



# EMERGING TRENDS IN INFORMATION ACCESS, SECURITY, AND PRIVACY COMPLIANCE

---

## Ontario Municipal Sector

AMCTO Zone 3 Meeting  
November 15th, 2023

# SESSION OBJECTIVES

- 1 **DISCUSS** emerging trends in information access, security, and privacy compliance
- 2 **SHARE** eight steps to implementing an effective information access, security, and privacy compliance program.
- 3 **QUESTIONS** please, ask away!

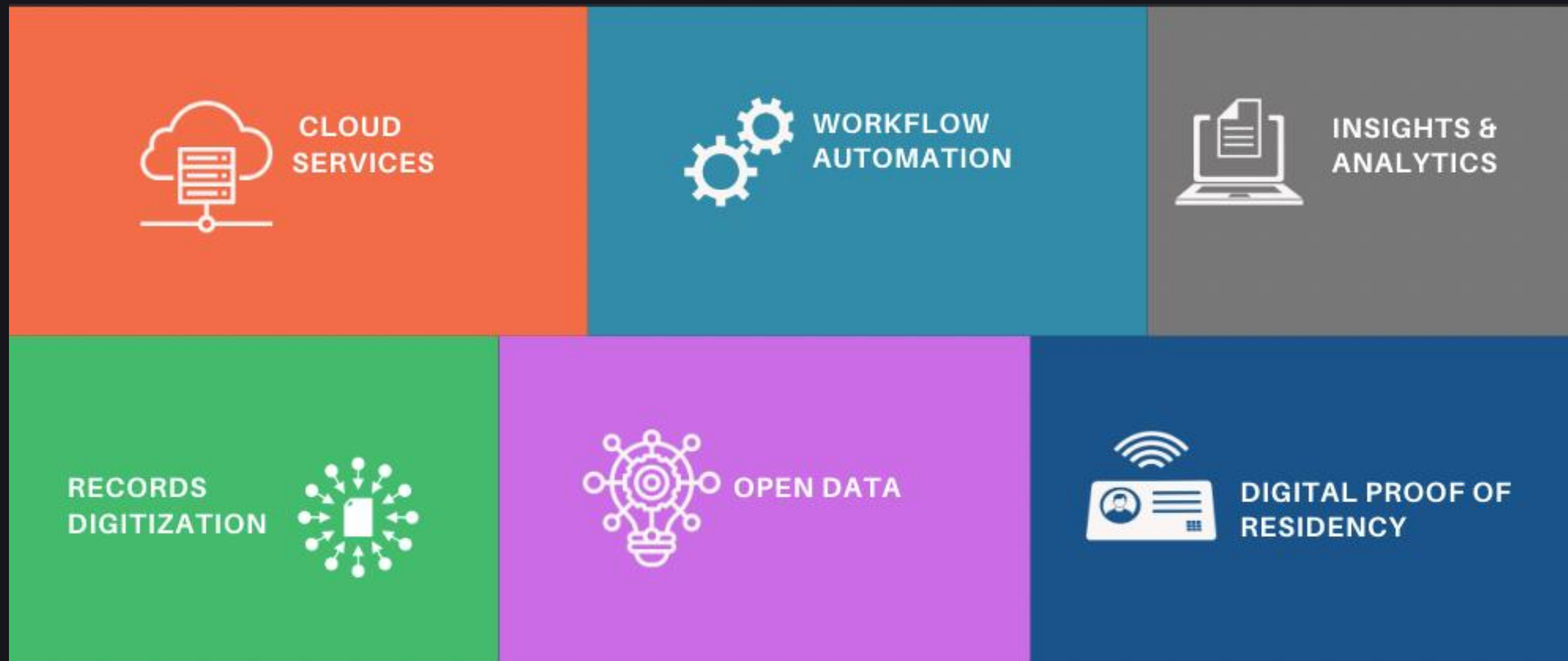


Four secular trends are bringing information compliance to the forefront of municipal risk discussions.

# #1

## MORE DATA IS MOVING ONLINE

Digital transformation initiatives are creating a surge in personal and sensitive information hosted internally and with cloud providers.





