大成 DENTONS

Regulating Artificial Intelligence (AI) in Canada and the US – Recent developments

WEBINAR SERIES
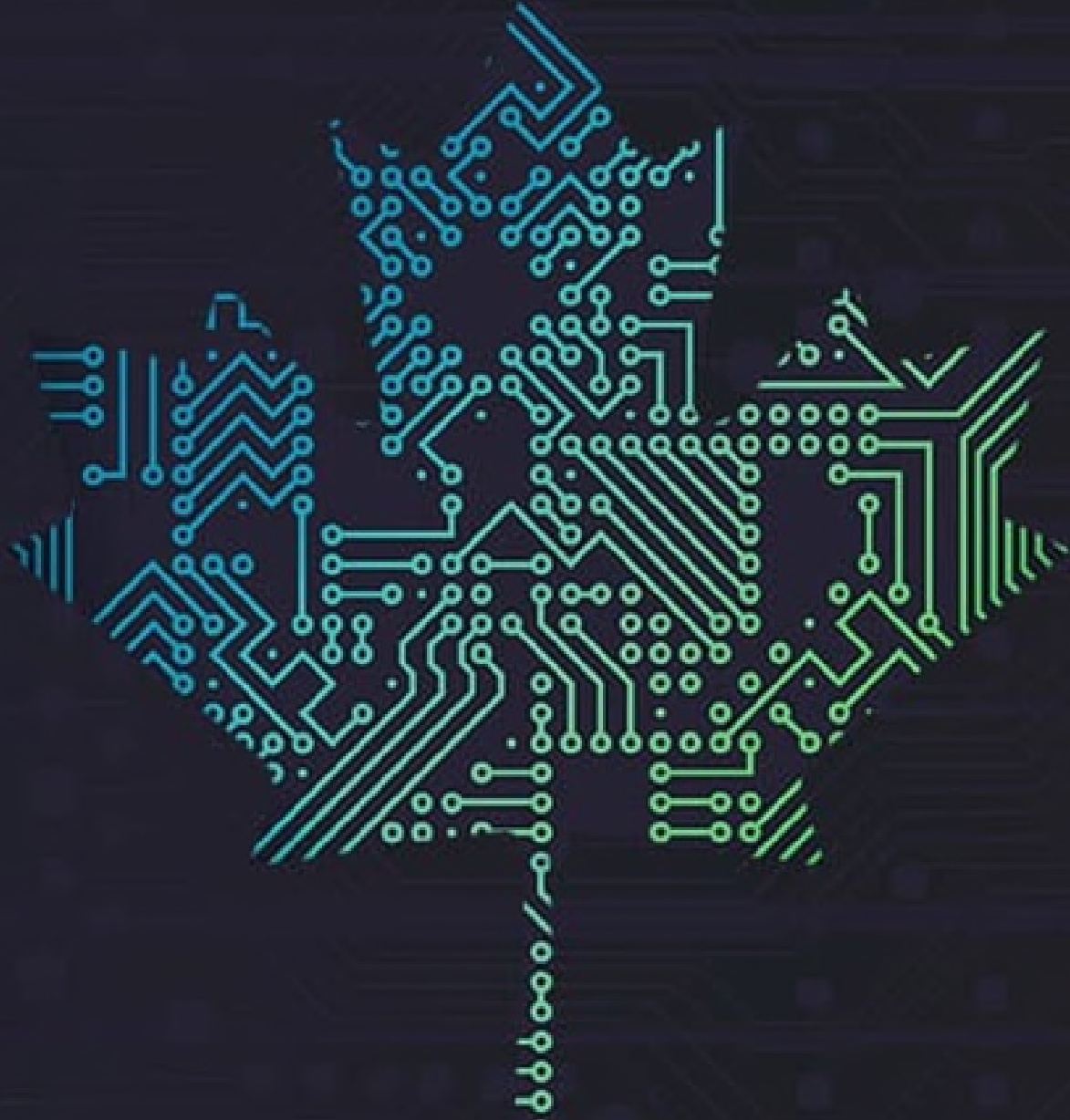DO YOU KNOW WHAT
YOUR NEIGHBOR IS DOING?

Your speakers

Peter Stockburger
Office Managing Partner, San Diego
+1 619 595 8018
peter.stockburger@dentons.com

Kirsten Thompson
Partner, Toronto
+1 416 863 4362
kirsten.thompson@dentons.com

AI regulation in Canada

Kirsten Thompson

AI in Canada

Fragmented…but developing quickly

- **Public sector developments**
  - **2019** – Directive on Automated Decision-Making (with compliance no later than April 1, 2020)
    - imposes requirements, primarily related to risk management, on the federal government's use of automated decision systems.
- **Private sector developments**
  - **2021** – Bill 64 in Quebec addresses "automated processing" (in effect September 2023)
  - **2022** – Bill C-27 introduced, rewrites federal privacy law and introduces new federal AI law for private sector

Artificial Intelligence and Data Act (AIDA)

Bill C-27

- **Key themes in AIDA:**
  - Concerned about bias, discrimination and harms to natural persons
  - Distinction between ordinary AI and high impact AI
  - Limited to activities carried out in the course of international or interprovincial trade and commerce
  - Really just a framework – content will be in anticipated regulations
- **Areas of regulation:**
  - Governance
  - Transparency
  - Ministerial orders
  - Penalties

AIDA - Definitions

Bill C-27

- **Artificial intelligence system** means "a technological system that, *autonomously or partly autonomously*, *processes data related to human activities* through the use of a genetic algorithm, a neural network, machine learning or another technique in order *to generate content or make decisions, recommendations or predictions*."

