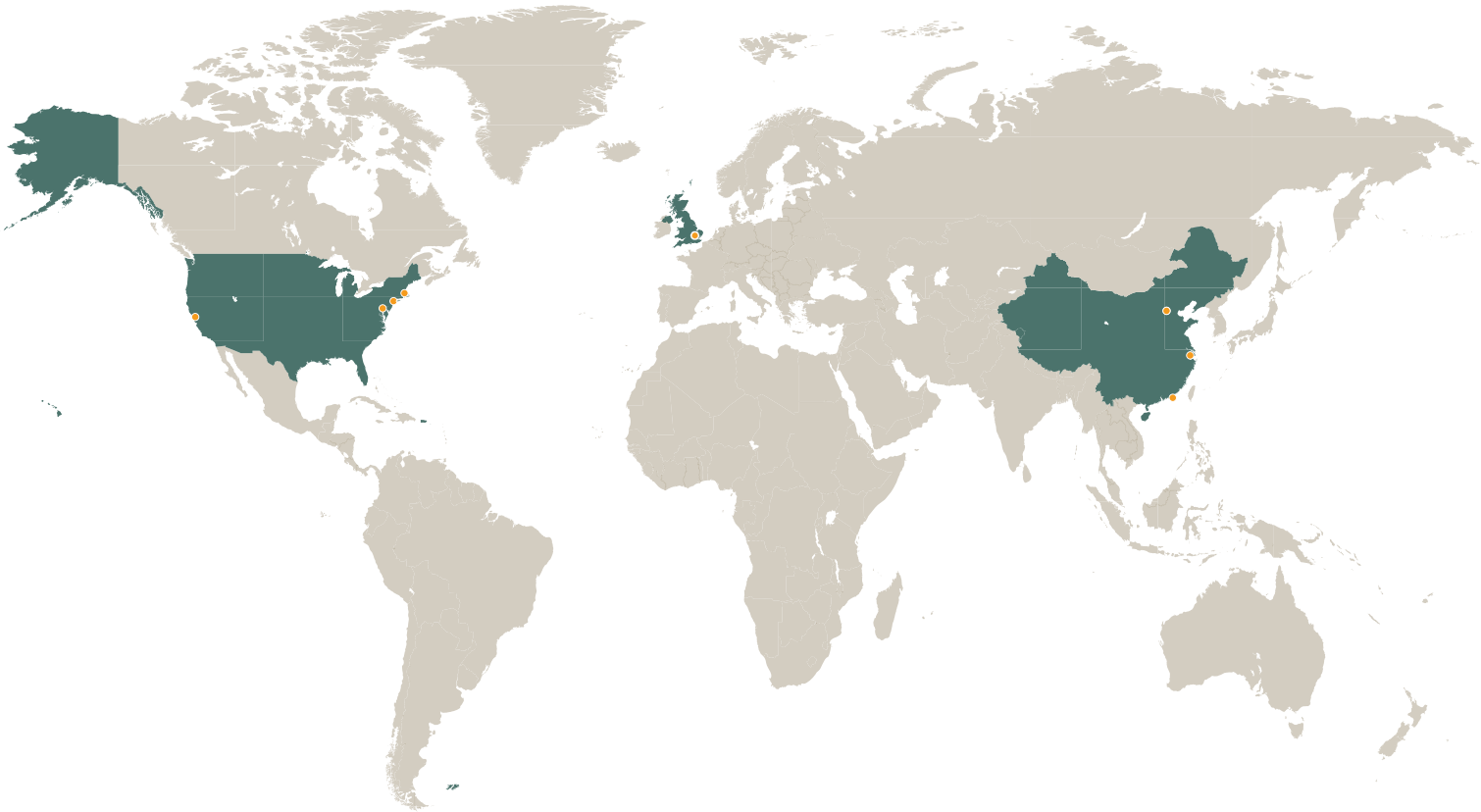
Hogan Lovells

# Artificial Intelligence and your business: A guide for navigating the legal, policy, commercial, and strategic challenges ahead

November 2018

# Global hotspots



## Silicon Valley

— Top global hub for startups with 12,000+ active startup businesses

— Global leader for venture capital (VC) investment

— Headquarters of many top high-tech companies

## Washington, D.C.

— Leading center for U.S. policy and regulation of Artificial Intelligence (AI), including health, automotive, space, drones, and education

## London

— Global finance center, supporting both investment and FinTech applications

— European leader of VC startup investments

## New York

— Leading hub for financial and media industries

— Strong funding ecosystem, second in the world after Silicon Valley for absolute number of early stage investments

## Boston

— Long history of cooperation between science and industry

— World-class universities such as MIT developing advanced technologies and providing a talent pipeline

## China

— Leading in volume of academic research output in AI coming from universities

— AI identified as a strategically important technology by the Chinese government

Contributing source: *Artificial Intelligence The Next Digital Frontier?*, McKinsey Global Institute, 2017

# What is Artificial Intelligence?

Virtually every industry is being reshaped with the use of Artificial Intelligence (AI) and advanced machine-learning, ranging from healthtech to self-driving vehicles, to education and smart homes, drones and space, social media, and everything in between and beyond. These new technologies present a variety of commercial opportunities and the potential to change our daily lives.

At the same time, new AI innovations bring many legal, policy, commercial, and strategic challenges that need to be considered thoughtfully across jurisdictions. In some instances, existing frameworks can be applied or adapted. For others, new paradigms and robust safeguards may be needed. And as machine-learning technologies continue to evolve, organizations will need dynamic, sophisticated compliance approaches.

In this guide, we highlight several of the key challenges and commercial opportunities for AI and advanced machine-learning.



Randy Segal
Partner, Northern Virginia, Silicon Valley, Washington, D.C.
T +1 703 610 6237
randy.segal@hoganlovells.com

Mark Brennan
Partner, Washington, D.C.
T +1 202 637 6409
mark.brennan@hoganlovells.com

Richard Diffenthal
Partner, London
T +44 20 7296 5868
richard.diffenthal@hoganlovells.com

# Unmanned Aircraft Systems (Drones)

Unmanned aircraft systems (UAS or drones) technology has moved forward rapidly in recent years, and what used to be considered toys are quickly becoming powerful commercial tools that can provide enormous benefits in terms of safety and efficiency. Consulting firms suggest that the estimated global market for commercial UAS technology applications currently stands at about US$2 billion, could increase to US$120 billion by 2020.

Advances in AI and machine-learning technology are allowing UAS to see and act like human pilots, and to process huge amounts of data in real time. Whether UAS are performing search and rescue missions, allowing farmers to be more efficient and environmentally friendly, inspecting power lines and cell towers, surveying and mapping large swaths of land, or performing package deliveries, AI is allowing drones to become more automated, safer, and efficient.

The applications for AI in the drone industry are limited only by our collective imagination. The use-cases range from data analytics for industrial infrastructure inspections to navigating warehouses efficiently and everything in between.

## Real-time data analytics

AI is allowing drones to collect and process huge volumes of data in real time. Aerial imagery that used to take humans hours, days, or weeks to review and analyze is being streamlined and automated by AI that strategically determines what kind of data and images are important enough to collect, and can simulate a human looking at thousands or millions of images. For example, drones being used to perform railway inspections can use a variety of onboard sensors (cameras) to inspect track conditions and identify defects that are invisible to the naked eye. Once detected, AI software can be used to provide recommendations on what, if any, maintenance may be necessary.

## Sense-and-avoid

A pilot manually flying a drone should be able to avoid obstacles like buildings or other aircraft; but what happens if a drone loses all connectivity? To fully enable many of tomorrow's most promising use-cases, drones will need to be capable of flying autonomously without human intervention, and this will require drones to be able to sense obstacles and react in time to avoid a collision. Computer vision, plus machine learning, is helping drones navigate more effectively by allowing drones to see the world as humans do. AI software is enabling drones to fly autonomously, even in the dark, obstacle-filled environments or beyond the reaches of GPS or other methods of connectivity.

## Swarm technology

AI technology is enabling swarms of tens or hundreds of drones to operate entirely autonomously. The swarm collaborates by staying in constant communication with itself and by changing its configuration to complete the mission if any one drone is lost.

## Situational awareness

AI is enabling better situational awareness and changing the way drones are able to interact with objects in their environment. In the not-too-distant future, AI technology will enable fully autonomous drone operations. Civil airworthiness authorities around the world maintain air safety by placing ultimate responsibility for safe operation of aircraft on the entity operating the aircraft and on the human pilot. Since fully autonomous drones will not have a human pilot, countries around the world will need to put in place policies, laws, and regulations that fully address this profound change.

