Embracing AI

A review of the legal and policy considerations that will shape the development of artificial intelligence

After decades of promise and false starts, the right combination of computer processing power, data availability and engineering methods has produced a sudden surge of progress in the development of artificial intelligence (AI). Twenty years after Deep Blue, the IBM supercomputer, defeated world chess champion, Garry Kasparov, AI is no longer relegated to the world of proofs of concept and marketing curiosities.

Information technology companies are now spending billions of dollars a year to build large-scale, operational AI systems with applications and implications for almost every industry. The public is generally unaware of how rapidly AI has been adopted in only the past three years. To highlight the surprising breadth of already in-use applications, this article presents a cross-industry survey of AI.

The current and future benefits of AI are immense, but as people begin to realize how pervasive AI is becoming, there is the potential for misunderstanding, distrust and even fear of the technology. It is reasonable to consider the issues that will arise as AI interacts with and even changes society. Interestingly, despite the fact that it is (and will be) used in a range of diverse and unrelated industries, the concerns raised by AI tend to be the same: transparency, accountability, privacy, security and sustainability.

Policymakers and the legal system should anticipate that AI will soon raise novel issues and begin to prepare thoughtful, forward-looking and deliberative responses. Otherwise, the time will soon come when the rapid development of the technology will force hasty decisions that either inadequately address the underlying issues, stifle innovation or create additional issues and concerns. Accordingly, after the survey of AI uses and the discussion of common concerns, this article concludes with suggested principles for AI governance that should allow the technology to flourish while addressing legitimate concerns with its use.

LAYERS OF LEARNING

The term "artificial intelligence" has existed since the 1950s, but confusion over what AI is (and is not), is common. In part due to pop-culture and science fiction, AI is sometimes assumed to refer only to fully autonomous systems that think and behave like humans—to the point of being indistinguishable. That type of AI, called general AI, is still many years from reality. Narrow AI, on the other hand, is the use of purpose-built computer systems that have the ability to make independent decisions in a specific operating environment.

> "The concerns raised by AI tend to be the same: transparency, accountability, privacy, security and sustainability.

Deep Blue is a perfect (though dated) example of narrow AI. The system could generate independent decisions as to what chess piece to move each turn. In that one task—playing chess—Deep Blue was the best mind in the world. But that intelligence could not easily be applied to other tasks: It would be futile, for example, to ask Deep Blue to act as a language translator. What made Deep Blue a breakthrough, however, was that its individual chess-move decisions were not the result of a computer following pre-coded "if–then" steps.

At the core of all computer programs are algorithms, which are the instructions that control the program's operations. Designed to follow a set of discrete steps from beginning to end, early algorithms were able to act based only on clearly defined data and variables. Those algorithms were inherently limited by the ability of programmers to parse data using relatively underpowered computing systems. The breathtaking expansion in the sheer volume of digital data—from email and the early web to social media and streaming entertainment—required engineers to develop new techniques to store, categorize and analyze information.

A useful, though perhaps oversimplified, way to understand the challenge facing analysts is that the existing algorithms required developers to know in advance what relationships the system should look for and compare within the available data. Because available data sets have grown so large, and the potential variables for study so vast, it has become nearly impossible for programmers to predict the connections that may exist within the data. One method engineers have developed to deal with the analytical challenge of "Big Data" is to let the algorithms themselves determine which information would be useful to analyze.

Machine learning, in general, is when computer programs are designed to change in response to new data. Machine learning is a collection of three overlapping and related techniques: supervised learning; unsupervised learning; and deep learning. In supervised learning, a computer system is asked to make a narrow range of decisions based on curated inputs, and the results are evaluated by humans.

For example, to use supervised learning to train a computer to identify pictures of cats, developers provide the system with a database filled with thousands of pictures of cats. After the system builds a baseline model, it is tested against a new database of pictures—some of cats but many of other animals or objects—and the program is asked to identify whether each is or is not a cat. By feeding both right and wrong answers back into the system, the developers allow it to learn the characteristics of a cat without providing specific rules (e.g., "cats have whiskers" or "cats have four legs").

