大成 DENTONS

Dentons Data Summit 2019 Whitepaper

The Dentons Data Summit

The Dentons Data Summit, an annual event held on June 6 this year, provided rich content that responded to the challenges faced by our clients as they work to transition their businesses to the digital economy.

The Data Summit reflected issues and topics that are current to the majority of Canadian entities, either public or private, and provided context for how each topic area is impacting companies' rapid digital transformation.

Contents

Introduction

Digital economy versus digital technology versus digital transformation

Digitization in the 1980s through to the early 2000s saw the adoption of computer technologies to digitize discrete functions. The new digital economy is much more than that. It builds on these technologies to create a mobile, electronically connected infrastructure that is characterized by three key components: (i) infrastructure (hardware, software, telecoms, networks, human capital, etc.); (ii) e-business (how business is conducted, any process that an organization conducts over computer-mediated networks); and (iii) e-commerce (a transfer of goods via an online network).

Digitization (1980s - 2000s)	The digital economy
Rise of the personal computer and automation of certain tasks (e.g., word processing)	**Sensors and networked devices (internet of things)**
Advent of the internet and its use to provide information (i.e., a one-way pipe)	**Smart phones that are used as entertainment platforms, payment vehicles, identity managers, etc.**
Introduction of cellular phones as a means of mobile communication	**Increasingly mobile technologies**
	Cloud computing
	Social media platforms
	Rise of the internet as an interactive, two (or more) -way pipe
	Artificial intelligence and data analytics to reshape business models

Forty-six percent of respondents at The Dentons Data Summit reported that they felt their organization's technological safeguards protecting their confidential information were inadequate.

Dentons Data Summit 2019

Digitization ≠ Digital transformation

Merely having computers and an internet connection does not mean a business is undergoing digital transformation. Digital transformation is the process of using digital technologies to create new—or modify existing—business processes, culture and customer experiences to meet changing business and market requirements. It is also marked by a fundamental change in how a business operates and delivers value to customers.

What gets transformed in digital transformation?

Companies can no longer be sure of their business model or market share. Many sectors are being disrupted by the rapid introduction of new technology, new digital business models, a change in consumer preferences, or new market entrants, often from seemingly unrelated industries. The boundaries and barriers that once influenced how businesses defined their market and how they operated are dissolving. The effect of online marketplace shopping on brick-and-mortar retail establishments is an example of this.

Businesses are responding both proactively and reactively to these pressures by embracing new technologies to transform their business models, drive growth and improve efficiency. They are leveraging data analytics to generate actionable competitive insights. Increasingly, they are entering into strategic transactions (mergers, acquisitions, alliances and joint ventures) to enhance their competitive advantage.

These rapid changes create an opportunity and a challenge for management, who must balance priorities and resources to help the organization address current risks, anticipate future risks and provide insights to maintain a competitive advantage.

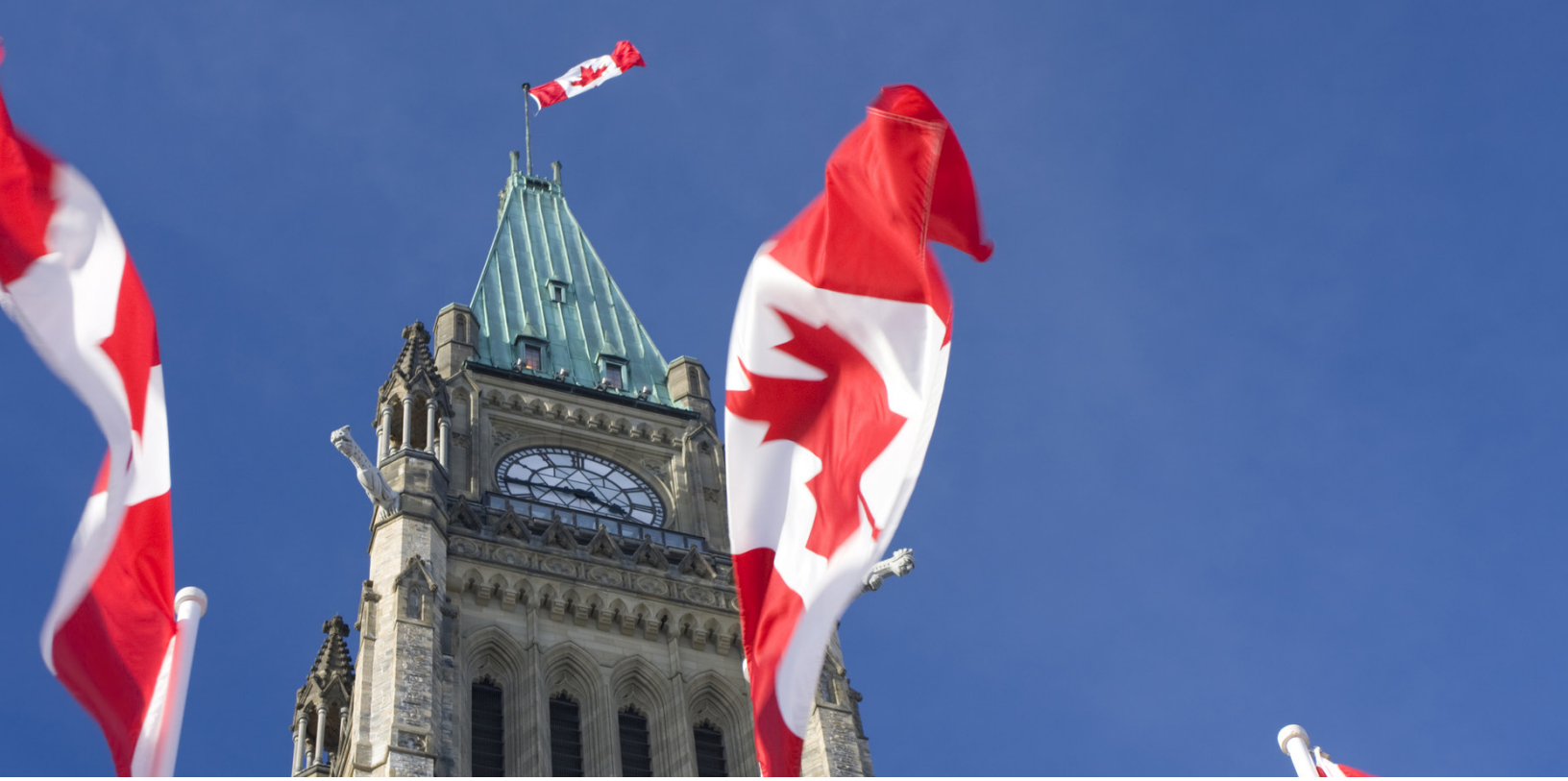
Dentons is embracing digital transformation

Organizations are moving beyond risk assessments, and asking counsel to act as advisors, to be more proactive at identifying and managing risks related to systems development, new product development and strategic transactions. Experienced counsel should also be able to meet an organization's demand for business insights.

