Artificial Intelligence 2023
Definitive global law guides offering comparative analysis from top-ranked lawyers

Canada: Law & Practice
Theo Ling, Jim Holloway, Michael Rubinger and Conrad Flaczyk
Baker McKenzie LLP

Canada: Trends & Developments
Theo Ling, Jim Holloway, Jacqueline Chan and Matthew Cook
Baker McKenzie LLP
Contents

1. General Legal Framework p.16
   1.1 General Legal Background Framework p.16

2. Industry Use of AI and Machine Learning p.16
   2.1 Industry Use p.16

3. Legislation and Directives p.17
   3.1 Jurisdictional Law p.17
   3.2 EU Law p.17
   3.3 US State Law p.17

4. Judicial Decisions p.17
   4.1 Judicial Decisions p.17
   4.2 Technology Definitions p.18

5. AI Regulatory Regimes p.18
   5.1 Key Regulatory Agencies p.18
   5.2 Technology Definitions p.19
   5.3 Regulatory Objectives p.19
   5.4 Enforcement Actions p.20

6. Proposed Legislation and Regulations p.20
   6.1 Proposed Legislation and Regulations p.20

7. Standard-Setting Bodies p.21
   7.1 National Standard-Setting Bodies p.21
   7.2 International Standard-Setting Bodies p.21

8. Government Use of AI p.21
   8.1 Government Use of AI p.21
   8.2 Judicial Decisions p.22
   8.3 National Security p.22

9. Generative AI p.23
   9.1 Generative AI p.23

10. AI in the Practice of Law p.23
    10.1 Uses of AI in the Practice of Law p.23
    10.2 Ethical Considerations p.24

11. Theories of Liability p.25
    11.1 Theories of Liability p.25
    11.2 Regulatory p.26

    12.1 Algorithmic Bias p.26
    12.2 Data Protection and Privacy p.26
    12.3 Facial Recognition and Biometrics p.27
    12.4 Automated Decision-Making p.27
    12.5 Transparency p.28
    12.6 Anti-competitive Conduct p.28

13. Sustainability and Climate Change p.28
    13.1 Sustainability and Climate Change p.28

14. AI in Employment p.29
    14.1 Hiring Practices and Termination of Employment Practices p.29
    14.2 Employee Evaluation and Monitoring p.29

15. AI in Industry Sectors p.29
    15.1 Digital Platform Companies p.29
    15.2 Financial Services p.30
    15.3 Healthcare p.31

16. Intellectual Property p.31
    16.1 Applicability of Patent and Copyright Law p.31
    16.2 Applicability of Trade Secret and Similar Protection p.32
    16.3 AI-Generated Works of Art and Works of Authorship p.32
    16.4 OpenAI p.33

17. Issues for In-House Attorneys p.34
    17.1 AI Issues for In-House Attorneys p.34

18. Advising Corporate Boards of Directors p.34
    18.1 Advising Directors p.34
Baker McKenzie LLP is the premier global law firm in North America. Recently recognised as one of the top 10 most innovative law firms in North America by the Financial Times, our 850 lawyers in the US and Canada provide strategic advice to domestic and multinational companies as they grow and manage issues close to home or across the globe. Over the last three years, we have handled more cross-border deals than any other firm, and our litigation, employment, IP, tax, international trade and other practices have been repeatedly named among the best in North America. For the past 50 years, our Canada office has been advising clients on federal, provincial and local laws with an unparalleled international perspective. Through our diverse information technology and communications practice, we guide our clients through the complex and emerging areas of artificial intelligence and machine learning (AI/ML) technology, financial technology, health technology, digital transformation, and more.

Authors

**Theo Ling** heads Baker McKenzie’s Canadian information technology/communications practice and is a member of the firm’s global IP/technology practice group, and technology, media and telecoms and financial institutions industry groups. Theo helps market-leading businesses develop and implement effective global strategies to support multijurisdictional commercial activities and manage complex cross-border compliance risks. The focus of Theo’s international commercial/regulatory practice is on data and technology-related issues, which include digital transformation and data governance projects that involve data privacy, data security, electronic payments, data monetisation, records retention, media/format, electronic signatures, cross-border data transfers, digitisation, fintech, and AI and machine learning considerations. Theo also advises clients on internet-related services that involve smart/connected devices, which are subject to regulation under telecommunications and broadcasting laws.

**Jim Holloway** is a partner at Baker McKenzie and a recognised and ranked leader in the areas of intellectual property and technology, a skilled and experienced trial and appellate advocate, and a trusted strategic advisor. Jim’s practice is focused on intellectual property law and technology, including trademark, copyright, patent and trade secret disputes. Jim also provides clients with strategic, pragmatic and commercial advice on the development, protection, monetisation and enforcement of their intellectual property assets, and how to avoid/manage risk. He also handles anti-counterfeiting litigation, diversion and grey market matters, unfair competition claims, marketing and advertising complaints, licensing and distributorship disputes, breach of confidentiality matters, and product liability claims involving technology.
Michael Rubinger is an associate in Baker McKenzie’s Intellectual Property Technology group. He regularly advises clients in connection with IP transactions and/or litigation, and assists clients with managing and enforcing their IP portfolios. Mike was recently recognised as a 2022 Rising Star in IPStars by Managing IP. Michael assists on a broad range of IPTech work, including global patent portfolio management, IP licensing, litigation and transactional matters. He also advises and presents on trademark and patent regulations. His clients include companies in the gaming, healthcare, transportation, engineering, and food industries.

Conrad Flaczyk is a technology and privacy lawyer in Baker McKenzie’s Canadian information technology/communications practice. He works closely with engineers and in-house legal teams to commercialise, protect, and ensure that the most cutting-edge technologies are rolled out lawfully and efficiently. Conrad’s practice focuses on cross-border privacy and cybersecurity matters, including cross-border data transfers, records retention, investigations, and complex cybersecurity breaches. He also advises on compliance issues relating to the roll out of new technologies and consumer offerings, including AI systems, virtual currencies, payment systems, video games, digital hardware products, mobile apps and other software in Canada.
1. General Legal Framework

1.1 General Legal Background Framework
Currently, there is no AI specific law in Canada. However, there are Canadian federal and provincial legal frameworks that apply to the different uses of AI. This includes laws related to consumer protection, criminal conduct, human rights, privacy and tort:

• Consumer protection laws at the provincial and territorial levels govern the interactions between businesses and their consumers to ensure fair treatment. These laws regulate misleading terms and conditions, misrepresentation of goods or services, and undue pressure.
• Product liability can also be imposed on the designers, manufacturers and retailers of AI products through contractual liability, sale of goods laws, consumer protection laws and tort law.
• The federal Criminal Code includes prohibitions against the destruction or alteration of computer data and the direct or indirect fraudulent procurement or use of a computer system or computer password.
• Federal and provincial human rights commissions can provide redress in cases of discrimination, including discrimination that occurs with automated decision-making systems.
• Tort law applies where an individual is harmed because of an AI system operated by another entity with whom there is no contractual or commercial relationship (ie, intentional tort actions, negligence and strict liability).
• In terms of privacy compliance, the federal Personal Information Protection and Electronic Documents Act provides the legal framework around how private sector entities collect, use and disclose personal information. Provinces with substantially similar private sector legislation (Alberta, British Columbia, and Quebec) provide similar rules. Effective 22 September 2023, private sector entities in Quebec are required to comply with new accountability and transparency requirements under the amended private-sector privacy legislation around the use of automated decision-making systems which rely on personal information (ie, notification, correction, complaints, etc).

2. Industry Use of AI and Machine Learning

2.1 Industry Use
In Canada, the key industry applications of AI and machine learning are found in the financial services, healthcare, automotive, and advertising and marketing sectors:

• The financial services sector is seeing a rise of new AI products and services in the areas of online lending, robo-advisers providing investment dealing and advice, insider trading and fraud detection, and market and trading predictions.
• The use of AI in the healthcare sector ranges from patient care solutions, administrative processes, payment processes (payer and pharma companies), and diagnosis and treatment applications. In particular for medical devices, AI capabilities include enhanced imaging systems, smart robots, wearable technology, AI-based data analysis, simulation platforms and more.
• There is significant progress in the use of AI in the automotive sector for autonomous and self-driving vehicles.
AI is being leveraged to help advertisers better promote products/services as well as profile and target consumers.

3. Legislation and Directives

3.1 Jurisdictional Law
Currently, there is no AI-specific law that is in force in Canada. The proposed federal private-sector privacy law, Bill C-27 (Digital Charter Implementation Act, 2022), introduces a new AI-specific legislation, the Artificial Intelligence and Data Act (AIDA), which aims to ensure the responsible development of AI in Canada. AIDA (if passed) is anticipated to enter into force no earlier than 2025.