# MFIPPA

# 2023

## #2

## LEGISLATION IS CHANGING

Modernized privacy legislation is being introduced at a country, province/state, and sector level across North America.



### FEDERAL LAW: BILL C-26 TABLED NOV, 2021

- Critical infrastructure focused
- Mandatory cybersecurity programs
- Implement defense technologies
- Supply chain risk management
- Incident records retention
- Significant fines



### FEDERAL LAW: BILL C-27/CPPA\* PASSED SECOND READING

- Privacy program required
- Possible PIA obligations
- Privacy by Design
- New consent rules
- New retention rules
- Minors classified as sensitive data
- Service provider compliance
- Significant fines (3-5%/\$25M)



### QUEBEC: BILL 64 ENACTED SEPTEMBER, 2021

- Designate Privacy Officer
- Privacy program required
- New PIA obligations
- Privacy by Design
- New consent rules
- Adequacy principle for data sharing
- Significant fines (4%/\$25M)



### B.C.: BILL 22 (FIPPA) ENACTED NOVEMBER, 2021

- Privacy program required
- PIA obligations
- Service provider compliance
- Data protection obligations
- New breach reporting obligations
- Repeals in-Canada hosting
- Significant fines for individuals, service providers, and corporations

\*Digital Charter Implementation Act 2022 has been referred to the House of Commons Standing Committee on Industry and Technology. Bill C-27 would repeal PIPEDA and enact the Consumer Privacy Protection Law (CPPA), Data Protection Tribunal Act (DIPTA), and the Artificial Intelligence Data Act (AIDA).

@Vayle Inc. All Rights Reserved.



# #3

## CYBER ATTACKS ARE SURGING

As municipalities move data online, their attack surface expands, creating more potential entry points for cybercriminals. This has led to difficulties in securing cyber insurance.

MANAGEMENT | CYBERSECURITY | SECURITY NEWSWIRE | CYBERSECURITY NEWS

### Global cyberattacks increased 38% in 2022

By Joy LePree Anderson



Image via Pixabay

FEDERAL POLITICS

## Hackers attacked the Canadian government 2,300,000,000,000 times last year

The Communications Security Establishment says its online defences search for unusual activity like efforts to deploy malware, map government computer systems, and extract information.

By Alex Ballingall Ottawa Bureau

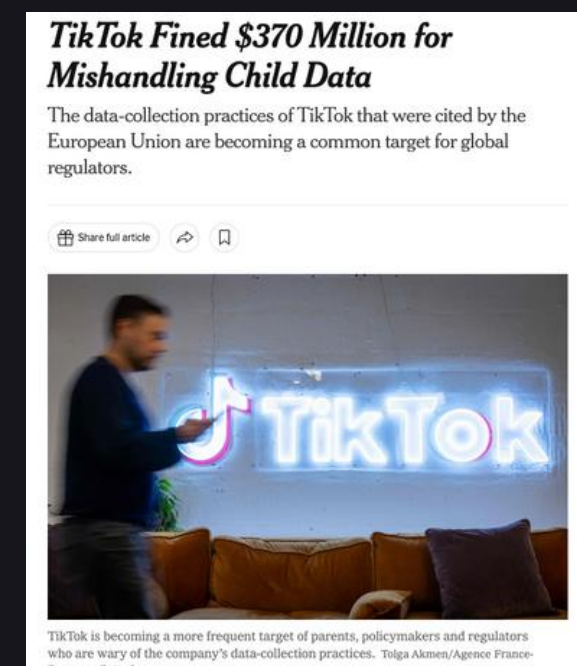
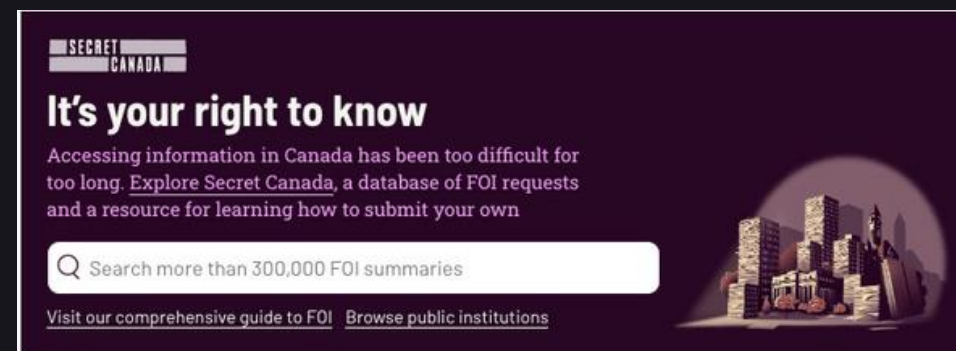
Thursday, June 29, 2023 | 2 min to read



