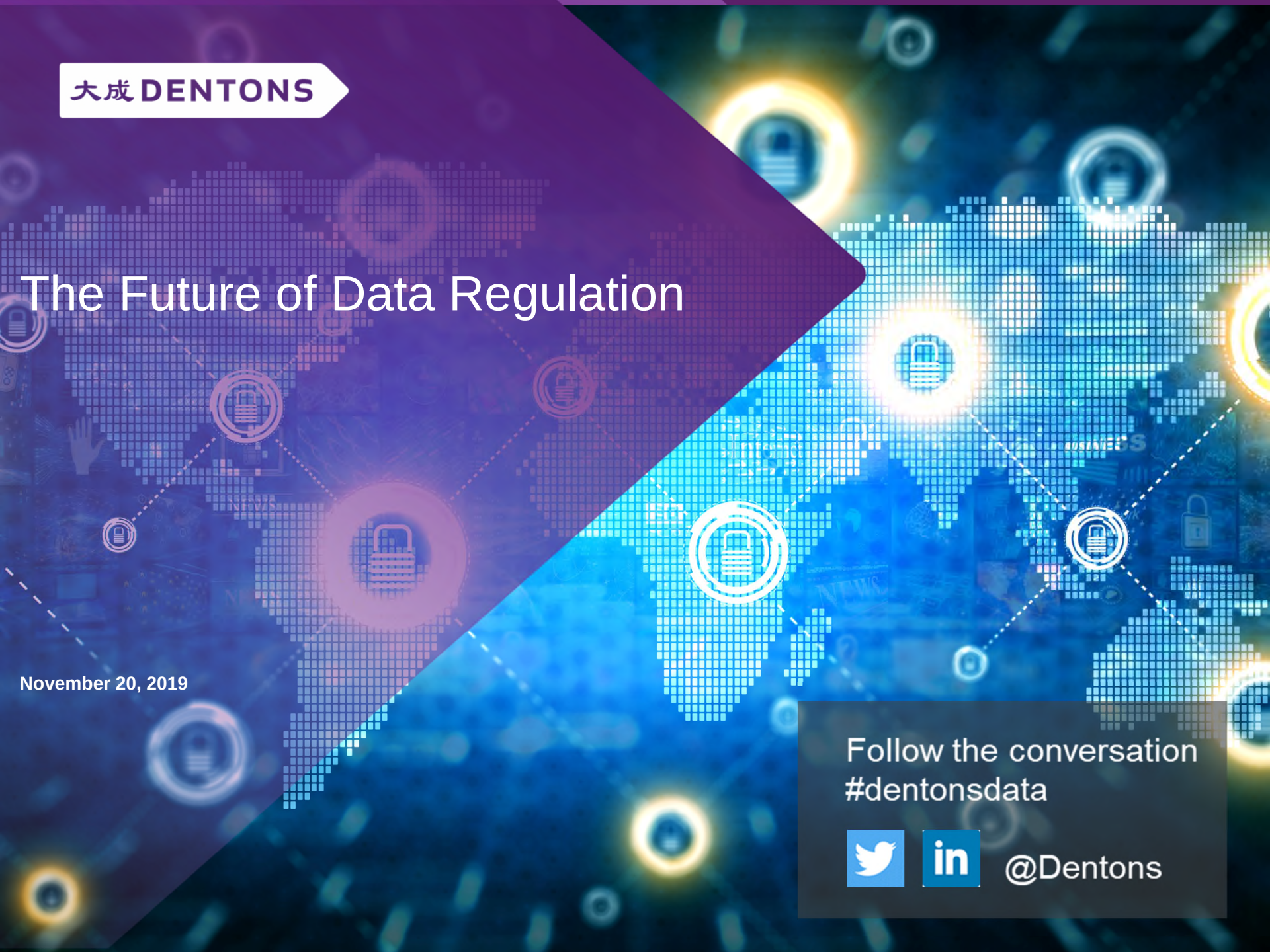

大成 DENTONS
The Future of Data Regulation
November 20, 2019
Follow the conversation
#dentonsdata
@Dentons

The Future of Data Regulation

Presented by: Kirsten Thompson, Partner and Lead, Transformative Technologies and Data Strategy
T +1 416 863 4362
kirsten.thompson@dentons.com

Follow the conversation
#dentonsdata

@Dentons

The highlights

1. **Privacy and Data 2.0**
    - Key developments in data regulation and what the next 18+ months hold
        - Transfers of personal information
        - Canada's Digital Charter
        - PIPEDA modernization
        - Competition call out
        - Vicarious liability for employees
2. **A Data *What*?**
    - What is a Data Strategy, and why a business needs one

Privacy and Data 2.0
Transfers of Personal Information

Transfers of PI

Key Question: Does a transfer of personal information require consent?

- Prior OPC Guidance:
  - OPC *Processing Personal Data Across Borders Guidelines*, January 2009 (*OPC Cross Border Guideline*)
  - PIPEDA Case Summary #2005-313, PIPEDA Case Summary #2008-393
- Transfer for processing is a "use" and not a disclosure, therefore **no new consent is required.**

> "Organizations must be transparent about their personal information handling practices. This includes **advising** customers that their personal information may be sent to another jurisdiction for processing and that while the information is in another jurisdiction it may be accessed by the courts, law enforcement and national security authorities of that jurisdiction."
>
> OPC Cross Border Guideline

