

# CANADA'S DATA PLAN: We Need a Data Strategy that Supports our Values and Encourages Innovation

As our economy becomes more data driven, Canadians need a national data strategy that encourages innovation, provides security and privacy, prioritizes transparency and oversight, and that transcends jurisdictional barriers. [By Teresa Scassa](#)



## SUMMARY AND RECOMMENDATIONS

Data is the fuel for the engines of big data analytics, artificial intelligence and other rapidly evolving and transformative technologies. Data's shift from being the "exhaust" of industrial and economic activity to being an asset in its own right means that data is harvested at every opportunity and in every context.

For example, The Internet of Things has expanded into homes, vehicles and public spaces, and much of the data collected is personal information, leading to growing anxieties about privacy. The few companies that are well-positioned to harvest data wield considerable and, arguably, excessive market power. The ability of Canadian governments and businesses to own and control the data they need to prosper economically is diminishing.

New uses are being found for data. While many promise innovative solutions to long-standing problems, others raise concerns about ethics, bias, fraud and manipulation. Fragmented and weak data governance threatens to undermine the trust of citizens and businesses alike. Within this rapidly evolving context, Canada's legal and policy infrastructure struggles to keep up, leading to calls for the development of a national data strategy. A failure to act quickly will leave us playing

Companies that harvest data are increasing in power, and Canadians are understandably anxious about it. As our economy becomes more data driven—and as data becomes more valuable—Canadians need a national data strategy that provides a common framework for data security and privacy, that prioritizes transparency and oversight in the processing of data, and that transcends silos and jurisdictional barriers. Such a strategy must embrace an innovative future and, at the same time, protect our society's most deeply held values.

To develop a national data strategy for Canada, governments must begin by:

- developing a statement of values for a digital society
- reforming data-protection and intellectual property laws to meet modern needs
- setting rigorous data-security standards for big data and Internet of Things technologies
- ensuring greater transparency and oversight of the algorithms used to process data

catch up with data, like we did with social media, as major technology companies stake out their turf.

In many ways, smart cities are a crucible for the data governance challenges we face. Smart cities depend on the collection of massive quantities of data about urban infrastructure and residents' activities. It is crucial to know who will own and

control this data, who will be able to access and reuse it, and for what purposes. The protection of privacy is also critical in cities in which data collection is constant and comprehensive. Data security is essential to protect both individuals and infrastructure. Smart cities will also require oversight to ensure that data- and algorithm-driven decision making is fair, accountable and transparent.

Yet smart cities initiatives are often seen as high-tech innovation projects that pay insufficient attention to important data stewardship issues. The [public pushback over Sidewalk Toronto's proposed development on the city's waterfront](#), combined with a [public scolding of Canada's Smart Cities challenge](#) by federal, provincial and territorial privacy commissioners, make it clear that a national data strategy is needed not just to support innovation, but also to provide a principles-based framework for innovation that is consistent with national values.

## The legislative and policy reform we need

There is no shortage of examples of areas where the demands of the digital economy and society require legislative and policy attention. Some of these are:

**Privacy and data protection:** Canada's private sector data protection law, the Personal Information Protection and Electronic Documents Act (PIPEDA), is [badly in need of reform](#). This was so even before Europe's new General Data Protection Regulation (GDPR) took effect; the European regulation just makes the need for reform more urgent. If Canadian law does not offer an adequate level of protection for personal data, the flow of data between Europe and Canada could be affected. While a reformed PIPEDA need not replicate the GDPR, the

status quo is unacceptable. Enforcement is a key area of weakness. Our consent-based regime may need to be supplemented, and there is considerable interest in consumer- and competition-friendly tools such as data portability.

**Consumer protection and competition:** Rapidly accumulating [concerns over unfair terms in consumer contracts for digital devices and services](#), a lack of competition, and deceptive commercial practices drive calls not just for better consumer protection laws, but also for a new federal focus in this area. Large concentrations of data in the hands of a few companies, combined with tight controls by those companies over access to and reuse of the data also [create competition law issues](#).

**Trade secrets and copyright:** The issue of protecting trade secrets and confidential information is receiving more attention internationally and domestically. Algorithms and the data that fuels them may be treated by companies as confidential commercial information. Their place at the heart of the digital economy means that there is pressure to offer more robust protection. At the same time, the use of algorithms and massive quantities of data to drive public and private sector decision making creates a need for new mechanisms to ensure that technology-driven decision making is fair, transparent and accountable.

Copyright law, strengthened over the years at the urging of content industries, may now be stifling innovation by creating costly and time-consuming barriers for the development of artificial intelligence. Calls for copyright reform that balances the rights of copyright owners with those who seek to use protected content for text and data mining are erupting in countries that seek to benefit from the development of artificial intelligence and machine



## There is no justification for practices that lead to social exclusion and discriminatory outcomes. Inadequate data governance may be more of a brake on the economy than thoughtful and responsible governance.

learning technologies.

**Cybersecurity:** More concerted attention needs to be paid to cybersecurity in the public and private sectors. To date, a rising number of [data security breaches](#) have been [associated with individual harms or losses](#), as well as [significant reputational and monetary losses](#) for organizations in some cases. Cybersecurity threats can also cause much broader disruptions, including to core utilities, services and even democratic institutions. As technology becomes more deeply enmeshed with our homes, our vehicles, our governments and our cities, cybersecurity becomes an increasingly urgent issue.