At Dentons, we understand this. We help you focus on the risks that matter. Through our work with clients, we have identified a number of the key risks that are on the minds of board members and management. Some of these are new risks, although in many cases, they are risks that have been managed for years but now manifest in different ways. In the following pages, we present some of these insights and hope you find them helpful as you steer your business on the course of digital transformation.

What gets transformed in digital transformation?

- **The organization's strategy: What business are we in? Where are our organizational boundaries? How should we be structured?**
- **The organization's customers: Who/where are our customers? What do they need/want?**
- **The competitive landscape: Who are our competitors? Who are our partners?**
- **The organization's talent pool: What jobs, skills, etc. do we need? Where should we be located?**



The regulation of data: Can companies keep up?

Changing privacy laws, the rise of non-personal data regulation, data localization as a trade issue, competition law implications and algorithms… how can companies keep up?

The Canadian federal government recently announced a new Digital Charter, a 10-point plan intended as a foundation to guide policy development and actions that will help build and regulate the digital and data economy in Canada, as well as boost confidence and trust in the security of the digital economy.[4]
As part of the Digital Charter initiative, the Canadian federal government also released *Strengthening Privacy for the Digital Age: Proposals to modernize the Personal Information Protection and Electronic Documents Act*, a discussion paper exploring proposed amendments to the *Personal Information Protection and Electronic Documents Act* (PIPEDA), Canada's federal privacy legislation.[5]

On February 19, 2018, after four months of public consultations, the Competition Bureau released "Big data and innovation: key themes for competition policy in Canada". In brief, the Bureau believes that the emergence of firms that control and exploit data can raise new challenges for competition law enforcement. Continuing this theme, on September 4, 2019, the Competition Bureau published a call-out for information, seeking information from businesses and other interested parties regarding certain strategies that firms may use to hinder competition in certain core digital markets, such as online search, social media, display advertising, and online marketplaces.[6]

---

4 The Digital Charter is available here: https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html. The accompanying Digital Charter Action Plan is available here: https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00109.html
5 The Discussion Paper is available here: https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html
6 The Competition Bureau Call Out is available herehttps://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04494.html

Canada's new Digital Charter and the related developments in privacy and competition are just some of many global efforts reflecting governments' increasing concern with the "wild west" nature of the digital economy. A myriad number of issues have captured the attention of the public and policymakers, including, but not limited to, the impact of "Big Tech" market dominance and influence, the rise of social media platforms, whose business model is based on the monetization of personal information, the use and participation of such platforms in the undermining of democratic processes and institutions, and the creation and exacerbation of digital divides between haves and have-nots.

As concern about these issues, and the impact they have on Canadians' trust and willingness to participate in the digital economy rises, the regulatory landscape is shifting to address these concerns. Businesses face unprecedented change in the data landscape, and with it, increasing risk and compliance costs, as well as the risk of adopting business models and data strategies that may not be future-proof.

Experience counsel can anticipate these issues, and help businesses start now to implement agile and phased implementations of data solutions that are not only resilient in the face of change, but comprise a clear competitive advantage.

What's on the horizon?

(i) Canada's Digital Charter

The Digital Charter is a whole-of-government approach to an end-state of greater trust online.

The Digital Charter was developed following public consultations, during which citizens voiced their lack of trust in how their personal data was being shared and used. The Digital Charter itself reflects the recognition that any approach taken to regulate online activity needs to be cohesive and coherent.

Businesses should view the Digital Charter as a roadmap to where privacy regulation and the data economy are heading, as well as an acknowledgment that the federal government is determined to reach the end-state the Digital Charter presents. Some principles articulated in the Digital Charter will have direct impacts on businesses; others, less so.

While not enforceable as law, these 10 principles are an opportunity for businesses to proactively review their corporate practices and policies, and determine if they are increasing transparency, enhancing control of data, and engaging in activities to build trust with consumers. It is a chance for businesses to test their resiliency in the face of what's to come. Working alongside a trusted advisor, businesses can develop an overall data strategy, close the white space and reduce risk, and ultimately use their new resiliency to beat the competition.

Canada's Digital Charter – 10 principles

1

Universal access

All Canadians will have equal opportunity to participate in the digital world (including tools such as access, connectivity, literacy and skills).

Implications for business

Primary impact will be on businesses in or adjacent to the telecom sector. Expect government attention on such things as increasing rural internet access, consumer rates, and creating programs to increase technological and data literacy.

2

Safety and security

Canadians will be able to rely on the integrity, authenticity and security of the services they use, and should feel safe online.

Implications for business

Expect increased regulatory attention to cybersecurity measures, either as part of a formal regulatory requirement or as less formal sector expectations via standards, codes, etc.

3

Control and consent

Canadians will have control over what data they are sharing, who is using their personal data and for what purposes.

Implications for business

Expect increased scrutiny of not only consumer-facing privacy policies, but also organization processes intended to give meaning to such policies.

4

Transparency, portability and interoperability

Canadians will have clear and manageable access to their personal data, and should be free to share or transfer it without undue burden.

Implications for business

Expect regulatory or legal developments requiring organizations to allow consumers to request that an organization transfer their personal information to a third party, likely without cost, and in a machine readable format.

5

Open and modern digital government

Canadians will be able to access modern digital services from the Government of Canada, which are secure and simple to use.

Implications for business

Primary impact will be on public sector agencies, but businesses adjacent to the public sector may see improved government interfaces and an increase in the amount of government-held data available publically.

6

A level playing field

The Government of Canada will ensure fair competition in the online marketplace, while protecting Canadian consumers from market abuses.

Implications for business

Expect increased scrutiny of digital markets and business models by the Competition Bureau.

7

Data and digital for good

The Government of Canada will ensure the ethical use of data to create value, promote openness and improve the lives of people.

Implications for business

Expect the development of extra-legal "ethical" mechanisms, such as codes, standards, and statements that will address the use of data (both personal and anonymous) and artificial intelligence.

8

Strong democracy

The Government of Canada will defend freedom of expression and protect against online threats and disinformation.

