EMERGING LEGAL ISSUES IN AN AI-DRIVEN WORLD

17 July 2019

Introduction

Artificial Intelligence ("AI") is the new marketplace reality. The increase in computing power, improved algorithms and the availability of massive amounts of data are transforming society. According to the International Data Corporation ("IDC"), the AI market is expected to hit $35.8 billion this year, which represents an increase of 44% since 2018. IDC has also projected global spending on AI to double by 2022, reaching $79.2 billion. In this article, we identify a number of emerging legal issues associated with the use of AI and offer some views on how the law might respond.

What is artificial intelligence?

AI describes the capacity of a computer to perform the tasks commonly associated with human beings. It includes the ability to review, discern meaning, generalize, learn from past experience and find patterns and relations to respond dynamically to changing situations.

In 2017, Accenture Research and Frontier Economics conducted research comparing the economic growth rates of 16 industries and projecting the impact of AI on global economic growth. The report concluded that AI has the potential to boost profitability an average of 38% by 2035 and lead an economic boost of US$14 trillion across 16 industries in 12 economies by 2035.
The promise of AI is better decision-making and enhanced experiences. In their book Machine, Platform, Crowd, MIT professors Andrew McAfee and Erik Brynjolfsson write "[t]he evidence is overwhelming that, whenever the option is available, relying on data and algorithms alone usually leads to better decisions and forecasts than relying on the judgment of even experienced and "expert" humans." The fear is that AI in an unregulated environment will lead to a loss of human supervisory control and unfortunate outcomes.

**The legal aspects of AI**

Commentators have recognized that the preponderance of AI will raise new and important legal and ethical questions. Some have identified the need for AI ethicists to help navigate where this technological advance might take us.

In October 2016, the British House of Commons published a report on Robotics and Artificial Intelligence, which highlighted certain ethical and legal issues including transparent decision-making, minimising bias, privacy and accountability. On December 18, 2018, the European Commission's High-Level Expert Group on Artificial Intelligence ("AI HLEG") released the first draft of the Draft Ethics Guidelines for Trustworthy AI. Pursuant to the guidelines, Trustworthy AI requires an ethical purpose and technical robustness:

1. **Ethical purpose:** Its development, deployment and use should respect fundamental rights and applicable regulation, as well as core principles and values, ensuring "an ethical purpose", and

2. **Technical robustness:** It should be technically robust and reliable given that, even with good intentions, the use of AI can cause unintentional harm.

In Canada, the Treasury Board Secretariat of Canada (the "Board") is looking at issues around the responsible use of AI in government programs and services. On March 2, 2019, the Board released a Directive on Automated Decision-Making, which takes effect on April 1, 2019, to ensure that AI driven decision-making is compatible with core administrative law principles such as transparency, accountability, legality, and procedural fairness.

To grasp an understanding of the legal aspects of AI, one of the central questions will be how the law will evolve in response to AI. Will it be through the imposition of new laws and regulation or will it be through the time-honoured tradition of having our courts develop new laws by applying existing laws to new scenarios precipitated by technological change?

AI has already been used and accepted in a number of US decisions. In Washington v Emanuel
Fair, the defence in a criminal proceeding sought to exclude the results of a genotyping software program that analysed complex DNA mixtures based on AI while at the same time asking that its source code be disclosed. The Court accepted the use of the software and concluded that a number of other states had validated the use of the program without having access to its source code. In State v Loomis, the Wisconsin Supreme Court held that a trial judge’s use of an algorithmic risk assessment software in sentencing did not violate the accused’s due process rights, even though the methodology used to produce the assessment was neither disclosed to the accused nor to the court.

In Canada, litigation involving AI is in its early stages. In 2018, the Globe and Mail reported that a lawsuit involving an AI system had been commenced in Quebec. Adam Basanta created a computer system that operates on its own and produces a series of randomly generated abstract pictures. Mr. Basanta was now being sued in Quebec Superior Court for trademark infringement because of an image created by the system. Amel Chamandy, owner of Montreal’s Galerie NuEdge, claimed that a single image from Mr. Basanta’s project All We’d Ever Need Is One Another violated the copyright on her photographic work Your World Without Paper (2009) and the trademark she owns associated with her name.