Generally, AI systems involve the collection, use and disclosure of personal information. Businesses involved in the development, deployment and use of AI should ensure compliance with Canadian federal and provincial privacy laws, consumer protection laws, human rights laws, criminal law, and industry-specific laws (where applicable), including:

- Privacy Laws (Private-Sector): Personal Information Protection and Electronic Documents Act (Federal); Personal Information Protection Act (Alberta); Personal Information Protection Act (British Columbia); and the Act respecting the protection of personal information in the private sector (Quebec);
- Canada Consumer Product Safety Act;
- Food and Drugs Act;
- Motor Vehicle Safety Act;
- Bank Act;
- Criminal Code; and
- Canadian Human Rights Act (federal) and provincial human rights laws.

3.2 EU Law
3.2.1 Jurisdictional Commonalities
The matter is not applicable in this jurisdiction.

3.2.2 Jurisdictional Conflicts
The matter is not applicable in this jurisdiction.

3.3 US State Law
The matter is not applicable in this jurisdiction.

4. Judicial Decisions

4.1 Judicial Decisions
To date, there have only been a few judicial decisions in Canada that have substantively addressed AI issues and only one decision related to generative AI and intellectual property rights. There have yet to be any reported decisions from the Canadian copyright board or patent appeal board regarding the issue of granting copyright or patents for AI-generated works, though more are expected in the future given the onset of filings related to AI-generated works.

Stross v Trend Hunter, 2020 FC 201, is the sole decision dealing with generative AI and intellectual property rights. In this decision, the Federal Court of Canada found that the defendant could not rely on the fair dealing defence for its use of a photo generated by AI that was found to have infringed the Plaintiff’s copyright. The Plaintiff was a professional photographer who photographed housing projects in the US. The defendants reproduced six of the plaintiff’s photographs on its website in an article, which was created using AI and personnel to process data generated by its website, which was then used to prepare consumer trend reports for clients. The Court found the defendants liable for copyright infringement because the defendant’s
The use of photographs did not constitute fair dealing. The Court did find that the defendants’ use of AI satisfied the first part of the fair dealing test because it met the definition of “research” under s. 29 of the Copyright Act as the use was described as a computerised form of market research that measured consumer interaction and preferences for the purposes of generating data for clients. However, part two of the fair dealing test was not satisfied because the defendants’ ultimate goal was commercial in nature, for the benefit of the defendant and its clients, with no benefit to the plaintiff and no broader public interest purpose.

In Haghshenas v Canadas (Citizenship and Immigration), 2023 FC 464, the Federal Court of Canada dismissed an applicant’s request for judicial review of a deportation decision by the Immigration Officer. The Court rejected the applicant’s argument that the officer’s decision was not procedurally fair because it was reached through the assistance of artificial intelligence. The Court found that the use of AI was not relevant to the duty of procedural fairness because an officer was involved in making the decision in question, and because judicial review addresses the procedural fairness and or reasonableness of a decision.

In James v Amazon.com.ca, Inc., 2023 FC 166, the Federal Court found that it was not within the Court’s jurisdiction to rule that the defendant’s AI-based and automated decision-making (ADM) data request process did not comply with the Personal Information Protection and Electronic Documents Act (PIPEDA). In this case, the defendant had used an automated decision-making process to deny the applicant access to personal information, which the applicant sought to argue was a violation of PIPEDA. The Court found that the use of this AI technology fell outside the scope of section 14, the matter was not raised in the complaint, was not addressed by the Privacy Commissioner and there was no basis in the record to entertain an argument around AI as an explanation for why access was denied.

4.2 Technology Definitions

The definition of AI has not been directly addressed by the Canadian courts. However, the courts have commented on the types of AI technology that exist. For instance, in Haghshenas v Canadas (Citizenship and Immigration), 2023 FC 464, the Federal Court described AI as a form of machine learning. In Drummond v The Cadillac Fairview Corp. Ltd., 2018 ONSC 5350, the Ontario Superior Court commented on the use of AI in the context of computer-assisted legal research, noting that “computer-assisted legal research is a necessity for the contemporary practice of law and computer assisted legal research is here to stay with further advances in artificial intelligence to be anticipated and to be encouraged.” (para 10)

5. AI Regulatory Regimes

5.1 Key Regulatory Agencies

In Canada, there is no overarching AI-specific law. For this reason, various government departments and regulatory agencies bear the responsibility for overseeing and administering laws specific to the different uses of AI as well as developing AI-specific guidance.

In 2019, the federal government appointed an Advisory Council on AI, which focuses on examining how to advance AI in Canada in an open, transparent, and human-rights centric manner. In particular, the Advisory Council in AI has a
working group on extracting commercial value from Canadian-owned AI and data analytics.

The Office of the Privacy Commissioner of Canada investigates complaints, conducts audits and pursues court action under the federal public sector and private sector privacy laws, including violations relating to the collection, use and transfer of personal information in AI systems. The provincial privacy commissioners in Alberta, British Columbia, Quebec, and other provinces with privacy laws also play a similar investigation and enforcement role with regards to the use of personal information in AI systems within the province. Further to this, if the proposed AIDA passes, the Minister of Innovation, Science, and Industry (“Minister”) will become responsible for the administration and enforcement of all non-prosecutable offences under AIDA. There would also be a new statutory role for an AI and Data Commissioner, who would support the Minister in carrying out these responsibilities.

Federal and provincial human rights commissions are also engaged in studies to understand the implications of AI on discrimination and other human rights issues, including data discrimination, racial profiling and failure to ensure community participation and human oversight over AI systems.

Industry-focused regulators are also making progress in Canada to address the impacts of AI within their regulatory authority. Health Canada issued guiding principles for the development of medical devices that use machine learning (a form of AI). The Office of the Superintendent of Financial Institutions is also updating its model risk guidelines to account for the use of AI and digital technologies and conducting AI-specific studies in an effort to establish safeguards around the use of AI in financial services. Canadian federal and provincial securities regulators are increasingly using AI to monitor customer identification and transactions to detect financial crimes, insider trading and market manipulation.

5.2 Technology Definitions
The federal government is increasingly using AI to make and support its administrative decisions in an effort to improve service delivery. In its Directive on Automated Decision-Making, artificial intelligence is defined as “information technology that performs tasks that would ordinarily require biological brainpower to accomplish, such as making sense of spoken language, learning behaviours or solving problems”.

The proposed Artificial Intelligence and Data Act focuses on AI at the systems level, defining an artificial intelligence system as 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”.

5.3 Regulatory Objectives
In Canada, the government agencies and regulators are working towards establishing an AI regulatory framework, regulatory guidance and tools to ensure “responsible AI”. In particular, there is a focus on addressing concerns that the use of automated systems may result in unfair, biased and discriminatory decisions.

In leading up to the introduction of the proposed Artificial and Intelligence Data Act, the Office of the Privacy Commissioner of Canada (OPC) released recommendations that a regulatory framework for AI in Canada must be technology-neutral and include the following elements:
• allow personal information to be used for new purposes (ie, responsible AI innovation and to benefit society);  
• permit these uses within a rights-based framework;  
• establish requirements specific to automated decision-making to ensure transparency, fairness and accuracy;  
• require businesses to show accountability to the regulator upon request (ie, proactive inspections and other enforcement measures); and  
• prohibit reckless and malicious uses of AI that cause serious harm through the creation of new criminal law provisions.

5.4 Enforcement Actions
On 4 April 2023, the Office of the Privacy Commissioner of Canada (OPI) launched an investigation into OpenAI, the company behind artificial intelligence-powered chatbot ChatGPT. The investigation was launched in response to a complaint alleging the collection, use and disclosure of personal information through ChatGPT is without consent.

In February 2021, the federal and provincial privacy commissioners (Alberta, British Columbia, and Quebec) (“Offices”) launched a joint investigation to examine whether Clearview AI, Inc.’s (“Clearview”) collection, use and disclosure of personal information by means of its facial recognition tool complied with federal and provincial privacy laws applicable to the private sector. The Offices found that Clearview engaged in the collection, use and disclosure of personal information through the development and provision of its facial recognition application, without the requisite consent and for a purpose that a reasonable person would find to be inappropriate. The Offices recommended that Clearview:

• cease offering the facial recognition services that have been the subject of this investigation to clients in Canada;  
• cease the collection, use and disclosure of images and biometric facial arrays collected from individuals in Canada; and  
• delete images and biometric facial arrays collected from individuals in Canada in its possession.