# #4

## MEDIA COVERAGE IS ON THE RISE

Articles related to data privacy, data breaches, and information access issues are surfacing in the media daily.



### Quebec municipal transportation data ends up on dark web forum after cyber attack

By Cosmin Dzsurdza - December 22, 2021





Eight best practices for municipalities to bolster their privacy and information access programs.



Rome Wasn't  
Built in a Day!



#1

# ESTABLISH PRIVACY MISSION AND PRINCIPLES

## Municipality Vision

*"Our Vision is that the Township of Anywhere..."*

## Municipality Privacy Mission

*(A simple and clear statement that reflects what you do every day)*

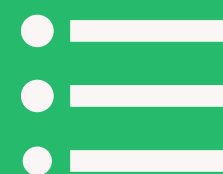
## Privacy Program Guiding Principles

*(A set of fundamental beliefs, values, or rules that you will use to guide decision making for your privacy program)*

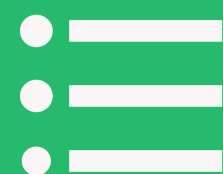
## Privacy Legislation and Municipality's Policy Requirements

## Privacy Program Pillars (Capabilities)

Governance



Responsible



Proactive



Transparent





# PRIVACY MISSION STATEMENT EXAMPLES



At Manulife, our Mission is to make decisions easier and our customers' lives better. We are putting our customers first and leveraging technology to deliver on this promise. **This includes protecting information in our care, including what we collect through digital channels like our Websites and Apps.**



At Microsoft, our mission is to empower every person and every organization on the planet to achieve more<...>**This starts with making sure you get meaningful choices about how and why data is collected and used and ensuring that you have the information you need to make the choices that are right for you across our products and services. We are working to earn your trust every day by focusing on six key privacy principles.**



# THE IMPORTANCE OF PRIVACY PROGRAM GUIDING PRINCIPLES

- **Defines** a set of fundamental beliefs, values, or rules you will use to guide decision-making for your municipality's Privacy Program.
- It distills the mandate (what to do) into statements of action and is directed at the stakeholders impacted by it.
- This differs from PIPEDA's 10 Fair Information Principles, which are rooted in legislation.




# PRIVACY GUIDING PRINCIPLES EXAMPLES

## Sunlife


## CRA


Our guiding data privacy principles highlight our commitment to Clients:



**1. We use Client data to deliver on our Purpose**


We're driven by our company's Purpose to help our Clients achieve lifetime financial security and live healthier lives. We use data to help create outcomes with our Clients' best interests at heart.


 [Learn more](#)



**2. We do not sell Client data**


We do not sell data that would identify an individual Client. There may be times when we share aggregate data and insights to help generate value for our Clients and align with our Purpose.

 [Learn more](#)



**3. We inform Clients about why we collect and use their data**

We are committed to being as clear as we can with our Clients about how we collect and use their data. We clearly outline their options. We continue to simplify the language we use to connect with our Clients.

 [Learn more](#)

**Privacy guiding principles**

To foster client trust and confidence in the CRA, we believe in establishing a language about privacy that will make sure we are working toward the same goals.

The following are our privacy guiding principles:

1. We value and respect the client data in our possession and help our clients clearly understand how and why we are using it.
2. We support our employees in understanding their data handling responsibilities, and we respond to our clients' requests promptly and helpfully to drive a seamless and efficient experience.
3. We put our clients at the heart of all changes and improvements to our service delivery by adopting innovative practices and including Privacy by Design principles into all that we do.
4. We collaborate with our employees and integrate effective and secure client data management across the CRA to foster a holistic approach to building and maintaining client trust.
5. We decide how we handle client data in line with legislative obligations and leading privacy practices and based on ethical standards.