A curated database of pictures, as in the example above, is a type of structured data. The algorithm was looking for a specific relationship among data that were already categorized and formatted. Unsupervised learning, in contrast, is when an algorithm is provided with unstructured data—data that is not labeled, formatted or categorized—and it is allowed to discover any relationships that may exist. With unsupervised learning, a system is able to detect and learn from patterns in data pools that would be too vast for a human to analyze in advance.

Creating AI is a process of building or layering learning cycles. Deep learning is when several algorithms are allowed to engage in parallel unsupervised learning, each programed to look for different types of patterns. When deep learning is combined with massive data sets and numerous learning cycles, the result is a system that is no longer strictly bound by its coding. AI, then, is a computer algorithm that can make decisions that are not directly derived from instructions, incorporate new and unstructured data, learn and update its decision-making based on the new data and, in general, can perform tasks that previously required human intelligence.

THE AI MOMENT

The seemingly sudden improvements in AI over the past few years are the result of a combination of advances in computer hardware, distributed processing, programming methods and availability of data. The increased use of social media, mobile phones, connected devices and streaming media give AI developers vast amounts of training material. Without this data, deep learning would be impossible and AI would be far less powerful. Famously, Google's Peter Norvig said: "We don't have better algorithms. We just have more data."

The relative availability of the power, programming and data necessary for AI has touched off something of an arms race. Technology companies, along with businesses that could benefit from AI applications, are pouring billions of dollars into acquisitions, research and investment. Worldwide spending on AI systems is forecasted to reach almost US$60 billion by 2021.[1]

> “
> **Worldwide spending on AI systems is forecasted to reach almost US$60 billion by 2021.**

The competition to develop and provide AI has increased dramatically. In 2015, there was less than US$1 billion in global merger and acquisition (M&A) activity related to AI, rising to approximately US$4 billion in 2016. Then, in 2017, AI-related M&A activity jumped to nearly US$22 billion dollars.[2]

The focus on AI development likely will continue to intensify, and AI will be found in many of the products and services people use regularly. AI is already more common than most realize, and 2018 may be the year that AI becomes ubiquitous. Now is the time to consider what it will mean to live in a society where technology makes decisions that may fundamentally alter our lives.

UNSEEN BUT NOT UNKNOWN

It is important to emphasize how widespread AI usage is and will be in the near future. The variety of applications is staggering, and today's implementations likely represent only a fraction of the full potential. AI is already being used in transportation, financial services, cybersecurity, energy management, healthcare and consumer devices. A full discussion of AI use in any one sector could fill an entire article; thus, this survey will provide an overview of and insights into the tremendous benefits provided by AI in each of these areas.

Transportation

One of the first, and best known, examples of AI in a consumer product is the development of self-driving cars—alternatively known as smart cars or autonomous vehicles. Waymo, Google's efforts to develop a self-driving car, dates back to 2009. Autonomous driving technology relies on AI to process and respond to information gathered by tools such as long-range radar, cameras, ultrasonic sensors and onboard GPS. AI is the essential component of the system, processing data from the sensors more quickly and accurately than a human could. The AI behind autonomous vehicles has been trained by driving millions of collective miles with humans guiding the process. Now, after nearly a decade of development, self-driving cars are taking test runs on public roads without a driver directly behind the wheel. Although AI has already proven itself to be safer than human drivers, many people still express skepticism over relinquishing control of their car.[3] Tesla's Autopilot, which is nearly autonomous but requires drivers to maintain awareness, is already fully operational and in use. Meanwhile, trucking companies have successfully run numerous tests on public roads where a platoon of several autonomous vehicles follows behind a single human-driven truck.

Consumer devices

Aside from self-driving cars, the general public is probably most familiar with AI-based smart assistants found across a variety of consumer devices. Apple's Siri and Google's Assistant are now core components of each company's mobile phone operating system. The voice component of these assistants is the interface of a complex system that combines multiple AI functions. For example, a smart assistant is able to understand verbal requests thanks to AI specializing in natural language processing (NLP). AI does not learn human language through programming grammar rules and vocabulary; rather, NLP is the result of training the system with billions of actual conversations.[4] When a smart assistant gives a user directions to a new restaurant, the route is designed by an AI that compares current traffic data to the patterns it learned by analyzing millions of previous trips.