6. Proposed Legislation and Regulations
6.1 Proposed Legislation and Regulations
In June 2022, “Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts”, also known as the Digital Charter Implementation Act, 2022, was introduced. Bill C-27 is designed to overhaul the federal private-sector privacy legislation, PIPEDA, and modernise the framework for the protection of personal information in the private sector. Bill C-27 is undergoing legislative review in parliament and if passed, would introduce the following legislative updates:

• The new Consumer Privacy Protection Act would require organisations to be open and transparent about the use of any automated decision system to make predictions, recommendations or decisions about individuals that could have a significant impact on them.  
• AIDA would introduce new measures to regulate international and interprovincial trade and commerce in artificial intelligence systems. This law is designed to protect individuals and communities from the adverse impacts...
associated with high impact AI systems, which is to be defined in future regulation. AIDA would establish common requirements for the design, development and use of AI systems, including measures to mitigate risks of harm and biased output. AIDA would also prohibit specific practices with data and artificial intelligence systems that may result in serious harm to individuals or their interests.

If passed, the provisions of AIDA would come into force no sooner than 2025.

7. Standard-Setting Bodies

7.1 National Standard-Setting Bodies
There are currently no AI-specific standard-setting bodies in Canada; however, the Canadian Institute for Advanced Research released in 2017 the Pan-Canadian Artificial Intelligence Strategy (PCAIS), which lays out Canada’s three-pillared strategy for becoming a world leader in AI.

As part of the PCAIS, the Government of Canada has pledged CAD8.6 million in funding from 2021-2026 for the Standards Council of Canada to develop and/or adopt standards related to artificial intelligence.

7.2 International Standard-Setting Bodies
In 2017, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) created a joint technical committee on AI: ISO/IEC JTC 1/SC 42 (“Joint Committee on AI”) that aims to provide guidance and develop a standardisation programme on Artificial Intelligence.

So far, the Joint Committee on AI has published 17 standards documents with 27 more under development. While the majority of these standards documents provide high level information on AI as opposed to specific guidelines, some of the concrete measures contemplated in the published and under development standards include risk management tools such AI impact assessments. Of note, the proposed Artificial Intelligence and Data Act would also introduce impact assessment requirements if it becomes law.

8. Government Use of AI

8.1 Government Use of AI
The extent of regulation associated with the government’s use of AI varies at the national and provincial/local level in Canada.

At the federal level, the Canadian government’s strategy on regulating AI and algorithms is managed by the Directive of Automated Decision-Making (DADM), while the Algorithmic Impact Assessment Tool (AIA) is used to empower the DADM. The DADM is the first national policy focused on algorithmic and automated decision-making in public administration in Canada. The DADM applies to any system, tool, or statistical model used to recommend or make an administrative decision about a client. Under the DADM, the Assistant Deputy Minister, or any other person named by the Deputy Head, is responsible for:

- completing an AIA and releasing the final results that are accessible on the government of Canada website;
- ensuring sufficient transparency in the system by providing notice before and explanations after decisions are made by the system;
ensuring quality assurance of the deployment and use of the system using AI or algorithms;

- providing recourse options to challenge the administrative decisions made by using AI or algorithms; and

- publishing information on effectiveness and efficiency of the system in meeting the administrative programme’s objectives.

The AIA supports the DADM as a risk assessment tool by determining the acceptability of AI solutions from an ethical and human perspective. It contains questions that assess areas of risk related to the project, system, algorithm, decision, impact and data used.

The provincial governments have not been as proactive as the federal government when it comes to AI and automated decision-making and there are not any provincial equivalents to the DADM. However, some provinces, like Ontario and Quebec, have started considering ways of regulating the use of automated systems in the public sector.

The Ontario government maintains a Digital and Data Strategy to regulate AI and algorithms in public decision-making. Ontario is in the process of developing its Trustworthy Artificial Intelligence framework, which is functionally similar to the federal DADM. The framework’s purpose is to ensure responsible AI use that minimises harm and maximises benefits for Ontarians.


8.2 Judicial Decisions

In Haghshenas v Canadas (Citizenship and Immigration), 2023 FC 464, the Federal Court of Canada dismissed an applicant’s request for judicial review of a deportation decision by a Federal Immigration Officer. The Court rejected the Applicant’s argument that the officer’s decision was not procedurally fair because it was reached through the assistance of AI, as the Court found that this consideration was not relevant to the duty of procedural fairness. The Court ultimately found that the use of AI was irrelevant because an Officer had made the decision in question, and that judicial review is meant to deal with the procedural fairness and or reasonableness of a decision.

8.3 National Security

In July 2017, the Canadian government released the CDS/DM “Joint Directive to Develop and Operationalize a Defence Program Analytics Capability”. The directive seeks to create analytics capability, drive digital transformation and establish data management as a core capability. The directive also created new positions, such as Chief Data Officer (CDO) for the Department of National Defence and Canadian Armed Forces (DND/CAF), and, in July 2018, the ADM of Data, Innovation, Analytics (ADM (DIA)). The scope of the DND/CAF strategy includes all data held in a repository in any format, and at any point in the data lifecycle, which includes data that is created, collected and/or used in both military operations and exercises, as well as in corporate administrative processes.

The Defence Research and Development Canada and the Centre for International Governance Innovation (CIGI) co-organised a nationwide workshop series in autumn 2021 and winter 2022, which examined AI from the perspective of defence and security, specifically in the con-
text of Canadian national security. The workshop focused on AI and semi-autonomous systems, AI and cybersecurity and enabling pan-domain C2. The participants of the workshop included key stakeholders from DND/CAF, the federal government and leading institutions supporting research on AI. The workshop examined issues such as data quality assessment, data format, data sharing, bias mitigation, human-machine teaming and the ethics of autonomous systems, and identified the need to upgrade government and military platforms around federated data networks, and for stronger collaboration between government, industry and higher education to scale Canada’s digital infrastructure.

9. Generative AI

9.1 Generative AI
Generative AI, or artificial intelligence tools that are capable of creating new data and content that did not previously exist, includes chatbots such as ChatGPT and image-generation tools such as DALL-E 2. Issues created by such generative AI tools span across multiple industry sectors and include generally intellectual property issues related to ownership, authorship, and originality, litigation and liability issues, and privacy law issues.

On the intellectual property front, the government of Canada, recognising that the issues posed by generative AI do not fit neatly into the current legislative and jurisprudential tools, engaged in a Consultation on a Modern Copyright Framework for Artificial Intelligence and the Internet of Things (“AI Consultation”). While the consultation acknowledged the issues related to ownership and infringement in copyright law, it did not provide any substantive guidance.

The Office of the Privacy Commissioner of Canada (OPC) has also acknowledged the potential privacy issues associated with generative AI. The OPC launched an investigation on 4 April 2023 into whether personal information is improperly collected, used, or disclosed as part of OpenAI’s training process.

10. AI in the Practice of Law

10.1 Uses of AI in the Practice of Law

Current uses of AI
As AI continues to develop, there are a growing number of use cases which may aid the practice of law. Areas of law practice in which AI have been increasingly used include the following.

E-discovery
AI-powered e-discovery tools assist with quickly and efficiently reviewing documents in the litigation discovery process. One such technique is through predictive coding. By using AI techniques, such as deep learning, AI-empowered tools use words and word patterns in a small set of documents marked as relevant and/or privileged and then apply it to a large dataset of other documents.

Legal research and legal analytics
More recently, AI tools have been introduced that purport to provide increased productivity and efficiency for legal research via use of natural language processing and machine learning technologies. For example, some offerings include AI-powered research tools that may provide answers to legal questions asked in plain language, as opposed to more traditional research searches using keywords and Boolean operators.
Legal technology companies are also harnessing the predictive ability of AI to forecast likely outcomes in court decisions. For example, in the tax context, Blue J Legal purports to predict outcomes of decisions with “90% accuracy” by analysing thousands of previous case law as comparators. Similarly, Lex Machina uses natural language processing to review court decisions to draw insights and predict how courts, judges and lawyers will behave, which in turn, allows lawyers to anticipate behaviours and outcomes that different legal strategies will produce.

**Contractual analysis**

AI technologies are being deployed to assist in contract analysis and review. AI can assist in quickly scrutinising contracts, identifying missing clauses, inconsistencies in terminology used or undefined terms across a single or multiple documents. For example, Kira Systems leverages the capability of machine learning to understand broad concepts, rather than a constrained rule-based “if-then” analysis, to identify and extract relevant clauses in its contract analyses.