"Advise", NOT consent

Transfers of PI cont'd

September 2017 massive data breach

Privacy Commissioner investigates

April 9, 2019 - PIPEDA Report of Findings #2019-001

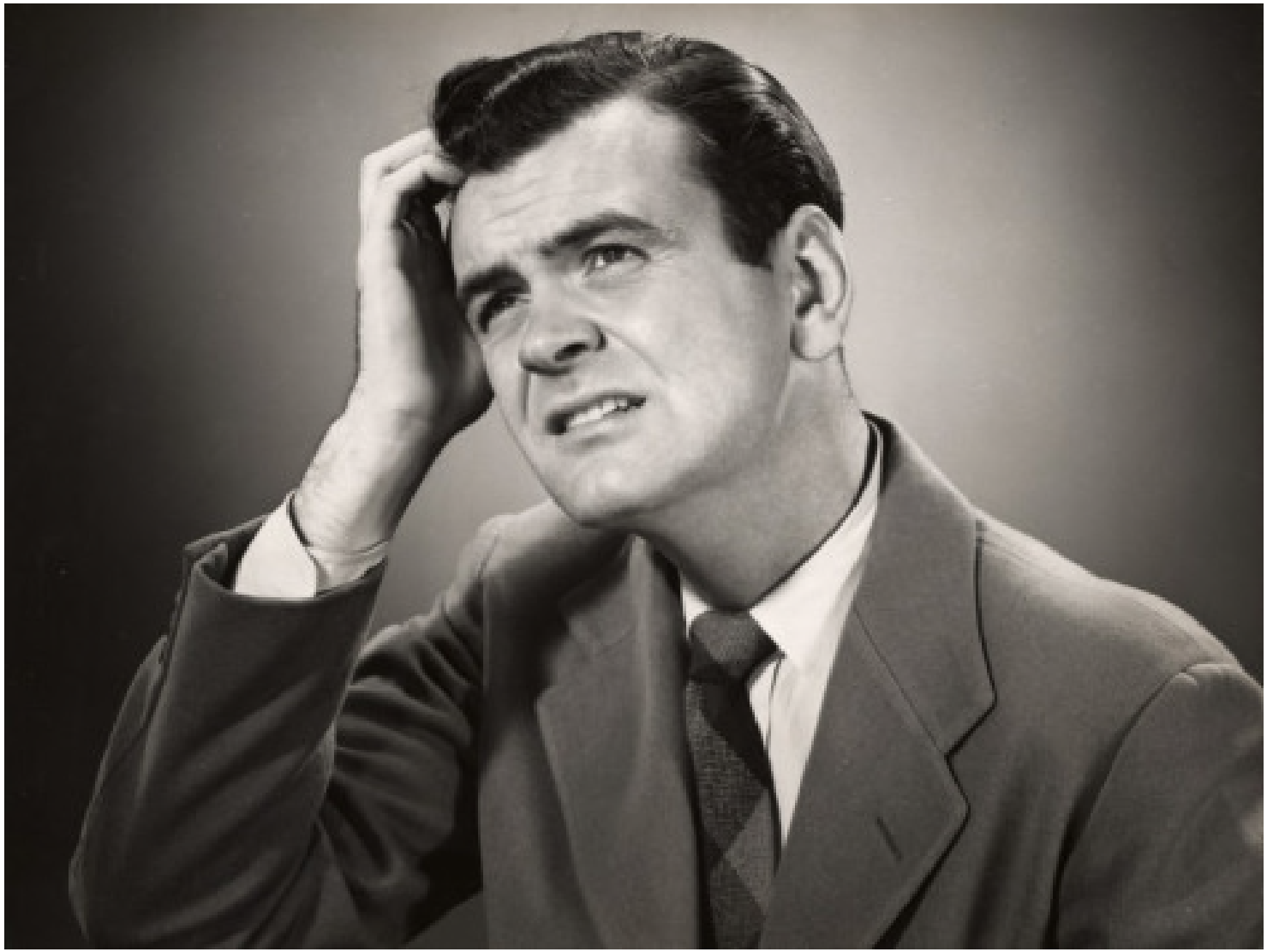
Transfers of PI cont'd

"[US Co.]… received **information transferred to it by [Canada Co.]** about those consumers to fulfil those products. Also as described in Section 3 of this report, [**Canada Co.] remained accountable for this information transferred to [US Co.]. for processing**, and responsible for the related obligations under PIPEDA 4.1.3.

At the same time, **these transfers for processing from [Canada Co.] to [US Co.] constitute disclosures** of personal information under the meaning of PIPEDA Sections 7(3), and 4.3."

PIPEDA Report of Findings #2019-001, paras. 100 and 101

Transfers of PI cont’d



Transfers of PI cont'd

- OPC *Consultation on transborder data flows* and the *OPC Consultation on transborder data flows and supplementary discussion document* → **a transfer is a disclosure**
- Government of Canada *Proposals to modernize the Personal Information Protection and Electronic Documents Act* → **a transfer is a disclosure…but consent may not always be required**
- OPC *Consultation on transfers for processing – reframed discussion document*:

> "To be clear, we would **not recommend that consent be required in the longer term in the context of data transfers for processing**, if other effective means are found to protect the privacy rights of individuals. But in situations where neither contractual clauses nor other means are effective, consent may be required.
>
> "The change in position by the OPC would require organizations to highlight elements that were previously part of their openness obligations and ensure that individuals are aware of them when **obtaining consent for transborder transfers**…"

Transfers of PI cont'd

- September 23, 2019 – OPC concludes consultation and states there will be **no change** in interpretation:

> "…concluded that its **guidelines for processing personal data across borders will remain unchanged under the current law.** The OPC will now focus its efforts on how a reformed law can best protect Canadians' privacy rights when their information is transferred between organizations.
>
> […]
>
> During its consultation, the Office received 87 submissions. Stakeholders […] [t]he vast majority took the view there was no requirement under [PIPEDA] to seek consent for transfers for processing and that doing so would create enormous challenges for their business processes"

- OPC clear that it views current position as inadequate, and will advocate for change in law - current emphasis will be on **transparency** and **meaningful consent**

Privacy and Data 2.0
Canada’s Digital Charter

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).
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.
3. **Control and Consent:** Canadians will have control over what data they are sharing, who is using their personal data and for what purposes.
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.
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.

Canada's Digital Charter – 10 Principles

6. **A Level Playing Field**: The Government of Canada will ensure fair competition in the online marketplace while protecting Canadian consumers from market abuses.

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.

8. **Strong Democracy:** The Government of Canada will defend freedom of expression and protect against online threats and disinformation.

9. **Free from Hate and Violent Extremism:** Canadians can expect that digital platforms will not foster or disseminate hate, violent extremism or criminal content.

10. **Strong Enforcement and Real Accountability**: There will be clear, meaningful penalties for violations of the laws and regulations that support these principles.

Canada's Digital Charter – next steps

- Proposed initial focus of the government's Digital Charter based actions is on modernizing PIPEDA
- Digital Charter will likely have broader industry-specific effect through anticipated changes in the *Competition Act*, *Canada's anti-spam legislation* (CASL), *Telecommunications Act*, *Broadcasting Act* and *Radiocommunication Act*.

Example: As part of the Digital Charter "action plan", the government also proposes to modernize CASL and to review enhanced e-protection measures, where appropriate, to make sure CASL is clear and effective.

Privacy and Data 2.0
PIPEDA modernization

PIPEDA Modernization

- Gov't released *Strengthening Privacy for the Digital Age* Discussion Paper on May 21, 2019 - proposals to modernize PIPEDA
- Seeks 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.
- PIPEDA modernization plan is focused on four areas:
  1. Enhancing **individuals' control**
  2. Enabling **innovation**
  3. Enhancing **enforcement**
  4. **Clarifying** PIPEDA

1. Enhancing Individuals' Control

- Provide more meaningful control, transparency and consumer choice by:
  - requiring specific, **standardized, plain-language** information on use of PI, the 3rd parties it's shared with, and prohibiting bundling of consent into a contract;
  - incorporating **alternative grounds to consent** (similar to GDPR's legitimate interests basis for processing PI);
  - 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 PI** and mandating defined retention periods but **not including the right to be forgotten** (aka de-indexing) because the matter is before the Federal Court of Canada.

2. Enabling Innovation

- To balance data-driven innovation with the need to ensure businesses are transparent, accountable and appropriately use data, the government proposes (among other things):
  - the creation of **codes of practice, accreditation/certification schemes and standards**, validated through recognition by the OPC.