#2

## ADOPT A PRIVACY FRAMEWORK

LEGISLATION &  
REGULATIONS



THE PRIVACY ACT  
PIPEDA  
(excl. BC/AB/QU)



FIPPA



MFIPPA

FRAMEWORKS

AICPA CICA PRIVACY FRAMEWORK

NIST PRIVACY FRAMEWORK

ISO/IEC 27701

### #3

## CONDUCT AN INTERNAL PRIVACY AUDIT

Jointly developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA), the AICPA CICA framework helps organizations strengthen their privacy policies, procedures and practices. It is based on Generally Accepted Privacy Principles (GAPP).

0%	AD HOC	Procedures or processes are informal, incomplete, and inconsistently applied.
25%	REPEATABLE	Procedures or processes exist; however, they are not fully documented and do not cover all relevant aspects.
50%	DEFINED	Procedures and processes are fully documented and implemented and cover all relevant aspects.
75%	MANAGED	Reviews are conducted to assess the effectiveness of controls in place.
100%	OPTIMIZED	Regular reviews and feedback are used to ensure continuous improvement towards optimization of the given processes.


\*Based on the AICPA/CICA Privacy Maturity Model (PMM).

# AICPA CICA PRIVACY FRAMEWORK

Jointly developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA), the AICPA CICA framework helps organizations develop and implement privacy programs.

GAP CRITERA	DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>Personal Information and Identification Classification (1.2.3)</b>	The types of personal information and sensitive personal information and the related processes, systems, and third parties involved in the handling of such information are identified . Such information is covered by the entity's privacy and related security policies and procedure.	The identification of personal information is irregular, incomplete, inconsistent, and potentially out of date. Personal information is not adequately addressed in the entity's privacy and related security policies and procedures. Personal information may not be differentiated from other information.	All personal information collected, used, stored and disclosed within the entity has been classified and risk rated.	All personal information is covered by the entity's privacy and related security policies and procedures. Procedures exist to monitor compliance. Personal information records are reviewed to ensure appropriate classification.	All personal information is covered by the entity's privacy and related security policies and procedures. Procedures exist to monitor compliance.	Management main- tains a record of all instances and uses of personal information. In addition, processes are in place to ensure changes to business processes and procedures and any supporting computerized systems, where personal information is involved, result in an updating of personal information records. Personal information records are reviewed to ensure appropriate classification.