## Lack of human judgment

Fully autonomous drones will raise important policy questions regarding the removal of human judgment from the equation. Human pilots make not only safety-related decisions, but in certain circumstances — especially emergencies — moral and ethical decisions, such as whether to crash land in a heavily populated area versus a less populated one. With the removal of the human pilot and human judgment, what level of AI will be needed for drones to learn from experience and use that learned knowledge to make appropriate moral and ethical judgments?

## Security

Who will have the legal responsibility to maintain the security of a fully autonomous drone, and to ensure that its automation, navigation, and communications systems are not hacked into?

## Regulatory and civil liability

What if something goes wrong with a fully autonomous drone? Who will be responsible from a regulatory compliance and civil liability perspective in the event of an incident involving personal injury or property damage, or a failure to comply with rules and regulations?

Lisa Ellman
Partner, Washington, D.C.
T +1 202 637 6934
lisa.ellman@hoganlovells.com

Matthew Clark
Senior Associate, Washington, D.C.
T +1 202 637 5430
matt.clark@hoganlovells.com

Gretchen West
Senior Advisor, Silicon Valley
T +1 650 463 4062
gretchen.west@hoganlovells.com

# Smart Homes

Today's designers of smart home systems can take advantage of ubiquitous broadband connectivity, which collects lots of data from a wide variety of sources, all of which can be fed into sophisticated algorithms that are very good at modeling and predicting human behavior. The past is prologue, and the future is bright for smart homes.

## Voice recognition

Another aspect of AI in smart homes is voice recognition. It is often said that AI is the new user interface. Rather than typing or clicking, we say or point. As we begin to implement home digital assistants, the true human interface to the world of computing will revolutionize how we interact with the everyday machines in our homes.

## Thermostats

Smart thermostats and similar devices are already a mature technology, going back to graduate-level AI research in the 1990s. In some ways, they are ideal for using most efficient AI techniques, especially unsupervised learning. As opposed to a hypothetical cat recognition machine, which learns from looking at millions of pictures that a human being has labeled as pictures of cats, all you need is the home occupant to lower the thermostat, and that will indicate to the system that the temperature was too high. The system then learns from that feedback. This is a key advantage.

An important drawback — as is true with most AI technology — is that full adoption is constrained by human expectations. The smart home systems on the market today — and certainly those coming in the near future — are fully capable of acting completely autonomously in making good decisions, for example, temperature or security features of our homes. But, we typically don't let them. All of those products come with configurable upper and lower temperature bounds outside which we don't trust the systems to go. In higher latitudes, we fear frozen pipes if our smart home turns out to be not so smart. In warmer climates, we envision pets suffering from a home that is not cool enough. As a result, human beings set those safety temperatures in unnecessarily narrow bands, eliminating much of the energy or cost savings that one would expect from investing into smart home technology. As AI technology becomes more known and pervasive, we will all become a lot more comfortable allowing these sophisticated algorithms to make these decisions, at which point the energy and costs savings will be truly realized.

## Lighting

Temperature control is just the beginning. Another technology with roots in the 1990s relates to smart lighting. Rather than reacting to a motion sensor to turn lights on, our smart homes will use the motions sensors to predict the occupant's path through a building, thus predicting where they will be in five or ten seconds from the present, turning the lights on and off accordingly. Also, the systems will make use of unstructured and unrelated data sources to make better decisions. For example, someone's work calendar alone may or may not give a good indication of when they'll be home. However, a combination of their calendar and social media feed, perhaps coupled with car navigation inputs, is likely to be spot on.

## Smart communities

Beyond our homes, these same AI techniques can be applied to our cities, communities, and even governments. Imagine a traffic light system that, instead of being pre-programmed, takes information from any number of different inputs to create a traffic flow that is optimized for that particular moment in time in that particular part of town. We have algorithms and data feeds to do that. Or, picture a community in which no one drives themselves because all the cars on the road are autonomous. We discuss the AI aspect of this technology elsewhere, but the impacts on the community will be tremendous. Just imagine a smart community that no longer needs 90 percent of its current parking lots, meters, or garages.

The idea of incorporating AI techniques to build smart homes is not new. As far back as 1995, researchers were publishing papers about topics like "Predictive Optimal Control Residential Heating Systems," which used neural network learning algorithms to predict the occupant's comings and goings, in order to minimize energy usage and maximize the occupants' comfort. Lucky Vidmar, a Hogan Lovells partner, was part of a team of graduate students who developed this project. They called it the Neurothermostat.

Lucky Vidmar
Partner, Denver and San Francisco
T +1 303 899 7328
lucky.vidmar@hoganlovells.com

Valerie Kenyon
Partner, London
T +44 20 7296 5521
valerie.kenyon@hoganlovells.com

"You may not realize it but AI is all around us."

*Judy Woodruff*

# Autonomous and Connected Vehicles

## Are you (still) in the driver's seat?

The automotive industry has evolved to be inclusive of both automobiles and the broader mobility sector in large part due to advancements in AI. This has led to an emphasis on technology, electrification, connectivity, and transportation shared services. As detailed in the January 2018 McKinsey report, "Autonomous driving…relies inherently on AI because it is the only technology that enables the reliable, real-time recognition of objects around the vehicle." and "…AI creates numerous opportunities to reduce costs, improve operations, and generate new revenue streams."

## Lots of opportunities, but also challenges

Vehicles have morphed from simply a means of personal transportation to multifunctional information centers that collect and communicate large volumes of data, such as position or driving behavior, to name a few. Along with benefits come challenges — including compliance with legal and regulatory obligations. New technologies also challenge pre-existing structures such as traditional insurance and liability systems. Legislative and regulatory changes are inevitable.

The modern motor vehicle is also increasingly connected. This enhances the vehicle's capacity and also allows the collection of data and the sale of services to vehicle occupants. The data and services are tantalizing new revenue streams.

## Less ownership, more usage

AI technologies integrated in vehicles will fundamentally alter not just the vehicle itself, but also the ownership model and enterprises engaged in the automotive industry. Many models have driver-assist technology giving the vehicle varying levels of semi-autonomous functionality. Electronics have become a significant part of the cost of a vehicle, and that percentage is likely to increase. On average, cars are driven under an hour a day, translating into US$20 trillion in assets, with a utilization rate of about 4 percent. If the driverless car is owned by car services and summoned on demand by those needing transportation services, the utilization rate could increase substantially and the cost would drop dramatically.

## No more human driver: a different perspective

Current regulatory structures and liability rules are based on the assumption of a human driver. Regulators will want to evaluate when humans drive and when the vehicle drives, and how that exchange occurs. Current safety rules are designed around crash survivability.

When vehicles seek to avoid accidents rather than survive them, the intellectual framework for the rules will need to shift. There will also be ethical challenges. Vehicles may require new certification procedures, as well as cybersecurity and data privacy protections given the connectivity. AI in connected and autonomous vehicles will require rethinking historical operating structures in the automotive industry.

## So what does this mean more specifically?

- **Regulatory framework:** While AI technology is increasingly ubiquitous, each country is applying its own set of road rules and vehicle considerations. International agreements, such as the UN Conventions on Road Traffic, are being rethought. It will take time and effort to ensure that rule changes as a result of this technology are forward thinking and nonrestrictive.
- **Product safety and liability:** It is increasingly important to anticipate and manage product safety risks arising from human error, but is blamed on alleged malfunctions in advanced technology.
- **Communications and spectrum:** Connected vehicle solutions involve embedded communications modules (SIM cards and modems) managed by mobile operators via central platforms. They involve telematics (machine-to-machine data transmissions), automatic emergency calling, in-car entertainment, and other communications packages enabled through various roaming arrangements, requiring centralized data management, and value-added services. Short-range radar used to avoid collisions, as well as vehicle communication links require reliable, interference-free spectrum resources. Setting aside spectrum for connected vehicle applications will require thoughtful policy advocacy on a national, regional, and international (ITU) level.
- **Open source and software:** The automotive industry plans a vehicle lifecycle of 15 to 20 years, but the product lifecycle of software is often measured in months. This variance in product lifecycles will need to be managed and appropriately regulated.
- **Data storage and data quality:** As vehicles become connected, huge amounts of information is gathered. Clarity is required on who owns the data and how it will be stored.
- **Privacy and data protection:** Connected and autonomous vehicles rely on vast amounts of data. This data may be linked to vehicles, their owners, and passengers. Legal frameworks will need to address issues such as notice, consent, the appropriate level of security, and acceptable uses of data.
- **Cybersecurity:** Cybersecurity is now an enterprise-level risk consideration to reassure consumers, investors, and regulators that appropriate protections are in place against malicious cyber attacks and accidents that can affect connected vehicles.
- **Intellectual property:** In addition to AI, connected vehicles incorporate technologies, such as mobile connectivity, antennas, touchscreens, cameras and lenses, onboard computers, apps, and integrated mapping/GPS. These areas have seen extensive patent litigation in the last five to ten years as patent holders and non-practicing entities seek to force competitors to license their patent portfolios. Original equipment manufacturers will increasingly have to manage intellectual property challenges, including patent and copyright, and protect themselves against patent trolls.