3. Enhancing Enforcement

- Enhancing the OPC's enforcement and oversight abilities by providing it with **order making powers** in the form of cessation and record preserving orders
- Proposals to **extend the existing fine regime** to other areas of PIPEDA, and **substantially increasing** the range of fines

4. Clarifying PIPEDA

- The proposed reforms also aim to clarify the application of PIPEDA (and thereby enhance accountability), including by **extending PIPEDA's applications to certain non-commercial data collection** activities.
- In an effort to address new business models, which do not fit in the traditional "controller-processor" framework, the government also plans to **update and clarify PIPEDA's applicability**, including in the context of transborder data flows.

Timing:

- Consultation period anticipated, but not yet announced
- Modernization necessary, in part to ensure Canada maintains its "adequacy" standing with the EU, which is up for review as early as 2020. However given the federal election this fall, unlikely to see any movement until sometime in 2020.

Privacy and Data 2.0
Competition call out

Competition Bureau “Call Out”

- On September 9, 2019, the Competition Bureau announced it was is “seeking information from market participants about conduct in the digital economy that may be harmful to competition.”

Competition Bureau “Call Out”

- **Key question:** Have certain core digital markets, like online search, social media, display advertising and online marketplaces, become increasingly concentrated, to the detriment of consumers and businesses.
- The Call Out paper explores two potential, and possibly complementary, explanations:
  - **Tipping:** Digital markets may ‘tip’ to a dominant firm: characteristics of certain digital markets may favour the emergence of a single winner or a small group of winners
  - **Anti-competitive conduct:** Leading firms may not have achieved success by outperforming their competitors, but rather by executing anti-competitive strategies that target existing or potential rivals

Privacy and Data 2.0
Employees

Employees

- **Vicarious liability for data breaches is unsettled in Canada**.
- An employer can be held vicariously liable for the tort of an employee where the act was either: **authorized**, or **unauthorized but so connected with the authorized acts** of the employee that they may be regarded as modes, albeit improper modes, of doing an unauthorized act.

What about when an employee goes rogue, and takes sensitive customer PI from the employer and releases it publically?
When customers sue, should the company be vicariously liable for the damages caused by the employee's bad acts?

Employees

- *Ari v. Insurance Corporation of British Columbia,* 2015 BCCA 468: **Claim for vicarious liability survives motion to strike**
- ICBC employee accessed the PI of Ari and 65 other ICBC clients; Ari commenced a class action against ICBC as representative plaintiff. One of the claims was for damages under BC's statutory tort of breach of privacy.
- **Key question:** could ICBC be vicariously liable for the rogue employee's breach of the personal privacy of the class?
- Although the Court recognized that the statutory breach of privacy under the *Privacy Act* requires willful conduct, the Court concluded that the **intentional aspect of the tort was not necessarily incompatible with the imposition of vicarious liability**.
- The Court ultimately found that it was necessary for it to receive evidence in order to address whether ICBC could be vicariously liable – and declined to strike the vicarious liability claim. The appellate Court upheld this finding.

Employees

- **Morrisons** case in the UK (*WM Morrison Supermarkets Plc v Various Claimants* [2018] EWCA Civ 2339 (22 October 2018))
  - payroll data which was stolen and then published online by a then-employee of Morrisons.
- Claim was for misuse of private information and breach of confidence.
- The Court held that **although Morrison's was not directly liable, the company was vicariously liable** under each cause of action for the actions of the employee
- Morrisons appealed the judgment on three grounds, including that the trial judge had incorrectly concluded that the wrongful acts of Morrisons' employee occurred during the course of employment.
- In October 2018, the appeal court dismissed all three of Morrisons' arguments and affirmed the High Court's decision finding Morrisons could be liable for its employee's intentional bad acts.

Morrisons subsequently applied to the Supreme Court for permission to appeal the judgement and this permission was granted on April 2019.

A Data *What*?
Data Strategy

Data Strategy

- A Data Strategy describes a set of choices and decisions that together, chart a high-level course of action to achieve high-level goals. It forms a coherent strategy for organizing, governing, analyzing, and deploying an organization's information assets that can be applied across industries and levels of data maturity.
- A well-developed Data Strategy has:
  - Identification of data assets (inventory)
  - A strong data governance model that includes regulatory and compliance guard rails and specifies accountabilities
  - Well-considered goals for the data assets under management, including managing and streamlining storage, provisioning and processing
  - Metrics and measurements of success
  - Short-term and long-term program objectives

Data Strategy

What will success look like?

Current State:

- Management of data is compliance driven
- *Ad hoc*, siloed; data seen as byproduct of business, not revenue generator
- Business doesn't have access to the data it needs
- Business units (BUs) don't know the holdings of other BUs
- BUs do not consistently collaborate or share data
- There is no strategic oversight to the use of data
- Data are not effectively leveraged for evidence-based decision-making
- Employees lack skills to use data effectively