Although smart assistants started on mobile phones, they have become stand-alone devices. Amazon's Echo (with Alexa AI) and Google's Home (with Google Assistant) went from rare novelty to almost commonplace in less than two years. These devices perform the same functions as phone-based AI, but can also connect with in-home climate controls, lighting, entertainment, and security systems. By the end of 2017, approximately 20 percent of US households had at least one AI-powered smart home device.[5] Other companies, including Microsoft, Apple and Samsung, all have AI- powered consumer devices coming to market during 2018.

Financial services

Banks and other financial services companies have been using AI in various capacities for several years. AI has powered high-frequency trading systems for some time, and at least one hedge fund uses AI to execute all of its trades without human intervention. More recently, banks and payments companies, such as PayPal, have begun using AI systems to detect fraudulent account activity and suspicious transactions. According to PayPal, its system can analyze more information and identify more sophisticated patterns than non-AI systems, reducing the number of false positives and avoiding situations in which legitimate customer transactions and accounts are blocked.

Banks and lenders are already using AI to better evaluate potential borrowers, particularly in areas such as small business loans where standard models are unable to draw inferences from non-traditional data sources. In addition, financial services firms are actively exploring ways for AI to manage their customer relationships, including hyper-personalization of products and customer service platforms.

Financial institutions (and regulated entities of all types) are also hopeful that AI will improve the systems used to comply with government regulations (regtech), such as in the area of compliance with anti-money laundering and sanctions laws and regulations. The common thread in all of these applications is cost: banks and financial institutions are focusing their efforts on places where AI is better, faster and cheaper than existing systems.

Cybersecurity

Cybersecurity was one of the first internal applications of AI to be adopted across industries. Systems using AI that is trained to monitor network events and detect attacks and intrusions have already proven to be invaluable.[6] Commercially available programs are able to process data from a variety of sources and analyze events simultaneously, improving both accuracy and efficiency. While this may seem similar to previous methods for providing network security, an AI-based system can simultaneously monitor unstructured information posted on millions of websites to identify and model emerging threats and then compare those models to internal network traffic across thousands of machines. Humans simply cannot match the power of AI in cybersecurity, and the technology will likely continue to be adopted at an increasing rate.[7] It is worth noting that the good guys are not the only ones with access to AI. Cyber attackers are also harnessing the technology, meaning AI is fast becoming a necessary component of every company's security system to counter such threats.

Energy management

As energy production becomes more widely distributed through the increased use of photovoltaic (solar) and wind generation, smart energy management using AI is helping to reduce the amount of energy lost in transmission. AI is already being used to optimize power generation—even in the fossil fuel plants that supply the majority of the baseload—to match daily cyclical demand. AI is also a major component of smart grids that can modify the flow of energy to account for variable inputs (such as roof-top solar) and sudden outages. Companies are also looking for AI to reduce their energy consumption, particularly in electricity-intensive industries, such as data processing. In aggregate, computer data centers are estimated to account for two percent of total global electricity usage.[8] Google, for example, is already using its DeepMind AI in conjunction with a data center intelligence team to reduce the amount of energy used for cooling by 40 percent.

