# Effective Data Governance for Changing Times


## Fred Carter

Senior Policy & Technology Advisor


Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

TDSB
IT Symposium 2022

7 July 2022

# Information and Privacy Commissioner of Ontario

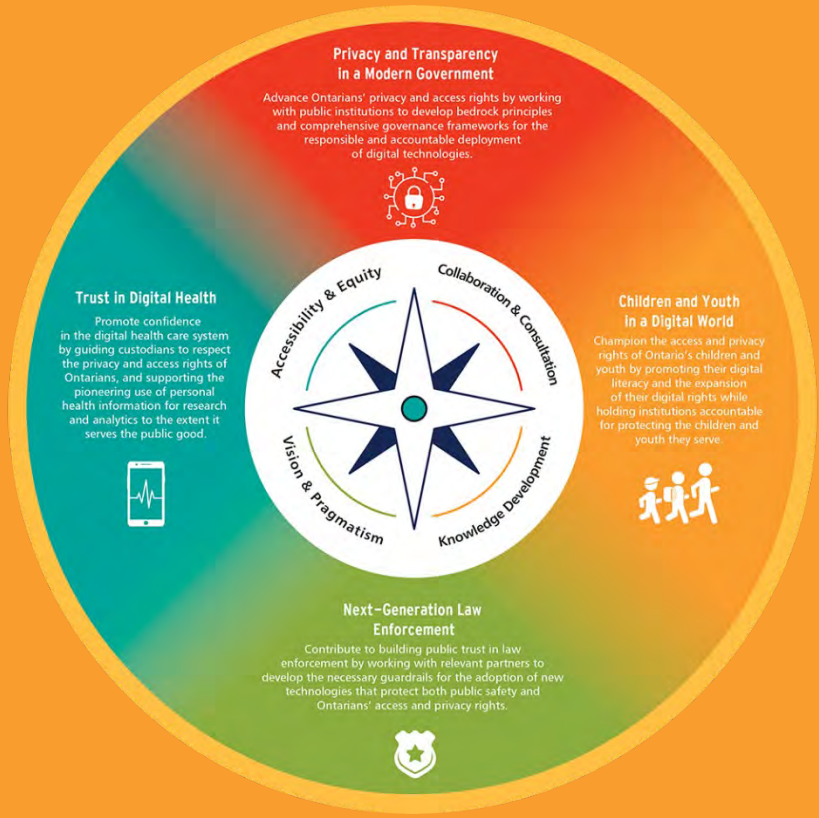
- investigates privacy complaints related to personal information
- resolves appeals when there is a refusal to grant access to information
- ensures compliance with the acts we oversee
- reviews privacy policies and information practices
- conducts research on access and privacy issues and provide comment on proposed government legislation and programs
- Outreach to public, media and other stakeholders about Ontario’s access and privacy laws and current issues affecting access and privacy

# IPC's Strategic Priorities

- Privacy and Transparency in a Modern Government
- Children and Youth in a Digital World
- Next-generation Law Enforcement
- Trust in Digital Health

# Children and Youth in a Digital World

Champion the access and privacy rights of Ontario's children and youth by promoting their digital literacy and the expansion of their digital rights while holding institutions accountable for protecting the children and youth they serve.



# IPC Interest in Educational Technologies

- Classroom management and learning apps
- Video conferencing platforms
- Remote proctoring
- Student monitoring and surveillance
- Cloud computing and other third-party platforms
- Breaches of privacy and security

THE WALL STREET JOURNAL.