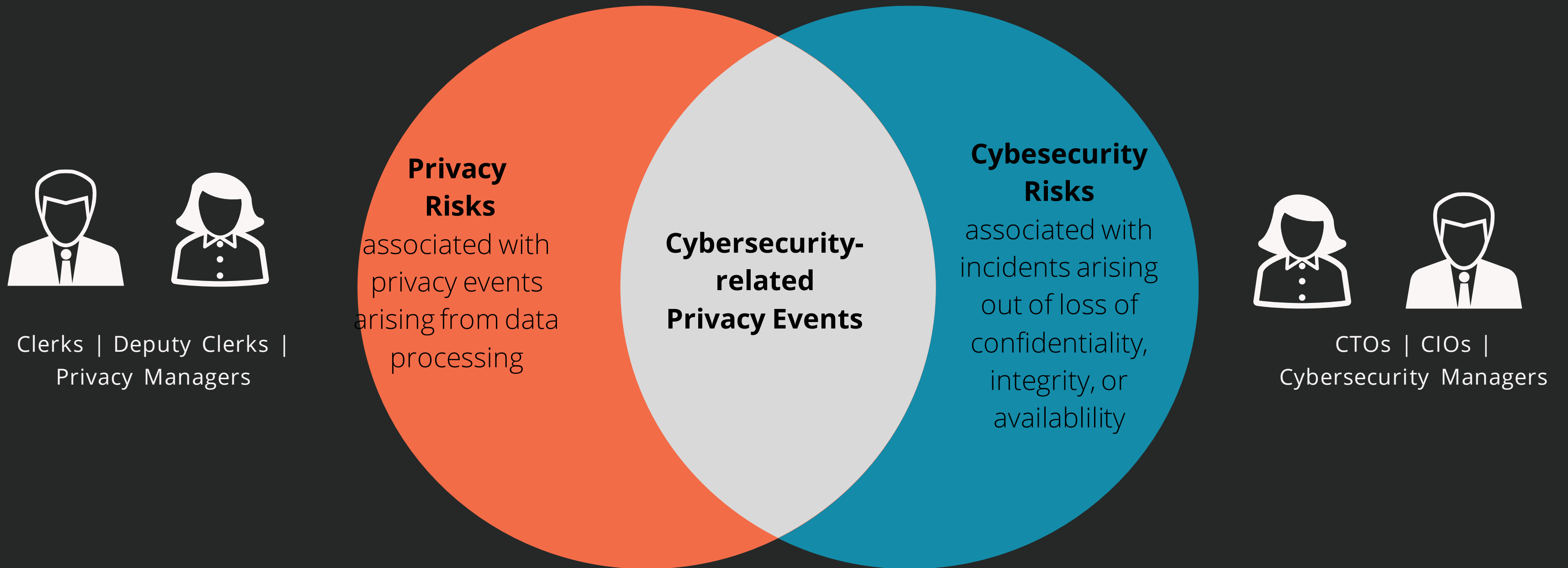


A black and white photograph of Tim Cook, CEO of Apple, speaking at a podium. He is wearing glasses and a dark zip-up jacket over a light-colored shirt. His right arm is extended to the side, and he is holding a small object in his left hand. The background is dark.

"Security is the foundation of privacy - because there is no privacy in a world where your private data can be stolen with impunity."

TIM COOK, CEO OF APPLE  
IAPP GLOBAL PRIVACY SUMMIT, APRIL 12th, 2022

Privacy compliance and cybersecurity have become increasingly interdependent, driven by emerging privacy regulations and controls frameworks.



Can you think of any examples where your municipality's ***Privacy*** and ***IT*** teams are interdependent?



# #4

## DEFINE ROLES AND RESPONSIBILITIES (RASCI)

Ensure that privacy and data protection roles and responsibilities are clearly defined and understood across the organization.



Privacy  
Champion

- Program Support
- Message from the Top



MFIPPA  
"head"

- Overall Compliance
- Policies & Procedures
- Training & Awareness
- Breach Oversight
- Reporting



Records  
Management

- Data Accuracy
- PIB Index
- FOI Records



FOI  
Lead

- FOI Request
- FOI Responses
- FOI Records



PIA  
Lead

- Risk Research
- Draft PIAs
- Vendor Assessments



Information  
Technology

- Data Protection
- Data Destruction
- STRAs
- Breach Readiness
- Breach Response

R

Responsible

A

Accountable

S

Supporting

C

Consulted

I

Informed

# RASCI - PI CLASSIFICATION

Consider utilizing a privacy framework to help create a RASCI for your municipality’s privacy program.

DELIVERABLE	CLERK	DEPUTY CLERK	RECORDS MGR	IT MANAGER	DB MANAGER
Maintain a record of all personal and sensitive information in the municipality’s custody and control.	Informed	Accountable	Responsible	Consulted	Supporting

## #4

# MAP AND CLASSIFY DATA

A Personal Information Bank ("PIB") is a collection of personal information ("PI") that is organized and capable of being retrieved using an individual's name or identifying number or other particular assigned to the individual.



