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

OPEN LETTER

September 17, 2019

The Hon. Lisa M. Thompson
Minister
Ministry of Government and Consumer Services
College Park, 5th Floor
777 Bay Street
Toronto, Ontario
M7A 2J3

Dear Minister Thompson:

Re: Government of Ontario's *Promoting Trust and Confidence in Ontario's Data Economy* Discussion Paper

We commend the Ontario government for embarking on the second phase of its consultation related to the development of an Ontario Data Strategy. The release of discussion papers on each of the strategy's pillars, with accompanying public and stakeholder engagement, will greatly inform the government's efforts to create a comprehensive, timely and effective data strategy.

The government has stated that it wants to introduce world-leading, best-in-class privacy protections to ensure public trust and confidence in the data economy. We strongly support this goal. Given our mandate, knowledge and experience related to privacy, the Office of the Information and Privacy Commissioner of Ontario is in a unique position to provide valuable input and assistance as the government moves forward.

Attached are our initial comments related to the four key areas discussed in the *Promoting Trust and Confidence in Ontario's Data Economy* discussion paper (Appendix A). The broad scope of many of the questions made it difficult to provide a detailed response with comprehensive recommendations. Accordingly, our comments here are of a preliminary and general nature.

As more specifics become available, we hope to work closely with the government to ensure privacy is properly protected in all facets of its data strategy. We would appreciate a definite commitment from the province to engage the IPC early in the development of related legislation, policy, standards and practices.

2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel/Tél: (416) 326-3333
1 (800) 387-0073
Fax/Téléc: (416) 325-9195
TTY/ATS: (416) 325-7539
Web: www.ipc.on.ca

We look forward to ongoing engagement with government on this matter. In the spirit of transparency, we are posting this letter and attachment on our website.

Sincerely,

Brian Beamish
Commissioner

cc: Dominic Roszak, Director of Operations, Stakeholder Relations and Appointments, Ministry of Government and Consumer Services

Hillary Hartley, Chief Digital and Data Officer, Deputy Minister, Cabinet Office

Appendix A
IPC Comments on the Ontario Government's *Promoting Trust and Confidence in Ontario's Data Economy* Discussion Paper

PRIVACY, DATA PROTECTION AND DATA GOVERNANCE

When the Government of Ontario launched its data strategy consultation in February 2019, it stated it would explore introducing "world-leading, best-in-class privacy protections."[1] The *Promoting Trust and Confidence in Ontario's Data Economy* discussion paper expands on this idea, and indicates that the province will work to:

- ensure that Ontarians' privacy and data rights are respected and upheld
- promote the continuous evolution of Ontario's privacy and security frameworks to keep pace with new technological developments and challenges
- help public sector organizations implement user-friendly and modern data protection programs in light of emerging data collection and analysis techniques
- promote the development of reusable and people-centered information, tools and methods that help small organizations practice privacy and data protection by design
- clarify and strengthen Ontario's jurisdiction and the application of provincial and federal laws over data collected from Ontarians

To support the province in achieving these objectives, the Office of the Information and Privacy Commissioner of Ontario offers our initial thoughts about necessary improvements to Ontario's privacy legislation. Vital to protecting privacy and defining appropriate and effective data governance is comprehensive legislation that ensures effective oversight for both the public and private sectors. We are fully committed to working closely with the province to enhance Ontario's legislative framework.

Modernizing Public Sector Privacy Legislation

Ontario has two public sector access and privacy laws:

- The *Freedom of Information and Protection of Privacy Act* applies to over 300 provincial institutions such as ministries, provincial agencies, boards and commissions, as well as community colleges, universities, local health integration networks, and hospitals
- The *Municipal Freedom of Information and Protection of Privacy Act* applies to over 1,200 municipal institutions such as municipalities, police services, school boards, conservation authorities, boards of health, and transit commissions

[1] *Ontario's Government Launches Data Strategy Consultations, Province takes steps to better equip for the rapidly advancing era of Big Data*, News Release, February 5, 2019, https://news.ontario.ca/mgs/en/2019/02/ontarios-government-launches-data-strategy-consultations.html.