**Parental Opposition Fells inBloom Education-Software Firm**

Privacy Concerns Over Use of Student Data Lead Company to Close

## inBloom:

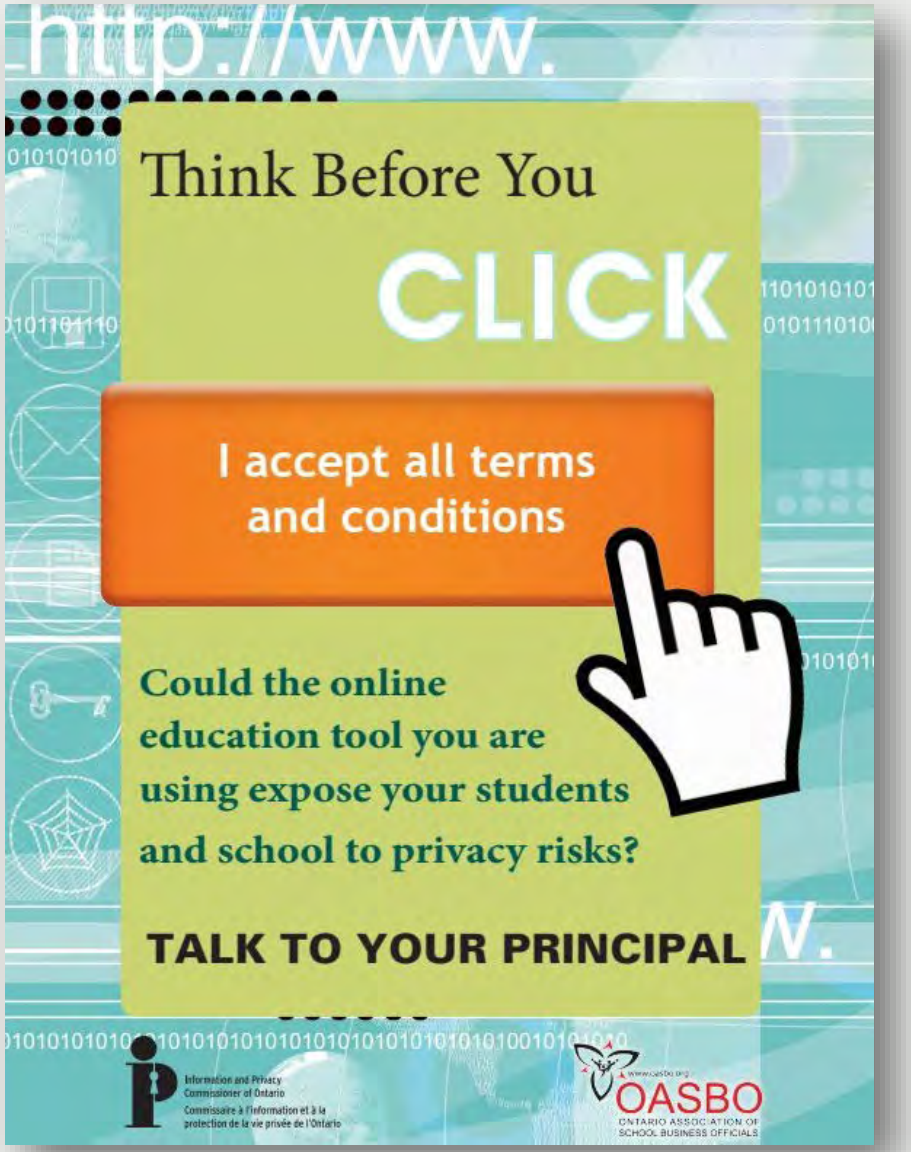
- Ambitious “high impact” ed tech initiative launched in 2013 with $100M funding
- Multi-state consortium and centralized cloud platform for data sharing, learning applications, and curricula
- “hydra-headed effort to collect personal data ... make it more easily accessible to ed tech vendors and other third parties without parental knowledge or consent.”