### MFIPPA Requirements for PIB Index Management:

- Name, location
- Data sensitivity category
- Legal authority
- Types of data
- How the data is used
- Who the data is shared with( i.e. Cloud Providers)

# PERSONAL INFORMATION

Includes "recorded information about identifiable individual", including:

Name	Race	Medical Information
Physical Address	National Origin	Biometrics
Telephone Number	Ethnic Origin	Employment History
Email Address	Religion	Financial Transactions
IP Address	Marital Status	Criminal Records
Age	Family Status	Personal Opinions
Sex	Sexual Orientation	Private Correspondence





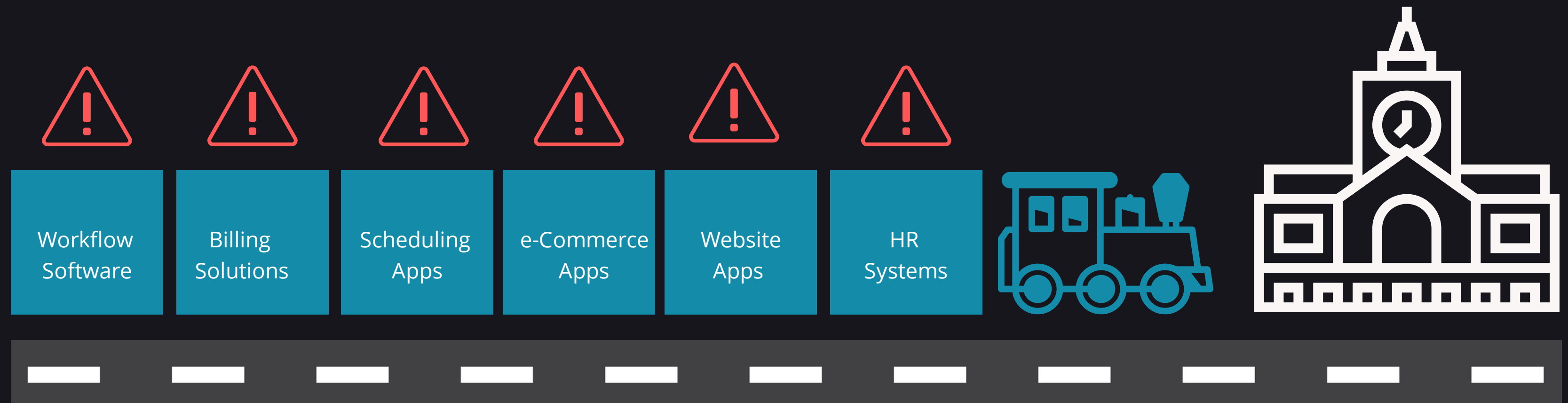
**Sensitive information** requires a higher duty of care. Examples include:

- Personal Health Information (PHI)
- Banking and Credit Card Data
- Ethnic and Racial Origins
- Political Opinions
- Genetic and Biometric Data
- Sexual Orientation
- Religious or Philosophical Beliefs
- **Tabled: Information Related to Minors**

# #5


## ASSESS AND MONITOR YOUR SUPPLIERS

Supply chain risks are introducing new privacy and data protection challenges for municipalities. Consider the applicable legislation when moving personal or sensitive information to the cloud.



# SBOM: WHY IT MATTERS

Organizations scrambled when trying to determine the risk associated with the Log4J vulnerability; the FTC threatened legal action for non-remediation.

 Government of Canada / Gouvernement du Canada

Search

MENU

[Canada.ca](#) > [Canadian Centre for Cyber Security](#) > [Alerts and advisories](#)

## Alert - Active exploitation of Apache Log4j vulnerability - update 7

From: [Canadian Centre for Cyber Security](#)

Number: AL21-019 - Update 7  
Date: December 10, 2021  
Updated: December 29, 2021

### Audience

This Alert is intended for IT professionals and managers of notified organizations. Recipients of this information may redistribute it within their respective organizations.

### Purpose

An Alert is used to raise awareness of a recently identified cyber threat that may impact cyber information assets, and to provide additional detection and mitigation advice to recipients. The Canadian Centre for Cyber Security ("Cyber Centre") is also available to provide additional assistance regarding the content of this Alert to recipients as requested.

January 11, 2022

## FTC Warns Use of "Full Legal Authority" on Companies That Ignore Log4j Risk

[in LinkedIn](#) [f Facebook](#) [t Twitter](#) [Send](#) [Embed](#)

BRACEWELL

The Federal Trade Commission (FTC) sent a strong message to organizations in the wake of the [Log4j security vulnerability](#): patch now or face regulatory scrutiny and potential legal action.