FROM

THROUGH

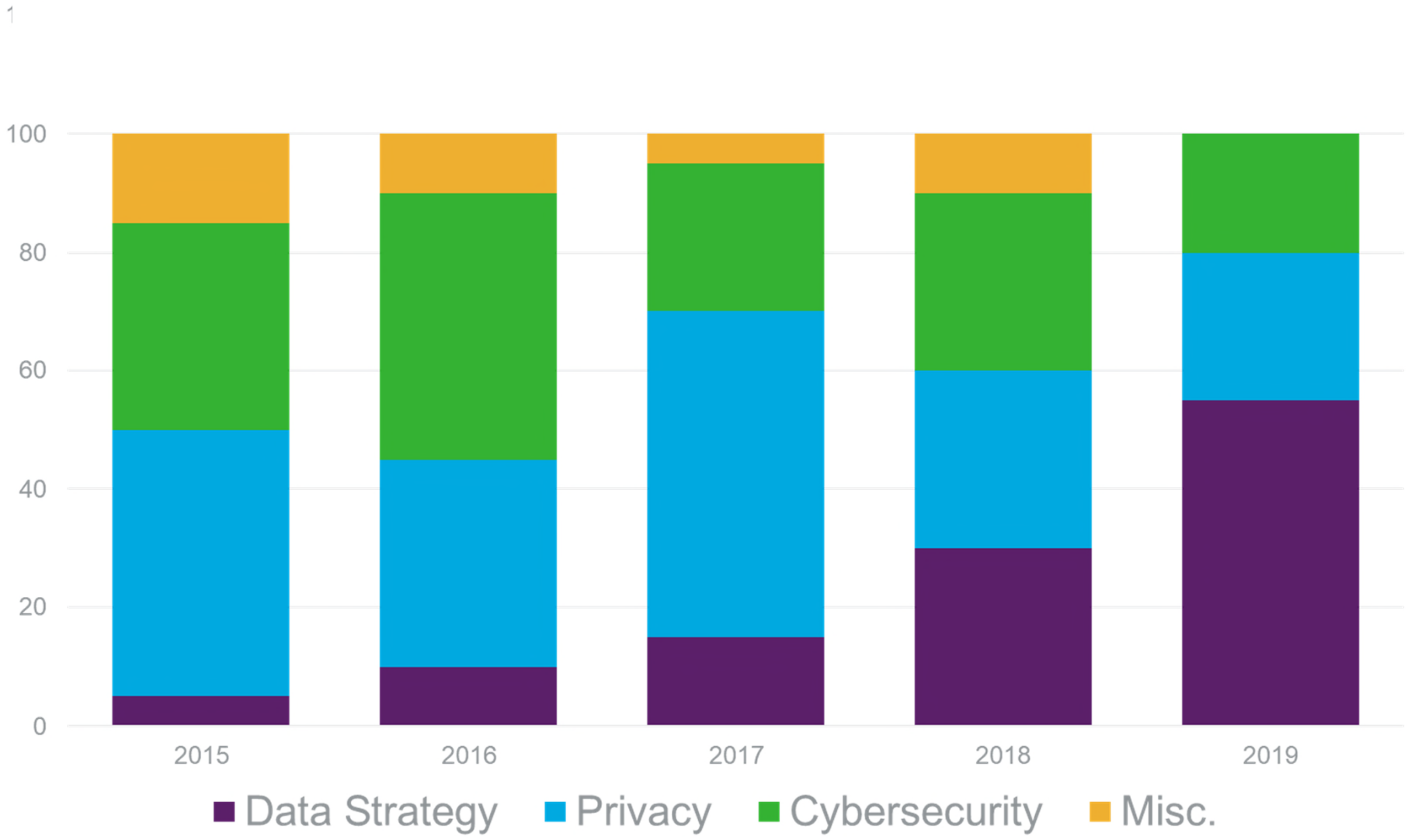
- Robust data governance, leadership, and stewardship
- Increased availability and interoperability of data
- Increased data analytics capacity
- Integration of data and analysis into decision-making processes
- Robust IT infrastructure
- Employee training and skills

New State:

- Improved services and products; new sectors
- Greater organizational value from data
- Protection of personal information and privacy (and security) by design
- Reduced cyber and litigation risk
- Sound governance of data, which is treated as a valuable strategic asset
- Better reporting on results
- Increased and targeted intra- and inter-organizational collaboration

TO

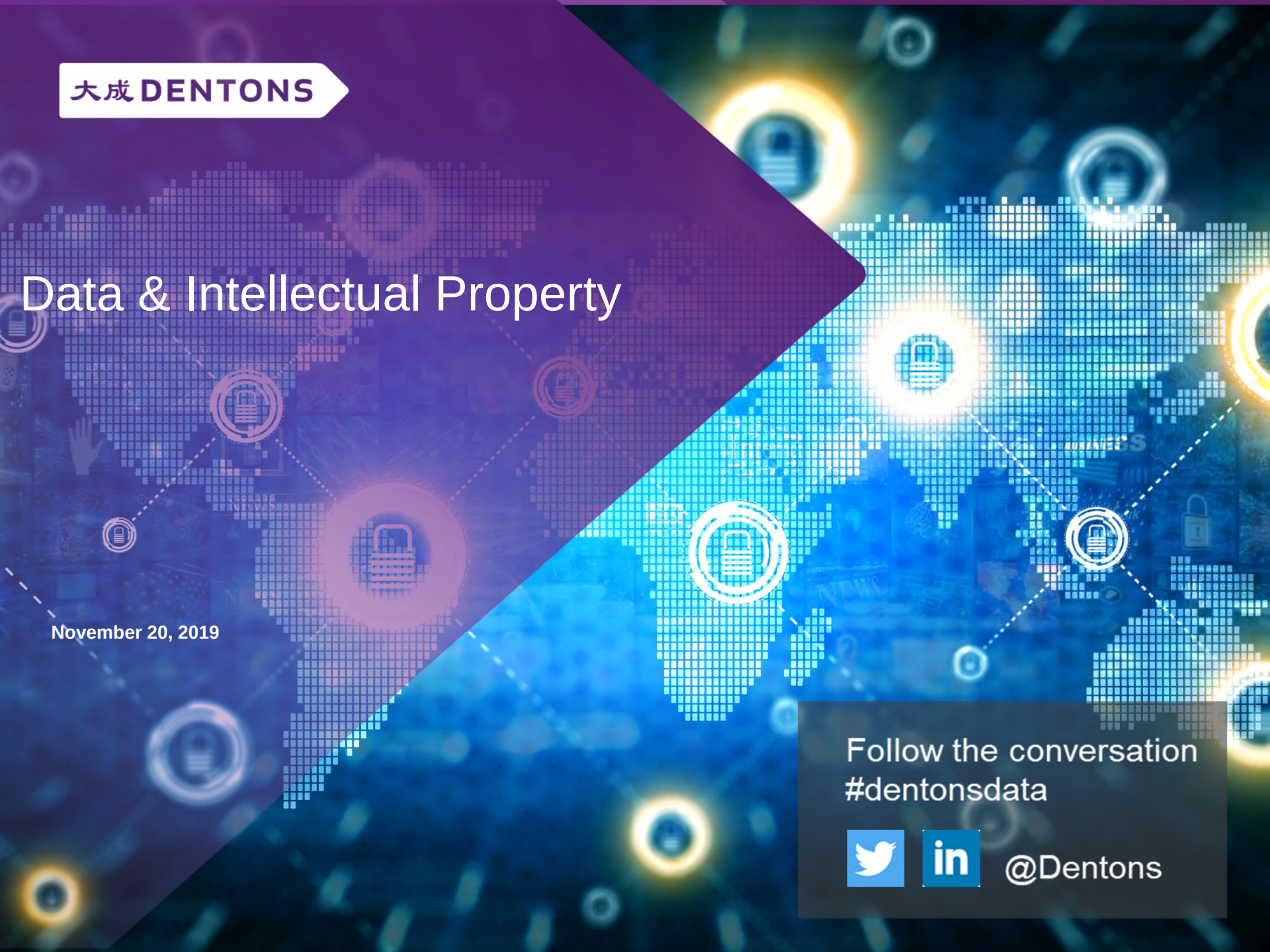
Change in work types



大成 DENTONS

Data & Intellectual Property

November 20, 2019



Data & Intellectual Property

Presented by: Panagiota Dafniotis,
Partner & National Lead, Intellectual Property
T +1 514 878 8878
panagiota.dafniotis@dentons.com

Intellectual Property and Data

- Intellectual property rights are an important part of a data management strategy
  - data collected, assembled or generated and
  - data system in which the data is stored
- What is protected by intellectual property rights?
- To navigate you should understand of the kinds of intellectual property rights that exist

Intellectual Property and data protection

Trademarks	Copyrights
Protects your brand identity Examples: word = *Nike* symbol = *Nike Swoosh*	Protects the expression of an idea, a work of authorship Examples: a song, a play, a book
Patents	**Trade Secrets**
Protects the functionality Examples: Apple iPhone or swipe, Ice Rink Resurfacing Machine	Protects valuable information you want to keep a secret Examples: customer data, Google search algorithm

Contracts

Intellectual Property and Data

- Ownership of Data: not a recognized form of IP rights in Canada
- Not all data is created equal – protection is specific to the form and content of data

= An important way to protect data is by asserting law and contracts governing confidential information and trade secrets

- Protection through other intellectual property rights:
  - Copyright: Some data can be protected by copyright law
  - Patents: Do not protect your data BUT may protect the way in which you manipulate data
- New property right for data?