These acts define the rules public organizations must follow to protect privacy, including:

- limits on the collection, use and disclosure of personal information
- requirements to inform individuals about the collection of their personal information and how it will be used
- standards for security, retention and secure disposal of personal information
- a right for individuals to access and correct their own personal information

As the province knows, the IPC is the oversight body for these acts. The Commissioner is an officer of the Ontario's Legislature and is independent of the government of the day.

Since the legislation came into force three decades ago, public expectations, technology, and the ways in which government does business have significantly changed. The IPC has repeatedly emphasized the need to update our public sector privacy laws to address these changes. They continue to fall behind rapidly evolving digital technology and data-rich information practices.

Technology available today has many benefits for society and enables government to deliver services more effectively and efficiently. It also collects, uses, and generates massive amounts of data, including personal information. As the discussion paper notes, data is being generated at an unprecedented rate. However, the use of data and technology must not come at the expense of privacy.

While Ontario's legislation has had some updates, including the recent data integration amendments, a comprehensive review is needed to ensure privacy rights of Ontarians continue to be protected in our changing environment. Other provinces have strengthened their laws to meet new privacy challenges.

As a foundational step for Ontario's data strategy, we recommend that the government commit to a comprehensive review of *FIPPA* and *MFIPPA* through an open process that encourages public participation. The IPC has numerous recommendations on how *FIPPA* and *MFIPPA* should be updated to keep pace with changes impacting privacy. We would be very pleased to discuss these, in detail, with the government. Outlined below is a key measure to enhancing privacy protection in the public sector.

Enhance oversight

FIPPA and *MFIPPA* give the IPC order-making power for access requests, but this power does not extend to privacy complaints. Our powers are limited to ordering an institution to stop a collection practice and to destroy collections of personal information that contravene the acts. When investigating other issues such as allegations of improper use, disclosure, retention and destruction of personal information, we can only make recommendations.

The authority to investigate and issue privacy-related orders exists in other Ontario statutes that relate to privacy, including Ontario's *Personal Health Information Protection Act*, Part X of the *Child, Youth and Family Services Act*, and the *Anti-Racism Act*. We know that order-making

power deters public organizations from behaviour that is not in compliance with *FIPPA* and *MFIPPA*. It also provides a strong incentive and motivation for early resolution, a cost efficient way of resolving privacy complaints.

We recommend the Ontario government amend the acts to provide this office with the authority to issue an order in the context of a privacy investigation to more effectively protect the privacy rights of all Ontarians.

Coverage of Political Parties

We also recommend expanding the coverage of privacy legislation to cover political parties. Currently, in Ontario, political parties are not covered by privacy laws at either the provincial or federal level. In British Columbia, political parties are subject to the province's private sector privacy legislation.

The large amount of sensitive personal information held by political parties, coupled with advances in the technology enabling them to collect, integrate and analyze data in ways that we could not have previously imagined, reveals a widening gap in protection and oversight of individual privacy rights. The most effective way of making Ontario's political parties accountable for protecting privacy is by making them subject to Ontario's privacy laws.

Build Capacity and Culture Concerning Privacy in Public Sector

Public organizations have been subject to Ontario's privacy legislation for over 30 years, but the need to build capacity and promote a privacy sensitive culture is ongoing. Evolving technology, information practices and service delivery channels, as well as constant staff turn-over, require a continuing commitment in public organizations to raising privacy awareness.

The two key elements that are essential to building capacity and promoting culture change concerning privacy in the public sector are:

- **Privacy Training:** Proper training gives staff the knowledge and skills to proactively identify potential privacy risks, and to take appropriate and timely action to eliminate or mitigate them. Training of new employees (including contract and temporary staff), at all levels of the organization, as well as advanced or role-based training for those in positions with increased privacy risks and responsibilities is crucial to protecting privacy. Periodic refresher training helps ensure staff continue to understand and meet relevant privacy legislation, policies and procedures. Privacy training for agents and contractors ensures they understand their privacy obligations related to the personal information they are charged to collect, use, process, retain, secure, disclose or destroy.

- **Defined Accountability:** For all public organizations, having established roles, responsibilities and accountability is crucial to protecting privacy. Management and staff in each program and business area dealing with personal information must understand their responsibilities to deliver their programs and services in compliance with *FIPPA* or *MFIPPA*. In addition, visible executive-level accountability for, and commitment to, privacy

protection greatly influences an organization's culture and helps the successful implementation of compliant privacy policies and practices.