**Patent and trademark searches**

AI is being utilised to benefit intellectual property practitioners by assisting in patent and trademarks searches. For example, NLPatent uses machine learning and natural language processing to understand patent language, which allows lawyers to search for patent terms and prior art in plain language, instead of relying on keywords. By describing the concept of an invention, prior art will be brought to the fore in AI-assisted patent searches.

In the trademark context, companies such as Haloo, utilise AI-powered searches to provide rapid and more expansive mark searches to ensure that there are no existing and conflicting marks that may interfere with registration of trademarks and tradenames.

**Emerging Uses of AI**

AI, with the ability for natural language processing, represents a large shift in how legal research can be conducted more efficiently and quickly. More recently, the release of more general-scope AI technologies, such as the ChatGPT, may represent an inflection point in the practice of law. Potential use cases for AIs like ChatGPT in the legal field include assisting in legal research, drafting standard legal documents, providing general legal information to the public and assisting in legal analysis.

**Rules or Regulations Promulgated or Pending by Law Societies/Courts**

Thus far, law societies in Canada have not promulgated rules directly to address the use of AI in the legal profession. However, the duty of lawyers to be competent may provide provisional guidance in this area until more concrete rules are provided. The commentary to Rule 3.1-2 of the Model Code of Professional Conduct, set out by the Federation of Law Societies, stipulates, “[t]o maintain the required level of competence, a lawyer should develop an understanding of, and ability to use, technology relevant to the nature and area of the lawyer’s practice and responsibilities. A lawyer should understand the benefits and risks associated with relevant technology, recognizing the lawyer’s duty to protect confidential information...”. Law societies in many jurisdictions, including Ontario, have amended their commentaries to include similar language.

**10.2 Ethical Considerations**

Lawyers in Canada abide by the ethical codes of conduct mandated by provincial and territorial law societies. Generally, all the law societies have similar requirements with respect to ethical...
codes of conduct. Notably, lawyers are required to be competent and efficient. Competency and efficiency requirements, in a future where AI is commonplace, may mean that lawyers must know how to effectively use these tools to assist clients.

However, the implementation of AI in legal practice still faces unresolved issues relating to client confidentiality. There are on-going investigations by Canada’s Privacy Commissioner into OpenAI relating to complaints of alleged collection, use and disclosure of personal information without consent. In Canada, lawyers are obliged not to reveal confidential client information. The use of AI models, such as ChatGPT and other large language models (LLMs), increases the risk of inadvertent disclosure of confidential information. Current rules do not address the situation of inadvertent disclosure.

Another professional and ethical challenge that must be considered is the accuracy and reliability of AI tools. With ChatGPT-3, there have been notable concerns regarding its “hallucinations”, that is, when it would confidently put forward factually incorrect statements as if true.

Finally, there remains the tension of access to justice and concerns for unauthorised practice of law, particularly in the context of public-use AI. AI tools have the potential to make basic legal information more easily accessible and digestible to the public at large. Notably, law societies in Canada do not have authority over the provision of legal information. Rather, law societies regulate the provision of legal advice. The distinction between legal information and legal advice is not clearly demarcated. Public use of Chatbots to request legal advice may raise concerns of unauthorised practice of law.

11. Theories of Liability

11.1 Theories of Liability

In Canadian law, tort law is the most relevant theory of liability for personal injury of commercial harm arising from AI-enabled technologies where the injured person has no pre-existing legal relationship (ie, by way of contract). Although it is possible for liability to arise through intentional torts or strict liability, negligence law will likely be the most common mechanism for plaintiffs seeking compensation for losses from the defendant’s use of an AI-system. The constituent elements of a negligence claim are:

- defendant owes a duty of care to the plaintiff;
- defendant’s behaviour breached that standard of care;
- plaintiff suffered compensable damages;
- damages were caused by the defendant’s breach; and
- damages are not too remote in law.

To bring a tort claim, the plaintiff has the burden of proof in establishing that an AI system was defective, the defect was present at the time the AI system was in the plaintiff’s control and that the defect contributed or caused the plaintiff injury. A defect related to manufacturing, design or instruction of an AI-based system could give rise to a tort claim.

Nevertheless, it may be difficult for plaintiffs to identify defendants. AI systems contain a complex array of components and contributors, software programming, data providers, owners and users of systems, and third parties. Furthermore, anonymous defendants present a concern because identifying humans behind remotely operated robotics systems may not be possible. Another challenge arises in determining the appropriate jurisdiction or venue for litigation.
when there are so many different contributors located in potentially different legal jurisdictions.

11.2 Regulatory
Canada does not presently have a strict liability regime under tort law for manufacturers of defective products. General principles in tort law in Canada are governed by common law rather than by statute, thus there are currently no proposed regulations regarding the imposition and allocation of liability as it relates to AI technologies.

12. General Technology-Driven AI Legal Issues

12.1 Algorithmic Bias
Biased outputs by AI systems may be found when they create an unjustified and adverse differential impact on any of the prohibited grounds for discrimination under the Canadian Human Rights Act, or provincial or territorial human rights or discrimination legislation. For example, if an AI system is used by an employer to triage applications for job openings, employers must make sure that prospective candidates are not being adversely ranked due to information in their applications about gender status, sexual orientation, disability, race or ethnicity status, or any other prohibited grounds for discrimination under local law.

Biased outputs by AI systems could also be derived indirectly, such as making adverse and systematic differentiations based on variables that may serve as proxies for protected grounds like race or gender, such as making onboarding decisions based on credit score.

Laws in Canada are evolving to regulate biased output risks by AI systems. In June 2022, the Government of Canada introduced Bill C-27, which, if passed, would enact AIDA, among other privacy-related statutes. AIDA would regulate the formation and subsequent utilisation of “high-impact systems” of AI. It would require businesses that design prescribed AI systems to mitigate biased outputs in their designs, document appropriate uses and limitations, and disclose such limitations. Businesses that use these regulated AI systems would be expected to consider the bias-related risks of these systems, monitor their use, and mitigate biased outputs.

12.2 Data Protection and Privacy
The regulation of AI under Canadian privacy law has taken several forms, including, but not limited to, new disclosure obligations when AI is used to make automated decisions about data subjects and regulations around the use of data for the creation of AI algorithms.

Under federal and provincial privacy laws in Canada, legislators have pushed to impose disclosure obligations on businesses in control of personal information where a technology or AI system is used by the business to make automated decisions that impact a data subject (e.g., if personal information is collected from job candidates and AI is used to conduct the initial triage of applications, where decisions are made exclusively by AI). These disclosure obligations have been introduced in Quebec by Law 25, amending the province’s Act respecting the protection of personal information in the private sector, which requires informing data subjects about use of an AI system.

Canada’s federal private sector privacy law, PIPEDA, could also be effectively replaced by the Consumer Privacy Protection Act (CPPA), which is being considered under Canada’s Bill
C-27. If Bill C-27 were to pass, businesses would be required to provide a general account of the business’ use of any automated decision-making system to make predictions, recommendations or decisions about individuals that have a significant impact on them.

Changes in Canada’s privacy landscape are being considered to regulate the databases that inform AI algorithms. For example, if Bill C-27 were to pass, AIDA would be enacted, which regulates the design and utilisation of prescribed AI systems. A new criminal offence would be created by the passing of AIDA relating to the knowing use or processing of unlawfully obtained personal information to design, develop, use or make available for use of an AI system (eg, knowingly using personal information obtained from a data breach to train an AI system).

12.3 Facial Recognition and Biometrics
Some recent changes have been introduced with respect to the collection, use and disclosure of biometrics-related personal information, including for facial recognition purposes. In the Province of Quebec, Law 25, An Act to modernise legislative provisions as regards the protection of personal information, amended the province’s Act to establish a legal framework for information technology (“Quebec IT Law”). The Quebec IT Law requires businesses that create a database of biometric characteristics and measurements (eg, a database of faces for facial identification purposes) to disclose the database to Quebec’s privacy regulator, the Commission d’accès à l’information, promptly and no later than 60 days after it is brought into service. This disclosure requirement requires businesses to complete and submit a prescribed disclosure form to the regulator, describing the biometrics database, how and why it is being used, and any potential risks associated with its use and subsequent maintenance.

Biometric personal information has also been expressly defined as “sensitive” by Quebec’s Law 25. As such, the collection, use and disclosure of biometrics personal information in Quebec requires express consent on the part of the respective data subject.