Healthcare

Radiologists and other physicians now routinely use computer-aided diagnosis (CAD) systems, AI-based programs that process and analyze medical images, to assist in the detection of tumors and other lesions.[9] In particular, CAD can both highlight atypical lesions that physicians may fail to detect and provide a "second opinion" to help assist with medical imaging interpretation and diagnosis. Engineers working with Google's DeepMind have similarly demonstrated that AI can be used to scan images of patients' retinas to detect diabetic retinopathy.[10]

In addition to clinical imaging analysis, other AI-driven programs are aimed at improving treatment and care. A DeepMind-powered application is already in use at Royal Free London hospital to identify acute kidney injury (AKI). AI has proved more effective at noticing subtle indicators of AKI in patient vital signs than human caregivers.[11] After reviewing the medical records of 1,000 cancer patients at the University of North Carolina School of Medicine, IBM's Watson for Oncology was able to recommend treatment plans that concurred with oncologists' actual recommendations in 99 percent of

> **"For companies that choose to provide AI enabled products and services, it is important to recognize that the apparent autonomy of AI does not shield them from the liability of their own choices.**

For AI to gain large scale acceptance, it will need to be better than both humans and existing technology at identifying and removing bias. Transparency and the ability to audit AI are important factors for developers to highlight as they work towards these goals.

cases.[12] In addition, because Watson for Oncology was able to process patient data and current cancer research almost simultaneously, it was able to recommend additional treatment options missed by physicians in 30 percent of cases.

COMMON CONCERNS ACROSS AI IMPLEMENTATIONS

The various uses discussed above are a sample of already operational AI, but represent only a tiny fraction of AI that will soon interact with people on a daily basis. To be sure, the power and possibilities of AI are amazing, but its growing use raises legitimate concerns. Companies developing and implementing AI should be aware of these concerns and find suitable solutions to ensure continued adoption and acceptance of their technologies.

Accountability

Once it is acknowledged that AI makes independent decisions, the first question that follows is: Who is responsible for the results of those decisions? Is it possible to hold AI accountable? Although this concern takes different forms depending on the particular use, accountability is an issue for every current implementation of AI. Generally, accountability is the easiest concern to identify, understand, and probably to address.

Consider AI driving a car that incorrectly determines there is a hazard in the road, swerves quickly into the adjacent lane, and crashes into a human-driven car. Who is accountable for the AI's error? As discussed below, existing product liability laws are generally sufficient to handle such a relatively clear-cut example. Difficulties arise, however, when there is no evidence of AI error, or worse, when AI is caught in a dilemma of selecting one harm over another.

In medical applications, patients will understandably want to hold AI accountable if, for example, it fails to detect a tumor. But neither doctors nor their instruments are expected to perform flawlessly, and missing a diagnosis is not necessarily indicative of a fault in the system. Would a doctor be held to a different standard of accountability if AI was used to confirm a diagnosis that later turned out to be incorrect? Perhaps, in the near future, the reverse will be true, and doctors will be held to a higher standard of accountability if they choose not to use AI.

For companies that choose to provide AI-enabled products and services, it is important to recognize that the apparent autonomy of AI does not shield them from the liability of their own choices. Ultimately, every decision made by AI is the direct result of the programming and training provided by its developers. Over the long term, accountability will come from practices that ensure end-users can clearly identify the company that designed any given AI.

Transparency

An inherent difficulty of a system built specifically to identify patterns and relationships too subtle or complex for a human to perceive is that the reasoning behind any decision it makes may be incomprehensible or unknowable to those operating the AI. AI developed through unsupervised learning—particularly if it is provided with access to open sources of data, such as websites or social media—may have incorporated uncertain variables or false information. Developers will need to create ways to visualize the inner workings of the AI decision engine.

The lack of transparency can cause two related challenges: AI bias and inability to audit. Bias, a potential pitfall in any decision-making process, is when one potential option is given more weight or is more likely to be selected than it would be with a purely objective analysis. In AI terms, bias can be positive or negative, as well as intentional or unintentional. For example, AI for cybersecurity may be intentionally biased to decide that an observed pattern is a cyberattack, thereby creating more false positives. But unintentional bias can cause significant harm, too. The data used to train AI are selected by developers who—like all people—have their own biases. Unless programmers diligently test and screen training data for bias, AI will learn and act on such bias.

The potential to perpetuate patterns of bias is particularly high in applications that use historical human decisions to train the AI. For example, financial AI trained to make lending decisions could be fed 50 years' worth of mortgage data in a given region. The past approvals and denials, however, may reflect lending patterns that were the result of then-existing racial discrimination. If the AI learns that these historical patterns are "correct," it will continue to make biased and discriminatory (and illegal) lending decisions.