Ideally, each public organization would have a well-funded, mature privacy management program in place, including comprehensive training and effective awareness campaigns. Unfortunately, the reality is that privacy protection often does not have dedicated resources, particularly in smaller organizations.

For this reason, the IPC strongly supports the government's commitment to promote the development of information, tools and methods to help small organizations proactively address privacy. We offer our assistance and would be pleased to work with the province to develop resources and training for all public sector organizations.

Promoting Privacy Protective Practices in Ontario's Private Sector

While Alberta, British Columbia and Quebec have their own private sector privacy laws, Ontario does not. The federal *Personal Information Protection and Electronic Documents Act* applies to private sector organizations in Ontario that collect, use or disclose personal information in the course of a commercial activity. The oversight body is the Office of the Privacy Commissioner of Canada.

Accordingly, *PIPEDA* is the necessary backdrop to any measures the province might take to promote privacy protective practices in the private sector. Unless Ontario businesses are exempt from its application through substantially similar legislation (discussed further below), they will need to continue to comply with *PIPEDA*.

Many Ontario businesses, including small and medium-sized enterprises, engaged in the data economy have international partners and clients, requiring personal information to flow across borders. If they control or process personal information in the European Union or of EU data subjects, Ontario businesses are currently required to meet the Europe's *General Data Protection Regulation*.

To avoid creating multiple privacy standards and adding to the regulatory burden on business, any action the province takes to promote privacy protective practices in the private sector needs to recognize that many Ontario businesses are already required to meet a privacy standard higher than *PIPEDA*'s.

Despite several comprehensive reviews and the widely recognized shortcomings of the legislation, *PIPEDA* has yet to be updated to ensure privacy is effectively protected in the private sector or to keep pace with evolving privacy legislation around the world. In May 2019, the federal government proposed to update the act, but given the upcoming federal election, likely this will not happen in the near future.[2]

---

[2] Innovation, Science and Economic Development Canada, *Strengthening Privacy for the Digital Age: Proposals to modernize the Personal Information Protection and Electronic Documents Act*, May 21, 2019, https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html.

We support the province's proposal to take action to promote privacy protective practices in the private sector. There are a variety of approaches ranging from education for businesses, self-regulation, co-regulation and legislation focussed on specific privacy risks (for example, smart cities). Another way Ontario could promote privacy protective practices in the private sector is to introduce comprehensive, substantially similar legislation. This would bring control over private sector privacy into the hands of the province.

While recognizing the challenges, and potential expense, for both government and business, made-in-Ontario private sector privacy legislation has a number of significant advantages, including:

- *PIPEDA* continues to have a number of substantial limitations related to its privacy principles, as well as oversight powers such as lack of order-making authority
- Efforts to strengthen *PIPEDA* have not yet succeeded, and are not in the purview control of the Ontario government
- Comprehensive Ontario private sector privacy legislation would enable the province to:
  - take control of the timing and process
  - determine what constitutes "world-leading, best-in-class privacy protections" for Ontario's private sector, tailoring the legislation to meet the needs of our residents and businesses, consistent with Ontario's data strategy priorities
  - define consistent privacy protections across all industries, as well as address additional requirements and controls for specific industries or data practices, as required (for example, those concerns highlighted in the discussion paper)
  - expand the scope of coverage for private sector privacy legislation (for example, British Columbia's *Personal Information Protection Act* does not limit application of that act to commercial activities, and it also applies to employee personal information)
  - adapt quickly and, as the province determines appropriate, to keep pace with technological advances, evolving information practices, and international developments in data protection requirements
- Avoiding duplication of oversight and provide clarity regarding applicable laws for initiatives involving public and private sector partnerships, such as smart cities

The IPC recommends the government consult with us on any measures it contemplates to promote privacy protective practices in the private sector, and to address new and growing challenges to privacy.

CONSUMER PROTECTION

Common to all digital businesses-to-consumer transactions regulated by the Government of Ontario is the collection and use of personal information. Not simply a by-product of a transaction, data now has its own economic value. The real value is no longer just the purchase of the product or service, but in the opportunities that can offer business in terms of accessing information about individuals and their consumption patterns.[3]

While the data economy brings many benefits to consumers, it also brings new challenges for consumer protection. Existing data are being used in new ways and new types of data generated through every transaction or engagement with technology in every aspect of life. More and more of what we do is recorded, with or without our knowledge and consent.