The collection, use and disclose of biometrics personal information without express consent has been the topic of a joint investigation by the Office of the Privacy Commissioner of Canada and provincial privacy regulators in Canada; namely, in the joint investigation of Clearview AI. Clearview AI’s facial recognition technology was found to scrape facial images and associated data from publicly accessible online sources (eg, public social media accounts) and to store that information in a database. While the information was scraped from publicly accessible social media accounts, Canadian privacy regulators found that the purposes for which Clearview AI used the facial images and associated data were unrelated to the purposes for which the images were originally shared on social media sites, thereby requiring fresh and express consent for new uses, and new purposes for using any of the facial images or associated data by a third party.

12.4 Automated Decision-Making
Automated decision-making technologies are being used across sectors, and involve the use of an AI algorithm to draw conclusions based on data from its database and parameters set by a business. Examples of automated decision-making technologies include AI screening processes that determine whether applications for loans online should be granted and aptitude tests for recruitment, which use pre-programmed algorithms and criteria to triage job
applications and reject applicants who do not meet certain criteria.

Use of automated decision-making technologies is regulated by federal and provincial privacy laws in Canada, mainly by imposing a disclosure obligation on business that use such technologies to make a decision that materially impacts data subjects based exclusively on the technology without further human involvement.

12.5 Transparency
There is currently no standalone federal or provincial law or regulation that applies specifically to chatbots or technologies that substitute for services rendered by natural persons. Use of such technologies is subject to the automated decision-making regulations under Canadian privacy law, whereby a business must inform data subjects that automated decision-making technologies are using their personal information to make automated decisions that could have a material impact on the data subjects.

Moreover, in June 2022, the government of Canada tabled Bill C-27, which, if passed, would enact AIDA, among other privacy-related statutes. AIDA would regulate the formation and subsequent utilisation of “high-impact systems” of AI. AIDA would impose requirements on businesses that design prescribed high-impact systems of AI, such as duties to mitigate and correct biased outputs, document the limitations of the AI system, and disclose limitations to users of the high-impact system.

12.6 Anti-competitive Conduct
Businesses must continue to comply with their obligations under Canada’s competition laws when an AI systems is being used. Canada’s Competition Act, for example, imposes a number of restrictions against misleading consumers (eg, certain uses of scarcity cues and drip pricing practices), which could be triggered by use of AI systems.

For example, bookings sites regularly use scarcity cues to inform users that only a certain number of rooms are available for their desired hotel or that a certain number of people are currently looking the same hotel. The Competition Bureau of Canada published the sixth volume of the Deceptive Marketing Practices Digest, which warns that, while use of scarcity cues can be permissible, they cannot be misleading (such as informing users that ten other users are concurrently viewing an offer when, in fact, they are viewing an offer that relates to a booking during another month or in a different city, thereby creating a misleading impression of scarcity when such scarcity does not exist). Businesses using AI must ensure that its use does not create misleading impressions.

13. Sustainability and Climate Change

13.1 Sustainability and Climate Change
The recent developments in AI technology mean it has the potential to be an essential tool for countries to meet and exceed their climate change targets. Particularly, AI’s ability to collate, distil and interpret large amounts of complex datasets may yield benefits in accelerating climate action. For instance, AI could be used to review large databases of corporate disclosures for climate-relevant information or to reduce carbon emissions by estimating transportation usage and modelling demand for public transportation and infrastructure. In the manufacture ring sector, AI is being used to discover more efficient materials to use as catalysts, which may in turn reduce energy requirements for chemical...
processes. In agriculture, AI is being integrated into tools to increase efficiency of crop yields and providing potential solutions to reduce greenhouse gas emissions.

In terms of development of industry standards, the precise role of AI is not entirely clear. Of course, with the many potential effects AI may have in the above-mentioned industries, AI could likely be an important tool for policy makers by providing information to make policy decisions. In addition, AI could be incorporated into models that are required to assess policy options.

14. AI in Employment

14.1 Hiring Practices and Termination of Employment Practices

Under federal and provincial laws in Canada, employers are restricted from taking actions that have or are intended to have an unjustified and adverse differential impact on employees under one or more prohibited grounds for discrimination, whether under the Canadian Human Rights Act or provincial or territorial human rights or discrimination laws. Risks are greater for employers where such decisions are systematic and involve a large number of employees. Therefore, when AI systems are being used by employer, whether during the onboarding, termination or employment phase of the relationship, employers have a duty to ensure AI systems are not discriminating against employees, directly or indirectly (such as by relying on data that serves as a proxy for discrimination).

Use of technologies to make automated decisions about employees is also regulated indirectly in federal and provincial privacy statutes, mainly by imposing a disclosure obligation on business that use such technologies to make a decision that materially impacts data subjects that is based exclusively on the technology without further human involvement (eg, if an AI algorithm rejects job applicants who are not Canadian citizens or permanent residents, without such decisions being reviewed by a human).

14.2 Employee Evaluation and Monitoring

In October 2022, the Province of Ontario amended its employment standards legislation, the Employment Standards Act, to require employers with 25 or more employees in Ontario, to have a written “electronic monitoring policy” in place to convey all the ways that electronic monitoring is being used by the employer to monitor employees. These could include, for example, monitoring attendance in the office, activity on a work computer, monitoring emails and other communications, or monitoring internet browsing activity. Employers need to share the electronic monitoring policy with existing employees, including, in certain circumstances, when it is materially updated, and need to provide new employees with the electronic monitoring policy within a prescribed period of onboarding.

In terms of evaluations, employers must disclose to employees when AI is being used to make automated decisions that can materially impact an employee, such as if AI is used to make evaluations about an employee’s performance without human involvement. Such uses of AI should be conveyed to employees in the context of an employee privacy policy.

15. AI in Industry Sectors

15.1 Digital Platform Companies

Digital platform companies using AI are subject to Canadian federal and provincial private-sector
privacy laws for the collection, use and disclosure of the personal information of customers. With regards to e-commerce, digital platform companies are also subject to Canada’s Anti-Spam Legislation (CASL). CASL protects consumers and businesses from the misuse of digital technology, including spam and other electronic threats. Digital platform companies are also subject to human rights and privacy laws in Canada with regards to the handling of employee personal information and any recruitment and hiring practices through automated decision-making systems.

Starting 22 September 2023, digital platform companies operating in Quebec must comply with new provincial private-sector privacy law requirements for transparent and accountable automated decision-making (ADM). This includes providing notice of ADM processes and complying with requests to correct personal information used in decisions. If passed, the proposed Artificial Intelligence and Data Act will apply to and govern the use of AI by digital platform companies.

15.2 Financial Services

In Canada, there is no specific AI legislation or regulation in financial services. In the absence of an AI-specific regime, financial institutions developing, deploying and using AI solutions must comply with all applicable existing laws, including financial services laws, consumer laws and privacy laws.

In Canada, there are different financial regulators, including the Office of the Superintendent of Financial Institutions (OSFI), the Financial Consumer Agency of Canada (FCAC), and the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), which regulate banks and financial services. Certain financial services are regulated provincially, such as in the areas of insurance and securities. The focus of Canadian banking and financial services regulators has been towards establishing regulatory guidelines and oversight over the responsible use of AI in the financial services sector, including measures to mitigate the risk of biases and discriminatory practices when dealing with customers and employees.

Canadian regulatory guidance with regards to the use of technology (including AI) in the provision of financial services includes the following:

- OSFI Guideline B-13 – Technology and Cyber Risk Management outlines the regulator’s expectations for FRFIs in relation to their use of technology and cyber risk management, including sound technology asset management practices and implementing a system development life cycle framework for the secure development, acquisition and maintenance of technology systems.
- OSFI Guideline B-10 – Third Party Risk Management Guideline, which provides enhanced risk management expectations for federally regulated financial institutions, including the use of third-party arrangements for their services such as the storage, use or exchange of data through cloud service providers and technology companies that deliver financial services.
- OSFI has proposed revisions to the Guideline E-23 on Risk Management, through which it plans to address emerging model risk management for federally regulated deposit taking institutions (DTIs), which includes the increasing use of AI and machine learning.
12-0364 – Guidance Respecting Electronic Trading”, require firms to adequately test algorithmic trading systems.