## Reactions:

- Huge public backlash
- Concerns about collection, use and disclosure of students’ personal information
- All nine participating U.S. states pulled out of InBloom, which ended in 2014
- Fallout led to student data privacy legislation, widespread attention to risks and vulnerabilities of ed tech projects

# Use of Online Educational Services

- School boards are accountable
- Caution when collecting, using or disclosing students' personal information online
- Some online educational tools and services:
  - collect personal information of students for non-educational purposes
  - track students' online activities outside of school
  - use students' behaviour and performance to target market products or services
  - disclose personal information to other parties




# Use of Online Educational Services

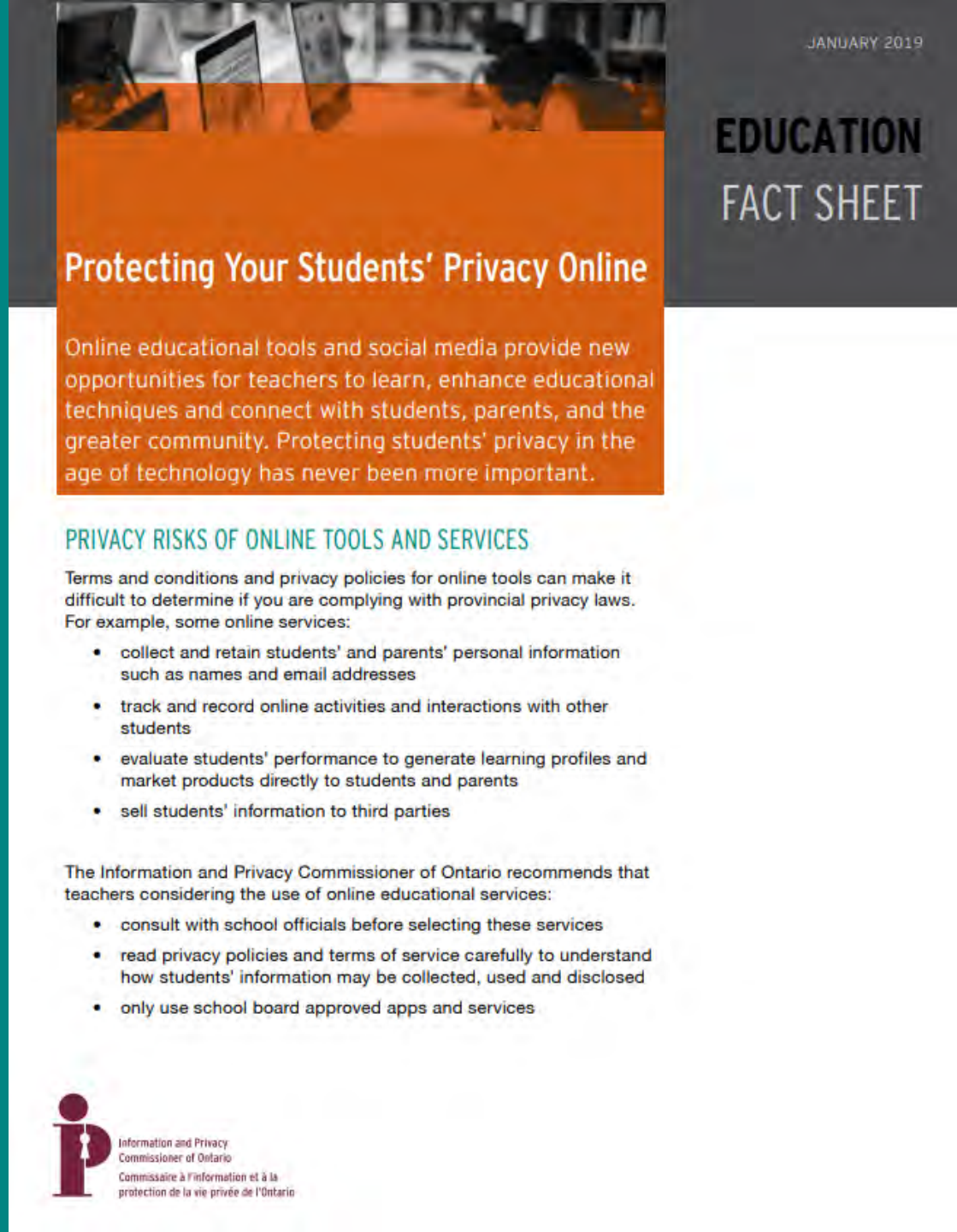
Best practices for school boards

- Policies to evaluate, approve online educational services
- Ensure staff and educators use only approved services
- Privacy and security training, ongoing support
- Notices of collection
- Opt-out (where feasible)
- Retention periods

