itworldcanada.com

Understanding Current Cybersecurity Challenges in Law: Legal Considerations for Artificial Intelligence and Technological Development (Article 6) - IT World Canada

Melissa Lukings and Arash Habibi Lashkari

14-17 minutes

With strong competition among countries around the world to become cutting edge leaders in AI, artificial intelligence has been a driving force of innovation in the digital economy. Indeed, Canada has been working to place itself among other global leaders in dynamic AI development, with the Canadian artificial intelligence sector receiving significant funding from governments – both federally and provincially – as well as investments and research funding through universities to develop innovative artificial intelligence programs.

While sometimes confused with the concept of automation, artificial intelligence presents novel legal and regulatory challenges that automation inherently does not. One of the largest regulatory obstacles we encounter with regard to artificial intelligence is the ineffectuality of creating overly-rigid legal approaches which may

quickly become outdated with the inevitable introduction of new and rapidly changing technologies.

In our previous articles in this series, we have discussed: the concept of data sovereignty as a legislative challenge in our global digital world; the role of digital governance and governance strategies in relation to the concept of digital social responsibility; the complexities inherent in assigning jurisdictional authority for the purpose of addressing online content and activities; the ongoing arguments for and against digital censorship in the Canadian legal landscape; and the challenges presented by data breaches and increased data awareness in the workplace. You can view our previous articles here:

- Understanding Current Cybersecurity Challenges in Law: Data Breaches and Increased Data Awareness (Article 5)
- Understanding Current Cybersecurity Challenges in Law: Balancing Responsibilities in Digital Content Censorship (Article 4)
- Understanding Current Cybersecurity Challenges in Law: Determining Online Jurisdictional Authority (Article 3)
- Understanding Current Cybersecurity Challenges in Law: Digital Governance and Social Responsibility Meet User-Generated Content (Article 2)
- Understanding Current Cybersecurity Challenges in Law: Data Sovereignty and Cross-Border Data Transfers (Article 1)

For our sixth, and final, article in our six-part series, “Understanding Current Cybersecurity Challenges in Law ”, we will discuss the challenges related to artificial intelligence in law and cybersecurity, including the issues associated with AI in legal

technology, legislative concerns, data protection, and creative content ownership and attribution.

What is Artificial Intelligence (AI)?

Artificial intelligence – or AI – is an umbrella term comprising a wide range of intelligent functions including pattern recognition and detection, optimization, natural language processing and translation, decision-making, hypothesis testing, and much more. In relation to the intelligence of machines, the goal of artificial intelligence often refers to reaching a point at which machines behave like humans, or become capable of actions that require functional intelligence, that is, inspired by the brains and behaviours of humans.

When we consider the ability to replace humans in actions that require mental skills, we can also extend our goal to idealize the ability of a system to act in a manner that was not previously programmed, as well as the ability to adapt the actions of that system to the nuances of a novel, dynamic, or changing environment. Some of the current applications being explored for artificial intelligence include:

- Advanced web search engines (e.g., Google)
- Recommendation systems (e.g., the types used by YouTube, Amazon and Netflix)
- Understanding human speech (e.g., Siri and Alexa)
- Self-driving cars (e.g., Tesla)
- Automated decision-making
- Competing in high level strategic games.

As machines become increasingly capable, tasks considered to require facets of intelligence often become gradually removed from the working definition of artificial intelligence. For example, optical character recognition – once an astounding technological novelty – is now frequently excluded from the definitions of processes which are considered to be based in, or driven by, artificial intelligence, having now become routine technology.

The use of artificial intelligence has become ingrained in our expanding modern digital world. Smart phones using facial and voice recognition have carried over into our homes where smart devices now have the ability to recognize and learn an individual's behaviour and recognizing patterns by adjusting the settings of appliances, thermostats, and home lighting systems. We see artificial intelligence programs being used by large retailers, like Amazon, to anticipate the needs and wants of consumers through the use of predictive analytics. Many financial institutions are now relying on artificial intelligence for fraud detection. We have even begun to see artificial intelligence and AI-technology seeping into our legal offices.

AI in Law

Artificial intelligence, as applied to the world of legal practice, involves the use of computers to apply the processes of learning, reasoning, and analysis in order to process information which is relevant to legal matters. The appeal of AI in legal practice is that by using machine learning, algorithms, and related technologies, the analytical product will become increasingly accurate, efficient and reliable over time. It should come as no surprise that artificial intelligence has already been implemented in document review,

legal research, drafting of pleadings, and case analysis in some of the larger law firms. The implications of such technology and its potential are nearly limitless. For example, a Beagle is an automated contract analysis system powered by artificial intelligence that reads contracts in seconds, highlights key information visually with easy-to-read graphs and charts and gets "smarter" with each reviewed contract. Although there is not a significant amount of AI legal technology being used by lawyers, law firms, or the public, it is not premature to start thinking very seriously about, and taking action on, the ethical issues raised by this technology in the context of legal services.

The legislative "elephant-in-the-room" of legal issues, with respect to artificial intelligence, comes down to the precarious balance of social and economic interests, both sides of which must be considered by our policy-makers in their efforts to legislate this area. As artificial intelligence has the potential to impact all aspects of society and economy, many governments have struggled in their efforts to balance the need to regulate this novel technology in an effort to protect the public, while also making certain not to stifle innovation by over-regulating a technology that is still rapidly advancing from its infancy.

AI Law in Canada

Up to this point, we have seen little solid movement in the creation of new laws to address artificial intelligence and the associated technological implications of AI in Canada. We have seen some jurisdictions begin to address automated systems, in a limited capacity, with respect to regulating information security and privacy interests, but the introduction of enforceable normative law has yet to be seen.

