

Implementing Artificial Intelligence:

Lessons from the Trenches

by Karl Schober, Jawaid Panjwani, Ryan Middleton,
Tracy Molino and Chloe Snider



Artificial intelligence (AI) is the simulation of human intelligence processes by machines, including learning (the acquisition of information and rules for using the information), reasoning (using rules to reach approximate or definite conclusions), and self-correction. AI promises substantial benefits to businesses and organizations. Organizations that develop and commercialize AI will likely have significant advantages in an increasingly digital world. AI technologies can improve operations, enhance productivity, and ultimately increase their bottom line.

At the same time, AI applications can pose potentially significant risks for businesses and industry sectors:

- AI-enabled automation threatens to disrupt labour markets and employment;
- Predictive analytics in finance, education, policing and other sectors can reinforce racial, gender and class biases; and
- Data used in AI development and applications are often collected in ways that may violate privacy laws or compromise the accuracy of AI outcomes.

Furthermore, a number of sectors and industries exploring the adoption of AI technologies often have no prior experience with data or data-driven technologies. As both public and private entities contemplate the various implications of AI in the context of their activities, there are a number of considerations and best practices to keep top of mind. Among these are:

- **Algorithmic transparency:** Many AI techniques are “black box” models, meaning it is difficult to relate the input data and variables to the outcome. This is a major disadvantage, as it is difficult to explain to stakeholders, including regulators, how the outcome was actually achieved. For instance, where the AI is used to make a decision (e.g., extend credit or not, hire someone or not), a “black box” model does not allow an organization to defend itself against allegations of bias or demonstrate why the model is accurate. Using a more transparent model provides significant advantages, including the ability to demonstrate to stakeholders that the model is accurate. In addition, a well-trained,

transparent model is often easier to implement, and requires less computing power and, perhaps, even less data to train than black box models

- **Documentation:** It is vital to document all stages of the AI process, as data science is not an exact art, and any two data scientists will take different approaches to the same problem due to their differing experience and knowledge. Proper documentation helps ensure seamless transitions between those working on a given project, as well as provides for higher quality peer review.
- **Verification of data quantity and quality:**
A minimum quantity of data is required to achieve statistical significance at certain confidence intervals, but too much data can create “analysis paralysis.” Laying out a clear plan at the beginning of data projects will help avoid work that is ultimately not useful. In addition, poor-quality data will only lead to serious errors. Investing time and effort to understand the data properly at the outset – verifying the source, checking missing values, identifying biases, and noting any anomalies – is likely to pay dividends in the form of better quality and more targeted results.
- **Fostering a data culture:** A business should not tackle a data project in isolation. Executive engagement and corporate communication are essential to determine the problems that require solving, set out the metrics that define a project’s success, and manage stakeholder expectations. Data scientists, business people and staff need to communicate to understand the challenges of working with data, and what is possible and what is not.
- **Ascertaining copyright:** Before using data, confirm that you have the necessary rights. If a third-party service provider generated the analysis based on your core samples or other property belonging to you, be sure to check the intellectual property clause in your contract. In the case of public sources, check the terms of service for the database, or the website from which the data was obtained to see what is and is not permitted.
- **Respecting confidentiality:** If the data was obtained from a third party, or created in partnership with another company, such as in the context of an option agreement or a joint venture, review your contractual arrangements to confirm whether they require the other party’s consent before giving access to an outside AI service provider.
- **Allocating responsibility for analysis:** If the results of the analysis are not up to par, it is important to know who is responsible for making it right. When signing a contract for AI services, responsibility for each part of the job—selecting the data, preparing it for analysis, interpreting the results, and so on—has to be clearly stated. That way, once the source of the problem has been identified, it will be easier to determine who has the burden of addressing it.
- **Training employees:** Ensure that you properly train your staff. They need to understand the software’s functionality and limitations to use it properly.
- **Solving the right problem:** Once you have seen AI in action, it can be easy to view data as the answer to all of your business challenges. Avoid the trap of throwing data science at every problem. Sometimes the simplest, non-data solution is actually the right one. Data science is best used under certain specific conditions, such as abundant data, repetitive and measurable processes that can be observed over time, and a real problem that makes a real difference to the end user or business partner.