This type of bias could be especially damaging in cases where AI is used in a judicial context. Some courts have experimented with using AI to predict an offender's probable recidivism as part of the sentencing process. Unfortunately, data based on historical policing patterns incorporated racial disparities in enforcement, and AI trained on such data wrongly predicted higher recidivism rates for minorities.[13]

"Explainable AI" is the goal of being able to identify accurately the factors that produced a decision. Explainability is an area of intense research, and it comes under the umbrella of designing methods to audit AI.[14] Without the ability to audit the decision-making process, developers are unable to know whether bias or other errors have crept into the system. Traditional computer models have long aided decision-making, but the results of such models are constantly tested and the inputs are adjusted accordingly. For AI to gain large-scale acceptance, it will need to be better than both humans and existing technology at identifying and removing bias. Transparency and the ability to audit AI are important factors for developers to highlight as they work towards these goals.

Privacy and security

What makes AI powerful may also be the source of public unease: data, and lots of it. As discussed above, large volumes of data are the key to training and improving AI. As a result, companies that develop and implement AI-powered solutions need a constant supply of new data. Depending on AI's purpose, the data involved is often considered sensitive or confidential. Moreover, AI-based products and services are designed to become progressively more personalized, which is only possible if the system constantly collects new data from the users themselves.

A self-driving car, for example, would learn the times and places where its owner travels—home, office, favorite restaurant, doctor's office, or an out-of-the-way bar—to better predict the routes it will take and the road conditions it will face. Will owners want their cars storing and learning that information? Will employees of the company have access? What about other family members? The challenge of privacy is even more acute with financial data. A bank could use AI to monitor a customer's account for potential fraud but, at the same time, learn customer's shopping, traveling and spending habits. Would customers want their bank to take notice of frequent trips to a home improvement store and respond with an offer for a home equity loan?

Most of the time, the data used to train AI is anonymized—personally identifiable information (PII), such as names, addresses and identification numbers are removed from the data set. However, as AI systems continue to aggregate data from multiple sources, it will soon become possible (and likely) for AI to have enough separate data points to determine the identity of the individual associated with a particular record.

Concerns regarding privacy are inseparable from issues of trust. Users of AI must be able to trust the companies that develop the system. This includes trust that their private medical history will not be shared by AI analyzing their MRI; trust that their photographs will not be made public by AI scanning for facial recognition; and trust that their smart home device will not eavesdrop on what is said inside their home. A delicate balance must be struck between privacy and personalization, and individual users will need AI-based products and services that can adjust to their preferences and, in some cases, rights.

Layered over privacy concerns is the constant need to protect data that has been collected. Data-intensive applications are irresistible targets for cyber attackers and are also vulnerable to inadvertent security breaches. Large technology companies, financial institutions and medical facilities are already accustomed to protecting themselves—not always successfully—against daily intrusion attempts. As AI spreads to smaller companies and to industries that may not have developed robust cybersecurity standards, there will be more exploitable vulnerabilities for hackers to access personal data.

> “
> **A delicate balance must be struck between privacy and personalization, and individual users will need AI-based products and services that can adjust to their preferences and, in some cases, rights.**

There are, of course, methods to secure the data powering AI, including encryption, multi-factor authentication and location-based authentication. Companies developing AI will need to ensure security protocols advance as quickly as technology.

Sustainability

There is, for some people, a persistent worry concerning how AI will affect the social and economic order. The concern is not the theatrical fear of AI destroying humanity—although there are those who genuinely predict such an apocalyptic outcome—but rather, one that is more practical, mundane and, paradoxically, more consequential. Will AI take my job? Will AI replace human intelligence to the point that society begins to lose knowledge? On the one hand, it is easy to dismiss these as the fears of luddites railing against the fabric mills. On the other hand, unlike previous technological revolutions, AI can replace thinking itself, and the potential for displacing workers is vastly larger.