We have, however, noticed the admirable introduction of “soft law” emerging around artificial intelligence, such as the creation of data governance standards, ethics codes, regulatory frameworks, and informal policies. While these guidelines may be helpful as practical suggestions, these types of “soft law” regulations lack clarity and are rarely enforced, operationalized, or made mandatory.

While it may not be entirely necessary for new laws to be introduced, there has been a growing need for some sort of new way for existing laws to be applied with regard to artificial intelligence, in that it would better ensure a semblance of oversight and enforcement.

Issues and Challenges

Growth in artificial intelligence has driven the demand for large quantities of data, however the links between personal data and many artificial intelligence applications raise privacy concerns, as well as questions regarding ethics and human rights. Many nations have outdated public and private sector data protection laws for which there have been numerous calls for legislative reform. These reforms must address both the need of the organisation to access the large quantities of data required for AI innovation as well as the imperative to properly protect the human right to privacy and data protection. There is also a need to comprehensively review federal and provincial laws that enable or authorise data sharing to ensure that they include safeguards and limitations which can be adapted and applied to provide greater clarity, transparency, and accountability in relation to artificial intelligence.

A more nuanced philosophically-based challenge in artificial intelligence is the question of creative content ownership and attribution when the content is created through AI or algorithmic automation. Consider the following scenario involving artificial intelligence and copyright law.

A computer uses AI to generate a novel. The novel is wildly popular, selling out in bookstores around the world. As a result of the success and the social impact of the novel, it wins many awards and achievements, and finally becomes a cultural masterpiece.

- *Should the AI-generated novel be protected by copyright?*

  If we determine that it should be given copyright protection, then…

- *Who, if anyone, should be deemed to be the author? Or, in whom should first ownership of the copyright vest?*

  If new protections are to be afforded to AI-generated works – as a matter of evidence-based policy-making – then…

- *What would be the appropriate scope and duration for those rights or copyright protections?*

  If it turns out that the AI-generated novel itself was a creation stemming from copyright infringement carried out by AI systems and beyond the control of the AI developer or user then…

- *What degree of involvement or control by the programmers, providers, or users of AI could produce direct or indirect liability? That is, at what point is the programmer, provider, or user responsible for the infringing act?*

  These issues cannot be satisfactorily addressed, however, until we tackle the larger gap in our normative and conceptual thinking

about the appropriate interaction of artificial intelligence and copyright law. Specifically, the extent to which the copyright system can and should play a role in encouraging, facilitating, restricting, and/or regulating the ongoing evolution of artificial intelligence.

There are certainly boatloads of other excellent examples and handfuls of hypotheticals which illustrate the numerous challenges associated with artificial intelligence and our legal structures. However, in the interest of brevity, suffice to say that there are many factors to be considered in the process of creating new laws or applying existing laws which can address artificial intelligence and its social and economic implications.

Conclusion

Canada is only at the beginning of developing new or existing laws to apply to artificial intelligence and its related technological advancements. While we are only just beginning to find ways to address these novel challenges, we can be certain that artificial intelligence will continue on its dynamic trajectory of innovation far beyond what we have so far seen.

In this series, we have explored many of the legal challenges relating to cybersecurity and digital advancement in our current time and space. With the ever-evolving nature of technological advancement, we can be certain that these challenges discussed in this series will not be viewed as challenges for very long, as we must come together to navigate our legal structures around these novelties. As technologies change and develop, new challenges will arise and we will, once more, look to address our legal structures to work with them. Rather than an obstacle to legal development, we must look to these future challenges as part of

the larger process of human growth and development, a cycle which will – and must – continue to evolve long into the future. Indeed, it is this growth that drives the flexibility and innovation which is both inherent to, and necessary for, our continued existence as human beings.

Melissa Lukings and Arash Habibi Lashkari

** Melissa Lukings is a senior JD student in the Faculty of Law at the University of New Brunswick (UNB) and former graduate of Memorial University of Newfoundland (MUN) holding a BA in Linguistics. She has a particular interest in cybersecurity and privacy law, criminal law, and grassroots community organizations - specifically those focusing on equality and inclusion, human rights, violence prevention, harm reduction, and / or relating to

equal and equitable access to justice. **** Dr. ARASH HABIBI LASHKARI is a senior member of the IEEE and an Associate Professor in Cybersecurity at York University. Prior to this, he was an Associate Professor at the Faculty of Computer Science, University of New Brunswick (UNB), and research coordinator of the Canadian Institute for Cybersecurity (CIC). He has over 23 years of academic and industry experience. He has received 15 awards at international computer security competitions - including three gold awards - and was recognized as one of Canada's Top 150 Researchers for 2017. He also is the author of ten published books and more than 100 academic articles on a variety of cybersecurity-related topics. In 2020, he was recognized with the prestigious Teaching Innovation Award for his personally-created teaching methodology, the Think-Que-Cussion Method. He is the author of 12 published books and more than 100 academic papers on various cybersecurity-related topics. He is the founder of the Understanding Cybersecurity Series (UCS), an ongoing research and development project culminating with a varied collection of online articles and blogs, published books, open-source packages, and datasets tailored for researchers and readers at all levels. His first two books in this series are entitled "Understanding Cybersecurity Management in FinTech - Challenges, Strategies, and Trends" and "Understanding Cybersecurity Law and Digital Privacy - A Common Law Perspective," published by Springer in 2021. The first online blog series of UCS entitled "Understanding Canadian Cybersecurity Laws", was recognized with a Gold Medal at the 2020 Canadian Online Publishing Awards (COPA). His research focuses on cyber threat modeling and detection, malware analysis, big data security, internet traffic analysis, and cybersecurity dataset generation.