Implications for business

Expect increased scrutiny of online communications; platforms and digital services may face increased accountability, including increased disclosure demands.

9

Free from hate and violent extremism

Canadians can expect that digital platforms will not foster or disseminate hate, violent extremism or criminal content.

Implications for business

Expect increased scrutiny of online communications; platforms Expect increased scrutiny of such platforms and moves to increase the accountability of such platforms, through regulation and potentially litigation.

10

Strong enforcement and real accountability

There will be clear, meaningful penalties for violations of the laws and regulations that support these principles.

Implications for business

Expect greater enforcement powers potentially across a variety of regulators (e.g., Office of the Privacy Commissioner of Canada, the CRTC, etc.), and the introduction or enhancement of monetary penalties.

For further reading please click here.

(ii) PIPEDA modernization

Along with the Digital Charter came a plan to modernize Canada's federal private sector privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA). PIPEDA applies to private-sector organizations in Canada that collect, use or disclose personal information in the course of their commercial activities.

The modernization efforts seek to create a modern regulatory privacy framework that is responsive and agile; has an enhanced, reasoned enforcement model; is interoperable with other jurisdictions; and balances support for data-driven innovation with respect for individuals' privacy by providing users with meaningful control.

The PIPEDA modernization plan is focused on four areas:

1. Enhancing individuals' control
2. Enabling innovation
3. Enhancing enforcement
4. Clarifying PIPEDA

The modernization proposals—which include calls for enhancing individual control of data, enabling responsible innovation, clarifying the obligations of organizations, and strengthening enforcement powers—have led to speculation that in its final form, PIPEDA may be similar to the European Union's General Data Protection Regulation (GDPR), causing many businesses to be concerned about an additional compliance burden. However, the modernization proposal largely treads a middle path, embracing many of the concepts enshrined in the GDPR, but adapting them for a uniquely made-in-Canada approach.

The Canadian federal government has acknowledged the compliance burden that concerns businesses, but is also aware of the need to harmonize PIPEDA's provisions with other regulatory regimes governing the global digital economy.

Evidence suggests that the majority of Canadians not only welcome but also look to engage in the new digital economy, which would include data sharing. However, Canadians are also expressing increasing unease with how their information is being used (for instance, the PIPEDA modernization proposal notes that 84 percent of Canadians are concerned with the use of personal information by social media platforms, and nearly three in four Canadians think they have less privacy protection than 10 years ago).

The National Data and Digital Consultations that led up to the modernization proposal showed that Canadians want more transparency in how their data is being collected and how it is being used. Canadians also want greater control over how their information is used, and need to see the value of the benefits it brings.[4]

The proposed modernization efforts attempt to provide more meaningful control, transparency and consumer choice by:

- Requiring specific, **standardized, plain-language** information on use of personal information, the third parties it is shared with, and prohibiting bundling of consent into a contract;
- Incorporating **alternative grounds to consent** (similar to GDPR's legitimate interests basis for processing personal information);
- Introducing the **right to data mobility**;
- Requiring enhanced transparency of business practices via "**demonstrable accountability**", including in the context of transborder data flow;
- Introducing **algorithmic transparency** requirements for automated decision-making;
- Adding a **definition of de-identified information** (and potentially pseudonymized data), plus an exception to consent for its use/disclosure for certain prescribed purposes and penalties for re-identification; and
- Introducing the **right to request deletion of personal information** and mandating defined retention periods.

The unique balance that will be struck in Canada will benefit a business that understands that landscape and

4 The details of the National Data and Digital Consultations are available here: https://www.ic.gc.ca/eic/site/084.nsf/eng/home

the anticipated changes. The development of flexible and adaptable data governance processes now reduce both present and future risk, but also allow companies to be resilient in the face of pending change, reducing compliance spend, minimizing time-to-sale, and creating a competitive advantage.

Growing concerns from the public regarding the safety and privacy of online commercial interactions are reflected in the modernization proposal, and businesses should expect enhancements to the Office of the Privacy Commissioner of Canada's (OPC) powers.

Providing increased discretion to the Commissioner on whether to investigate complaints, and allowing for consideration of adherence to standards, certification or codes of practice in making decisions to investigate, are among the proposals being considered. Providing for increased flexibility for the OPC auditing or reviewing organizations' practices has also been proposed.

The modernization proposal suggests providing the OPC with some order-making powers, as well as extending the existing regime for fines (although the OPC would still be required to refer matters of concern to the Attorney General of Canada for investigation.

In an effort to develop an agile data governance framework that can be adapted to particular sectors, activities or technologies, the federal government has said it will also look at how codes of practice, certification and standards can be leveraged to supplement PIPEDA. These have the potential to impose more specific requirements for certain sectors or activities.

(iii) Competition law

The Competition Bureau has begun examining concerns that certain core digital markets, like online search, social media, display advertising and online marketplaces, have become increasingly concentrated, to the detriment of consumers and businesses.

In its recent call-out discussion paper, it explores two potential, and possibly complementary, explanations:

- **Digital markets may 'tip' to a dominant firm:** Characteristics of certain digital markets may favour the emergence of a single winner or small group of winners; and
- **Anti-competitive conduct rather than competition on the merits:** Leading firms may not have achieved success by outperforming their competitors, but rather by executing anti-competitive strategies that target existing or potential rivals.

The tendency for a single organization, or a small group of organizations, to take control of certain digital markets is referred to as 'tipping'. Tipping is most likely to occur where organizations benefit from:

a. Strong network effects

- Network effects exist when the value or benefit to a particular user of a product or service depends on the number of other users. These effects can be direct (for instance, consider a social media platform, which is more valuable to a user if their friends and family also use it), or indirect, such as when a product or service brings together two or more distinct types of users (for instance, of an online marketplace where more buyers and more sellers)

b. Economies of scale and scope

- A firm that already provides a variety of products or services can be more efficient at entering another product or service market than new entrants. For example, it may be less costly for a firm that controls a leading search engine to capture other markets because it can take advantage of its existing resources. This may include using data it has already accumulated, leveraging its existing user base, or redeploying technologies to help ease expansion.

c. Access to large volumes of data

- Access to large volumes of data can help keep competitors at bay. For instance, when organizations are able to use data collected from their users to improve the quality of their product or service, which, in turn, attracts more users. As incumbents take advantage of these kinds of feedback loops, it becomes harder for rival firms with less, or no, data to keep up.

Collectively, these market characteristics may lead to less competition.