# Protecting Students' Privacy Online

Teachers considering the use of online educational tools and services should:

- **Consult** with school officials
- Read and understand privacy policies and **terms of service**
- Use only apps and services **approved** by the school board and Ministry of Education
- Provide students with **guidance on use**
- Use services that **minimize** collection, use and disclosure of identifiable information



JANUARY 2019

EDUCATION
FACT SHEET

## Protecting Your Students' Privacy Online

Online educational tools and social media provide new opportunities for teachers to learn, enhance educational techniques and connect with students, parents, and the greater community. Protecting students' privacy in the age of technology has never been more important.

### PRIVACY RISKS OF ONLINE TOOLS AND SERVICES

Terms and conditions and privacy policies for online tools can make it difficult to determine if you are complying with provincial privacy laws. For example, some online services:

- collect and retain students' and parents' personal information such as names and email addresses
- track and record online activities and interactions with other students
- evaluate students' performance to generate learning profiles and market products directly to students and parents
- sell students' information to third parties

The Information and Privacy Commissioner of Ontario recommends that teachers considering the use of online educational services:

- consult with school officials before selecting these services
- read privacy policies and terms of service carefully to understand how students' information may be collected, used and disclosed
- only use school board approved apps and services

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

# IPC Privacy Complaint Reports

Use of cloud-based educational services by Ontario school boards:

1. MC18-48 – Security of attendance reporting platform (13 Apr 2021)
2. MC17-52 – Use of Google G-Suite for Education (23 Jul 2021)
3. MC18-17 – Use of third-party apps (7 Feb 2022)

Full text of these decisions available at:
www.ipc.on.ca/decisions

# MC18-48

**Complainant's concerns included:**

- board failure to obtain parental consent
- adequacy of notice of collection
- potential misuse of information by service provider
- adequacy and enforceability of board's contract terms
- Inadequate oversight of service provider's security measures

**Complainant also raised concerns relating to:**

- service provider's terms of use and privacy policy
- a specific security vulnerability that was exploited by the complainant.

# MC18-48

**Report concluded:**

- collection, use and disclosure of students' personal information was in compliance with MFIPPA
- reasonable contractual measures were in place to ensure the privacy and security of students' personal information
- board had not demonstrated reasonable oversight measures were in place to enforce contracted security obligations

Cont'd

# MC18-48

**Report recommended that the board:**

- amend contract with service provider
- strengthen and document board oversight of security measures
- advise parents that contract with the service provider prevails over the portal's posted terms of use and privacy policy

Cont'd

# MC17-52

**Complainant's concerns included:**

- failure to notify parents, and obtain consent to collect, use, and disclose students' personal information
- use of personal information beyond scope permitted under MFIPPA
- storage of personal information outside of Canada
- inadequate security protections
- lack of adequate data deletion and retention practices

# MC17-52

**Report concluded:**

- collection, use, and disclosure of personal information were in compliance with MFIPPA
- notice of collection was deficient
- reasonable contractual and oversight measures in place to ensure privacy and security of students' personal information

# MC17-52

**Report recommended the board:**

- improve transparency of collection notices
- improve oversight of service provider's security practices
  - regular security updates and briefings
  - evidence of compliance with contract commitments
- review significant developments in the scope of services and update privacy and security assessments as required

Cont'd

# MC18-17

**Complainant's concerns included:**

- failure to regulate third-party apps available to students
- failure to track which apps collected students' personal information and what information had been collected
- students' public posts exposed personal information
- third-party advertising to students
- reasonable measures not in place to ensure third parties protect students' personal information