Dr. Patrick Ayad
Partner, Munich
T +49 89 290 12 216
patrick.ayad@hoganlovells.com

Lance Bultena
Senior Counsel, Washington, D.C.
T +1 202 637 5587
lance.bultena@hoganlovells.com

Richard Horan
Partner, Northern Virginia
T +1 703 610 6111
richard.horan@hoganlovells.com

Charlotte Le Roux
Associate, Paris
T +33 1 53 67 18 56
charlotte.leroux@hoganlovells.com

# Space and Satellite

The nature of the space and satellite industry presents a quintessential use case for AI. Everything about the industry requires machine intelligence and assistance to launch, operate, maintain, control, repair, and ensure achievement of the business mission. Mission success heavily relies upon sophisticated computer-assisted models, algorithms, robotics, and communications across long distances (from geostationary earth orbit (GEO) to low earth orbit (LEO), and everything in between (medium earth orbit (MEO)). Some examples of potential AI applications include:

- **Remote sensing and monitoring** of a broad array of potential targets, including environmental changes, dark ships and national security, fleet management, and aircraft and maritime tracking.
- **Communications** between ground and space, and from satellite-to-satellite (in the case of a multi-satellite constellation), using radio frequencies, optical-laser communications, radar and other technologies, along with growing complexity of satellite-to-satellite handoffs between satellites in different orbits.
- **Robotics** in space, including mission extension vehicles, space docking, satellite health monitoring, manned space vehicles support (including health, safety, medical, analytics, and repair), and spacecraft, such as automated transport vehicles, designed to make their own decisions to explore, learn, identify, and adapt during missions; and carry out repairs.
- **Data analytics** including the policy and regulatory issues inherent in gathering large amounts of information, and how that information can be used, from national security (and sovereignty), data privacy, and proprietary perspectives.
- **Reusable launch and manned vehicles** including sophisticated AI for return to Earth for completion of mission.
- **Asteroid mining** including analytics of substances discerned from asteroid samples, and remote mining of the same.
- **Remote missions** to Mars and beyond (and a broad variety of information transit, maneuvers, and return).
- **Satellites as alternative to terrestrial-based systems** including cloud computing, cross-border broadband services, and other multi-jurisdictional data and information transfer.

The breadth of these space-based services requires consideration of a broad range of legal, policy, and commercial issues, including:

## Regulatory jurisdiction

For traditional GEOs, single jurisdiction (plus applicable International Telecommunications Union) rules govern, with a more limited scope of cross-border questions raised based on landing rights. As systems expand to LEO and MEO orbits and operate in the area of more innovative technologies (e.g. remote sensing, high resolution data gathering, and dark ship monitoring), the exercise of jurisdiction on a global basis becomes more complex. Additional complexities occur with new satellites in innovative missions, such as mission extension vehicles and satellite health monitoring, where the satellite missions require continued relocation amidst a field of other satellites.

## Cross-border data collection and dissemination rules

A space-based business operating in multiple jurisdictions has to address the multi-jurisdictional rules on information gathering and collection. The space-based AI is subject to all privacy and data protection rules and any government national security restrictions (including those that may apply to their own airspace).

## Product liability, cybersecurity, insurance, and litigation

Satellites and launches can give rise to large liabilities in the event of a satellite failure, collision, destruction (self or involving other satellites), or cybersecurity incidents. AI can be used to protect the safety and security of operations, but can also be used as a tool for interference, hacking, and/or destruction.


Randy Segal
Partner, Northern Virginia,
Silicon Valley, Washington, D.C.
T +1 703 610 6237
randy.segal@hoganlovells.com

Steven Kaufman
Partner, Washington, D.C.
T +1 202 637 5736
steven.kaufman@hoganlovells.com

Stephen Propst
Partner, Washington, D.C.
T +1 202 637 5894
stephen.propst@hoganlovells.com

Federico Hernández Arroyo
Partner, Mexico City
T +52 55 5091 0164
federico.hernandez@hoganlovells.com

Jeffrey Epstein
Counsel, Northern Virginia
T +1 703 610 6144
jeffrey.epstein@hoganlovells.com

Tony Lin
Counsel, Washington, D.C.
T +1 202 637 5795
tony.lin@hoganlovells.com


# U.S. Life Sciences

The use of AI techniques such as machine and deep learning have become common in the development of algorithms used for medical analytics. Given the availability of extremely large sets of data via electronic health records and other sources, health care is an especially attractive space for use of these methodologies. Today, tools built using these methods are assisting cardiologists in reviewing echocardiograms, analyzing electrocardiograms and other wearable sensor data, predicting occurrence of life-threatening conditions such as sepsis in intensive care units, and screening for severely debilitating diseases such as diabetic retinopathy. Algorithms and various AI techniques also revolutionize a health care provider's interaction with patients as in telemedicine, the records associated with patient interactions, and the billings and recoveries of reimbursement for medical services. On the next frontier, tools that allow for real-time learning will facilitate exponentially faster development and improvement in all these areas.

The breadth of the potential applications in medicine and health require consideration of a broad range of legal and regulatory issues.

## Licensor and U.S. state regulators

In the United States, companies developing health care products should be mindful of whether or not the technology or service will be viewed as involving the practice of medicine or another type of health profession and subject to state licensure and regulation.

## Health care privacy regulation

The United States has a patchwork of privacy laws. Those most relevant to products in the health care space are the Federal Trade Commission's (FTC) consumer protection laws and HIPAA. States also have consumer protection and privacy laws. For more details on AI privacy issues, please see our Privacy and Cybersecurity section on page 26.

## Medical device regulation

When tools leveraging AI techniques are used in the medical care of individuals, they may meet the definition of a medical device in multiple global jurisdictions, triggering regulation by the Food and Drug Administration (in the United States) and other regulatory authorities. Regulation is often directly related to the intended use of the product, so product design and marketing claims should be considered carefully to determine regulatory strategy. Regulation as a medical device carries a number of other regulatory considerations and so should be built into the long term business plan for the product.

## Health care fraud and abuse regulation

In the United States, business arrangements among health care providers and those involving the referral of patients for health care items or services, particularly if they are reimbursed by federal programs like Medicare or Medicaid, are subject to federal and often state fraud and abuse laws. Arrangements that are common in non-health care industries may be prohibited as kickbacks and subject to civil and criminal penalties in the health care setting. Thus, any business relationships and interactions with health care providers should be structured and carried out in a careful and planned manner.

## Coverage and reimbursement

The most traditional model of payment in the U.S. health care system involves reimbursement by a patchwork of public and private payers. In 2015:

— 56 percent of Americans were covered by employer-sponsored or individual health plans

— 20 percent were covered by Medicaid, the state-federal program for low-income individuals

— 14 percent were covered by Medicare, the health care program for those older than 65 or disabled

— 2 percent were covered by programs for veterans or the armed services

— 9 percent percent were uninsured.

Companies planning to make use of this model of payment must consider coverage and reimbursement in their business planning. Billing and electronic health records systems use adaptive learning and algorithms to generate accelerated financial records, claims and bills, and reimbursement at lower costs and greater efficiency and returns. But they also bring higher risk. When translational or coding errors are made, they can be repeated and compounded at significantly high volumes, and consequently high dollar values.

## Product liability

Although use of AI in health care is somewhat new and presents unique legal challenges, some of which likely have yet to be conceived, companies with products in this sector and customers in the United States should be aware that the United States has a complex set of liability considerations for medical products. For more details on AI products liability issues, please see our Product Liability section on page 28.

## Advertising and unfair competition issues

The U.S. Lanham Act, 15 U.S.C. § 1125, and numerous state advertising laws prohibit false or misleading statements in commercial advertising or promotion. Many states also have unfair competition laws that govern advertising, promotion, and other conduct facing the marketplace. In addition, technologies that are aimed at connecting patients or consumers with health professionals should be aware of state law restrictions on advertising by physicians and other health professionals.

## Regulation of deceptive advertising

Virtually every U.S. state has broad consumer protection laws that prohibit "deceptive and unfair business practices," which can be used by consumers to challenge allegedly false claims about a digital health product that uses artificial intelligence. The same conduct can also bring federal scrutiny. For example, in February 2015 the Federal Trade Commission (FTC), which regulates product claims, among other things, challenged several companies that claimed a mobile app could detect symptoms of melanoma in its early stages. The FTC pursued federal litigation against the companies that refused to enter settlement agreements.