For society to continue to support AI innovation and expansion, developers need to address sustainability head-on. AI implementations can, in some cases, increase employment in a given business. For example, a financial institution that uses AI to reduce the manual burden of regulatory compliance filings can free up resources for more productive purposes. An energy company that deploys AI to more efficiently route power from diffuse generation sources can trigger an increase in small-scale photovoltaic installations. By focusing on opportunities for AI to augment human productivity rather than replace it, developers can help AI achieve a sustainable relationship with society.

POLICY AND PRINCIPLES

Policymakers have an important role not only in addressing the concerns associated with the increasing use of AI, but also in creating an environment where the technology itself can flourish. As one technology company put it, "[o]versight by regulators will be essential for society to trust AI."[15] But oversight can take many forms, and policymakers should establish a governance framework that fosters trust without dampening innovation. Ideally, a governance framework would incorporate the following principles:

Provide clarity

Technology changes and progresses more quickly than laws and policies. When officials are asked to address AI-related issues—for example, whether it is legal in a given state to operate a self-driving vehicle—it may take months (or years) to provide a regulatory response. Policymakers should clearly communicate to developers and the public what AI issues are under consideration, any additional information needed to address such issues and the status of each pending answer. New laws, regulations, or guidance should aim to provide clarity and certainty, rather than to cover every possible scenario with potentially vague language.

Use existing tools
The technology is new, but the potential concerns are not. Privacy, data security and liability are already addressed by existing laws. Although the context may be different, regulators should seek to use available tools for AI oversight. This approach is faster to implement than attempting to create AI-specific laws, but more importantly, it ensures a familiar legal framework that has already been subject to regulatory and judicial interpretation.

Application neutral
When policymakers need to implement AI-specific regulations, they should avoid doing so by targeting particular implementations of AI (e.g., AI in mobile phones or AI in medical scanners). Instead, they should identify the underlying process or procedure at issue and create a rule that applies consistently across all AI applications. As AI advances and blurs the distinctions among its various uses, it will be increasingly important to avoid a fragmented AI governance framework.

Lead by example
Policymakers should serve as an example to the public and developers. For the public, governments can show that AI-based systems can increase efficiency, improve quality and reduce costs. For companies developing AI-based products and services, policymakers can model appropriate AI implementations by including privacy controls, cybersecurity protections, as well as bias screening, testing and auditing procedures.

Encourage responsible innovation
Governments should work with technology companies that are engaging in responsible experimentation and innovation. Policymakers are uniquely positioned to allow AI to be tested in open, yet controlled environments. The program for autonomous vehicles, which has ten sites around the country designated as official proving grounds, should be replicated for other AI applications. In addition, governments should partner with companies that are demonstrating a responsible approach to promote best practices and help create sound AI standards.■

> **By focusing on opportunities for AI to augment human productivity rather than replace it, developers can help AI achieve a sustainable relationship with society.**

ENDNOTES

1 *Spending Guide Forecasts Worldwide Spending on Cognitive and Artificial Intelligence Systems to Reach $57.6 Billion in 2021,* International Data Corporation (IDC) (Sep. 25, 2017), https://www.idc.com/getdoc.jsp?containerId=prUS43095417.

2 *Google Leads in the Race to Dominate Artificial Intelligence,* The Economist (Dec. 7, 2017), https://www.economist.com/news/business/21732125-tech-giants-are-investing-billions-transformative-technology-google-leads-race.

3 John R. Quain, *Skeptics of Self-Driving Cars Span Generations,* The New York Times (Jun. 16, 2016), https://www.nytimes.com/2016/06/17/automobiles/wheels/skeptics-of-self-driving-cars-span-generations.html.

4 Gideon Lewis-Kraus, *The Great A.I. Awakening,* The New York Times Magazine (Dec. 14, 2016), https://www.nytimes.com/2016/12/14/magazine/the-great-ai-awakening.html.

5 RJ Reinhart, *Most Americans Already Using Artificial Intelligence Products,* Gallup (Mar. 6, 2018), http://news.gallup.com/poll/228497/americans-already-using-artificial-intelligence-products.aspx.