Cont'd

# MC18-17

**Report concludes:**

- board's catalogue system regulating apps is in partial compliance with MFIPPA, but the board's notice of collection was deficient
- personal information was used for marketing purposes, contrary to MFIPPA
- board did not have reasonable contractual and oversight measures in place to ensure privacy and security of students' personal information

Cont'd

# MC18-17

**Report recommended the board:**

- review agreements with third-party service providers
  - expressly prohibit use of personal information for advertising or marketing
  - ensure personal information only used for education-related purposes
- revise agreements to require service providers to
  - notify board when compelled by law to disclose student data
  - ensure deletion of accounts no longer in use
  - Include audit requirements


www.ipc.on.ca/media-centre/blog/

# Back to school: Lessons learned about online educational tools and platforms

Sep 09 2021

Last fall, when the COVID-19 pandemic steered students away from schools and into their homes, school boards and schools needed to pivot on a dime and be certain that the online tools and data management systems they adopted kept students' personal information safe and secure. Following a long shutdown, public schools across the province have welcomed students back into the classroom, but many of the online educational tools are here to stay.

Ontario's municipal privacy law, *MFIPPA*, requires that public school boards and schools ensure that online tools and data management systems properly protect students' personal information. Despite this, it is not unusual for my office to hear from concerned parents and guardians about the adequacy of the privacy and security measures used by their kids' schools.

To help schools navigate this tricky terrain and support compliance, my office has posted a new **webinar** for teachers and school administrators on their access and privacy obligations under *MFIPPA*. It offers a refresher on *MFIPPA* requirements and includes details about recent investigations by my office related to the use of cloud-based data management systems by two of the largest public school boards in the province.

Both these investigation reports bring to light the responsibility of institutions to maintain strong oversight over their service providers and to ensure the personal information they transfer to their service provider for processing is managed in accordance with Ontario's privacy laws.

The York District School Board (YDSB) **investigation** involves the use of Edsby, a cloud-based data management service that stores and processes student attendance information. Our investigation found that while the YDSB had included appropriate provisions in its contract with CoreFour Inc. (Edsby's parent company), it did not have reasonable oversight measures in place to ensure fulfillment of the contract and prevent security vulnerabilities. To address this, our report recommends the school board strengthen and document the steps they have taken to ensure CoreFour has fulfilled the mandatory security requirements of their agreement. This includes, among other measures, confirming the company has implemented the recommendations made in an independent security assessment and having information security policies and controls that align with recognized standards.

# Holding Institutions Accountable

- IPC concluded three privacy complaint investigations involving Ontario school boards' use of online educational services.
- Each investigation differed in important ways, but all involved:
  - procurement and use of cloud-based services of third-party private-sector service providers acting as agents
  - direct access and use by students of online, account-based services
  - Parent concerns about improper collection, use and disclosure of students' personal information