- **Biased output** means "*content that is generated, or a decision, recommendation or prediction that is made*, by an artificial intelligence system and that *adversely differentiates, directly or indirectly and without justification*, in relation to an individual *on one or more of the prohibited grounds of discrimination* set out in section 3 of the *Canadian Human Rights Act*, or on a combination of such prohibited grounds." (excludes use of same to alleviate disadvantage)

- **Harm** means

   (a) physical *or psychological harm* to an individual;

   (b) damage to an individual's property; or

   (c) economic loss to an individual.

AIDA - Definitions

Bill C-27

- **<u>Person who carries out any regulated activity</u>** means "(a) *processing or making available for use* any *data relating to human activities* for the purpose of designing, developing or using an artificial intelligence system; (b) designing, developing or making available for use an artificial intelligence system *or managing its operations*."

- **<u>Person responsible for an AI system</u>** means "a person is responsible for an artificial intelligence system if […] they *design, develop or make available for use* the artificial intelligence system *or manage its operation*."

- **<u>High-impact system</u>** ("**HIS**") means an AI system that meets the criteria for a high-impact system set out in regulations.

EU uses "high risk" systems, which include AI technology used in:

- **critical infrastructure that could put the life and health of citizens at risk** (e.g. transport), ;
- **educational or vocational training, that may determine access to education and professional course of someone's life** (e.g. exam scoring);
- **safety components of products** (e.g. AI application in robot-assisted surgery);
- **employment, management of workers and access to self-employment** (e.g. CV-sorting software for recruitment procedures);
- **essential private and public services** (e.g. credit scoring denying citizens opportunity to obtain a loan);
- **law enforcement that may interfere with people's fundamental rights** (e.g. evaluation of the reliability of evidence);
- **migration, asylum and border control management** (e.g. verification of authenticity of travel documents);
- **administration of justice and democratic processes** (e.g. applying the law to a concrete set of facts).

AIDA - Governance

Bill C-27

- **System assessment**: Person *who is responsible for an AI system* must assess whether it is a HIS according to regulation to be provided.

- **Risk management**: Person *who is responsible for a HIS* must establish measures to identify, assess and mitigate the risks of harm or biased output that could result from the use of the system.

- **Monitoring**: Person *who is responsible for a HIS* must establish measures to monitor compliance with the risk management measures, as well as their effectiveness.

- **Data anonymization**: Person *carrying out a regulated activity* and who processes or makes available for use anonymized data in the course of that activity must establish measures with respect to the manner in which the data is anonymized and the use or management of anonymized data.

- **Record keeping**: Person *carrying out a regulated activity* must keep records describing in general terms the measures they establish for risk management, monitoring, and data anonymization as well as the reasons supporting their assessment of whether a system is a "high-impact system."

AIDA - Transparency
Bill C-27

- **Publication requirements**: Person who manages or makes available for use a HIS must publish on a publicly available website a plain-language description of the system that includes an explanation of:
  - how the system is intended to be used;
  - the types of content that it is intended to generate and the decisions, recommendations or predictions that it is intended to make;
  - the mitigation measures set up as part of the risk management measures requirement; and
  - any other information prescribed by regulation.
- **Notification in event of harm**: Person responsible for a HIS must notify the Minister as soon as possible if the use of the system results in, *or is likely to result in*, material harm.

AIDA – Ministerial Orders

Bill C-27

- **<u>Record collection:</u>** The Minister may order that anyone provide them with their records related to system assessment, risk management, monitoring measures, and data anonymization.

- **<u>Auditing</u>**: If the Minister has reasonable grounds to believe that anyone has contravened any of the aforementioned requirements or an order made under its record collection powers, the Minister may require an audit to be conducted. The Minister may then order that person to implement any measures to address issues revealed by the audit report. *Cost is borne by audited entity*.

- **<u>Cessation</u>**: The Minister may order that any person who is responsible for a HIS cease using it or making it available for use if there are reasonable grounds to believe that its use gives rise to a serious risk of imminent harm.

- **<u>Publication</u>**: The Minister may order that anyone responsible for a HIS, or who engages in regulated activity, publish information related to any of the requirements listed above on a publicly available website (excluding confidential business information). The Minister may also publish information that relates to a party's use of an AI system if there are reasonable grounds to believe that such the use gives rise to a serious risk of imminent harm and the publication of the information is essential to prevent the harm.