Some consumer protection issues are just online versions of existing problems, such as unsafe products or misleading advertising. Others are uniquely challenging in the digital world such as the resulting information asymmetry; various social engineering schemes like baiting and phishing; profiling leading to price and service discrimination; and online advertising auctions that allow companies to compete for available digital advertising space in real time. These and other new and pervasive practices in the data economy create substantial privacy risks.

The IPC endorses the government's consumer protection goals identified in the discussion paper. While recognizing that consumer rights extend beyond privacy protection, we recommend that any additional or new measures focussed on the collection, use and disclosure of consumers' personal information be addressed in privacy legislation rather than in the existing patchwork of Ontario's consumer protection legislation. This would ensure consistent privacy requirements and oversight, which would benefit both business and consumers. Unique threats, risks and challenges related to specific industries or data practices could be addressed by supplemental privacy requirements or carve-outs, as may be appropriate.

HUMAN RIGHTS AND CIVIL LIBERTIES

The IPC strongly supports the Government of Ontario's commitment to promote transparency, accountability and the ethical use of data-driven technology by the public sector, with an interest in upholding the fundamental rights of individuals.

Privacy is a fundamental right. While the *Canadian Charter of Rights and Freedoms* does not specifically mention privacy or the protection of personal information, the Supreme Court of Canada has determined that the concept of privacy underlies several of the rights expressed in the *Charter*. Primarily the Supreme Court has used Section 8, the protection against unreasonable search and seizure, to advance the argument for a right of privacy for Canadians.

---

[3] European Political Strategy Centre, *Enter the Data Economy: EU Policies for a Thriving Data Ecosystem*, EPSC Strategic Notes, Issue 21, January 11, 2017, https://ec.europa.eu/epsc/sites/epsc/files/strategic_note_issue_21.pdf

As Justice La Forest stated in *R. v. Dyment*: "… society has come to realize that privacy is at the heart of liberty in a modern state…Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual."[4] There is also a common understanding that control over one's own personal information is central to a self-determining and responsible being. People feel that the loss of that control has a significant impact on their ability to be autonomous.

The IPC recommends the province explicitly include privacy in its consideration of human rights and civil liberties as it proceeds with its data strategy. We also recommend that the Government of Ontario consult with the IPC, as well as the Law Commission of Ontario and the Ontario Human Rights Commission, to better understand the impacts of data-driven technologies on the human rights of Ontarians.

Digital and Data-Related Threats to Human Rights and Civil Liberties

The current landscape of threats posed by new and emerging technology and data-driven practices is complex. Data-driven practices, particularly profiling, can significantly heighten the risk of discrimination and other detrimental action. The discussion paper outlines a number of threats including surveillance, bias and discrimination, and behavioural manipulation. These and other threats engage a number of interests, both at the individual and societal level.

As noted in the discussion paper, automated decision-making systems (ADSs) and other artificial intelligence (AI) driven applications are creating new threats. They automatically sort, score, categorize, assess and rank people, often without their knowledge or consent, and frequently without the ability to challenge the accuracy or effectiveness of those processes and resulting decisions.[5] The opaqueness or black box nature of many ADSs make it difficult for individuals to detect, understand and combat potential threats. A worst-case scenario is when indecipherable algorithms are developed with inaccurate, discriminatory or otherwise unwanted biases embedded within them.

ADSs are increasingly used by both the public and private sectors to make services more efficient, accurate and objective. Examples of where ADSs are currently being used include health, public housing and social services, criminal justice, policing, national security, online services, credit, employment, advertising and insurance, among others.

The European Parliamentary Research Service's April 2019 paper, *A governance framework for algorithmic accountability and transparency*, thoughtfully discusses the social effects or impacts of algorithmic systems for decision-making on individuals, groups and society. The paper highlights the entwined social values potentially undermined through the operation of these systems, including equality of opportunity and outcome, justice, truth, and autonomy.[6]

---

4 *R. v. Dyment* (1988) 55 D.L.R. (4th) 503 at 513 (S.C.C.).

