided tour

START A FREE TRIAL

TERAMIND

- TIME TRACKING
- BI REPORTS
- DASHBOARDS
- MONITORING
- RISK
- PRODUCTIVITY
- BEHAVIOR
- EMPLOYEES
- COMPUTERS
- CONFIGURE
- SYSTEM

TRY TERAMIND

Snapshots of Chadwick Singh

Screen snapshots

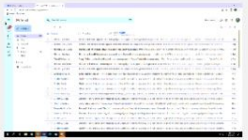
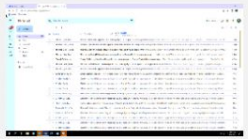
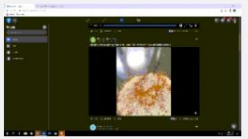
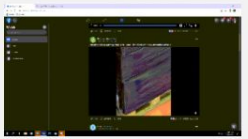
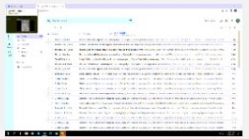
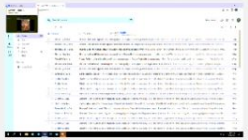
Ozzy Admini
Administrator

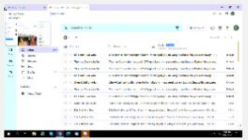
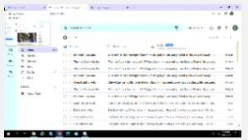
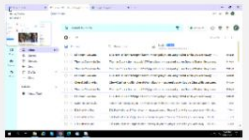
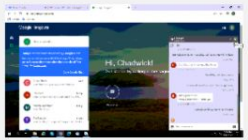
‹ Sep 19, 2022 ›