- **Regular re-evaluation:** The process of deriving benefits from AI does not end when an insight is generated, or a predictive model is built. It is essential to check accuracy against real-world results. Discrepancies can occur for a multitude of reasons: initial conditions could vary from the original data, or a key variable may have been omitted unknowingly from the original analysis. In some cases, the very fact of measuring and predicting can change the outcomes (very common when making predictions about human behaviour). Constant monitoring is vital to ensuring the work remains relevant, useful and accurate.



Organizations that develop and commercialize AI will likely have significant advantages in an increasingly digital world.

The use, value and application of AI will differ by sector or industry, but there are also key commonalities. Many sectors and industries will face opportunities and challenges, including difficulty gathering consistently high-quality data to develop models; industry culture resisting the adoption of AI; reluctance to invest in AI because initial adoption often involves impacts to daily operations and does not yield immediate returns for shareholders; and the high cost of integrating new or upgrading existing technology. Some sectors, such as the mining sector, will generally not be interested in data sets that contain personal information, and as a result, are free from many of the privacy concerns and restrictions facing companies in other sectors such as retail where certain data containing personal information is highly valuable. AI is becoming a powerful tool for analyzing data in operations, ranging from managing transport and logistics, to human resources and supply chain management. AI can identify patterns that are useful in reducing expenses, optimizing resources, reducing waste, improving planning, and increasing return on investment. In short, AI can enable companies of all types to become insight-driven enterprises.



A version of this article also appears in the Dentons Data Summit 2019 Whitepaper. The full Data Summit report is available at <https://www.dentons.com/en/insights/guides-reports-and-whitepapers/2019/november/29/dentons-data-summit-2019-whitepaper>

Jawaid Panjwani is a partner in Dentons Regulatory, Privacy and Cybersecurity, and Transformative Technologies practice groups. Based in Ottawa, he practices regulatory and corporate law with a strong focus on the communications, technology and digital media sectors. He provides advice to national and international organizations, including telecommunications and technology companies, cloud storage service providers and digital media companies. He also has worked with satellite operators that provide communications and earth observation (big data) services to navigate ISED's licensing procedures and requirements, and advises clients on privacy matters related to mobile applications, Internet search, online advertising, e-commerce, social media, data security, encryption technology, cross-border data transfers and cloud computing and lawful access issues.

Karl Schoeber is a Senior Associate with Dentons' Privacy and Cybersecurity group, and Transformative Technologies and Data Strategy practice. He is a former officer with the Office of the Privacy Commissioner of Canada, as well with the Competition Bureau. He provides advice on all matters related to privacy law and data governance in the emerging technology sphere, including wearable devices, smart homes, connected and autonomous vehicles, smart cities and the Internet of Things. Karl is a distinguished international speaker, and writes about developments and tips on privacy, as well as anti-spam issues.

Chloe Snider is a partner in Dentons Litigation and Disputes and Transformative Technologies groups in Toronto. A prolific writer, she has authored articles on contact tracing apps, privacy risk, data breach liability and crypto exchanges among many other topics. She is a co-author, along with Karl Schoeber and others of a Dentons Privacy and Data Toolkit to help businesses restart during COVID-19 economic recovery.

Ryan Middleton is a Partner in Dentons Toronto office. His expertise is in the areas of banking and finance. He has been recognized as one of Canada's leading banking lawyers. He has written frequently on issues related to crypto currencies, blockchain, and smart contracts.

Tracy Molino is Counsel in Dentons Banking and finance Group in Toronto. She is an expert in payments law and technology and consumer protection issues, with a keen interest in FinTech, PayTech, blockchain, crypto currencies and other innovative technologies. She previously worked as a director at Payments Canada where she supported efforts to modernize Canada's national payments system, and was senior counsel at the Bank of Montreal.



See <https://www.dentons.com/en/insights/guides-reports-and-whitepapers/2020/may/22/dentons-data-covid-19-restarting-your-business-privacy-and-data-toolkit>