5 Privacy International, *Profiling and Automated Decision Making: Is Artificial Intelligence Violating Your Right to Privacy?*, December 5, 2018, https://privacyinternational.org/blog/2537/profiling-and-automated-decision-making-artificial-intelligence-violating-your-right.

6 European Parliamentary Research Service, *A governance framework for algorithmic accountability and transparency*, April 2019, http://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)624262_EN.pdf.

Advancing and Upholding Human Rights and Civil Liberties

The government will need to play a leading role in developing appropriate legislation and other measures to prohibit discrimination and other actions that negatively impact individuals, groups and society.

Given the IPC's mandate, we stress the importance of strong privacy laws for both Ontario's public and private sectors. Robust and modern privacy laws, with effective oversight, are the critical underpinning necessary to upholding human rights and civil liberties.

The discussion paper asks several questions related to how the province can improve transparency and accountability concerning the use of ADSs in the public and private sectors. As the government knows, there are numerous governance models being used or contemplated around the world – ranging from self-regulation to legislation (for example, the recently introduced federal United States *Algorithmic Accountability Act*).[7]

An example is the Government of Canada's *Directive on Automated Decision-Making*, which took effect on April 1, 2019.[8] One of the directive's requirements relates to transparency. It defines the need to post a prominent and plain language notice on the program or service website before decisions, as well as to provide meaningful explanations to affected individuals after decisions, on how and why the decisions were made. The directive also requires the completion of an algorithmic impact assessment (AIA), which is a questionnaire designed to assess and mitigate the risks associated with deploying an ADS.

To promote transparency and accountability about the use of ADSs and other AI driven applications in the OPS, as a starting point, the IPC recommends that the province move swiftly to implement a directive akin to the federal one. Completing an AIA, similar to a privacy impact assessment and threat/risk assessment, as part of the OPS's governance processes, would require programs to proactively identify and address the potential impacts of ADSs, prior to their development or acquisition.

This would help determine whether a proposed use of an ADS and other AI driven application is appropriate, ethical, privacy protective and does not violate human rights and civil liberties. The directive could be supplemented, or superseded, once the province determines how ADSs should be regulated in the broader public and private sectors (for example, if legislation were enacted).

The IPC also recommends that the province define rules governing its procurement of algorithmic systems and AI driven applications, including levels of accountability and transparency. The government should require openness about the use of ADSs and AI by all its agents, contractors and partners.

---

7 *Algorithmic Accountability Act of 2019*, https://www.wyden.senate.gov/imo/media/doc/Algorithmic%20Accountability%20Act%20of%202019-%20Bill%20Text.pdf.

8 Government of Canada, *Directive on Automated Decision-Making*, https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592.

To ensure the design, procurement, and implementation of algorithmic processes in more thoughtful and transparent ways, government contracts could require vendors to create and deliver records to it that explain key policy decisions and validation efforts, without necessarily disclosing precise formulas or algorithms. *FIPPA* and *MFIPPA* would protect trade secrets should there be access requests. Other records related to use of ADSs could be proactively and reactively disclosed, to support meaningful accountability and transparency, as well as public debate without adversely affecting contractors' competitive positions.[9]

Regarding regulating ADS in the private sector, as the province knows, other jurisdictions have adopted different approaches ranging from voluntary adoption of the AIA model, establishing a legislative framework that requires completion of an AIA in certain circumstances,[10] or something more expansive like the *GDPR* requirements.

New Rights in Relation to Data and Data-Driven Practices

The IPC is pleased that the Government of Ontario is engaging with the public on the issue of new rights related to data and data-driven practices. This is a significant and far-reaching question. Unfortunately, the scope, as stated in the discussion paper, is ill-defined. Until more details are known, it is not possible for us to respond in a meaningful way as this discussion question just raises more questions. For example:

- Would the right to data ownership only relate to personal information or all data?
- Would the data owner be able to licence use or get paid a user fee?[11]
- Would ownership be defined as a property right[12] or in some other manner?

On the matter of new rights related to data-driven practices, generally the IPC would support the province's efforts to increase privacy protection for Ontarians. However, much more study of this important issue is needed.

If the province decides to introduce substantially similar private sector privacy legislation, consideration can be given to the rights identified in the discussion paper, such as the right to erasure. Also, as previously noted, Ontario businesses involved with international commerce are already following the requirements of the *GDPR* and similar legislation in other jurisdictions.