Chadwick Singh

win-035khor8ter

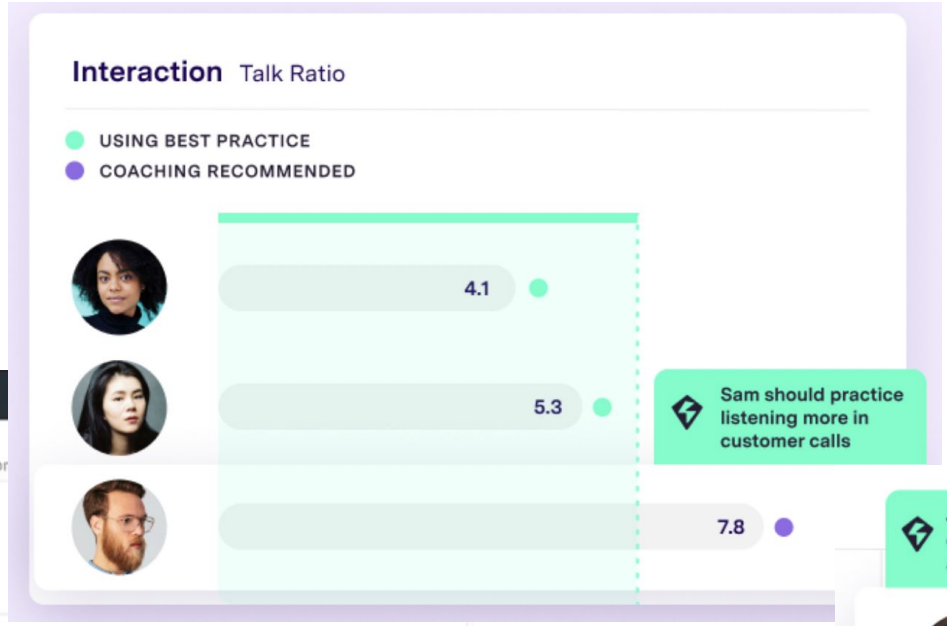
ADD/REMOVE TIME

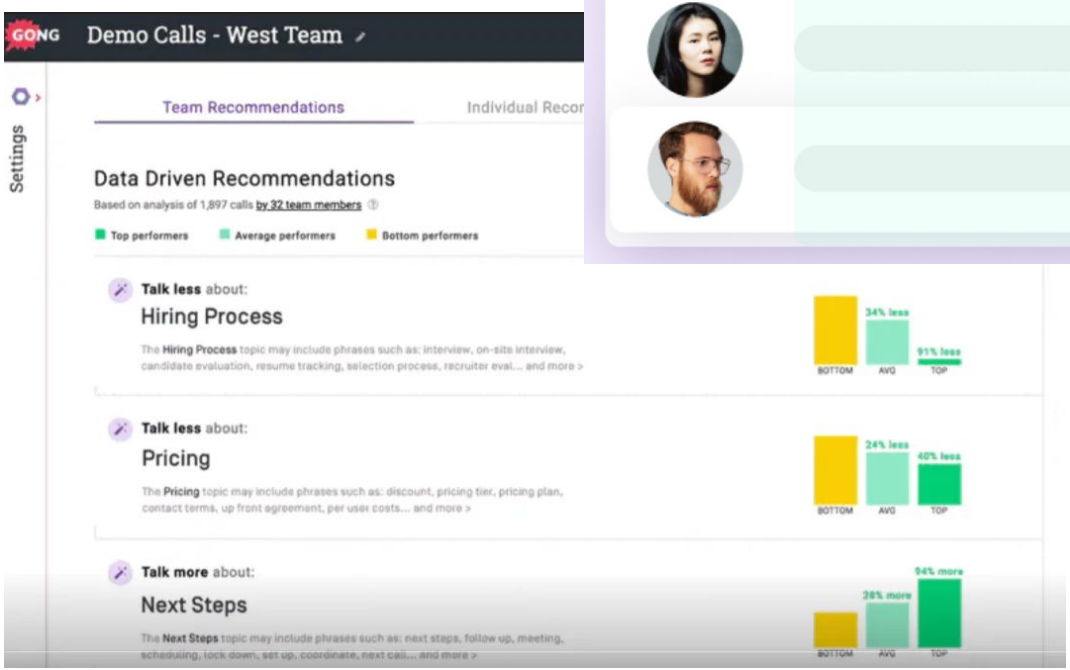
0:00	0:10	0:20	0:30	0:40	0:50
Productive	Productive	Unproductive	Productive	Unproductive	Productive
					
Plan 1%	Plan 12%	Plan 18%	Plan 10%	Plan 13%	Plan 0%

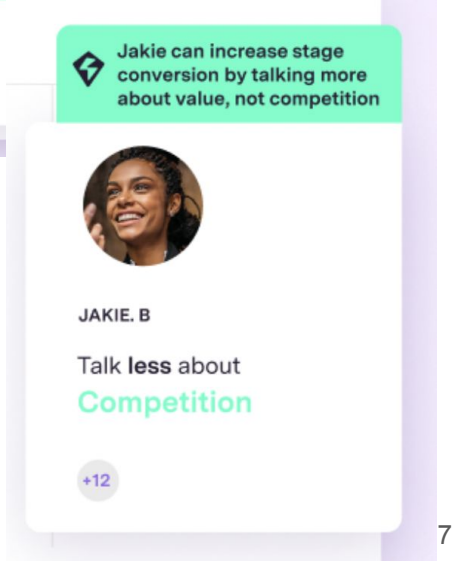
1:00	1:10	1:20	1:30	1:40	1:50
Productive	Productive	Productive	Productive	Productive	Productive
					
Plan 47%	Plan 43%	Plan 40%	Plan 48%	Plan 91%	Plan 32%

Help

GONG


Interaction Talk Ratio
USING BEST PRACTICE
COACHING RECOMMENDED
4.1
5.3
7.8
Sam should practice listening more in customer calls


GONG
Demo Calls - West Team
Settings
Team Recommendations
Individual Recor
Data Driven Recommendations
Based on analysis of 1,897 calls by 32 team members
Top performers
Average performers
Bottom performers
Talk less about:
Hiring Process
The Hiring Process topic may include phrases such as: interview, on-site interview, candidate evaluation, resume tracking, selection process, recruiter eval... and more >
34% less
91% less
BOTTOM
AVG
TOP
Talk less about:
Pricing
The Pricing topic may include phrases such as: discount, pricing tier, pricing plan, contact terms, up front agreement, per user costs... and more >
24% less
40% less
BOTTOM
AVG
TOP
Talk more about:
Next Steps
The Next Steps topic may include phrases such as: next steps, follow up, meeting, scheduling, lock down, set up, coordinate, next call... and more >
28% more
94% more
BOTTOM
AVG
TOP

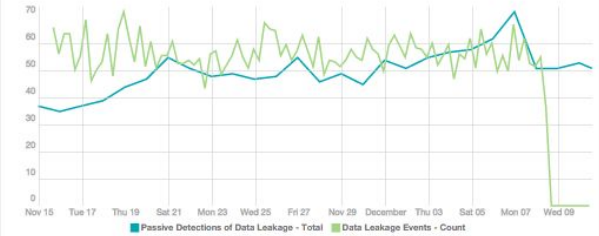

Jakie can increase stage conversion by talking more about value, not competition
JAKIE. B
Talk less about
Competition
+12

SecurityCenter | Dashboard | Analysis | Scans | Reporting | Assets | Workflow | Users

Data Leakage Monitoring

Switch Dashboard | Options

Data Leakage Monitoring - 25-Day Trend



Last Updated: 1 minute ago

Data Leakage Monitoring - Vulnerabilities that Could Lead to Data Leakage

Account	Anonymous	Authenticate	Bypass	Certificate
Credentials	Crypto	Default	Disclosure	Leak
Man-in-the-Middle	MitM	Password	SSL	TLS

Last Updated: Less than a minute ago

Data Leakage Monitoring - Activity with Potential for Data Leakage

Cloud Services	Cloud Storage	E-mail Attachment	FTP
Internet Messaging	Large Xfr TCP	Long TCP	Outbound to External IP
Outbound to Malicious IP	Peer-to-Peer	USB	USB Events