## Telephone Consumer Protection Act

Companies that contact consumers or businesses via telephone, text message, or fax must comply with the U.S. Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227, or risk regulatory scrutiny and the threat of class action lawsuits. Some health care tools, particularly those used in telemedicine, may fall within the requirements of this Act.

## FCC regulation

The U.S. Federal Communications Commission (FCC) regulates non-federal government use of the radio spectrum. Organizations must consider the FCC's requirements for medical device products that incorporate radio frequency (RF) transmission. For more details on AI telecommunications issues, please see our Telecommunications section on page 32.

## Foreign regulatory considerations

Although the sections above primarily address U.S. legal and regulatory considerations, there are numerous other regulatory considerations depending on the specific jurisdiction. Many of them mirror those discussed above, but individual jurisdictions may have unique regulatory obligations for health care products.

## HiTech Act and the Office of National Coordinator

The HiTech Act of 2009 (Health Information Technology for Economic and Clinical Health) promoted the adoption and meaningful use of electronic health technology. It established standards for electronic health records systems, their certification under the standards, and monetary incentives for health care providers to move from inefficient and less accurate paper record systems and communication to standardized and certified electronic records and communications. For example, the statute and enabling regulations encourage physicians and hospitals to keep records in standardized codes to enable accurate communication with pharmacies, laboratories, imaging centers, skilled nursing, rehabilitation services, and others who treat patients.

This standardization, certification, and incentive system is overseen by the recently-established Office of National Coordinator (ONC) in the U.S. Department of Health and Human Services, whose own regulations apply to the development, maintenance, operation, and use of electronic records and information systems, modules, and their associated communications. It has also established meaningful use regulations applicable to health care providers who seek incentive payments from federal health care programs for using certified electronic records and communications. The ONC has surveillance and investigative authority, which it delegates in part to authorized certifying bodies and authorized testing laboratories, to oversee the integrity and compliance of these systems of records and communications. It also has public notice and reporting requirements to ensure health care provider users know the status of electronic records and modules they may utilize.

For a more complete discussion of the health care issues identified in this section, please see *Digital Health: The issues you need to consider to leverage its full potential in 2018.*


Virginia Gibson
Partner, Philadelphia
T +1 267 675 4635
virginia.gibson@hoganlovells.com

Yarmela Pavlovic
Partner, San Francisco
T +1 415 374 2336
yarmela.pavlovic@hoganlovells.com

Melissa Bianchi
Partner, Washington, D.C.
T +1 202 637 3653
melissa.bianchi@hoganlovells.com

Maria Durant
Partner, Boston
T +1 617 371 1024
maria.durant@hoganlovells.com

William Kettlewell
Partner, Boston
T +1 617 371 1005
bill.kettlewell@hoganlovells.com

Elizabeth Halpern
Partner, Washington, D.C.
T +1 202 637 8609
elizabeth.halpern@hoganlovells.com

Brooke Bumpers
Counsel, Washington, D.C.
T +1 202 637 5800
brooke.bumpers@hoganlovells.com

Matthew Felwick
Counsel, London
T +44 20 7296 5741
matthew.felwick@hoganlovells.com

# EU Robotics

Robots are defined by the International Federation of Robotics and the ISO standard n°8373 as "an actuated mechanism programmable in two or more axes with a degree of autonomy (i.e., without human intervention), moving within its environment, to perform intended tasks." Although Asimov's Three Laws of Robotics were the first rules to regulate robot manufacturing in an ethical manner, these rules are insufficient to consider the legal implications of robots. A single legal framework for robots does not cover the plurality and diversity of robots (e.g., drones, autonomous cars, or androids); different legal frameworks shall therefore apply depending on their use and functions (e.g., medical, industrial, and toy).

## Medical robots

Robots have increasingly emerged in the medical industry with various applications such as diagnostic support robots, surgeon robots, caregiver robots, or robotic prostheses. These mechatronic devices qualify as medical devices and in this respect must comply with specific regulations, such as the EU Directive on Medical Devices. Under the latter, manufacturers, importers, and distributors of medical robots face a strict liability scheme. Notwithstanding compliance with personal data protection standards, in particular on health information, manufacturing medical robots also requires compliance with stringent security rules, as the ones set out in ISO Standards n°13482, 13485, and 13485.2. Current regulations will rapidly become inadequate as medical robots become increasingly autonomous with technological progress.

## Industrial robots

Depending on their functionality, industrial robots may be qualified under the EU Machinery Directive as machinery (i.e., an "assembly, fitted with or intended to be fitted with a drive system other than directly applied human or animal effort, consisting of linked parts or components, at least one of which moves, and which are joined together for a specific application"). Inclusion or not in the scope of the Machinery Directive can be difficult to determine for certain types of robots, such as humanoid robots used in the service sector. As a consequence of being qualified as machinery, strict obligations may apply to stakeholders involved in manufacturing and marketing industrial robots, in order to ensure the health and safety of workers.

## Toy robots

Toy robots can come in different forms (e.g., game, animal, and humanoid) and be used for different purposes (e.g., entertainment, educational). Toy robots are governed by specific obligations including security risk assessments prior to their placement on the market.

The EU Directive on the safety of toys defines toys as "products designed or intended, whether or not exclusively, for use or play by children under 14 years of age." This definition can cover many products, even products that were not originally intended to be used as toys. Manufacturers and sellers must pay closer attention to the terms and conditions of their products prior to their commercialization.

# Consumer

AI is reshaping all aspects of the consumer experience, providing manufacturers and marketers of consumer products with new ways of targeting and engaging with consumers, while at the same time revolutionizing customer expectations as to customization, selection and delivery time. Content-heavy interactive applications designed to deepen and personalize the customer relationship; customization programs; algorithms that optimize advertising content delivery; voice-activated devices; self-operated home appliances; health and wellness-monitoring devices; applications that select products and services—everywhere we look artificial intelligence is changing how consumer companies interact with customers.

Innovations in AI in the consumer arena create game-changing opportunities. Social media programs can be used to shape preferences and target potential buyers. Voice-activated smart devices simplify the buying experience. Proprietary algorithms and databases continually improve the customization of the shopping experience, predicting what merchandise or services are likely to appeal to a particular consumer and allowing on-line retailers to move beyond the provision of merchandise to offering a bundled and personalized shopping experience. Big data analytics has increased the number of customer touch points by providing marketers with data on everything from consumer demographics, political beliefs, and cultural, social and artistic preferences to browsing, reading and viewing habits, dietary, sleep and exercise routines, to usage rates, ancillary purchases and pricing sensitivity. Marketers know our measurements, which websites we visit, and even if we linger over particular merchandise. And the incorporation of AI into consumer electronics ensures marketers continue to receive data to refresh the marketing cycle following purchase.

Artificial Intelligence is reshaping all aspects of the consumer experience, providing manufacturers and marketers of products with data unimaginable a decade ago and new ways of targeting and engaging with consumers.

## These developments raise interesting and new legal and regulatory issues:

### Privacy and Consumer Protection

Governments around the world regulate the protection and use of personal data, with some even issuing guidelines for the ethical use of the vast amounts of data available in an AI environment. The EU's General Data Protection Regulation (GDPR), which is broadly focused on limiting the purpose for which data can be used, disclosure of what personal data is being collected and for what purposes and limiting data collection and retention, has broad implications for AI, which depends on the continuous collection and utilization of data. Compliance in the U.S. is made challenging by the patchwork of state privacy and consumer laws that, along with the Federal Trade Commission's consumer protection laws that together make up the privacy framework. Many traditional privacy and consumer rights disclosures are not suited to an environment where data is collected continuously and by visual, auditory or sensory means.

### Competition

The rise of AI and big data analytics potentially raises antitrust and unfair competition issues. Global, national, and regional regulators are taking notice, contemplating questions such as whether algorithms can collude, for example by artificially raising prices in violation of prohibitions against unlawful agreements in restraint of trade. Similarly, regulators have questioned whether companies' possession of massive customer datasets can confer unfair advantages or promote the existence of an unlawful monopoly.

### Advertising and Unfair Competition

Advertising laws around the world prohibit false or misleading advertising. Many countries also have unfair competition laws governing advertising, promotion, and other conduct in the marketplace. In the U.S., federal statutes and individual state statutes in this area can be broad, including the prohibition of any acts that are an unlawful, unfair or fraudulent business act or practice or unfair, deceptive, untrue or misleading advertising. In addition to general unfair competition laws, many jurisdictions have rules on advertising claims that prohibit deceptive and false claims about products that use artificial intelligence or products sold through interactive devices.