Anti-competitive strategies may also be effective and especially profitable in digital markets. Such strategies may include, among other things:

- Refusal to deal: This occurs when a firm that controls an important input or channel refuses to provide access to actual or potential competitors.
- Self-preferencing: This occurs when a firm that controls a platform props up its own products and services over those of its rivals.

In many cases, the types of conduct identified above will not raise competition concerns and the Competition Bureau has indicated its focus will be on the particular circumstances in each case, with a view to determining whether the conduct is more likely to harm or enhance competition in the short and/or long run.

Companies may find themselves on either side of a perceived competition law issue, either as the target of complaints by new entrants and other up-and-comers attempting to gain access to the data resources or digital market they need to succeed, or as the initiator of a complaint, arising from alleged barriers or other obstacles created by data and digital incumbents.

Regardless of which side of a competition law issue an organization may fall on, organizations should be reviewing their business model and data strategy for potential competition law issues.

How businesses can manage the changing data landscape

There is no question that the regulatory landscape for data and other digital innovation is changing. In many cases, it is not a case of organizations working to get ahead of change, but rather working to simply keep up. While harnessing the power of data is the desired end state for many organizations, the path to harnessing that power may seem complex, time consuming and expensive.

Dentons understands that, and the Dentons Data suite of solutions is designed to get businesses rapidly moving forward on the path towards deriving value from their data, while at the same time ensuring they keep up with the changes in the data landscape. The phased, scaleable, fixed-fee solutions mean things get done on time and on budget.

When Dentons Data Summit participants were told a data genie would grant them a wish to use Dentons Data to solve one data headache, fifty-eight percent of respondents use their wish to solve data/records retention issues, beating out CASL, Privacy and E-contracting issues combined.

Dentons Data Summit 2019

Implementing artificial intelligence: Lessons from the trenches

Artificial intelligence (AI)—the simulation of human intelligence processes by machines, including learning (the acquisition of information and rules for using the information), reasoning (using rules to reach approximate or definite conclusions), and self-correction—promises substantial benefits to businesses. Businesses that develop and commercialize AI will likely have significant advantages in an increasingly digital world. We believe that organizations that adopt AI technologies can improve operations, enhance productivity, and ultimately increase their bottom line.

However, for all the possibilities, AI applications pose potentially significant risks for businesses and industry sectors:

- AI-enabled automation threatens to disrupt labour markets and employment;
- Predictive analytics in finance, education, policing and other sectors can reinforce racial, gender and class biases; and
- Data used in AI development and applications are often collected in ways that may violate privacy laws or compromise the accuracy of AI outcomes.

Furthermore, a number of sectors and industries exploring the adoption of AI technologies often have no prior experience with data or data-driven technologies.

As both public and private entities contemplate the various implications of AI in the context of their activities, there are a number of considerations and best practices to keep top of mind:

- **Algorithmic transparency:** Many AI techniques are "black box" models, meaning it is difficult to relate the input data and variables to the outcome. This is a major disadvantage, as it is difficult to explain to stakeholders, including regulators, how the outcome was actually achieved. For instance, where the AI is used to making a decision (e.g., extend credit or not, hire someone or not), a "black box" model does not allow an organization to defend itself against allegations of bias or demonstrate why the model is accurate. Using a more transparent model provides significant advantages, including the ability to demonstrate to stakeholders that the model is accurate. In addition, a well-trained, transparent model is often easier to implement, and requires less computing power and, perhaps, even less data to train than black box models.

- **Documentation:** It is vital to document all stages of the AI process, as data science is not an exact art, and any two data scientists will take different approaches to the same problem due to their differing experience and knowledge. Proper documentation helps ensure seamless transitions between those working on a given project, as well as provides for higher quality peer review.
- **Verify data quantity and quality:** A minimum quantity of data is required to achieve statistical significance at certain confidence intervals, but too much data can create "analysis paralysis." Laying out a clear plan at the beginning of data projects will help avoid work that is ultimately not useful. In addition, poor-quality data will only lead to serious errors. Investing time and effort to understand the data properly at the outset – verifying the source, checking missing values, identifying biases, and noting any anomalies – is likely to pay dividends in the form of better quality and more targeted results.
- **Foster a data culture:** A business should not tackle a data project in isolation. Executive engagement and corporate communication are essential to determine the problems that require solving, set out the metrics that define a project's success, and manage stakeholder expectations. Data scientists, business people and staff need to communicate to understand the challenges of working with data, and what is possible and what is not.

Thirty-nine percent of respondents attending the Dentons Data Summit reported that they are actively implementing or have just implemented AI in their organization. Another twenty-two percent reported that they have been using AI for some time now.

Dentons Data Summit 2019

- **Remember copyright:** Before using data, confirm that you have the necessary rights. If a third-party service provider generated the analysis based on your core samples or other property belonging to you, be sure to check the intellectual property clause in your contract. In the case of public sources, check the terms of service for the database, or the website from which the data was obtained to see what is and is not permitted.
- **Respect confidentiality:** If the data was obtained from a third party, or created in partnership with another company, such as in the context of an option agreement or a joint venture, review your contractual arrangements to confirm whether they require the other party's consent before giving access to an outside AI service provider.
- **Who is liable?** If the results of the analysis are not up to par, it is important to know who is responsible for making it right. When signing a contract for AI services, responsibility for each part of the job—selecting the data, preparing it for analysis, interpreting the results, and so on—has to be clearly stated. That way, once the source of the problem has been identified, it will be easier to determine who has the burden of addressing it.
- **Consider employees:** Ensure that you properly train your staff to get the most out of their digital colleague. They need to understand the software's functionality and limitations to use it properly.
- **Solve the right problem:** Once you have seen AI in action, it can be easy to view data as the answer to all of your business challenges. Avoid the trap of throwing data science at every problem. Sometimes the simplest, non-data solution is actually the right one. Data science is best used under certain specific conditions, such as abundant data, repetitive and measurable processes that can be observed over time, and a real problem that makes a real difference to the end user or business partner.
- **Re-evaluate regularly:** The process of deriving benefits from AI does not end when an insight is generated, or a predictive model is built. It is essential to check accuracy against real-world results. Discrepancies can occur for a multitude of reasons: initial conditions could vary from the original data, or a key variable may have been omitted unknowingly from the original analysis. In some cases, the very

fact of measuring and predicting can change the outcomes (very common when making predictions about human behaviour). Constant monitoring is vital to ensuring the work remains relevant, useful and accurate.