AI is also being utilized to render judicial decisions. In Argentina, AI is being used to assist district attorneys in writing decisions in less complex cases such as taxi licence disputes that presiding judges can either approve, reject or rewrite. Using the district attorneys’ digital library of 2,000 rulings from 2016 to 2017, the AI program matches cases to the most relevant decisions in the database, which enables it to guess how the court will rule. Thus far, judges have approved all of the suggested rulings—33 in total.

**Privacy**

The volume and relativity of data collection will keep privacy at the forefront as one of the most significant legal issues that AI users will face going forward. AI systems use vast amounts of data; therefore, as more data is used more questions are raised. Who owns the data shared between AI developers and users? Can data be sold? Should this shared data be de-identified to protect privacy concerns? Is the intended use of data appropriately disclosed and compliant with legislation such as the Personal Information Protection and Electronic Documents Act (“PIPEDA”)?

Governments now are updating their privacy legislation to respond to privacy concerns fueled by the public outcry against massive data breaches and the unfettered use of data by large companies. Consumers have become increasingly concerned with the potential misuse of their personal information. In 2015, the European Commission conducted a survey carried out in 28
member states of the European Union that demonstrated that roughly seven out of 10 people expressed concern about their information being used for a different purpose than the one for which it was collected.\textsuperscript{24}

The EU and international regulators have taken an active interest in AI, not only recognizing its benefits but also being mindful of potential risks and unintended consequences.\textsuperscript{25} The European Parliament enacted the General Data Protection Regulation ("GDPR"), which is a comprehensive set of rules designed to keep the personal data of all EU citizens collected by any organization safe from unauthorized access or use.\textsuperscript{26} Under the GDPR, companies must be clear and concise about their collection and use of personal data, and indicate why the data is being collected and whether it will be used to create profiles of people’s actions and habits. In other words, organizations must be transparent about the type of information they collect about consumers and how this information will be used. Critics contend that the GDPR could present an obstacle to developers looking to design more complex and sophisticated algorithms.\textsuperscript{28}

Unlike the EU, US federal lawmakers have yet to establish regulations to govern the use of personal information in the AI world.\textsuperscript{29} Sensing the inevitability of data regulation, some large American companies like Apple are encouraging the introduction of regulation in the United States.\textsuperscript{30} On January 18, 2019, Accenture released a report outlining a framework to assist US federal agencies to evaluate, deploy and monitor AI systems.

Canada has yet to adopt regulations the likes of the GDPR. However, the new federal mandatory data breach notification regulations that came into force on November 1, 2018, were drafted with a view to harmonize the requirements of the GDPR to the extent possible.\textsuperscript{32} The Breach of Security Safeguards Regulations under PIPEDA set forth certain mandatory requirements for organizations applicable in the event of a data breach.\textsuperscript{33} PIPEDA defines a breach of security safeguards as "the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization’s security safeguards."\textsuperscript{34} Should a breach of security safeguards occur, organizations are required to do the following: report data breaches to the Office of the Privacy Commissioner of Canada, keep and maintain a record of every breach of safeguards involving personal information under their control, and provide the records of the breach to the Commissioner upon request. Organizations will need to not only evaluate their compliance in terms of privacy legislation, but also ensure that their data handling practices are sufficiently secure to prevent cybersecurity breaches.

Contracts
The inherent nature of AI may require individuals or entities contracting for AI services to seek out specific contractual protections. In the past, software would literally perform as it was promised. Machine learning however is not static, but is constantly evolving. As noted by McAfee and Brynjolfsson, "[m]achine learning systems get better as they get bigger, run on faster and more specialized hardware, gain access to more data, and contain improved algorithms." The more data algorithms consume, the better they become at spotting patterns.

Parties might consider contractual provisions, which covenant that the technology will operate as intended, and that if unwanted outcomes result then contractual remedies will follow. These additional provisions might include an emphasis on audit rights with respect to algorithms within AI contracts, appropriate service levels in the contract, a determination of the ownership of improvements created by AI, and indemnity provisions in the case of malfunction. AI will dictate a more creative approach to contracts where drafters will be forced to anticipate where machine learning might lead.