### Product Liability and Safety

As the complexity and functionality of AI products evolves, so too do legal expectations as to how companies evaluate and minimize risk. Risk assessments become more complex when AI combines common household products, such as electronic and other control devices, in ways not previously incorporated into conventional products. The potential for AI products to make decisions or take actions that could result in adverse outcomes greatly increases the risk of product liability. To avoid liability, marketers should investigate, assess the potential risk based on real-world uses of the products, and evaluate reporting responsibilities to consumer protection agencies, while considering proactive steps that may lessen the risk of becoming targets of product liability litigation or regulatory action.

### Telephone Consumer Protection Act

Consumer companies are increasingly under pressure to engage actively with their customers. But whether communicating for order delivery updates, coupon announcements or service inquiries, or engaging in other customer communication, marketers will need appropriate operational compliance processes, disclosure and consent mechanisms, recordkeeping, and other actions in place as they engage in an AI environment. Organizations that contact consumers or businesses via telephone or text message (or fax) in the U.S. must comply with the U.S. Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227, or risk regulatory scrutiny and class action lawsuits

## Discriminating and Profiling

AI has the potential to improve the consumer experience by enabling companies to provide more personalized and efficient services. However, enhanced profiling also raises the potential for unintended discrimination or unwanted and adverse decision-making. In the just the past few years, we have seen high-profile examples of commercial AI products allegedly acting in discriminatory ways, perhaps as a result of inherently biased or otherwise flawed training data used to develop algorithms. The consequences of deploying AI without appropriately addressing discrimination risk range from reputational harm to the company (e.g., chatbots gone awry; unintended revelations of sexual orientation or other sensitive issues; or product recommendations reflecting cultural bias) to causing economic harm to consumers (e.g., loan denials, increased insurance rates, or pricing models that lead to higher prices for certain demographic groups). See page 27 for more information on antidiscrimination laws.

## Other Regulated Areas

Interactive applications that direct a client to a particular consumer product or provide advice could, depending on the jurisdiction, be deemed to be the rendering of medical advice and, consequently, be subject to regulation.


Kelly Hardy
Partner, Washington, D.C. and Baltimore
T +1 202 637 5647
kelly.hardy@hoganlovells.com

Richard Welfare
Partner, London
T +44 20 7296 2000
richard.welfare@hoganlovells.com

Steven Steinborn
Partner, Washington, D.C.
T +1 202 637 5969
steven.steinborn@hoganlovells.com

Dr. Salomé Cisnal De Ugarte
Partner, Brussels
T +32 2 505 0908
salome.cisnaldeugarte@hoganlovells.com

Michael Turrill
Partner, Los Angeles
T +1 310 785 4707
michael.turrill@hoganlovells.com

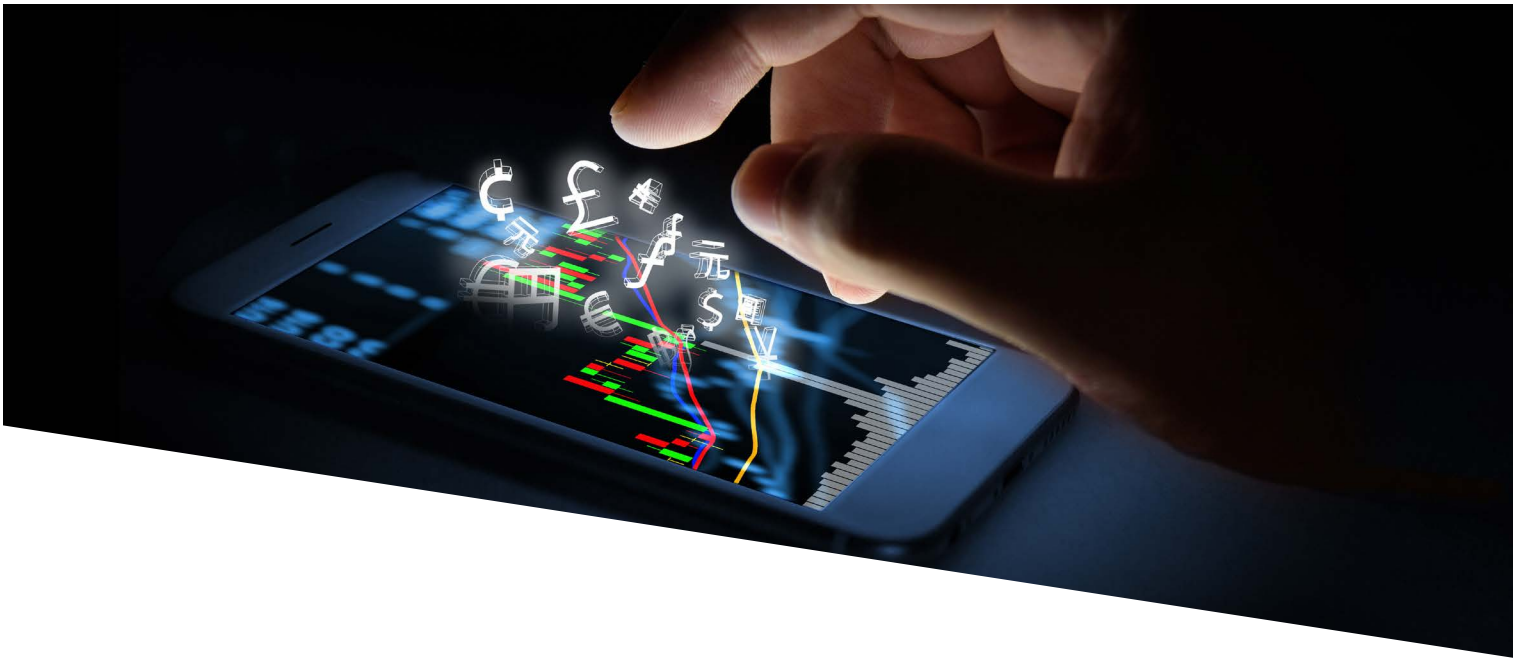
W. James Denvil
Senior Associate, Washington, D.C.
T +1 202 637 5521
w.james.denvil@hoganlovells.com

Meryl Bernstein
Partner, Washington, D.C. and New York
T +1 703 610 6229
meryl.bernstein@hoganlovells.com

Meghan Rissmiller
Partner, Washington, D.C.
T +1 202 637 4658
meghan.rissmiller@hoganlovells.com

Phoebe Wilkinson
Partner, New York
T +1 212 918 3010
phoebe.wilkinson@hoganlovells.com


PAID



# FinTech

The financial services sector is undergoing a period of rapid development, due in no small part to the rise of FinTech. Now, more than ever, the customer journey is key and financial institutions are increasingly applying AI throughout the value chain to deliver cost-cutting solutions and to improve customer experiences. As AI, and particularly machine learning technology, continues to evolve FinTech companies are collaborating with financial institutions to harness the technology to address particular areas of concern for both institutions and customers. These areas range from detecting fraud and onboarding customers quickly, to the provision of advice and the offering of personalized products to suit customer needs. AI uptake continues to expand into many different areas, some of which may not even have been conceived at this stage. Some applications of the technology in the FinTech space are below.

## Anti-Money Laundering (AML) and Know Your Customer (KYC)

The use of AI to detect money laundering activity offers the potential for financial institutions to dramatically reduce compliance spending. Machine learning techniques offer the potential for AI to efficiently analyze large amounts of customer data and screen customers against a number of different risks within a short period of time. Financial institutions benefit from the speed and accuracy of the AI system, which is more likely to uncover money laundering risks than many compliance employees. Meanwhile, customers experience a streamlined automated onboarding process which will attract more customers.

## Fraud minimization

Similarly to AML and KYC checks, banks and insurance companies are able to analyze data relating to areas at risk from fraud (e.g., payments or insurance claims, respectively) to identify patterns that may emerge. Machine learning can offer banks increasingly thorough risk profiling of claims and payments as the system continually analyzes and learns from increasing numbers of data sets. AI solutions making use of machine learning techniques are helping financial institutions to identify an increasing number of fraud instances, which saves money for financial institutions and can lower costs or premiums for non-fraudulent customers.

## Robo-advice

AI offers the opportunity to provide automated financial advice to customers, enabled by data analytics, machine learning techniques, and the development of natural language processing (NLP). Robo-advisers will be able to analyze data relating to a customer and their requirements, learn from patterns or requirements based upon experience with other customers, and uniquely interact with customers (as a result of advanced NLP). Customers will benefit from personalized advice tailored to their specific needs. Robo-advice is particularly prevalent in relation to wealth management and insurance products.

## Customer service

Many customers will already be familiar with AI chatbots. AI enables customers to solve their more basic problems without the typical waiting time associated with a call center. AI also offers unique customer service opportunities such as pre-emptive customer service, anticipating customer needs by analyzing customer activity data and identifying needs or areas of concern. These personalized services are likely to set certain financial services firms apart from others in the battle for customer retention.