Last Updated: Less than a minute ago

Data Leakage Monitoring - Indicators

Confidential Data	Credit Card Number	Credit Card Number	Office File
Password	PDF File	Private Key	PST / OST File
Sensitive Data	Social Security Number	Social Security Number	User Info
Email Attachment	FTP	Client Data Leakage	Server Data Leakage
File Detection	Files Detection	File Download	File Upload

Last Updated: Less than a minute ago

Data Leakage Monitoring - Top 10 Subnets with the Most Passive Detections

IP Address	Total	Vulnerabilities
[redacted]	9	3, 6
[redacted]	9	3, 6
[redacted]	5	5
[redacted]	4	4
[redacted]	3	3

Last Updated: 1 minute ago

Data Leakage Monitoring - Top 10 Systems with the Most Passive Detections

IP Address	DNS	MAC Address	Total	Vulnerabilities
[redacted]			1	1
[redacted]			1	1
[redacted]			1	1
[redacted]			1	1
[redacted]			1	1

Last Updated: 1 minute ago

Data Leakage Monitoring - Top 10 Ports Most Associated with Passive Detections

Port	Total	Vulnerabilities
59998	2	2
51496	2	2
50781	2	2
80	45	45

Last Updated: 1 minute ago

Data Leakage Monitoring - Top 10 Most Prevalent Passive Detections

Plugin ID	Name	Severity	Host Total	Total
4674	Flash '.swf' File Detection	Info	31	31
7137	Client Data Leakage Detection (Username and Password)	Medium	6	6
4677	User Credentials Stored in Cookie	Info	6	6
3963	.pdf Document File Detection	Info	3	3
4711	'.dll' File Detection	Info	2	2

Last Updated: 1 minute ago

Data Leakage Monitoring - Top 10 Most Prevalent Events (Last 72 Hours)

Event	Count	Trend Data
PVS-Credit_Card_Client_Data_Leakage_Detected	25	
Snort-Sensitive_Data	21	
PVS-Credit_Card_Server_Data_Leakage_Detected	19	
PVS-Social_Security_Number_Client_Data_Leakage_Detected	19	
iGuard-ACT-DBF_Leaving_Network	12	
iGuard-Unauthorized_Desktop_Sharing	11	
iGuard-Audit_Examination_Reports	10	
iGuard-Compress_Attachments	10	
iGuard-Credit_Report	10	
iGuard-Financial_Reports	10	

Last Updated: 1 minute ago

tenable

What monitoring activities are in place?

- Ask people!
  - Most employee monitoring activities are carried out for reasonable purposes - set the tone and demonstrate you understand this by using a prepared agenda
  - Expect (and respect/appreciate) reluctance to share details
- Help people double check
  - List of common software tools - don’t forget to consider ‘Shadow IT’
  - Consider the tools as well as the features including free trials and ‘beta’ versions

Ask yourself

and your IT, HR, Operations, Security, Sales, and management teams…

- Does this spark joy?
- What is the goal or purpose of this monitoring activity?
- Is it the least privacy intrusive way to accomplish that goal?
- Is it working?
- How do you know?

Think about the (natural) consequences

In addition to the the legal and regulatory consequences in Ontario...

- How will your employees feel about it?
- How will your employees in BC, Alberta, or Quebec (provinces with privacy laws that protect employees) react?
- How will look on TikTok? Glassdoor? Twitter?

Decide what to do
(you have options)

- Stop doing it or adjust the approach
  - Limit collection, adjust settings
  - Brag about it! (put it in the policy)
- Keep doing it, and be transparent
  - Publish a policy in compliance with Ontario Bill 88
- Keep doing it, don't tell anyone, and hope no one finds out
  - Understand and accept the (ESA legal) risk

What policies are in place?

- Review what policies are already in place that may need to be synced up:
  - monitoring employees
  - remote working
  - expectation of privacy language
  - online/offline conduct
- Unionized? Work with the union to sync up Collective Agreement language (and expectations)

Communicate thoughtfully

- Go beyond what is required by law
- Explain why the monitoring is necessary
- Share how employee's privacy is protected - what are their rights? How do you control access to and use of the data?
- Consider providing alternatives, such as a company issued device instead of installing endpoint monitoring on personal devices

We can help...

SWAT Team Service Package

Meet with experts in employment law, privacy law, and operational privacy

Employee Monitoring Policy Template - customized

Interview Accelerators

- Pre-interview questionnaire
- List of commonly used tools that have monitoring capabilities

Summary report

- What we found
- Issues & recommendations

Thank you! Questions?

Lisa Stam
lstam@springlaw.ca

Constantine Karbaliotis
ckarbaliotis@nnovation.com

Lauren Reid
lauren@theprivacypro.com

Spring LAW

NNovation LLP

THE PRIVACY PRO