The use, value and application of AI will differ by sector or industry, but there are also key commonalities. For example, the Dentons Data Summit focused on the mining sector, but the lessons from that sector are applicable to many others. Similar to many other sectors and industries when trying to understand where and how AI applies and adds value, mining faces many of the same opportunities and challenges, including difficulty gathering consistently high-quality data to develop models; industry culture resisting the adoption of AI; unwillingness to invest in AI because initial adoption often involves impacts to daily operations and does not yield immediate returns for shareholders; and the high cost of integrating new or upgrading existing technology.

One interesting difference for many mining companies using AI is that, in contrast to other sectors, such as retail, mining companies are generally not interested in data sets that contain personal information, and as a result, are free from many of the privacy concerns and restrictions facing companies in other sectors. As such, AI is enabling mining companies to become insight-driven enterprises that utilize data to derive key benefits.

As with many other sectors, AI is becoming a powerful tool for analyzing data in operations, ranging from managing transport and logistics, to human resources and supply chain management. AI can identify patterns that are useful in reducing expenses, optimizing resources and reducing waste.

Through the use of a variety of AI applications, AI is able to analyze vast quantities of geological and mapping data to better predict where to find better resources. This reduces exploration time, improves planning and increases return on investment.

Legal risk is a significant concern among organizations using AI, and the more these organizations understand the risk, the more concerned they are. Twenty-eight percent of respondents at The Dentons Data Summit indicated they didn't fully understand the risks, but were nonetheless concerned about them. That number more than doubled (to fifty-nine percent) amond respondents who said they fully understand the risks.

Dentons Data Summit 2019

Smart building, smart cities, smart risk management

Smart cities are ecosystems of connected buildings or infrastructure that collect data on the people, devices and assets using electronic sensor networks—Internet of Things (IoT). Using monitoring equipment and device environments, as well as managed services and applications, smart cities supply data that enable the optimization of operations at a reduced cost.

Advances in communication and information technology, sophisticated computing and smart algorithms in an increasingly connected environment, present new opportunities for managing buildings and structures. Enabled by these new technologies, smart buildings consume less energy, generate less waste and provide better quality spaces to inhabitants. Smart buildings provide a framework to allow sector participants to capitalize on digital innovation.

It is the lack of a robust regulatory framework governing the monitoring, collection and use of such data that may be hindering the wider adoption of smart city planning around the world.

Questions about smart infrastructure are typically raised around three main areas: privacy and data security concerns, telecommunications, and access to public infrastructure.

Privacy and data security

Smart infrastructure collects a large amount of data, including personal data. This raises a number of privacy-related issues: How is consent obtained in a smart city environment? Who owns the data collected? How is it shared? Who has access to the data? How is the data protected? Is it possible to be de-identified and/or anonymized, and if so, how?

The data produced by smart cities and the people who move through them can be monetized and generate revenue, but participants in a smart city infrastructure will need to be clear about where they fit into the business model, and what their relationship is to the data and the players in the larger ecosystem.

Data and IT security risks increase in environments emphasizing smart infrastructure. Building management systems, which handle everything from air conditioning to closed-circuit television, access control, lighting and door locks, traditionally

worked on serial networks and were segregated from conventional IT networks. These systems are now internet-enabled, and open to the range of threats that afflict conventional IT systems. The potential harm is significant.

Increasingly, a company's "cyber readiness" is a key issue in determining future business partnerships. Companies without demonstrably robust cybersecurity controls and information governance protocols introduce risk into the entire connected environment; a risk that may not be acceptable to the other smart city participants. Similarly, insurance companies are re-evaluating policies based, in large part, on the security measures in place.

Telecommunications

The arrival of 5G connectivity and smart solutions have paved the way for possibilities that seemed futuristic not long ago.

Only a few years ago, there was little demand by residential tenants for full connectivity; however, we are now seeing a dramatic shift. Residents want fibre connections in their suite. With the increased popularity of smart speaker and personal assistant devices (and whatever is next on the horizon), this demand is expected to grow.

At the institutional level, fibre connectivity in assisted living facilities (which provide increasing levels of care for ageing residents) has enabled residents to have access to specialty systems and healthcare analytics previously only available in hospitals. Real-time location systems, facial recognition access (especially useful to tenants with memory loss), and wandering patient tracking are now available in many of these facilities.

In addition to privacy and data security, there is uncertainty around the application of Canada's telecommunications rules to IoT service providers, including those that dominate the smart cities ecosystem.

Access and speed

IoT suppliers may need access to public (e.g., municipal) infrastructure, such as light poles, street furniture, transit shelters and buildings, in order to deploy the wireless equipment, devices and sensors that provide connectivity for smart cities. However, physical access is just the beginning – connectivity, especially the speed of that connectivity, is also a concern. This will become even more pronounced with the deployment of 5G networks, and the proliferation of small cells that will need to attach to the infrastructure in a timely manner. As more IoT devices, sensors and vehicles come online, the infrastructure must be able to handle the increased network traffic at a speed that allows for timely actions. For instance, a traffic light that has a transmission lag of even a few seconds, could create a risk to property and life.

Beyond Bitcoin: Applications of blockchain and distributed ledger technology

Blockchain goes beyond cryptocurrency. While still in its infancy, it is evident that blockchain has applications and benefits across numerous sectors. What is less obvious, however, are the potentially far-reaching implications of the implementation of blockchain technology in these sectors.

The core technology behind blockchain – distributed ledger technology (DLT) – could offer significant advantages for traditional financial institutions, and other organizations that must safeguard confidential data and personal information. Because of its decentralization, DLT is more secure than traditional, centralized ledger technology, which increases its dependability, transparency, trust and identity verification for the online world.

An end to digital silos

Organizations are focusing on blockchain as a way to simplify processes and eliminate duplication (and, therefore, reduce costs). For example, financial institutions expend a large amount of time and money on Know Your Customer (KYC) and Anti-Money Laundering (AML) processes, which take, on average, between 30 and 60 days to complete per customer. Often new KYC and AML checks are needed within the same organization.

Leveraging blockchain technology can provide easier access to client information within the organization, streamline KYC and AML checks, and facilitate the identification, verification and compliance processes. In addition, because there is no central data store, sensitive information is better protected than with traditional databases, which may have a single point of failure. The technology also allows institutions to conduct real-time monitoring and reporting to help identify fraud earlier, enabling a proactive, rather than reactive, stance when dealing with financial crimes.

Trust anchors

Trust anchors are authoritative entities or collections of entities for which trust is assumed and not derived from an external source. As trusted authentication services, these organizations leverage their infrastructure and reputation using blockchain technology to provide

a baseline for shared reference. These baselines are truthful by nature, possess the ability to verify critical information and validate factual claims for third parties.