## Personalized product recommendations

Customers may not always be aware of the range of products that a financial institution can offer to them. AI allows banks and insurance firms to identify potential needs of their clients and recommend complementary products and services. The data analysis involved is likely to provide more sales opportunities than a traditional website or human-to-human service.

While AI offers promising opportunities within the financial services industry, there are still a number of regulatory questions to answer for start-ups and firms looking to branch into the field of AI.

## Fairness

One of the key concerns with AI is accountability for any promotions made by AI solutions. An AI customer service bot may decide to promote certain financial products to customers. It is likely that such promotions will fall within the financial promotions regime. Institutions that operate AI solutions need to consider the risk of their AI solution circulating promotions that do not abide by the fair, clear, and not misleading principles under the regime.

## Discrimination and profiling

There have been a number of high-profile commercial examples of AI products that have allegedly acted in a discriminatory way. This has been more prevalent in the area of chatbots, but there is a risk of this also occurring following the more widespread adoption of AI. Firms need to consider how they audit the decisions made by AI (e.g., decisions to grant or refuse products to certain customers, particularly in light of the right to an explanation for decisions, under the GDPR). Customers also have the right to refuse to be subject to an automated decision under the GDPR, so firms will have to evaluate their mechanisms for dealing with such refusals.

## Rules governing advice

The provision of financial advice is governed by different rules depending on the jurisdiction involved (e.g., in the EU, where giving financial advice related to investment products is governed by the Markets in Financial Instruments Directive, and to insurance-based products governed by the Insurance Mediation Directive). Financial institutions will need to consider whether their robo-advisers fall under the rules in the relevant jurisdiction and will need to take the necessary measures to comply with the applicable rules.


John Salmon
Partner, London
T +44 20 7296 5071
john.salmon@hoganlovells.com

Richard Schaberg
Partner, Washington, D.C., New York
T +1 202 637 5671
richard.schaberg@hoganlovells.com

Gregory Lisa
Partner, Washington, D.C., New York
T +1 202 637 3647
gregory.lisa@hoganlovells.com

Bill Lovett
Partner, Boston
T +1 617 371 1007
william.lovett@hoganlovells.com

# Education

Higher education institutions are at the forefront of AI development, having long engaged in related teaching and research. For example, the *Journal of Artificial Intelligence Research*, an open-access, peer-reviewed scientific journal was founded in 1993 – at the dawn of modern AI.

More recently, colleges and universities have used AI for a range of purposes. For example, higher education institutions may use drones for research and educational purposes, whereas students fly them as a hobby. Furthermore, campuses may also start using this technology for operational purposes. Educational institutions already widely employ data analytics for marketing, recruiting, and supporting students' academic progress, and AI can enhance the available information. Smart systems on campuses may also increasingly manage energy use, building security, and more through use of AI. As the technology matures, AI will start to appear in classrooms at the elementary and secondary school levels as well as college courses.

The increasing use of AI for instructional purposes may raise accreditation and other education regulatory compliance issues, ultimately requiring the adaptation of current standards and laws. Educational institutions at all levels are generally subject to the Family Educational Rights and Privacy Act, which protects the privacy of education records and may figure in AI applications. The use of AI with or by minors may heighten these privacy concerns. For example, the Pupil Rights Protection Act requires parental consent to certain studies involving minors, and the Children's Online Privacy Protection Act requires certain websites or online services to obtain parental consent before collecting personal information from children under 13.


Elizabeth Meers
Partner, Washington, D.C.
T +1 202 637 8676
elizabeth.meers@hoganlovells.com

Stephanie Gold
Partner, Washington, D.C.
T +1 202 637 5496
stephanie.gold@hoganlovells.com

Jody Newman
Partner, Boston
T +1 617 371 1006
jody.newman@hoganlovells.com

Justin O'Brien
Partner, Boston
T +1 617 371 1035
justin.obrien@hoganlovells.com

# Ethics in AI

Big data analytics and complex algorithms depend on AI. The amount of data and its analysis cannot practically be accomplished by humans alone. But one of the most difficult issues – particularly as algorithms increase in complexity - is ensuring that the algorithms (and their own self-evolutions) do not include biases. With the increasing complexity of algorithms, it becomes more difficult to unpack the analysis to ensure transparency and lack of bias.

AI brings with it huge advantages for humanity, healthcare, assessing climate change, accessibility and improving lives (such as bringing image recognition to the blind, or drone delivery of medical supplies), mapping, understanding of space, farming, airplane flight paths, financial services, and adaptive biotech, among others.

At the same time, engineers, lawyers, and futurists alike are considering the need for human involvement in the equation to moderate the process and ensure, among others:

— Fairness
— Transparency
— Safety
— Security
— Privacy
— Inclusiveness
— Core of Empathy
— Dignity

# Areas to consider in AI development

# AI in the Asia Pacific

In the Asia Pacific region, as data protection regimes mature, we are increasingly seeing lawmakers and regulators crafting regulation and compliance guidance that specifically address data protection aspects of advancing technologies in areas such as AI, biometrics, big data, and the internet of things. The tightening of Asia's data protection regulatory environment, and the emergence of cybersecurity regulation, comes at the same time as personal data has developed into an increasingly valuable business asset. Regulators are issuing detailed guidance and taking enforcement action on these issues, and the associated policy considerations often bring wider geopolitical and national security concerns into play. The availability of large volumes of data and the freedom to move it across geographic borders can be a critical requirement for the development of AI, meaning that regulatory developments in data protection and cybersecurity are certain to raise important policy challenges for the region's lawmakers as their AI development agendas move forward.

China's broader policy position in relation to AI is the most striking in the region, with its sights set squarely on displacing the United States as the world leader in this space. China aims to become the world's primary AI innovation center by 2030, with industry sector output aimed to exceed US$1.5 trillion by that date. The importance that the Chinese government is placing on AI reflects more than just a statement of economic development goals, and is an encouragement of indigenous innovation and productivity. China's focus on AI also reflects the fact that the technology can very likely serve as an important instrument of social and economic control. Their movement towards a "social credit system" that analyzes large volumes of its citizens' behavioral and transactional data is a case in point for AI deployment. Data protection laws have been progressively strengthened in China in recent years, but the application has been inconsistent. Given that the state has supreme power and can easily override the data protection requirements, the current data protection environment is broadly supportive of state-led AI initiatives. AI development is heavily dependent on the availability of large volumes of data, and in this respect, China's data protection framework supports a state-led push for innovation and growth. China's controversial Cybersecurity Law also raises important implications. This law reflects a move by China to secure the sovereignty of its cyberspace and ensure that technology used within its borders is secure and controllable. This has led to widespread concerns that foreign technology will be excluded from Chinese markets. The Cybersecurity Law's data localization measure, which applies to all personal data and "important data" collected or generated in mainland China, also raises important implications in the context of AI development, placing large volumes of data under tighter Chinese control, within Chinese borders. Observers have also noted that China's push for its own distinct set of national standards in areas such as the internet of things and cloud computing could also favor domestic AI technologies over foreign ones, providing indirect support to state-sponsored growth of China's AI leaders.

## Latest thinking

### Drones

— Real-name registration requirements imposed for civilian-use drones in China, *June 2017*

— Hong Kong Privacy Commissioner for Personal Data issues guidance on the use of drones, *April 2015*

### Life Sciences

— Regulatory Regime for Internet Distribution of Medical Devices, *April 2017*

— China to grow big on e-healthcare data, *August 2016*

### FinTech

— China issues its second Draft E-Commerce Law, *December 2017*

### Privacy and Cybersecurity

— Evolving landscape for international cloud providers in China: Why US technology giants are pairing up with local partners, *March 2018*

— China releases the Information Security Technology - Personal Information Security Specification, *March 2018*

— A brief analysis of the draft key information infrastructure protection measures, *August 2017*

— China's new rules on security review of network products and services fail to alleviate foreign investor concerns, *June 2017*

— China's revised draft data localisation measures, *August 2017*


Stephanie Keen
Partner, Singapore
T +65 6302 2553
stephanie.keen@hoganlovells.com

Jun Wei
Partner, Beijing
T +86 10 6582 9501
jun.wei@hoganlovells.com

Hiroto Imai
Partner, Tokyo
T +81 3 5157 8166
hiroto.imai@hoganlovells.com

Jeff Olson
Partner, Ho Chi Minh City, Hanoi
T +84 28 3829 5100
jeff.olson@hoganlovells.com

Mark Parsons
Partner, Hong Kong
T +852 2840 5033
mark.parsons@hoganlovells.com

Sherry Gong
Counsel, Beijing
T +86 10 6582 9516
sherry.gong@hoganlovells.com

# Drafting contracts with AI

As shown by the examples above, AI has or will transform virtually all industries including in ways not yet known. With this transformation will come uncertainties as to how existing and new legal frameworks will apply to the new technologies and the liabilities that may follow.