---

9 Robert Brauneis & Ellen P. Goodman, *Algorithmic Transparency for the Smart City*, 20 Yale J. L. & Tech. 103 (2018), https://yjolt.org/sites/default/files/20_yale_j._l._tech._103.pdf.

10 European Parliamentary Research Service, *A governance framework for algorithmic accountability and transparency*, April 2019, http://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)624262_EN.pdf, p. 73.

11 A survey by Insights Network earlier this year found that 79% of consumers said they want compensation when their data is shared, https://www.brookings.edu/blog/techtank/2019/06/26/why-data-ownership-is-the-wrong-approach-to-protecting-privacy/.

12 For example, the American S.806 - *Own Your Own Data Act* introduced early in 2019, each individual would own and have an exclusive property right in the data that they generate on the internet.

The province can learn from the implementation and ongoing compliance challenges related to the *GDPR* and other similar legislation. We look forward to working with the government as it determines how to move forward on this important matter.

PUBLIC EDUCATION AND AWARENESS

Given the complexity of data-driven practices and technology, and the rapid pace of change, public education and awareness are essential to enable individuals to understand and manage potential risks when engaging with online and other digital services. They also will help the government reach its goal of "putting the people first in everything it does by adopting new digital practices and technologies that will deliver simpler, faster, better services to Ontarians."[13] Steps must be taken to ensure that no one gets left behind.

This is reflected in the discussion paper, where the Ontario government said it will work to:

- promote public education and awareness through useful information, tools and resources to help Ontarians understand and protect themselves against data-related harms online
- encourage useful resources that promote cybersecurity, privacy and safety online

The IPC applauds the government for this commitment, but we recommend the province do more than just encourage useful resources – the government should direct and play an active role in developing the tools, guidance and other resources.

As the province knows, given the diversity of Ontario's population and the range of knowledge, experience, skills and abilities, languages, and economic resources, the spectrum of its approaches and messaging for public education and awareness will need to be varied and tailored. Additionally, the public's needs and priorities will evolve as the population ages, and technology, service delivery and business practices change.

While education and awareness about the threats and risks of data-driven practices are important for all Ontarians, they are critical for children. Young people need to be able to harness the full potential of online resources while protecting their privacy and themselves from threats, such as cyberbullying. Those who learn to control their personal information and protect their online reputation will be able to safely participate in the online economy and community.

In 2016, a group of international data protection and privacy commissioners adopted an International Competency Framework on Privacy Education.[14] The commissioner's resolution called for more privacy education in schools and training opportunities for educators. In 2018, the international commissioners followed up with a resolution on E-learning Platforms, which included 24 recommendations and guidance to protect privacy when developing, implementing,

---

[13] Ontario Digital Service webpage, https://www.ontario.ca/page/ontario-digital-service.

[14] The 38th International Conference of Data Protection and Privacy Commissioners, *Resolution for the Adoption of an International Competency Framework on Privacy Education*, October 18, 2016, https://icdppc.org/wp-content/uploads/2015/02/Resolution-2016-on-Privacy-education.pdf.

and using online educational services.[15] Also, in 2018, Canada's federal, provincial, and territorial privacy authorities, including the IPC, jointly released a three-volume set of lesson plans designed for educators to teach students about privacy rights, digital literacy and online safety.[16]

The IPC recommends the province begin its education efforts with young people who are actively engaging with digital services. The new Grade 10 careers course requirements on digital literacy learning are a good first step. However, the Ministry of Education should direct the development and use of age-appropriate curriculum requirements and tools for teachers of all age groups.

We offer our support as the province defines and implements its public education and awareness program. The Commissioner has a legislative duty to conduct public education. We would be pleased to work with the province, and its partners, on the public education and awareness initiatives that arise from the data strategy.

---

15 40th International Conference of Data Protection and Privacy Commissioners, *Resolution on E-Learning Platforms*, October 23, 2018, https://icdppc.org/wp-content/uploads/2018/11/20180918_ICDPPC-40th_DEWG-Resolution_ADOPTED.pdf.

16 IPC, *New Lesson Plans for Educators: Privacy Rights, Digital Literacy and Online Safety*, June 18, 2018, https://www.ipc.on.ca/new-lesson-plans-for-educators-privacy-rights-digital-literacy-and-online-safety/.