6 *See* Alex Konrad, *IBM Turns Watson Into a Cybersecurity Weapon Amid White House Interest,* Forbes (Feb. 13, 2017), https://www.forbes.com/sites/alexkonrad/2017/02/13/ibm-turns-watson-to-cyber-security; see also Avneet Pannu, *Artificial Intelligence and its Application in Different Areas,* International Journal of Engineering and Innovative Technology, Vol. 4, Issue 10 (April 2015) at 79, 81, http://www.ijeit.com/Vol%204/Issue%2010/IJEIT1412201504_15.pdf.

7 IBM Press Release, *IBM Delivers Watson for Cyber Security to Power Cognitive Security Operations Centers* (Feb. 13, 2017) (predicting that the percentage of security professionals using cognitive will triple from the current rate of seven percent over the next 2-3 years), https://www-03.ibm.com/press/us/en/pressrelease/51577.wss.

8 Google Environment, *Machine learning finds new ways for our data centers to save energy,* https://environment.google/projects/machine-learning.

9 *See* Junji Shiraishi, Ph.D., Qiang Li, Ph.D., Daniel Appelbaum, MD, Kunio Doi, Ph.D., *Computer-Aided Diagnosis and Artificial Intelligence in Clinical Imaging,* Seminars in Nuclear Medicine, Vol. 41, Issue 6, 449-462 (Nov. 2011); *Computer Technology Helps Radiologists Spot Overlooked Small Breast Cancers,* Oncology, Vol. 14, Issue 10 (Oct. 1, 2000), http://www.cancernetwork.com/articles/computer-technology-helps-radiologists-spot-overlooked-small-breast-cancers.

10 Lily Peng, MD, Ph.D., Varun Gulshan, Ph.D., *Deep Learning for Detection of Diabetic Eye Disease,* Google Research Blog (Nov. 29, 2016), https://research.googleblog.com/2016/11/deep-learning-for-detection-of-diabetic.html.

11 Royal Free London NHS Foundation Trust Press Release, *New App Helping to Improve Patient Care* (Feb. 27, 2017), https://www.royalfree.nhs.uk/news-media/news/new-app-helping-to-improve-patient-care.

12 Danny Vena, *IBM's Watson is Tackling Healthcare with Artificial Intelligence,* The Motley Fool (Mar. 19, 2017), https://www.fool.com/investing/2017/03/19/ibms-watson-is-tackling-healthcare-with-artificial.aspx.

13 Julia Angwin, Jeff Larson, Surya Mattu, Lauren Kirchner, *Machine Bias,* ProPublica (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

14 *See* Ariel Bleicher, *Demystifying The Black Box That Is AI,* Scientific American (Aug. 9, 2017), https://www.scientificamerican.com/article/demystifying-the-black-box-that-is-ai/; Deborah Santiago, Teresa Escrig, *Why Explainable AI Must Be Central to Responsible AI,* Accenture Blog (Jul. 28, 2017), https://www.accenture.com/us-en/blogs/blogs-why-explainable-ai-must-central-responsible-ai.

15 Dr. Naveen Rao, *Artificial Intelligence: The Public Policy Opportunity,* Intel Corporation (Oct. 18, 2017), https://blogs.intel.com/policy/files/2017/10/Intel-Artificial-Intelligence-Public-Policy-White-Paper-2017.pdf.

Contacts

Kevin Petrasic
Partner, Washington, DC

T +1 202 626 3671
E kevin.petrasic@whitecase.com

Benjamin Saul
Partner, Washington, DC

T +1 202 626 3665
E benjamin.saul@whitecase.com

Max Bonici
Associate, Washington, DC

T +1 202 626 3589
E max.bonici@whitecase.com

whitecase.com

In this publication, White & Case means the international legal practice comprising White & Case LLP, a New York State registered limited liability partnership, White & Case LLP, a limited liability partnership incorporated under English law and all other affiliated partnerships, companies and entities.

Attorney Advertising. Prior results do not guarantee a similar outcome.