15.3 Healthcare
In Canada, there is no AI-specific law for the healthcare and medical devices sector. Health Canada is focused on establishing a regulatory framework for the use of machine learning in medical devices. To this end, Health Canada, in collaboration with the US Food and Drug Administration (FDA), and the United Kingdom’s Medicines and Healthcare products Regulatory Agency (MHRA) have jointly identified ten guiding principles that can inform the development of Good Machine Learning Practice (GMLP). These guiding principles will help promote safe, effective and high-quality medical devices that use artificial intelligence and machine learning (AI/ML):

- Multi-disciplinary expertise is leveraged throughout the total product life cycle;
- Good software engineering and security practices are implemented;
- Clinical study participants and datasets are representative of the intended patient population;
- Training datasets are independent of test sets;
- Selected reference datasets are based upon best available methods;
- Model design is tailored to the available data and reflects the intended use of the device;
- Focus is placed on the performance of the human-AI team;
- Testing demonstrates device performance during clinically relevant conditions;
- Users are provided clear, essential information; and
- Deployed models are monitored for performance and re-training risks are managed.

16. Intellectual Property

16.1 Applicability of Patent and Copyright Law
To address potential issues with copyright, the Government of Canada issued a Consultation on a Modern Copyright Framework for Artificial Intelligence and the Internet of Things. The Government has not provided any suggestions based on that consultation yet.

Canada’s Copyright Act does not provide a definition of “author” but previous case law related to injunction applications states that copyright can only exist in works authored by a human being. However, recently, the Canadian Intellectual Property Office (CIPO) granted a copyright registration to copyright that was completely generated by AI. Although the copyright registration was granted, it is unclear how this registration will be enforced. The CIPO states that they do not guarantee that “the legitimacy of ownership or the originality of a work will never be questioned.” While the software supporting AI may be copyrightable, this copyright does not automatically mean that the output of the software or AI is protected by copyright.

Ownership issues arise with patents as well. Under Canada’s Patent Act, an inventor and the party entitled to the benefit of the invention must be listed in the patent application. According to the Federal Court, an inventor must be (i) the person who first conceives of a new idea or discovers a new thing that is the invention; and (ii) the person that sets the conception or discovery into a practical shape. In 2020, a patent was applied listing the inventor as an AI system. This application is currently undergoing examination and has not been granted yet.
16.2 Applicability of Trade Secret and Similar Protection
Trade secrets can be used to protect the software and algorithms of AI technology. Trade secrets are protected in Canada under common law and the Civil Code of Quebec. Trade secrets regarding AI can also be protected by contract. In theory, this means that the AI technology, as well as the training data that the AI trained on, such as text or images, can be protected by trade secrets. Copyright, to a certain extent, can protect a compilation of data but there is a question as to whether another person using a copyright protected dataset infringes that copyright if they use the dataset to train their own AI program.

16.3 AI-Generated Works of Art and Works of Authorship
AI-Generated Works of Art and Works of Authorship can include, for example, literary, dramatic, musical and artistic works, all of which can be the subject of copyright protection in Canada. Before AI-generated works can be copyright protected however, they must first overcome two major hurdles: (i) formal requirements for copyright protection, and (ii) the question of to whom authorship should be attributed for AI-generated works.

Formal Requirements
Copyright protects the original expression of ideas that are fixed in a material form. Outputs from generative AI programs are expressions of ideas that are fixed in a material form, but there is some question as to their originality.

Originality in Canada requires that skill and judgement was involved in the expression of the idea. The Supreme Court of Canada in CCH Canadian Ltd. v Law Society of Upper Canada, 2004 SCC 13, defined “skill” as the use of one’s knowledge, developed aptitude, or practiced ability, and “judgement”, as the use of one’s capacity for discernment or ability to form an opinion or evaluation by comparing different possible options and producing a work. In addition, the work involved must be something more than a purely mechanical exercise.

Canadian courts have not yet had to reckon with whether AI-generated work involves skill and judgement that goes beyond a purely mechanical exercise, but one can imagine that it will largely depend on the facts of the situation. Where a very basic prompt is given, such as “draw me a flower”, or “write me a poem about flowers”, it will likely be difficult to establish that skill and judgement went into the creation of the resulting generated image.

Authorship
The author of a copyrighted work is the person who exercised the skill and judgement in its creation. There are therefore three potential candidates for authorship of AI-generated works: the user inputting the prompt, the person who created the AI model, or the AI model itself.

As discussed above, the person who input the prompt can be said to exercise skill and judgement in creating the work depending on the complexity of the prompt that they input.

The creator of the AI model exercised skill and judgement in the creation of the model, and no doubt owns copyright to the code associated with the model, but the connection between their skill and judgement and the outputted work is likely too tenuous to establish authorship.

Attributing authorship to the AI model itself creates a number of issues both conceptual and logistic. Conceptually, one might argue that
generative AI, regardless of how “human” it may seem in its outputs, is still nothing more than a computer program applying complex rules to inputs in order to produce outputs. If courts or regulators adopt this philosophical view then it would be hard to argue that generative AI's “if x then y” approach to creating original works could ever amount to more than a purely mechanical exercise.

Logistically, copyright protection in Canada subsists for the life of the Author plus 70 years, creating obvious issues for generative AI models that do not “die”. Furthermore, section 5(1) (a) of the Copyright Act states that an author must be “a citizen or subject of, or a person ordinary resident in, a treaty country”. This seems to contemplate that the author is a natural person. Finally, section 14.1(1) of the Copyright Act conveys moral rights, or rights to the integrity of the work, that are separate from copyright rights. Generative AI models, which are (so far) non-sentient, cannot properly exercise their moral rights to the integrity of their works.

16.4 OpenAI
There are generally five considerations when commercialising or otherwise incorporating into your business the outputs of generative AI models such as OpenAI:

Licensing Considerations
Each generative AI model has different policies related to the use and ownership of the inputs (user prompts), and outputs of the program. Under OpenAI's policy, the users own all of the inputs, and OpenAI assigns to the user all of its right, title and interest in and to the output. However, other generative AI programs might retain some interest in the output of the program, so users should carefully review the legal policies associated with the program that they are using.

Inaccuracies
Generative AI programs consisting of LLMs such as ChatGPT are prone to inaccuracies, or “hallucinations”, whereby the program will produce a seemingly correct answer to a question that actually has no grounding in reality. Inaccurate outputs might lead to a number of legal liabilities, such as under defamation law, consumer product liability law, tort law, etc.

Litigation Risk
Generative AI models are trained on massive data sets scraped from the internet, which often include data points such as images that are subject to intellectual property law protection. There is a risk that, by using these protected data points as inputs for generative AI models, the outputs of those models might infringe upon those protected works. Furthermore, and as discussed above, output inaccuracies can lead to litigation risk.

Privacy Considerations
A large number of the data points fed into the generative AI models as training data are likely considered “personal information” under Canadian privacy law, meaning informed consent is likely necessary before collecting, using, or disclosing the personal information as part of the AI model.

Furthermore, consideration should be given to the user inputs and potential confidentiality breaches that might occur if sensitive information is input into the system.

Bias
Generative AI models, like all AI models, are susceptible to bias stemming from the personal bias of their programmers and any bias baked into their training data.
17. Issues for In-House Attorneys

17.1 AI Issues for In-House Attorneys
For in-house attorneys, AI evolves the practice of law and enhances the way in which in-house teams collaborate together. AI can assist in-house teams to simplify and automate processes, reduce costs and improve productivity. In terms of current use, in-house teams have been leveraging machine learning tools for legal research and predictive legal software for litigation outcomes. AI tools are also being used for contract management processes.

In-house attorneys should ensure that the development, deployment and use of AI systems in Canada is in compliance with applicable privacy, consumer protection and, as required, industry specific laws.

18. Advising Corporate Boards of Directors

18.1 Advising Directors
AI systems and tools can be used within an organisation to support and enhance corporate governance through data-driven decision-making, financial assessments, market predictions, and to facilitate customer and shareholder interests in the organisation. However, there are risks associated with using AI in corporate governance, including gender and racial bias, data disruption and poisoning, customer and employee privacy, cybersecurity, reputational harm, and operational issues.

Corporate boards of directors ("boards") play a vital role in overseeing the use of AI systems and tools in their organisations, including the use of such tools to make strategic corporate decisions. In assisting with corporate decision-making, AI tools may leverage data from within the organisation or access data from external sources (including data purchased by the organisation).

To mitigate against the risks associated with AI adoption, boards should ensure that they are aware of, and receive training on, the types of AI systems and tools that are used within their organisations, the nature of the data used to operate and train such systems and associated risks, and engage appropriate stakeholders from within the organisation in AI-related decision-making processes (ie, IT, legal and human resources).