Intellectual Property Best Practices

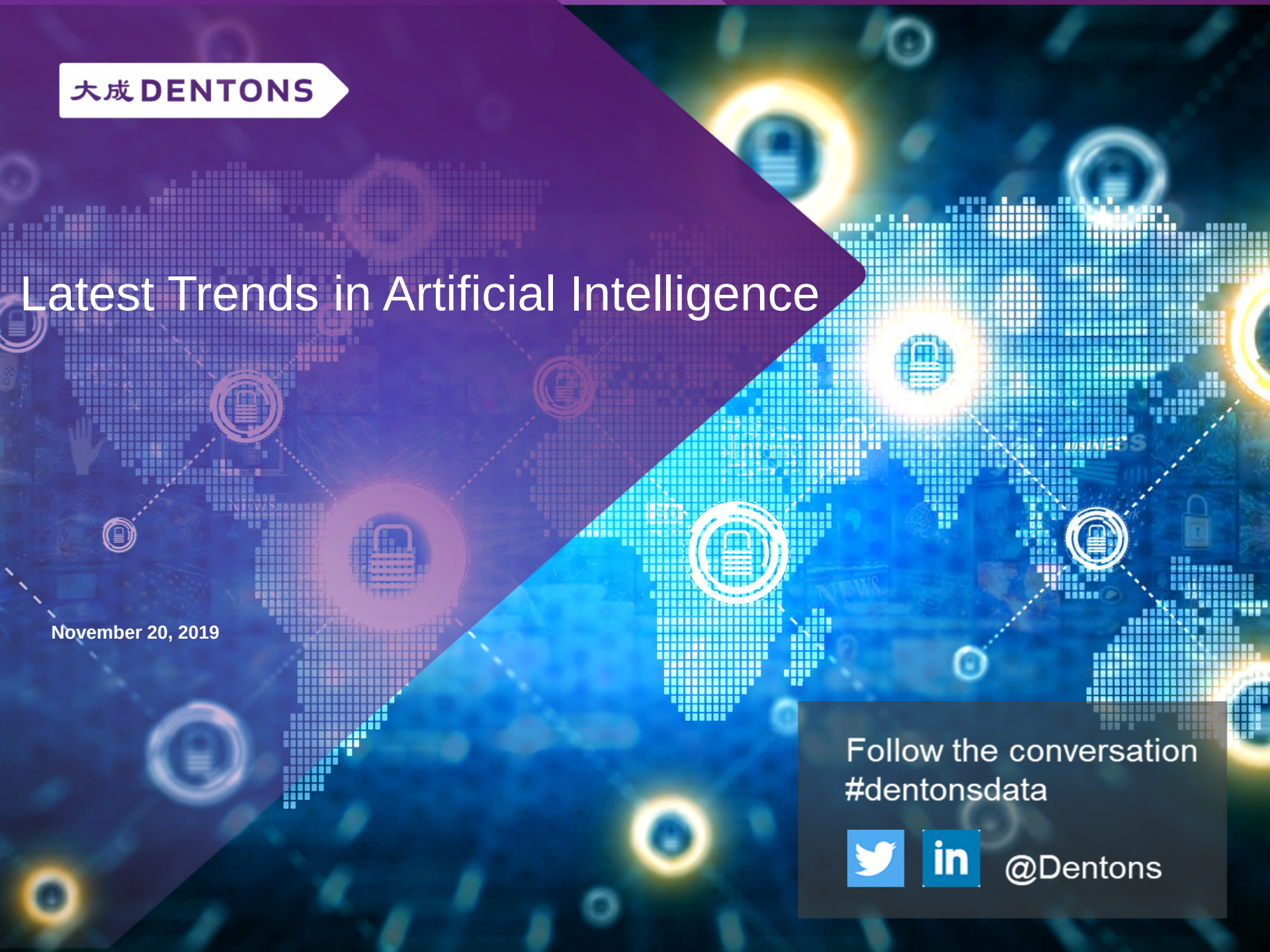
For all areas of IP

- Consider the kind of data in order to consider ownership and how it is protected
- Have measures in place for internal handling and marking of confidential information to treat information as a trade secret
- Define data ownership and usage rights in your company and in your contracts with third parties
- Have robust confidentiality provisions in your contracts to obligate third parties to protect data as a trade secret
- Mark your copyright protected work (website, marketing content etc.) with a © notice
- Routinely consider valuable patent filing opportunities
- Think of ownership, protection and use from all sides

大成 DENTONS

Latest Trends in Artificial Intelligence

November 20, 2019



大成 DENTONS

Latest Trends in Artificial Intelligence

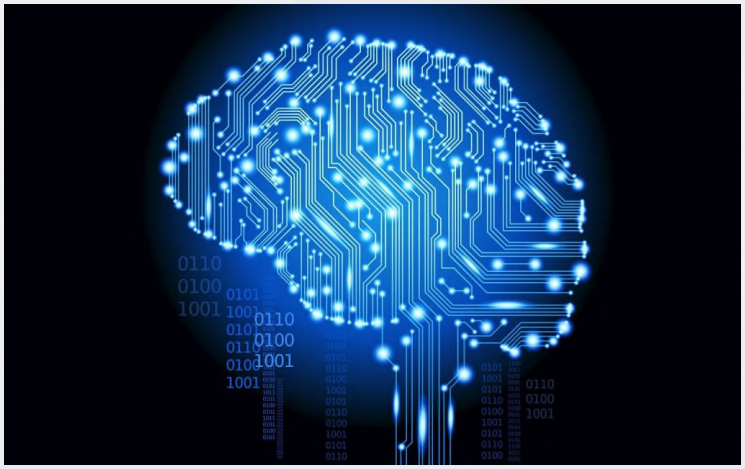
Presented by: Adam Allouba, Partner and Montreal Lead, Transformative Technologies and Data Strategy
T +1 514 878 8871
adam.allouba@dentons.com

Follow the conversation
#dentonsdata

@Dentons

AI Basics: a quick refresher

1. **Traditional AI was programmed with rules**
2. **Modern AI derives rules from observation**
    a. Requires large quantities of data
3. **Goal is to emulate human reasoning**
    a. Provide recommendations for human action
    b. Take independent action