Blockchain can enable traditional trusted institutions, such as non-governmental organizations (NGOs) and banks, to become trust anchors, and share reliable data with organizations.

As an immutable ledger—a record that cannot be altered—DLT provides transparency, efficiency and security, because information recorded on a blockchain is verified as true. Data that is input can only be changed by following a pre-determined protocol. Discrepancies in client data are easy to identify, and institutions have access to all documents and compliance activities related to each client.

Clients who have been verified by a trust anchor have a digital identity that is portable, and could be accepted by other organizations as trusted and accurate. Because of the trust in the trust anchors, clients could then use their digital identity as a type of signature, which would be accepted in various industries, such as finance, healthcare and government.

By becoming trust anchors, organizations potentially create an additional revenue stream. Because of the accuracy and reliability of the information these trust anchors hold, the data could be monetized as identity verification services sold to third parties. For third parties, this service offering could be attractive because it would allow them to rely on trust anchors for KYC and AML compliance, rather than completing the processes and procedures themselves. However, there is also the view that the monetization of personal digital identity, and the authentication and verification services that surround and support that digital identity, should be prohibited. This area is still evolving.

Self-sovereign identity and identity verification

Blockchain and the use of trust anchors have empowered consumers by paving the way for self-sovereign identity; a concept that individuals should have complete access to, and control of, their data. Self-sovereign identities do not rely on any centralized authority.

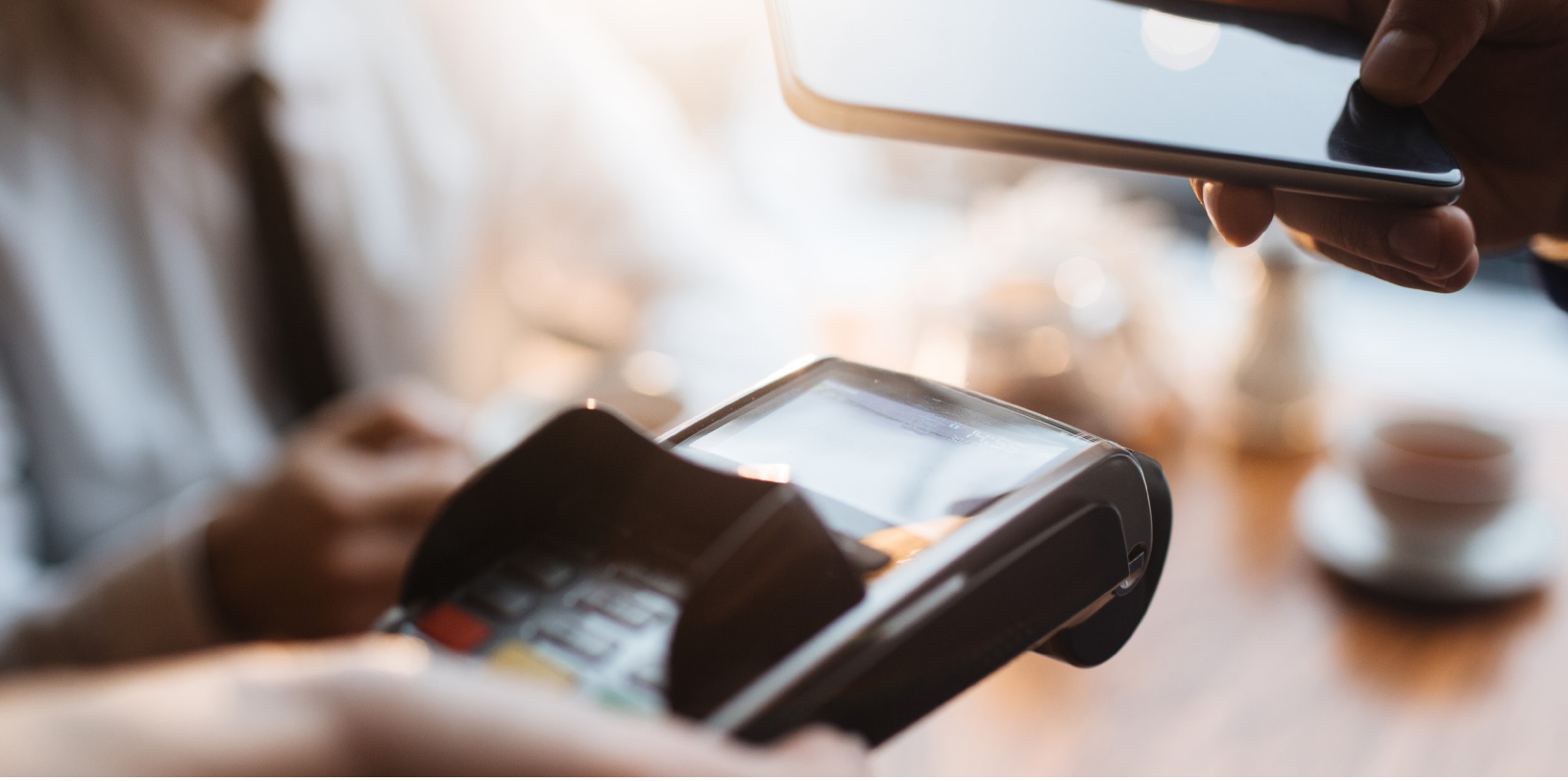
DLT allows people to control their private data (such as internet browsing history, financial records and medical information), and securely share some or all of that information with selected third-party entities, empowering individuals to control how their data is used and by whom. The transparent nature of DTL provides users with a full audit trail of their data, so they can ensure it was used for the intended purpose.

Smart contracts and legal frameworks

The ability to audit and accurately verify information using blockchain has led to 'smart contracts'. A standard contract outlines the terms of a relationship, which are enforceable by law. A smart contract outlines the terms of a relationship and enforces the relationship with a cryptographic code. Smart contracts automatically execute, as outlined by their creators, helping people or businesses exchange money, property, shares, or anything of value, and avoids the services of a middleman.

Smart contracts offer additional layers of transparency, integrity and automation not available in traditional contracts. Because the contract is virtual (with no need for paper documents), delays in processing no longer occur. Transactions executed via smart contracts are visible to all parties and verified automatically, adding an extra level of objectivity about the 'who', 'when', and 'why' of a contract, and an audit trail for verification.