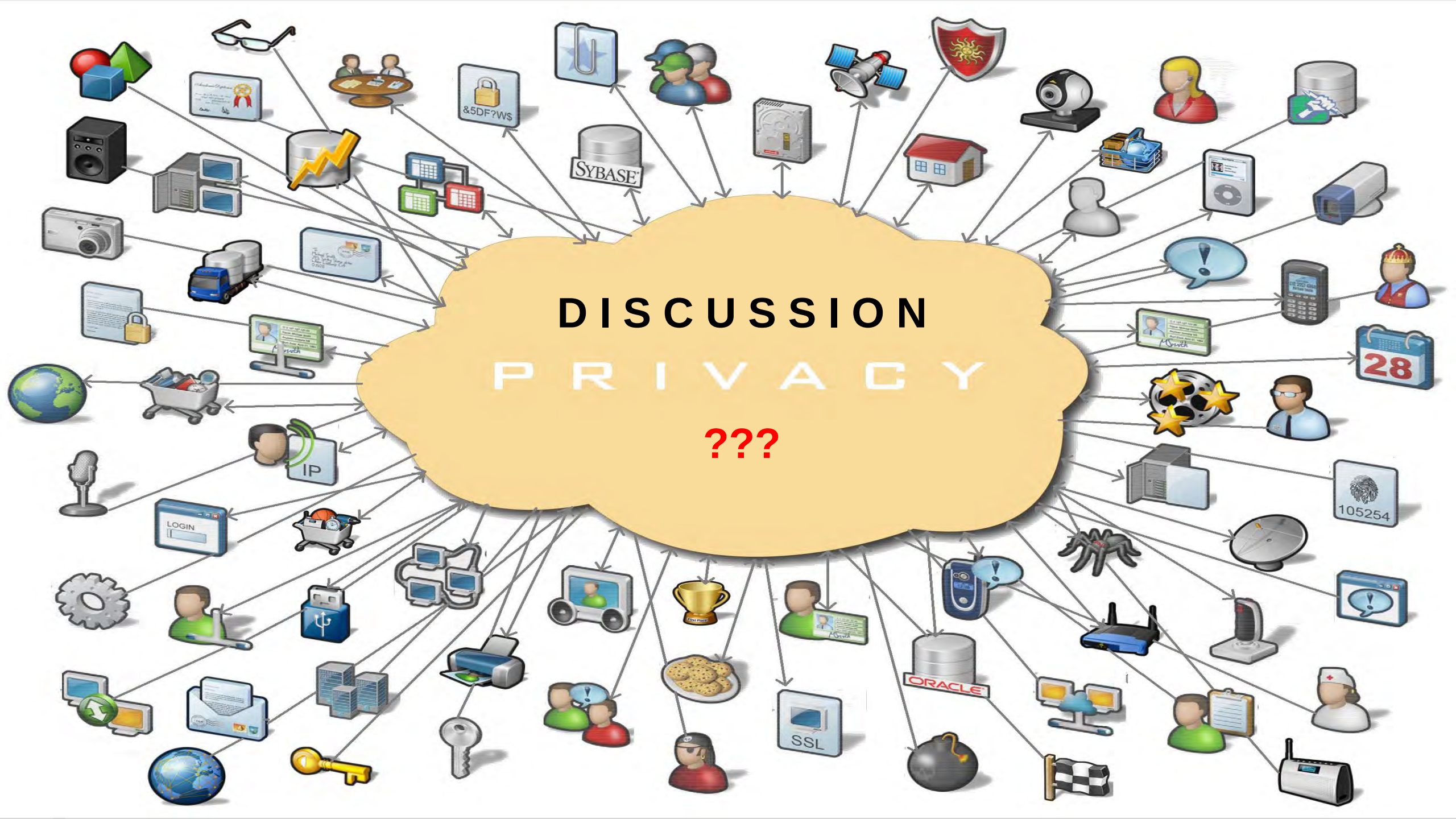
Cont'd

# Holding Institutions Accountable

- IPC investigators found school boards broadly in compliance with MFIPPA, but made recommendations to address some deficiencies, notably to:
  - improve transparency of information management practices, including enhanced notices of collection
  - establish clear privacy and security requirements, consistent with MFIPPA obligations, when contracting online educational services
  - ensuring privacy and security requirements in contracts are kept up to date, and enforced

# Takeaways

- IPC privacy complaint reports:
  - provide guidance to school boards, who retain technology service providers to help deliver their education mandates, on the types of contractual provisions they should seek to include in their contracts
  - serve as a reminder that, to fulfil privacy and security obligations, boards must couple a strong contract with appropriate monitoring and oversight
  - help ensure there are no inBlooms in Ontario!


DISCUSSION
PRIVACY
???
&5DF?WS
SYBASE
IP
LOGIN
ORACLE
SSL
105254
28

# HOW TO CONTACT US

## Information and Privacy Commissioner of Ontario

2 Bloor Street East, Suite 1400

Toronto, Ontario, Canada  M4W 1A8

Phone: (416) 326-3333 / 1-800-387-0073

TDD/TTY: 416-325-7539

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca

Media: media@ipc.on.ca / 416-326-3965