Boards should establish AI-focused specialist committee(s), conduct routine risk assessments of AI systems, develop AI risk mitigation and management policies and measures, and communicate such policies and measures to senior management and employees. The board should have a strategy in place to implement AI within their organisations and assign roles and responsibilities to senior management in executing such strategies.
Trends and Developments

Contributed by:
Theo Ling, Jim Holloway, Jacqueline Chan and Matthew Cook
Baker McKenzie LLP

Baker McKenzie LLP is the premier global law firm in North America. Recently recognised as one of the top 10 most innovative law firms in North America by the Financial Times, our 850 lawyers in the US and Canada provide strategic advice to domestic and multinational companies as they grow and manage issues close to home or across the globe. Over the last three years, we have handled more cross-border deals than any other firm, and our litigation, employment, IP, tax, international trade and other practices have been repeatedly named among the best in North America. For the past 50 years, our Canada office has been advising clients on federal, provincial and local laws with an unparalleled international perspective. Through our diverse information technology and communications practice, we guide our clients through the complex and emerging areas of artificial intelligence and machine learning (AI/ML) technology, financial technology, health technology, digital transformation, and more.

Authors

Theo Ling heads Baker McKenzie’s Canadian information technology/communications practice and is a member of the firm’s global IP/technology practice group, and technology, media and telecoms and financial institutions industry groups. Theo helps market-leading businesses develop and implement effective global strategies to support multijurisdictional commercial activities and manage complex cross-border compliance risks. The focus of Theo’s international commercial/regulatory practice is on data and technology-related issues, which include digital transformation and data governance projects that involve data privacy, data security, electronic payments, data monetisation, records retention, media/format, electronic signatures, cross-border data transfers, digitisation, fintech, and AI and machine learning considerations. Theo also advises clients on internet-related services that involve smart/connected devices, which are subject to regulation under telecommunications and broadcasting laws.
Jim Holloway is a partner at Baker McKenzie and a recognised and ranked leader in the areas of intellectual property and technology, a skilled and experienced trial and appellate advocate, and a trusted strategic advisor. Jim’s practice is focused on intellectual property law and technology, including trademark, copyright, patent and trade secret disputes. Jim also provides clients with strategic, pragmatic and commercial advice on the development, protection, monetisation and enforcement of their intellectual property assets, and how to avoid/manage risk. He also handles anti-counterfeiting litigation, diversion and grey market matters, unfair competition claims, marketing and advertising complaints, licensing and distributorship disputes, breach of confidentiality matters, and product liability claims involving technology.

Matthew Cook is an intellectual property and technology lawyer in Baker McKenzie’s Toronto office. He helps businesses both protect and commercialise their brands, ideas and technology. He has experience working with businesses to protect, manage and enforce their intellectual property, including in the fields of trademark, copyright, patent and trade secrets. He also works closely with businesses to ensure that their IP and technology is properly commercialised at all stages of development and use, by providing regulatory guidance in a number of fields, providing advice related to privacy law, and providing transactional support from an IP and privacy perspective.

Jacqueline Chan is an IP/tech lawyer focusing on advisory, transactional and litigation matters in Baker McKenzie’s Toronto office. Jacqueline holds a Bachelor of Applied Science and a Master of Applied Science in industrial engineering from the University of Toronto. Prior to law school, she worked as a process improvement analyst at a major teaching hospital and a business analyst at a global technology consulting firm, where she advised clients on information privacy and security compliance. Jacqueline assists on a variety of intellectual property matters, particularly in relation to patent, copyright and trademark disputes. Jacqueline has experience assisting clients in the healthcare, technology, transportation and food industries, and has acted as counsel on matters before the Ontario Superior Court of Justice, the Ontario Court of Appeal, the Federal Court, the Federal Court of Appeal and the Supreme Court of Canada.
Overview of AI in Canada
Currently, Canada does not have an AI-specific legal framework. There are various legal frameworks related to consumer protection, privacy, criminal conduct, tort and human rights, which are applicable to the different uses of AI. Furthermore, there is government and industry-specific guidance and tools that seek to regulate the development, deployment and use of AI systems in Canada. In the past few years, there have been various federal government initiatives and regulator-focused studies on the ethical development and responsible use of AI. However, common rules and standards have not yet been established and implemented.

To address the lack of comprehensive AI regulation, the federal government introduced legislative proposals to overhaul and modernise the federal private-sector privacy regime in Canada, including a new Artificial and Intelligence Data Act (AIDA). In doing so, Canada is one of the first jurisdictions in the world to propose a law to regulate AI. If passed, AIDA will introduce new requirements for organisations to ensure the safety and fairness in the design, development and deployment of high-impact AI systems. Organisations will also be required to implement new governance mechanisms and policies to consider and address the risks of their AI system and provide users with enough information to make informed decisions.

As the development and use of AI continues to rapidly expand, we examine below the key legal areas and developments related to AI in Canada, with regards to intellectual property and data privacy developments, litigation developments and trends, the use of AI in the practice of law, and financial services industry updates. We also examine the different legal implications associated with generative AI from a data privacy, litigation and intellectual property perspective.

Al and Privacy
The following are key areas of privacy developments related to the development, deployment and use of AI in Canada:

**Biased outputs**
There is increased regulation and scrutiny over the outputs of AI algorithms. Federal Bill C-27, which, if passed, would enact AIDA, and regulate the formation and subsequent utilisation of “high-impact systems” of AI; in particular, imposing obligations on businesses to prevent and correct “biased outputs” by AI algorithms creating any unjustified and adverse differential impacts under one or more of the prohibited grounds for discrimination under federal or
provincial human rights legislation. Biased outputs by AI systems could trigger discrimination-related claims under employment laws in class action proceedings, and will require businesses to monitor the impacts of their AI systems for bias that materially and adversely impacts their workforce, customers, or any third parties.

**Monitoring**

Ontario was the first province to introduce legislation that imposes electronic monitoring disclosure requirements on businesses; in particular, the obligation to inform employees, by way of a written electronic monitoring policy, whenever any means of electronic monitoring of employees is carried out in the workplace, including by any means that use AI. Work from home trends and an increased reliance on digital communication mean that electronic monitoring is increasingly prevalent in workplaces and businesses, and other jurisdictions in Canada may also pass legislation imposing similar or additional electronic monitoring obligations.

**Automated decisions/disclosures**

Federal and provincial laws in Canada are incorporating disclosure requirements into their privacy laws for businesses that use technology and AI to make automated decisions about data subjects. Such obligations require businesses to inform data subjects before such decisions are made (eg, to update privacy policies to describe the use of personal information for making automated decisions). Privacy regulators may increasingly investigate or enforce the business practices involving these decision-making technologies.

**Regulation of biometrics**

Biometric personal information is treated as sensitive, requiring express consent from data subjects before it is collected, used, or disclosed for commercial purposes. Moreover, in the Province of Quebec, biometric databases need to be formally registered with the province’s privacy regulator through the submission of a prescribed form. Following recent investigations by privacy regulators of businesses that utilise biometric databases (eg, the processing of facial images for identity verification purposes), it is possible that there will be increased scrutiny of the collection, use and disclosure of biometric data, and other Canadian provinces could adopt formal registration obligations such as in Quebec.

**AI and Intellectual Property (IP)**

The following are key IP-related developments related to AI in Canada.

**Copyright consultation**

The Government of Canada issued a Consultation on a Modern Copyright Framework for Artificial Intelligence and the Internet of Things. The purpose of this consultation is to identify gaps in Canada’s copyright framework with respect to AI and the internet of things and provide policy considerations that should be addressed with respect to copyright. So far, no recommendations have been prepared based on this consultation, but recommendations are anticipated. Some of the copyright concerns that need to be addressed are ownership, as well as the length of copyright. Currently copyright exists in work for 70 years following the death of the author, however if an AI can be the author, then the length of the copyright will need to be determined. These types of issues will hopefully be addressed in the results from the consultation.

**Ownership of AI**

With the rise of AI, and specifically generative AI, one of the main discussions surrounding intellectual property (IP) is whether AI can own IP or an AI system has IP rights associated with
a work. Currently, AI-created IP is being tested through the Canadian Intellectual Property Office. Both copyright and patents require the owners, authors or inventors to be identified as part of the application and registration process. With AI, it is unclear who the owner, author, or inventor of the work may be. For example, in patent law, the courts have primarily demonstrated that an inventor must be a human, however currently there are patent applications being prosecuted in Canada where an AI system is the inventor. Similarly, in copyright, although the term “author” is not defined in the Copyright Act, it is unclear whether an AI system can be an author. These applications are being closely watched to determine the status of AI ownership in Canada.