In the [notice issued last week](#), the FTC acknowledged and emphasized that the Log4j vulnerability is being exploited by a growing set of attackers, which “risks a loss or breach of personal information, financial loss, and other irreversible harms.” The FTC made clear that, pursuant to federal laws such as the Federal Trade Commission Act and the Gramm-Leach-Bliley Act, organizations have “a duty to take reasonable steps to mitigate known software vulnerabilities.” Finally, the FTC cited to prior enforcement actions and stated that the agency will not hesitate to use its full legal authority “to

WRITTEN BY:

BRACEWELL  
[Contact](#) [+ Follow](#)

PUBLISHED IN:

[Cybersecurity](#) [+ Follow](#)

[FTC](#) [+ Follow](#)

[FTC Act](#) [+ Follow](#)

[Gramm-Leach-Bliley Act](#) [+ Follow](#)

[Homeland Security Cybersecurity & Infrastructure Security Agency \(CISA\)](#) [+ Follow](#)



#6

## CONDUCT PRIVACY IMPACT ASSESSMENTS

A Privacy Impact Assessment (PIA) is a process which assists organizations in identifying and managing the privacy risks arising from new projects, initiatives, systems, processes, strategies, policies, and business relationships.

1

CONDUCT PRELIMINARY ANALYSIS

2

ASSEMBLE PIA TEAM

3

DATA INVENTORY AND MAPPING

4

ESTABLISH LEGAL AUTHORITY

5

CONDUCT PRIVACY ANALYSIS

6

PREPARE PIA REPORT

7

MONITOR COMPLIANCE & CHANGES

# FOI PROGRAM CHALLENGES

Over 100 Ontario local government entities recently participated a research study conducted by Vayle; the majority cited lack of resources to address increasing FOI volumes.

1

FOI REQUESTS UP

Most municipalities (52%) and police agencies (67%) experienced increased FOI requests, particularly among higher-volume processors.

2

BUDGETS FLAT

Despite increased volumes, most municipalities (90%) and police agencies (76%) budgets remained flat.

3

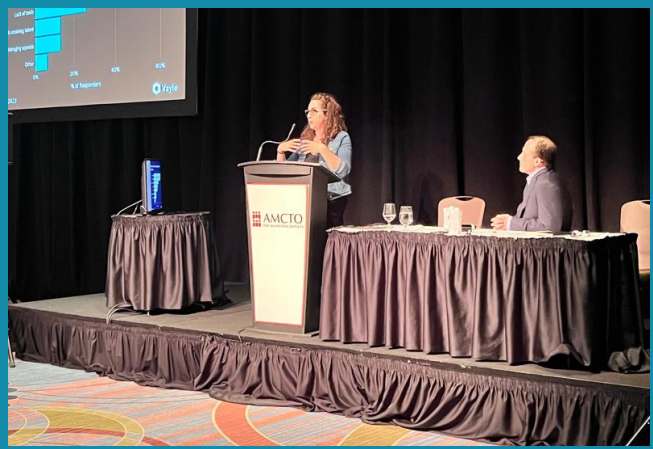
LACKING TOOLS

Most municipalities continue to use inefficient and non-purpose-built applications such as Microsoft Word, Excel, and Adobe.

4

TOP CHALLENGES

The top challenges cited by municipalities and police agencies cited a lack of FOI team resources, responding in a timely manner, and increased FOI request complexity.



# #7

## AUTOMATE COMPLIANCE PROCESSES

Organizations that embrace technology to automate their information compliance programs can save time, reduce costs, and mitigate risks. **AI will be a critical enabler.**



Information compliance automation opportunities:

- Data mapping and classification
- Vendor questionnaires and tracking
- Online training, testing and simulations
- FOI request management



#8

## CREATE AN INTEGRATED TRAINING APPROACH

Cybersecurity and privacy compliance training is most effective when provided in an integrated curriculum and medium.