Innovations raise many regulatory questions, not just about compliance, but about the fundamental nature of the innovation itself. The issues range from whether and how the new technology is to be regulated, to whether the regulatory scheme to be applied will support innovation or, conversely, create hurdles that will stand in the way of (or even block) its development. These innovations will also raise cross-border jurisdictional issues, application of multiple regulations, and how to navigate the rules in product development, deployment, and contracting matters.

## So what do you do?

As in the case of all innovations and disruptive technologies, you should start with the basic premise that using contract boilerplate for the main terms and conditions will not achieve a good result. The contract for a new business model involving disruptive technologies must be built from the ground up, with a clean sheet of paper architecting the end-to-end system and service expectations, including technology development, technical capabilities, customer experience, financial model, risks, budgeting and handling cost increases, regulatory hurdles and changes, and termination strategy, to name a few. And you must build in provisions for systemic change, in other words have a contract that itself can evolve.

Care must be taken to consider:

— how will this new system operate,

— what flexibility is needed (or can be provided), and

— how are unknowns and possible (or probable) risks taken into account?

Next, you must consider what goes on the clean sheet of paper, as it forms the essence of the business arrangement between or among the parties. We have divided this analysis into three parts, which reflect three different goals in the contracting process.

### First, develop a contract that contains the necessary terms and reflects the company's strategy

This includes taking an inventory of the knowns and unknowns of the technology to develop a contractual roadmap that will contain sufficient flexibility to change course based on technology, regulatory, and other developments. It also requires you to design an acquisition strategy, including:

— how to acquire the relevant rights for what exists today,

— how to acquire rights to the next stage of the technology (at least to the extent it is developed by the counterparty),

— how to price these acquisitions (including receiving credit for obsolete technology that has to be replaced),

— appropriate acceptance criteria,

— how much control and exclusivity is desired (considering exclusivities, rights of first refusal (ROFRs), and most favored nations (MFN) provisions,
— and appropriate decision mechanisms with off-ramps to protect the parties against situations too far from the envisioned business model.

Maintaining flexibility for change is valuable in a changing technology and regulatory landscape. There is no one-size-fits-all solution and only a careful consideration of your business situation, aligned with the legal and commercial toolkit of terms, will enable you to determine the likely optimal terms for your new technologies. In all cases, the ability to foresee the future will be imperfect, but careful planning and strategic thinking will help improve the clarity and certainty of reaching the best solution.

### Second, anticipate third party events that need to be factored in, dealing with the changing regulatory landscape for the new technology and providing for its effects on the parties' deal

AI brings with it significant new issues involving product liability, data privacy, intellectual property, and almost every area of the law. When this is layered atop the global reach of products using AI, the cross-border challenges in a developing legal and regulatory landscape are tremendous. In some cases, regulatory conditions should be considered to bound liability issues within your tolerance for risk and/or business model, since the changing regulation may well make achievement of certain contract goals impossible and these situations need to be handled by specifying some outcome. Allocation of responsibilities and costs for compliance with future laws should be considered since these costs could be substantial.

### Third, overlay the standard allocation of known or anticipated risks between parties, with separate provisions for allocating unknown risks through contract adjustments or exit strategies

Thinking these issues through is critical, and it may be advantageous to set cost and liabilities expectations, rather than leaving the implications of changes to later dispute resolution. All reasonable scenarios should be contemplated when drafting agreements to ensure that all compliance, approval, cost, indemnification, termination, insurance, and financing provisions support the desired business outcome.

Once there is agreement on the allocation of liabilities and risks, the parties need to support that agreement with appropriate indemnification provisions. These clauses, often considered boilerplate in more routine arrangements, take on greater importance because there are so many uncertainties with respect to which indemnification provisions may be called upon to address risk allocations. Insurance can play an important role to backstop indemnification provisions and the attendant risks, including the risk that the indemnifying party may not, as a practical matter, have the ability to step up to its contractual commitments.

In addition to this, there may need to be an overlay for unknown risks. When the parties' goals are frustrated, do you bring in an industry expert to reform the contract to best implement the parties' expectations? Or do you build in renegotiation points along the way, noting always the risks of an unenforceable agreement to agree? This can be done in bold ways, with agreements to supply based on technologies not yet developed, with prices to be set based upon future market conditions. There must also be a series of off-ramps, where the exposure gets too high (as specified in contract clauses) and the parties have the right to stop. This relies upon mutual assured injury to encourage a further negotiation at that time based upon new data.

## There is no one best answer as to what goes on the clean sheet of paper

Indeed, it will vary based on the particular business plan, the nature of the contracting parties, the specific business plan risks, relative leverage, and many other factors. But one common theme is critical to all cases: taking the time to carefully consider a full range of outcomes and possibilities while structuring your contract. Even terms of early stage contracts can have long-lasting impacts on business flexibility, market positioning, and customer commitments. Therefore, getting it right from the start is imperative.

Randy Segal
Partner, Northern Virginia, Silicon Valley, Washington, D.C.
T +1 703 610 6237
randy.segal@hoganlovells.com

Steven Kaufman
Partner, Washington, D.C.
T +1 202 637 5736
steven.kaufman@hoganlovells.com

# Privacy and Cybersecurity

The large volumes of data collected by AI systems, and the extensive and complex processing such data undergoes, may create challenges for compliance with laws focusing on individual privacy, and how such data is secured.

Many privacy regimes around the world are based on internationally recognized privacy principles known as the Fair Information Practice Principles (FIPPs), and several of the FIPPs may be challenging to implement in the context of AI. For example, the principle of data minimization, which calls for collecting only the minimum amount of data necessary to accomplish a specified purpose, is in tension with the need for AI systems to gather large amounts of data, not all of which may be able to be identified as relevant at the outset of collection.

In the U.S., there is no singular, comprehensive data privacy law, but rather a patchwork of sector-specific privacy protections. Although these laws were not drafted with AI systems in mind, companies will need to be mindful of the restrictions such laws may place on specific AI projects, which may need to track certain individual level activity or functions over time. For example, the health care industry is a ripe target for AI innovation, as AI products may help improve the speed and accuracy of diagnoses and refine and tailor treatment plans. Achieving these outcomes may require tracking individuals' treatment and response over time. However, obtaining the medical data necessary for training AI may be a challenge, as the federal Health Insurance Portability and Accountability Act (HIPAA) places restrictions on how health plans, health care clearinghouses, and health care providers can use and disclose protected health information. State medical privacy laws may similarly restrict access to health information. Thus, companies seeking to innovate in the health care space will need to thoughtfully consider how to lawfully obtain comprehensive data sets that can enhance learning and treatment.

Another example of a U.S. privacy law that may impact AI systems is the Fair Credit Reporting Act (FCRA), which governs the use of credit reports – essentially any information collected or compiled that will be shared with others for use in credit, insurance, or employment eligibility determinations. The FCRA provides consumers with broad rights of access and correction, and it imposes various requirements on consumer reporting agencies. Companies working on AI systems may inadvertently become swept into the purview of the FCRA depending on how recipients of the information developed make use of the information.

In the European Union, a new regulation coming into effect on May 25, 2018 will have far-reaching impacts on AI products. The General Data Protection Regulation (GDPR) defines personal data broadly, such that much of the data processed by AI systems arguably would likely be covered. The GDPR requires data controllers to provide individuals with privacy notices. For example, where the data processing involves "automated decision-making, including profiling," the privacy notice must include "meaningful information about the logic involved." The difficulties posed by AI in readily translating how algorithms function specifically may make such an explanation difficult to provide. Further, the GDPR requires appropriate precautions to avoid discriminatory effects from profiling. It may be challenging for companies to fully account for all unintended biases depending on how AI outputs are used, especially as the uses may not be controlled by the entity that developed a particular AI solution.

The GDPR also requires data controllers to provide individuals with rights of access, rectification, erasure, restriction of processing, data portability, and objection to certain types of processing. Companies will have to design AI products with these rights in mind and provide mechanisms for individuals to exercise such rights where AI outputs may include personal data. Similar issues may arise under other privacy law regimes globally. This likely will require creativity and careful construction throughout the design process.

From a cybersecurity perspective, the threats to AI data from attackers or negligent handling are many and varied. It is important to reasonably secure any personal data that AI outputs may analyze, especially where the information reveals sensitive characteristics, such as medical conditions or financial history.

In addition to protecting the underlying information analyzed, companies may need to protect their algorithms and AI outputs, which in many cases will be confidential and proprietary as to the AI company itself or its customers. Companies will also need to develop and implement comprehensive cybersecurity programs to help protect information and implement, test, and adjust their programs and incident response plans as threats continually evolve.