**AI training and IP**

AI systems are trained on massive datasets that are often scraped from the internet. Depending on the AI model, these can include texts and images that may be subject to copyright protection, or other intellectual property protection. Since protected data may be used for training, there is a risk that AI systems may infringe upon intellectual property to produce an output. Additionally, the training data may have infringed upon intellectual property rights if the data was not licensed for AI training.

**Generative AI**

Generative AI, or artificial intelligence models that are capable of creating new data and content that did not previously exist, has forced both legislators and regulatory bodies across a number of fields to reckon with the limitations of their current legal instruments. In particular, generative AI creates novel issues for intellectual property law in relation to authorship, infringement, liability, and to data privacy law in relation to the collection and use of personal information for training purposes.

**Intellectual property concerns**

Intellectual property rights inure to the author, owner, or inventor of a work or invention. Generative AI, which is capable of producing complex creative works and inventions, therefore complicates the fundamentals of intellectual property. Canadian patent legislation and jurisprudence has been quite clear that inventors are humans, therefore blunting any debate, for the time being, as to whether a generative AI model such as ChatGPT can be an inventor. Canadian copyright law, however, is much less certain. With a generative model creating fully realised creative works based solely on user inputs – which can be very rudimentary – the question arises as to whether the user is exhibiting a sufficient amount of skill and judgement in the expression of the idea. Furthermore, the process by which the generative AI model created the output based on the user input is shrouded within a “black box”, whereby even the AI model programmer cannot identify exactly how the final expression was created. Drawing authorship into question creates a cascading effect whereby key determinants for infringement, such as access to the original copyrighted work, become harder to establish, and liability, if infringement is found, becomes harder to pin down.

The government of Canada has acknowledged in their Consultation on a Modern Copyright Framework for Artificial Intelligence and the Internet of Things (the “AI Consultation”) that the current Copyright Act is ill-equipped to address the novel questions posed by generative AI. Despite acknowledging this deficiency, the AI Consultation does not provide suggestions for addressing these issues. Suffice to say that the government of Canada is alive to the intellectual
property issues posed by generative AI, and significant legislative and regulatory amendments should be coming soon.

Data Privacy Concerns
On the privacy front, generative AI programs, especially programs such as ChatGPT, are currently coming under fire for their potential breaches of privacy rights with respect to their data collection and use for training the AI model. The Office of the Privacy Commissioner of Canada (OPC) officially launched an investigation into OpenAI, developer of both ChatGPT and DALL-E, on 4 April 2023. While details of this investigation have not yet been disclosed, the OPC likely shares the concerns of many EU regulators; namely, that OpenAI scraped personal information from the internet without proper consent and used this personal information to train the AI model. In addition, there is a concern that OpenAI is using all user inputs, including potentially sensitive personal information, in order to further train the AI model. This concern appears to be well-founded given that OpenAI recently announced the introduction of what some have called “incognito mode” on ChatGPT, as well as a “ChatGPT business subscription” that allows users to better control their data. The introduction of both of these features appears to confirm that OpenAI is currently using user inputs to, at the very least, train the AI model. In addition, there is a concern that OpenAI is using all user inputs, including potentially sensitive personal information, in order to further train the AI model. This concern appears to be well-founded given that OpenAI recently announced the introduction of what some have called “incognito mode” on ChatGPT, as well as a “ChatGPT business subscription” that allows users to better control their data. The introduction of both of these features appears to confirm that OpenAI is currently using user inputs to, at the very least, train the AI model.

AI Liability
In Canada, AI liability may arise in several forms, including in the context of intellectual property litigation or product liability litigation.

Generative AI and IP litigation
To date, there have only been a few judicial decisions in Canada that have substantively addressed AI issues and only one decision related to generative AI and intellectual property rights. There have yet to be any reported decisions from the Canadian copyright board or patent appeal board regarding the granting of copyright or patents for AI-generated works, though more are expected in the future given the onset of filings related to AI-generated works. Issues that may be dealt with by the copyright or patent board include the assignment of authorship or ownership over AI-generated works. AI-generated works may also give rise to potential liability in the form of copyright infringement, where a work generated by AI is found to be substantially similar to an existing copyrighted work. For instance, in Stross v Trend Hunter, 2020 FC 201, the Federal Court of Canada found a defendant liable for copyright infringement for its use of a photo generated by AI, ruling that they could not rely on the fair dealing defence.

Product liability litigation and AI technology
The ability of AI to act autonomously raises novel legal issues, particularly with respect to how to assign fault when an AI product causes injury or damage. In Canadian law, although there have yet to be any reported cases to date, tort law remains the most relevant theory of liability for personal injury of commercial harm arising from AI-enabled technologies where the injured person has no pre-existing legal relationship (ie, by way of contract). Negligence law will likely be the most common mechanism for plaintiffs seeking compensation for losses from the defendant’s use of an AI-system. However, barriers may arise in accessing remedies through tort law, including the fact that it may be difficult for plaintiffs to identify defendants. Outside the context of tort law, liability in contract may also present a concern in that parties may use the law of contracts and the contracting process to inappropriately limit or avoid liability by contract.
As litigation involving generative AI continues to increase in other jurisdictions such as the US, it is expected that Canadian courts will adjudicate similar cases in the future likely involving violation of copyright law due to generative AI technology and product liability litigation arising from AI products that result in injury.

**AI and the Practice of Law**

**AI tools used in law**

AI has been and continues to be leveraged in the practice of law. While recent discussions have homed in on the potential and capabilities of generative AI, AI tools have been assisting lawyers for years via e-discovery, legal research and analytics, contract analysis and in intellectual property searches. The consistent theme, across these areas in which AI tools are integrated, is that AI speeds up the process of searching through large sets of data. Whether it be documents for discovery, review of contractual clauses and searching for key words in legal research, AI has transformed legal practice, making information increasingly accessible and more speedily obtainable.

The next leap in AI technology appears to be generative AI, as described above. The release of these more powerful AI tools may represent an inflection point in the practice of law. However, it remains to be seen how the legal profession will adapt to these new technologies. Potential use cases include further refinement in legal research and potentially legal drafting and summarising of case law. For example, recently released versions of AI programs that support litigation, purport to search, summarise and draft from its database of authoritative materials. It appears to have a similar interface and functionality to chatbots, in that it understands queries asked in natural language. Ultimately, however, it must be remembered that it is the lawyer that is providing advice to clients, and who is responsible for such advice.

**Ethical considerations of AI use in law**

Lawyers are required to be competent and efficient. Accordingly, in a future where AI use is commonplace, it may mean that lawyers must know how to effectively use these tools to assist their clients. Notably, the Model Code of Professional Conduct from the Canadian Federation of Law Societies emphasises in its commentaries the importance of technological competence.

With respect to efficiency, one 2018 Ontario Superior Court case held that a lawyer's costs claim for legal research was problematic and that if AI sources were employed, there would be no doubt that the lawyer's preparation time would have been significantly reduced. The twin requirements of competency and efficiency may very well require lawyers in the future to be familiar and, more likely, adept at navigating these new technologies.

**AI Trends in Financial Services**

AI tools are only as effective as the data model they rely on. The main risks stemming from AI come from compromises to the data relied on. Without appropriate safeguards, the risks associated with the use of AI in the financial services sector can have profound implications for the use of AI for customer identification, consumer credit services, securities trading and investment advisory services. The increasing use and systemic risks associated with AI in the financial services sector, has Canadian financial regulators collaborating with global AI research organisations and regulators from other jurisdictions to conduct AI risk studies and develop sector-specific risk management frameworks, tools and guiding principles.
In April 2023, the Office of the Superintendent of Financial Institutions (OSFI) and the Global Risk Institute (GRI) jointly released a report on the ethical, legal and financial implications of AI for financial services institutions. The discussions have led to the development of EDGE principles (Explainability, Data, Governance and Ethics):

- **Explainability** enables customers and relevant stakeholders to understand how an AI model arrives at its conclusions.
- **Data** leveraged by AI allows financial institutions to provide targeted and tailored products and services to their customers or stakeholders. It also improves fraud detection, enhances risk analysis and management, boosts operational efficiency, and improves decision-making.
- **Governance** ensures a framework is in place that promotes a culture of responsibility and accountability around the use of AI in an organisation.
- **Ethics** encourages financial institutions to consider the broader societal impacts of their AI systems.

The report signals progress by financial regulators in Canada, such as OSFI, towards developing a comprehensive AI regulatory framework that will implement safeguards and mitigate risks associated with the use of AI systems in the financial sector. This also aligns with the global approach towards AI regulation, in which regulators are seeking to find a balance between regulation and innovation, establishing comprehensive regulations while ensuring that banks and financial institutions continue to innovate, transform and remain competitive.
Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com