- **<u>Disclosure:</u>** The Minister may disclose information they obtain to other public bodies such as the Privacy Commissioner, the CRTC, or the Human Rights Commission, for the purpose of enforcing other laws.

AIDA - Penalties

Bill C-27

- **Administrative monetary penalties ("AMPs")**: The federal government can establish an AMPs scheme for violations of the AIDA and regulations made under it.

- **Fines for breaching obligations**: It is an offense for anyone to contravene their governance or transparency requirements. Breaching those obligations can result in a fine of up to the **greater of $10M and 3% of gross global revenues** (for summary offense, fine is up to the greater of $5M and 2% of gross global revenues). For individuals, the court may issue a discretionary fine or, in the case of a summary conviction, a fine not more than $50,000. **Due diligence defence available.**

- **Criminal offenses related to AI systems**:

    (i) knowingly using personal information obtained through the commission of an offence under a federal or provincial law to make or use an AI system;

    (ii) knowingly or recklessly designing or using an AI system that is likely to cause harm and the use of the system causes such harm; and

    (iii) causing substantial economic loss to an individual by making an AI system available for use with the intent to defraud the public.

    - Fines of up to **the greater of $25M and 5% of gross global revenues** (for summary offense, fine is up to the greater of $20M and 4% of gross global revenues. For individuals, jail time and fines are possible.

AI issues in the US

Peter Stockburger

AI issues in the US

Workplace risk

- **State developments**
  - **2019** – Illinois passed the Artificial Intelligence Video Interview Act.
  - **2020** – Maryland passed law restricting use of facial recognition services during preemployment interviews.
  - **2023** – NYC restricts use of "automated employment decision tools" and requirement for bias audit.
  - **DC** – Stop Discrimination and Algorithms Act.
  - **California** – DFEH proposed regulations.
- **2022 EEOC & DOJ guidance**. Focus on ADA compliance and mitigating bias.
- **Key takeaway**. Before employing any tools for employment decision making, interrogate underlying components and capabilities.

AI issues in the US

Public accommodation risk

- **Federal ADA requirements**. Prohibits "discrimination" in the offering of "public accommodations." What is a "public accommodation"? What is "discrimination"?

- **State counterparts**. California and other states likewise prohibit discrimination in the offering of services to the public (e.g., ladies night cases).

- **Key takeaway**. Audit algorithms to examine whether they "significantly" rely on protected characteristics to make a product or service offering. Remove characteristic to see if result would be different.

AI issues in the US

Data privacy risk

- **California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)**. The CCPA does not expressly regulate AI, but implicates. CPRA calls out potential area for rulemaking.

- **Virginia, Colorado, Utah, and Connecticut**. Address AI in some respects.

- **State bills pending**. Multiple states considering data privacy changes.

- **Federal data privacy law discussions**. Federal bills are gaining steam, some versions address AI.

- **Key takeaway**. When addressing data privacy compliance, examine the use of algorithms and how personal information is utilized, minimized, and stored.

AI issues in the US

Regulatory outlook

- **States are leading**. 17 bills introduced in 2021. Some focused on insurance offerings, mitigating bias, mitigating security risks, and ensuring government accountability for use in public agencies. State privacy laws in California, Virginia, Colorado, Utah, and Connecticut.

- **Federal bills are cooking**. Federal Algorithmic Justice and Online Platform Transparency bill, which proposes whole-of-government approach to mitigating bias.

- **Federal agency developments**. EEOC guidance, DOJ guidance, additional guidance?

- **NIST framework**. Public workshops in spring. Reviewing use of AI across organizations.

- **Key takeaway**. Watch this space…

Thank you

Peter Stockburger
Office Managing Partner, San Diego
+1 619 595 8018
peter.stockburger@dentons.com

Kirsten Thompson
Partner, Toronto
+1 416 863 4362
kirsten.thompson@dentons.com

大成 **DENTONS**

Did you know Dentons produces podcasts on a variety of topics?

Agribusiness	Mining
Arbitration	Smart Cities
Business Insights	Tax
Employment and Labour Law	Transformative Technologies and Data
Entertainment and Media Law	Women in Leadership and Entrepreneurship
Intellectual Property	
Life Sciences and Health Care	

Visit our Podcast page and subscribe: https://www.dentons.com/en/insights/podcasts

Grow | Protect | Operate | Finance

大成 **DENTONS**

We also have blogs in various areas.

Commercial Litigation	Occupational Health and Safety
Commercial Real Estate	Privacy and Cybersecurity
Drone Regulation	Regulatory
Employment and Labour	Tax Litigation
Entertainment and Media	Technology, New Media and IP Litigation
Insurance	Transformative Technologies and Data
Mining	Venture Technology

Visit our Blogs and Resources page: https://www.dentons.com/en/insights/blogs-and-resources

Grow | Protect | Operate | Finance