As smart contracts continue to evolve, there is a need to develop an overarching legal framework. Guidelines need to be established regarding the consequences of coding errors in blockchain and DLT. While blockchain technology is highly secure, no code is infallible, and there is always the potential for human error. If coding errors are introduced into this otherwise secure technology, what type of legal intervention is possible, available or recommended? These issues have been and continue to be the subject of debate within the industry.



The evolution of retail payments

Payments, once a relatively staid area of financial services, are poised for rapid innovation and wholesale change.

Payment system modernization, open banking/consumer directed banking, and proposed amendments to modernize privacy legislation have expanded the scope of interest for retail payment regulation beyond financial institutions. With the prospect of more and different providers being given access to players within the regulatory perimeter, or being invited within the regulatory perimeter itself, the opportunities for new business are plentiful.

The modernization of payment systems' impact on financial services (i.e., the addition of the real-time rail, open APIs and data portability, and in the context of retail payments) cannot be understated. Staying current on the latest developments will position your business to leverage the opportunities these changes bring, and enable rapid execution on digital innovation, a key market differentiator in the financial services sector.

Consumers expect fast, friction-free payments, and modern payments infrastructure is crucial. Today, more than 40 countries, including Australia, the UK, and the US, are actively undertaking payments modernization and innovation for a fast, more flexible, and secure payments infrastructure.

While Canadian consumers have been introduced to some new payments technologies (more than 40 percent of all consumer payments in Canada are now contactless transactions, relying on NFC-chip-enabled cards), and methods (such as using their smartphone or smartwatch to pay for their groceries), the wholesale change in payment system modernization already established in other countries is just beginning in Canada.

While, for example, Australia and the UK have implemented real-time payment systems that can be used for both retail and corporate payments, many corporate payments are still made by cheque in Canada. Electronic fund transfers or payments from overseas can still take several days to complete. However, change is coming to the Canadian payment ecosystem. In 2015, a project begun by Payments Canada—a public purpose corporation that owns and operates national core payments clearing and settlement infrastructure in Canada—is attempting to address the issues impacting payment system users.

Within the next several years, the creation of new payment infrastructure, along with a new legislative framework, will have a profound impact on Canada's entire payments system.

Pain point

A 2015 survey released by Payments Canada highlighted two major pain points for payments across the country: the slow speed of payments and the lack of data travelling with payments, which could give transactions added context. Additionally, there is a considerable cost associated with traditional payments processing. Researchers suggest that in Canada, companies spend more than CA$5 billion annually on payment processing.

Consumers and businesses increasingly expect near real-time funds availability, and businesses want data-rich payments to enable the implementation of new payment products and services. Infrastructure modernization is also needed to meet regulatory requirements around system stability, consumer protection, financial inclusion and customer experience.

Payments modernization in Canada

Canada has a history of pioneering payment solutions, the most recognized of which is the Interac payment system in the 1980s and 1990s. Interac is an interbank network that links financial institutions and other enterprises for the purpose of exchanging electronic financial transactions; it serves as the Canadian debit card system.

Following the road map from Payments Canada, the Canadian payments industry is working toward more openness and innovation, so that Canadian businesses and consumers can benefit from cutting-edge technological advances in payments.

Real-time payment rail

In Canada, one of the primary goals of modernization is to make payments and settlements happen almost instantly using what has been dubbed the "real-time rail." Slated for tentative rollout beginning in 2020, real-time rail will facilitate real-time delivery of lower-value payments.

Consumers may believe that debit card and e-transfer payments are instant, however, in actuality, Canadian banks assume some risk by floating transactions overnight until payments are reconciled between financial institutions. Real-time rail will eliminate this exposure for banks, allowing for faster alternatives to slower payment methods, such as cash and cheques. It will also allow for convenient small-value payments using simple identifiers, such as mobile phone numbers or email addresses, rather than banking information, and will confirm receipt of such funds. Real-time payments could also mitigate cash flow issues for many small businesses, which tend to rely on payments made by cheque.

It is hoped that the real-time rail will spur innovation in the fintech sector, opening up new business models and partnerships between fintechs, banks and other financial institutions.

In the UK, real-time payments have been widely adopted. The Faster Payment Service has reduced payment times for amounts up to £250,000, from three working days to a few seconds. To be competitive globally, Canada must also reach this level.

ISO 20022

ISO 20022, an internationally-used, universal payments standard that allows for more data-rich payments, will form the backbone of the real-time rail. Since 2014, payment system operators have been adopting the ISO 20022 payment standard as a way to reduce friction in the traditional paper-based B2B payments process, and standardize cross-border communication between financial institutions.

ISO 20022-compliant payment systems will provide speed, and allow for greater transparency, because of the ability to complete data-rich transactions. This information gives businesses additional insight into the nature of their business, and enables faster reconciliation because the data flows with the payment itself, rather than through another mechanism.

To maximize the benefits of a standard like ISO 20022, it will require the commitment of the entire payments ecosystem – from banks and other financial institutions, to fintechs and startups. Based on other jurisdictions, it will likely be the paytech and fintech early adopters that focus on B2B, loans and personal financial management that will drive banking partners to adopt the ISO 20022 standard.

Implications for small business

The benefits of the real-time-rail for Canada's small businesses could be substantial.

In 2018, as part of an effort to increase payment speed, banks in Canada added a third exchange window for companies making electronic funds transfer (EFT) payments. This change had immediate positive effects on cash flow, by giving companies another opportunity to submit payment files, leading to faster funds availability. This third window is of particular value to west coast companies operating in the Pacific Time Zone.

Due to continuing friction within Canada's existing payments system, many small businesses do not yet accept electronic or online payments, because credit card payments can take several days to reach a merchant's account, cheques do not clear and settle immediately, and international cheques can take weeks to process.

Real-time, data-rich payments will have a positive impact on small businesses. Individual business owners will be able to better manage cash flow, and understand on a day-to-day basis the financial standing of their business, positively impacting their ability to grow and contribute to the economy as a whole.

As a result, and based on the experience of small businesses in the US, we should expect that ISO 20022-compliant instant payments will change the business model of many small businesses. Reliance on same-day or real-time settlement improves a company's operating cycle, allowing for improved cash flow and its associated benefits.

ISO 20022-compliant payment systems will also allow small businesses to take advantage of more seamless reconciliation and additional analytics. With Canadian companies spending as much as CA$5.2 billion on payments processing annually, the ability to avoid slow, manual reconciliation of invoices and payments, and set aside legacy infrastructure in favour of instant, automatic reconciliation, could produce immense savings for small businesses and corporations alike.

Organizations identified privacy compliance and data security incidents as the biggest litigation risk facing their organization, with sixty-seven percent of respondents saying this was the case.