Torts

Machine learning constantly evolves, making more complex decisions based on the data it operates on. While most outcomes are anticipated, there is the distinct possibility of an unanticipated or adverse outcome given the absence of human supervision. The automated and artificial nature of AI raises new considerations around the determination of liability. Tort law has traditionally been the mechanism used in the law to address changes in society, including technological advances. In the past, the courts have applied the established analytical framework of tort law and have applied those legal principles to the facts as they are presented before the court.

We start the tort analysis with the following questions: Who is responsible? Who should bear liability? In the case of AI, is it the programmer or developer? Is it the user? Or is it the technology itself? What changes might we see to the standard of care or the principles of negligent design? As the AI evolves and makes its own decision, should it be considered an agent of the developer and if so, is the developer vicariously liable for the decisions made by the AI that result in negligence?
The most common tort—being the tort of negligence—focuses on whether a party has a duty of care to another, whether the party has breached the standard of care, and whether damages have been caused by that breach. Reasonable foreseeability is a central concept in negligence. Specifically, the test is whether a reasonable person is able to predict or expect the general consequences that would result because of his or her conduct, without the benefit of hindsight. The further that AI systems move away from classical algorithms and coding, then they can display behaviours that are not just unforeseen by their creators but are wholly unforeseeable. When there is a lack of foreseeability, are we placed in a position where no one is liable for a result, which may have a damaging effect on others? One would anticipate that our courts would respond to prevent such a result.

In a scenario where there is a lack foreseeability, the law might replace its analysis based on negligence to one based on strict liability. The doctrine of strict liability also known as the rule in Rylands v Fletcher provides that a defendant will still be held legally responsible when neither an intentional nor a negligent act has been found and it is only proven that the defendant's act resulted in injury to the plaintiff.

Should a negligence analysis remain, then the standard of care requirements will need to be redefined in an AI context. Some of the following questions will be central to the court’s consideration:

i. Is the decision-making transparent so that the court can determine how the "black box" reached the outcome it did?
ii. What steps were taken to monitor outcomes arising from machine learning?
iii. Was the integrity and quality of the data appropriate for the purpose for which it was intended?
iv. Was the data used representative or does it promote bias and/or discrimination?
v. Was the algorithm appropriately designed to guard against unintended outcomes?

One can envisage a growth industry in negligence actions against software development companies and programmers.

Product liability is another arm of tort law that may take on more significance when looking at liability should AI become defective. Under the common law, product liability focuses on negligent design, negligent manufacture and breach of the duty to warn. It generally addresses the liability of one or more parties involved in the manufacture, sale or distribution of a product. For this doctrine to apply, the AI system in question must qualify as a product, and not a service. Ascertaining where the defect occurred in the supply chain of an AI product may be difficult given the autonomous and evolving nature of machine learning and algorithms. Commentators have noted that product liability will become relevant with respect to issues
Bias/discrimination

Companies like Microsoft and Google have recognized that offering AI solutions that raise ethical, technological and legal challenges may expose them to reputational harm. The issues of bias and/or discrimination have become more prevalent as more companies and governmental entities turn to AI systems in their decision-making processes. For example, a 2016 investigation by ProPublica revealed that a number of US cities and states used an algorithm to assist with making bail decisions that was twice as likely to falsely label black prisoners as being at high-risk of re-offending than white prisoners.

To mitigate against built-in biases in collected data and in the decision-making process, a number of companies have developed bias-detection algorithms. Accenture developed a tool that enables companies to identify and eliminate gender, racial and ethnic bias in their AI software. IBM's OpenScale is an AI platform that provides the ability to explain how AI decisions are made in real time to ensure transparency and compliance, which may also have relevance to the definition of the standard of care. However, these solutions may not necessarily solve the problem. A senior researcher at Microsoft acknowledged that "if we are training machine learning systems to mimic decisions made in a biased society, using data generated by that society, then those systems will necessarily reproduce its biases."

Setting ethical parameters within which AI systems will operate is paramount to addressing the issue of bias. Regulating AI will not be an easy feat. Given that AI is constantly evolving, any ethical regulation concerning the use of AI must also continually evolve to remain relevant to the technology.