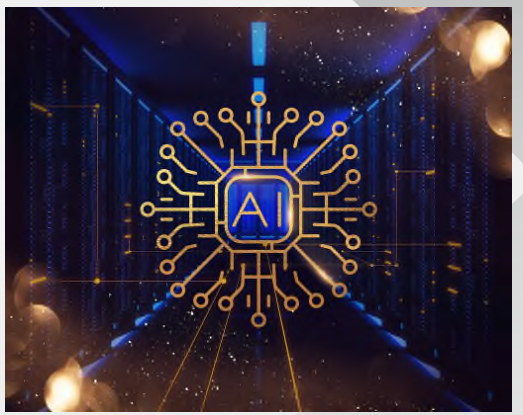
Key Legal Issues in AI

Intellectual Property ✓

Privacy ✓

Civil Liability

Civil Liability in AI



1. **Contractual**
    a. Developer
    b. Data source
    c. Trainer
    d. Manufacturer
    e. Distributor
    f. User
2. **Extra-contractual**
    a. Any third party affected by use of AI

How to Mitigate Civil Liability

1. **Ethical Frameworks**

2. **User Documentation**
   a. Define intended use
   b. Set out technological limitations
   c. Who are intended users
   d. Define how data must be structured

How to Mitigate Civil Liability (cont.)

3. **Contractual Clauses**
   a. Limitation of Liability
   b. Indemnification
   c. Representations & warranties
   d. Allocation of roles & responsibilities

Contractual Clauses

1. **Limitation of Liability**
   a. Link limitation to intended use & compliance with documentation

2. **Indemnification**
   a. Breach of IP rights by AI
   b. Unforeseeable outcomes

Contractual Clauses (cont.)

3. **Representations & warranties**
   a. Consents for use and disclosure of personal information
   b. IP rights in databases with training data
   c. IP rights in output
   d. Fitness for clearly-defined purpose
   e. Level of accuracy

Contractual Clauses (cont.)

4. **Allocation of Roles & Responsibilities**
    a. Source of data
    b. Structuring/analyzing data
    c. Training of algorithms
    d. Interpretation of output

Ethical Frameworks

Why do they Matter?

a. Legal obligations may be unclear
b. Recognized frameworks provide guidance
c. Reflect best practices & public expectations (social acceptability remains key)

Algorithm Watch counts *82* published frameworks

Ethical Frameworks (cont.)

1. European Commission: *Ethics Guidelines for Trustworthy Artificial Intelligence*
2. Université de Montréal: *Montreal Declaration for a Responsible Development of Artificial Intelligence*
3. Government of Canada: *Directive on Automated Decision-Making*

Ethical Frameworks: Common Themes

1. **Individuals must be advised when dealing with AI**
   a. Interaction with chatbots
   b. Rosenbach v. Six Flags (Illinois)

Ethical Frameworks: Common Themes

1. **Highly sensitive decisions must not be fully automated**
    a. Articles 13 & 22 *General Data Protection Regulation* (GDPR)

Ethical Frameworks: Common Themes

1. **Decisions based on AI must be explainable (in proportion to their importance)**
   a. Articles 13 & 15 GDPR

Ethical Frameworks: Common Themes

1. **AI must be minimally intrusive**
   a. AI-assisted surveillance
   b. Consent to collection & use of information?

Ethical Frameworks: Common Themes

1. **AI must not reproduce or exacerbate bias**
   a. Alzheimer's test calibrated for Torontonians
   b. HR system that set aside women's CVs

Ethical Frameworks: Common Themes

1. **AI must not homogenize society**
   a. AI may inadvertently discriminate against "out of the box" situations (ex: loan applications)

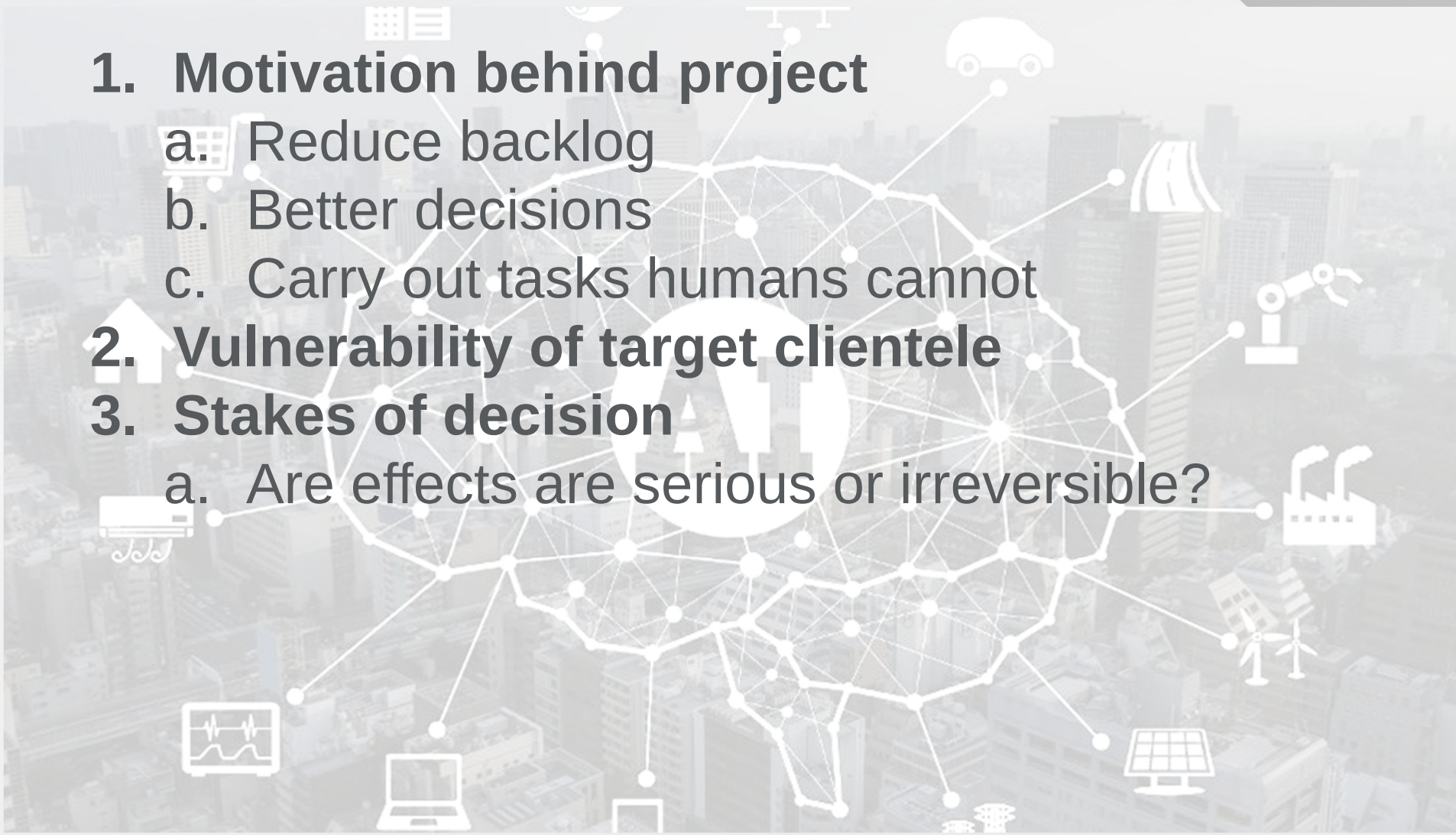
Ethical Frameworks: Common Themes

1. **Cost/benefit analysis is required when principles conflict**
   a. At design stage of project
   b. Monitor output and consequences
   c. Ongoing process