Dentons Data Summit 2019

Litigation in the digital economy

Litigation in the digital economy

Litigation is a risk in any business. As companies adopt new technologies, embrace new business models, and enter into markets and sectors, this risk is significantly amplified. When we consider the digital economy and, in particular, data, privacy and class actions, jurisdiction and the internet, and cryptocurrency litigation, uncertainty in litigation is compounded by a lack of case law.

Dealing with novel issues created by new technologies and business models, and the courts' unfamiliarity with them has increased litigation risk in many of these areas. There are steps businesses can take to mitigate this risk, and actions they can take if faced with litigation.

Proactive:

Privacy – data mapping, risk assessment and mitigation: Understanding what information you have and how it is held will help you understand your potential exposure in the event of a data breach. Consider what customer and employee information you have, who has access and what safeguards are in effect. Know where your personal information is stored and processed (and by whom), what privacy laws apply, and what contractual obligations you may have with vendors, suppliers and service providers. Having the answers at hand will allow you to understand your potential exposure, and properly assess whether you met the duty of care in the event of a breach. Ensure (and document) that appropriate measures and safeguards are in place. This will affect the assessment of whether any duty of care has been met in the event of a breach.

Jurisdiction and arbitration: As companies move away from bricks-and-mortar establishments, it is increasingly open to debate exactly where a business is being conducted, which can lead to disputes about which laws apply, and where disputes should be heard. Speak with counsel to understand what your key risk areas are, and what jurisdictions may be more favourable to you if disputes should arise. Consider where your employees and customers are located, including from where they are accessing your website, to avoid advertent jurisdictional issues. Consider and consult with counsel on an appropriate jurisdiction or arbitration clause, ideally one that will be considered

fair (and, therefore, enforced) by any reviewing court.

Cryptocurrency: Cryptocurrency disputes have just begun to hit the courts. The main takeaway from this early litigation is there is still uncertainty about how crypto-assets will be characterized by courts. For instance, are crypto-assets merely assets, or are they more in the nature of a security that would trigger securities regulation? Getting this wrong can result in a company being forced to shut down. Even where the crypto-asset is correctly characterized, its novelty will not be an excuse for ignoring regulations. What is clear is that general principles, laws and regulations regarding corporate governance and business law are likely to apply. Businesses should take care to ensure misrepresentations are not made (even in presentations and YouTube videos), and consult with counsel on corporate governance matters.

Reactive:

Class action strategy and goal-posts: If a class action proceeding is commenced, set goal-posts: What can you accomplish? What goals are realistic and can you achieve what you need (e.g., do you need to win this at all costs … or is a quick settlement more aligned with your goals? Is Canadian litigation driving your strategy, or is there foreign litigation that presents a higher risk such that the Canadian litigation must be managed accordingly?) What is the best way to spend your litigation budget? Working with counsel to set expectations and priorities will result in a litigation strategy that is economical, efficient and serves business outcomes.

In the context of a privacy or data breach class action, ensure counsel has experience specifically in this area, and understands the interplay between global data protection authorities and litigation. Data breach class actions law in Canada is still developing, so working with counsel who already know and follow the law in this area will ultimately provide a cost saving.

Proactive management of privilege, especially over IT forensic reports, will be important. Counsel should have existing relationships with third party vendors, such as call centre providers, credit monitoring companies, and public relations/government relations firms.

Jurisdiction: Consider what court or tribunal is the appropriate forum for the dispute. Work with counsel to determine whether there is a jurisdiction that may be more favourable to you. Can you rely on a forum selection or arbitration clause contained in any relevant agreement?

Cryptocurrency: Consider what principles of corporate governance and business law you can rely on, for offensive or defensive purposes. Is the issue one that falls outside the scope of existing laws or regulations, such that novel arguments can be made?

Engaging with litigators on a proactive basis minimizes risk to businesses. We provide insights as to how litigation would play out if and when issues arise, allowing businesses to work backwards and develop appropriate strategies, policies and practices, as well as help you understand and mitigate risk.

Dentons Data Suite of services

Dentons Data suite of services

In response to challenges faced by organizations as they are swept along by digital transformation, we have launched the Dentons Data suite of services. These services are fixed-fee, project-based solutions to common data-related problems. Dentons Data solves problems – data retention issues, cybersecurity readiness, compliance headaches, privacy audits, data governance, IT forensic investigations, and a host of other issues. Dentons Data can also work with your business to create, develop and implement a longer term data strategy. We help you manage risk as part of strategic planning and execution, not apart from it.

With your data challenges solved, you'll be better able to anticipate change, be more agile, and more adept at identifying and pursuing opportunities to enhance your business strategy and long-term growth plans.

Dentons Data

- **Unbundled: You select only what you need.**
- **No billable hours: Solutions are fixed fee, so you get budget certainty.**
- **Scaleable: Our solutions can be scaled up or down, depending on the size and needs of your organization.**
- **Phased: Short, defined phases to complete projects, and avoid overwhelming your internal resources.**

Dentons Data

Dentons Data provides a one-stop shop for organizations of all sizes: sophisticated legal advice + best-in-class process management + IT forensics and procurement capabilities.

Key contact

Kirsten Thompson
Partner, National Lead
of Transformative Technologies
and Data Strategy Group, Toronto
D +1 416 863 4362
kirsten.thompson@dentons.com

Authors

Adam Allouba
Partner, Montreal
D +1 514 878 8871
adam.allouba@dentons.com

Karl Schober
Senior Associate, Toronto
D +1 416 863 4483
karl.schober@dentons.com

Jawaid Panjwani
Senior Associate, Ottawa
D +1 613 783 9632
jawaid.panjwani@dentons.com

Ryan Middleton
Partner, Toronto
D +1 416 361 2367
ryan.middleton@dentons.com

Tracy Molino
Counsel, Toronto
D +1 416 862 3417
tracy.molino@dentons.com

Chloe Snider
Partner, Toronto
D +1 416 863 4674
chloe.snider@dentons.com

ABOUT DENTONS

Dentons is the world's largest law firm, delivering quality and value to clients around the globe. Dentons is a leader on the Acritas Global Elite Brand Index, a BTI Client Service 30 Award winner and recognized by prominent business and legal publications for its innovations in client service, including founding Nextlaw Labs and the Nextlaw Global Referral Network. Dentons' polycentric approach and world-class talent challenge the status quo to advance client interests in the communities in which we live and work.

dentons.com

CSBrand-19383-Dentons-Data-Summit-Whitepaper-06 — 30/10/2019