Cyber Security



Privacy and FOI

Check out our latest op-eds and Blogs at [www.vayle.io](http://www.vayle.io)



## **AUTOMATE! AUTOMATE! AUTOMATE!**

Media Publications

[Read more ▶](#)



## **Bolstering your municipality's data privacy and protection program**

Media Publications

[Read more ▶](#)

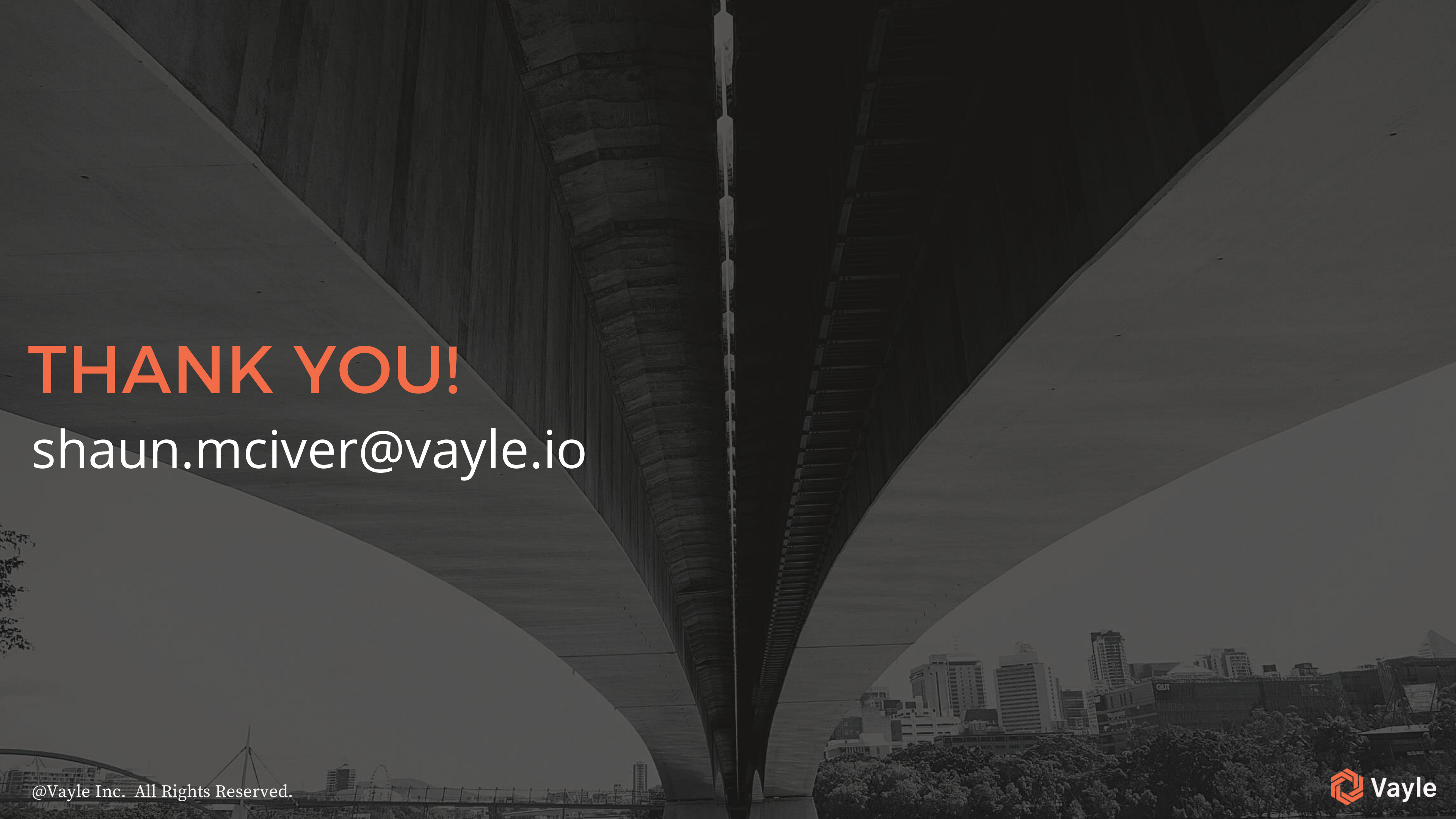


## **7 steps to undertaking a Privacy Impact Assessment**

Media Publications

[Read more ▶](#)





**THANK YOU!**

shaun.mciver@vayle.io