Algorithmic Impact Assessment (AIA)

1. **Tool to study risks involved with use of AI**
2. **AIA published by Government of Canada**
   a. For use by government departments
   b. Useful to business to evaluate their AI projects

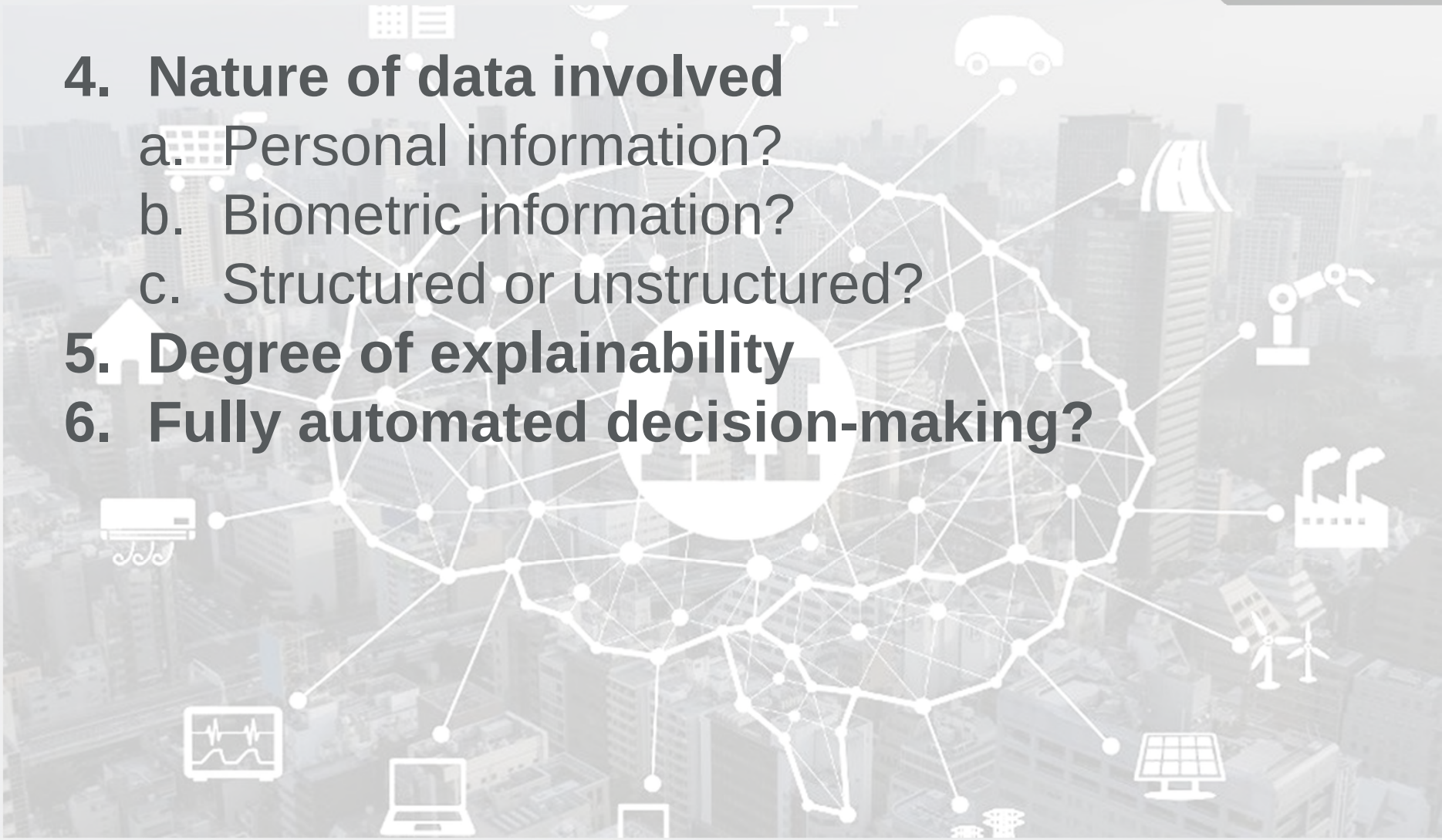
Algorithmic Impact Assessment (cont.)



1. **Motivation behind project**
   a. Reduce backlog
   b. Better decisions
   c. Carry out tasks humans cannot
2. **Vulnerability of target clientele**
3. **Stakes of decision**
   a. Are effects are serious or irreversible?