**Transcending silos:** In addition to outdated laws, we are faced with the reality that our legal infrastructure has built rigid silos to address and contain certain issues. Many of the challenges we face in the big data era can no longer effectively be addressed in this manner. In theory, privacy problems are the domain of the federal or provincial privacy commissioners, competition problems go to the federal Competition Bureau, and human rights issues fall to the appropriate human rights commission.

But the big data context raises issues of human rights, privacy and competition that cannot so easily be disentangled. The denial of services to

an individual based on a profile generated using massive quantities of personal information and a non-transparent algorithm may simultaneously raise issues of discrimination, privacy, human rights and consumer protection. To make matters more complicated, the division of powers between federal and provincial governments creates further silos that can be barriers to robust and responsive public policy. A national data strategy must find a way to create law and policy that transcends these silos, facilitates redress and minimizes jurisdictional barriers.

### How will a national data strategy look?

On June 19, 2018, Canada's Minister of Innovation, Science and Economic Development announced the start of [national consultations on digital and data transformation](#). The three themes of the consultation are broad: unleashing innovation; trust and privacy; and the future of work. The consultation could lead to the development of a national data strategy.

But what, exactly, is a national data strategy? One view is that it should be something concrete, manageable and realizable. [Estonia's digital public service innovation](#) is perhaps the most well-known example of such a project—one that has received global acclaim. More controversially, China is pursuing [e-government reforms](#) based on big data and artificial intelligence, drawing on massive



stores of both private and public sector data. In the U.K., work to develop a national data strategy will involve [the creation of a Centre for Data Ethics and Innovation](#) that will support the responsible and ethical use of artificial intelligence.

There is no shortage of suggestions for a possible project for Canada, including development of the [infrastructure needed for network sovereignty](#); taking global leadership in [big health data](#); and developing [big data capacity around Canada's primary industries](#).

The project-based approach is no doubt attractive to government. It is certainly more manageable than a complete overhaul of laws and policies. If successful, such an approach will yield visible, measurable results. Canada could become the international poster child for the chosen project in much the same way that Estonia is now the global e-society darling. Beyond this, a successful project will build capacity and will foster trust in government data stewardship. But even if a project-based approach is adopted, Canada will have to grapple with the cumbersome and outdated law and policy infrastructure that leaves it ill-prepared to meet the challenges of the data economy and society.

## Pursuing innovation consistent with society's values

The expanded role and importance of data creates new social and economic challenges. [Lisa Austin](#) has [criticized](#) the federal government's approach to its digital strategy consultation for "fram[ing] the central issue as seeking a balance between economic innovation and privacy." This tired paradigm creates a binary proposition in which choosing privacy means stifling innovation, and it fails to adequately recognize the important human and social dimensions of data that go beyond privacy. The complex web of values impacted by data was evident in the recent Cambridge Analytica scandal, in which massive amounts of personal information were used to subvert democratic processes. It is also evident in concerns about how non-transparent and potentially biased algorithms or training data may adversely impact individuals and communities.

While we cling to an individual, consent-based model for data protection, it is increasingly obvious that personal privacy is not the only right or value threatened by the unchecked and unaccountable collection of personal information. Equality, free-



## 'Economic innovation vs. privacy'

**This tired paradigm creates a binary proposition in which choosing privacy means stifling innovation, and it fails to adequately recognize the human and social dimensions of data that go beyond privacy.**



dom of expression, justice and transparency are all at stake. In a world where data is used to influence and manipulate to unprecedented extents, we need transparency and accountability not just to protect consumers, but also to protect communities and democratic institutions. The issue is not that we face a choice between either pursuing technological innovation or preserving human values; it is about deciding that we will pursue technological innovation that is consistent with and supportive of human values.

There is no justification for practices that lead to social exclusion and discriminatory outcomes. Inadequate data governance may be more of a brake on the economy than thoughtful and responsible governance. Data security breaches and irresponsible data practices undermine confidence and carry with them increasingly burdensome economic costs.

## RECOMMENDATIONS

In developing a national data strategy, the government should consider the following to adapt our legal and principles-based infrastructure for the age of big data:

- 1 **Develop a statement of values for the digital society that will inform how laws are developed, interpreted and applied, and that makes explicit the implicit (and therefore often overlooked) principles that should guide the adoption of new technologies. These values should**
- 2 **be drawn from existing, enacted instruments, including human rights legislation and the Canadian Charter of Rights and Freedoms, and should be adapted to the digital context.**
- 3 **Reform Canada's public and private sector data protection laws to deal with the realities of the big-data environment. Reforms must be ones that enable technological advancement consistent with values that go beyond individual privacy.**
- 4 **Reform intellectual property law in ways that are sensitive to data and information as building blocks of expression, innovation and communication—and not just as assets to be owned and exploited.**
- 5 **Develop laws and policies that allow Canadian governments and businesses to retain sufficient control over the data we need to govern ourselves and flourish in a digital economy.**
- 6 **Set rigorous data security standards for big data and Internet of Things technologies and ensure they are met with a view to providing appropriate levels of protection against economic, social and individual harm.**
- 7 **Ensure greater transparency and oversight of the algorithms used to process data and influence decision making.**

---

**Teresa Scassa** is the Canada Research Chair in Information Law and Policy at the University of Ottawa, Faculty of Law. She is also a senior fellow with the Centre for International Governance Innovation's International Law Research Program and a member of the Waterfront Toronto Digital Strategy Advisory Panel.

For her helpful feedback and comments on an earlier draft, the author would like to thank Bianca Wylie.