Conclusion

AI will continue to develop and to disrupt society in ways that we cannot yet imagine. It is challenging to keep pace with the speed of developments with which AI systems are being deployed. One developer recently described it like "a sort of peanut butter you can spread" across multiple disciplines and industries. As the peanut butter is spread, organizations must prepare not only for the positive but also for the unintended and likely unfortunate negative consequences technology like this will bring. It is largely unknown how the law will react to this new reality but anticipating what those impacts might be is a timely first step.

Sources

2. Ibid.


4. Ibid.


8. House of Commons Science and Technology Committee, "Robotics and artificial intelligence" (12 October 2016), online: https://publications.parliament.uk/pa/cm201617/cmselect/cmsctech/145/145.pdf


10. High-Level Expert Group on Artificial Intelligence, "Draft Ethics Guidelines for Trustworthy AI: Working Document for Stakeholders' Consultation" (18 December 2018), European Commission, online: https://ec.europa.eu/digital-single-market/en/news/draft-ethics-guidelines-trustworthy-ai. At page 17, robustness is defined as follows: "Trustworthy AI requires that algorithms are secure, reliable as well as robust enough to deal with errors or inconsistencies during the design, development, execution, deployment and use phase of the AI system, and to adequately cope with erroneous outcomes."

11. Ibid.


15. Ibid.


17. Chris Hannay, "Artist faces lawsuit over computer system that creates randomly generated images" (4 October 2018), The Globe and Mail, online: https://www.theglobeandmail.com/arts/art-and-architecture/article-artist-faces-lawsuit-over-computer-system-that-creates-randomly/

18. Ibid.

19. Ibid.

20. Ibid.

21. Patrick Gillespie, "When AI writes the Court Ruling" (29 October 2018), Bloomberg Businessweek.

22. Ibid.

23. Ibid.


30. Mike Allen and Ina Fried, "Apple CEO Tim Cook calls new regulations "inevitable"" (18 November 2018), Axios, online: https://www.axios.com/axios-on-hbo-tim-cook-interview-apple-regulation-6a35ff64-75a3-4e91-986c-f281c0615ac2.html


34. Personal Information Protection and Electronic Documents Act, SC 2000, c 5, s 2(1).


36. McAfee & Brynjolfsson, supra note 6 at 85.

37. David Meyer, "A strict regulatory regime may promote public confidence in the use of technology but it might also be seen as an impediment to innovation and progress" (25 May 2018), Fortune, online: http://fortune.com/2018/05/25/ai-machine-learning-privacy-gdpr/

38. CED 4th (online), Torts, "Principles of Liability: Standard of Liability: Strict Liability" (II.1.(c)) at §18.


40. Ibid at 197.


42. Murawski, supra note 7.


46. Dave Gershgorn, "Microsoft warned investors that biased or flawed AI could hurt the company's image" (5 February 2019), Quartz, online: https://qz.com/1542377/microsoft-warned-investors-that-biased-or-flawed-ai-could-hurt-the-companys-image/

47. Spencer Bailey, "Designed by A.I.: Your Next Couch, Sweater, and Set of Golf Clubs" (15 February 2019), Fortune, online: http://fortune.com/2019/02/15/artificial-intelligence-ai-design/

NOT LEGAL ADVICE. Information made available on this website in any form is for information purposes only. It is not, and should not be taken as, legal advice. You should not rely on, or take or fail to take any action based upon this information. Never disregard professional legal advice or delay in seeking legal advice because of something you have read on this website. Gowling WLG professionals will be pleased to discuss resolutions to specific legal concerns you may have.
<table>
<thead>
<tr>
<th>Todd J. Burke</th>
<th>Scarlett Trazo</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Partner - Ottawa</strong></td>
<td><strong>Associate - Ottawa</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Email</strong></th>
<th><strong>Email</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:todd.burke@gowlingwlg.com">todd.burke@gowlingwlg.com</a></td>
<td><a href="mailto:scarlett.trazo@gowlingwlg.com">scarlett.trazo@gowlingwlg.com</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Phone</strong></th>
<th><strong>Phone</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>+1 613-786-0226</td>
<td>+1 613-786-3250</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>vCard</strong></th>
<th><strong>vCard</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Todd J. Burke</td>
<td>Scarlett Trazo</td>
</tr>
</tbody>
</table>