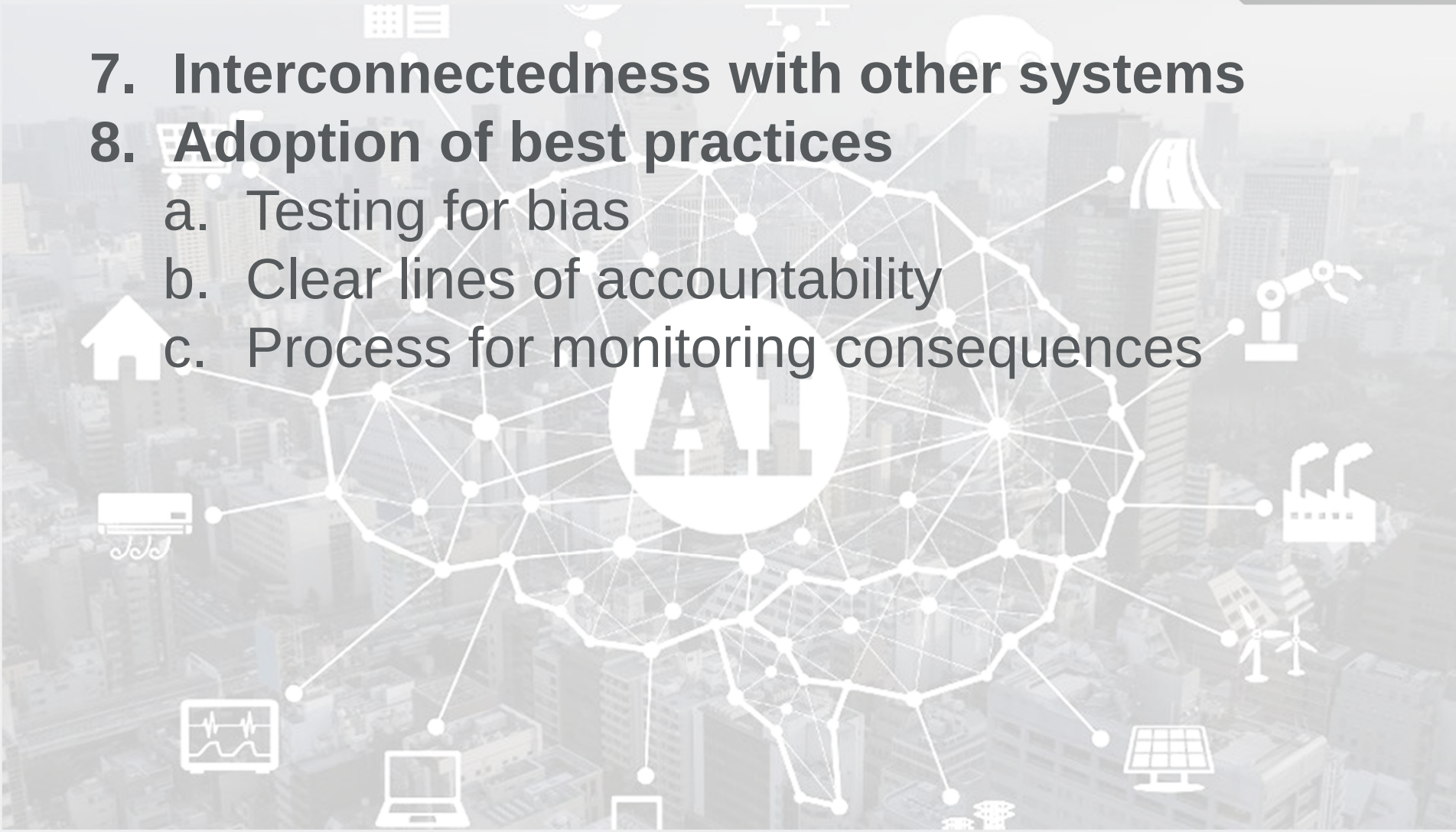
Algorithmic Impact Assessment (cont.)

4. **Nature of data involved**
   a. Personal information?
   b. Biometric information?
   c. Structured or unstructured?
5. **Degree of explainability**
6. **Fully automated decision-making?**



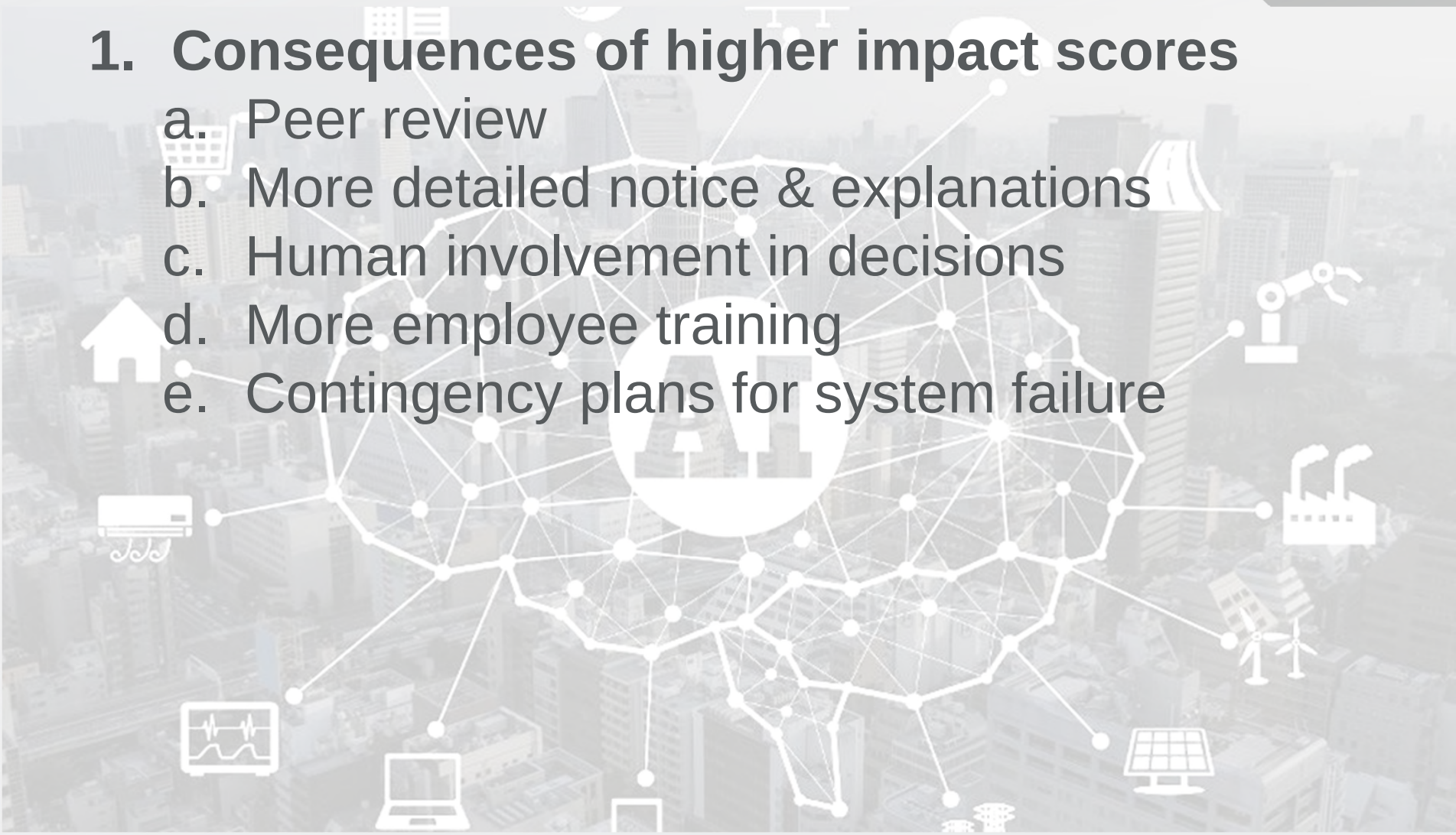
Algorithmic Impact Assessment (cont.)

7. **Interconnectedness with other systems**
8. **Adoption of best practices**
   a. Testing for bias
   b. Clear lines of accountability
   c. Process for monitoring consequences



Algorithmic Impact Assessment (cont.)

1. **Consequences of higher impact scores**
   a. Peer review
   b. More detailed notice & explanations
   c. Human involvement in decisions
   d. More employee training
   e. Contingency plans for system failure



Thank you

Dentons Canada LLP
1 Place Ville-Marie
39th Floor
Montréal, Québec H3W 4M7
Canada

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.
www.dentons.com