## Discrimination

AI can help make decisions based on historical data. However, the outcome of the data analysis may yield results that are socially unacceptable. The algorithm may predict that someone is a bad credit risk because they grew up in a certain part of Oregon, or because their parents were born in another country. In most instances, the algorithm itself is not the origin of the bias. The problem relates to the data that are analyzed. AI analyzes historical data from real life. Data from real life is messy, and reflects the biases and bigotry of human society — in other words, garbage in, garbage out.

The designers of AI systems are working on solutions to the problem. Ideally, we would analyze data from the world as we would like it to be, not the world as it actually exists. The answer may be to ensure that decisions that result from AI are checked by humans before they create effects for an individual. This kind of human review is precisely what Article 22 of the GDPR (EU Regulation 2016/679) attempts to do. The GDPR gives individuals an absolute right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects. In addition, existing laws prohibit all forms of discrimination based on sex, skin color, or religion whether in a work place or elsewhere. The existing legal mechanisms are not perfect, but they do exist.

AI applications will merit testing and risk assessments before they are deployed, to anticipate potential problems such as illegal discrimination. Article 35 of the GDPR requires data protection impact assessments to be conducted for any risky processing. These impact assessments should be expanded to cover other risks associated with AI, such as risks of discrimination.


Timothy Tobin
Partner, Washington, D.C.
T +1 202 637 6833
tim.tobin@hoganlovells.com

Winston Maxwell
Partner, Paris
T +33 1 53 67 48 47
winston.maxwell@hoganlovells.com

Harriet Pearson
Partner, Washington, D.C., New York
T +1 202 637 5477
harriet.pearson@hoganlovells.com

Bret Cohen
Partner, Washington, D.C.
T +1 202 637 8867
bret.cohen@hoganlovells.com

Eduardo Ustaran
Partner, London
T +44 20 7296 5249
eduardo.ustaran@hoganlovells.com

Sam Choi
Associate, London
T +44 20 7296 5756
sam.choi@hoganlovells.com

# Product Liability 

Fast-paced development and innovation can raise interesting product liability challenges for manufacturers and businesses in the product supply chain, including ensuring that new products meet the requirements of relevant regulatory regimes, while also seeking to minimize future litigation risks. The latter can be especially difficult as regulatory and legislative regimes, and even the common law, often have not kept pace with product innovation. These considerations are especially relevant in light of the rapid advancements in AI in recent years.

## AI's place in the product compliance and liability landscape

A number of jurisdictions including the U.S., EU, South Korea, and Japan have started to consider whether AI products need specific legislation, regulations, and standards. By way of example, from an EU perspective, there is currently no set of laws or regulations that apply to AI in particular. Instead, a manufacturer would need to look at the wider EU legislative landscape applicable to products. As for any product, that landscape will depend, among other things, on the product's features and functionality. The existing product laws and standards would need to be considered in much the same way as when any new product is being designed for market launch.

Similarly, existing U.S. legal requirements are likely to regulate AI, at least initially. Identifying pertinent legal standards, however, will not always be straightforward. For instance, courts will have to answer if, and under what circumstances, AI that is incorporated into a tangible object, such as an autonomous vehicle, qualifies as a product subject to strict liability.

When looking to launch a new AI product in a market there are likely to be additional complicating factors such as:

— the identification of appropriate safety and other product standards,

— determining the application of relevant product laws in circumstances where the laws could not possibly have envisioned the technology in question (and where relevant guidance or case law may be thin on the ground, or especially challenging to apply);

— and the appropriate testing of the product (this could include, for example, identifying a test house with the requisite expertise, experience, authority, and equipment).

## The challenge of AI to existing product liability regimes

It has been argued that the most challenging legal issues arise when human intervention is taken out of the equation and AI begins to make its own independent decisions. For example, most defects traditionally exist at the time when the product was sold. But AI will increasingly be capable of learning on its own. If an AI product learns to become unsafe in response to its external environment, would the capacity to learn to become unsafe make it a defective product, bringing it within the scope of product liability regimes? What types of injuries would be the foreseeable consequences of AI continuing to learn? Who would be liable and under what theories (e.g, the product programmer/designer, the manufacturer who puts the "nuts and bolts" of the product together, or less traditional strict liability defendants like the owner of the AI's algorithm?) What about the consumer who home-programmed the product? These are the type of issues which manufacturers will need to grapple with assessing litigation risks associated with marketing new AI products.

There are also interesting practical and evidentiary issues to be considered. For example, a judge or jury may prefer the testimony or video recording of an AI product to a competing first-hand (human) witness of fact. Could an AI product perjure itself and if so, would the manufacturer be held liable for this offense? Perjured testimony by AI could be particularly damaging given the public's historical overreliance on the accuracy and reliability of new technologies.

To start addressing these issues, some commentators have argued that it would be sensible to assign legal personality or personhood to sophisticated AI products rather than placing the entire burden on the manufacturer (but it's important to note that this does not equate to giving machines legal rights). This would mean that a product/robot could be held liable for any damage it causes and could be sued in its own right. Of course, this approach would require that the product be covered by insurance. However, this approach is not without its own pitfalls. It remains to be seen whether the insurance market will offer affordable policies covering new AI products.

## Conclusion

The fundamental question is how to ensure the safety and performance of AI products while not stifling their development and introduction to the market. Existing product compliance and liability regimes will be tasked with answering this question while AI-specific rules continue to develop. AI's fit within these legal regimes may at times be awkward, but is by no means impossible if past technological advances are any guide. Meanwhile, the AI-specific rules that emerge are an opportunity for creative, practical solutions and should be tailored to avoid a legal environment which becomes characterized by inefficiencies, stifled innovation, wasted opportunities, and the need for constant amendments as these emerging technologies present new challenges.


Christine Gateau
Partner, Paris
T +33 1 53 67 18 92
christine.gateau@hoganlovells.com

Valerie Kenyon
Partner, London
T +44 20 7296 5521
valerie.kenyon@hoganlovells.com

Michael Kidney
Partner, Washington, D.C.
T +1 202 637 5883
michael.kidney@hoganlovells.com

Dr. Sebastian Polly
Partner, Munich
T +49 89 290 12 192
sebastian.polly@hoganlovells.com

# Intellectual Property

## Ownership: Patents and copyrights

Patents and copyrights are forms of intellectual property (IP) in which the government grants protections to the creators of novel works – patents protect new and useful inventions, and copyrights protect original works of authorship fixed in any tangible medium of expression.

The twin questions of "Who is the inventor?" and "Who is the author?" bring up interesting and complex questions in the field of AI. For example, when an AI system creates visual images or audio compositions, are they copyrightable? To some extent, this is an extension of the monkey selfie case several years ago, in which it was argued that when a photographer set up his camera in the forest and a Celebes crested macaque managed to press the shutter-release button while looking into the lens, the monkey should be considered the author of the resulting photo. Similar questions arise when AI algorithms are able to develop new and useful objects (or even other algorithms). Is the AI the inventor or author? Can inventorship or authorship be attributed to a nonhuman?

Moreover, in the case of patentable inventions, if the solution to a technical problem is developed by the AI system, yet is obscured by the black box of the AI algorithm, how can the proprietors of the AI system even recognize or determine that the AI has devised a solution that is sufficiently novel to be potentially patentable? It may, for example, be entirely obscured how the solution is carried out.

Relatedly, can the human developers of the AI system be deemed to be the inventors or authors of the AI system's output? Would the answer be different when an AI system develops inventions or art or music that was not specifically foreseen by the human developers of the AI system?

## Ownership: Trade secrets

Trade secret law, another traditional field of IP, raises a different, but equally challenging set of issues. To be protected as a trade secret, information must have independent economic value from not being generally known to the public, and must be subject to reasonable efforts to maintain its secrecy. In trade secrets litigation, it is common to require that the claimant specifically identify its trade secrets, and also explain the efforts to maintain secrecy.

Trade secret misappropriation generally involves taking, disclosing, or using trade secrets under circumstances where the taking, disclosure, or use is improper (such as stealing them or violating confidentiality agreements). Even where one party has trade secrets, it is generally not misappropriation to independently develop the same technology, or to reverse engineer publicly available aspects of the technology.

If an AI system comes up with a technical solution that happens to infringe on third parties' patent rights, or develops art or music that has too-uncanny similarities to known, existing works, who is the infringer?

Where information is the product of AI, it is possible to theorize that it could have independent economic value from being nonpublic, and that it would be subject to reasonable efforts to maintain its secrecy. The problems of inventorship or authorship may not arise in the same way they do with patents and copyrights. But, where the information is the product of an AI system – particularly where it is within the black box of how the AI system performs its analysis – there may be difficulties articulating specifically what the trade secrets are, and possibly also how their secrecy has been maintained.

## Ownership: Data

A further area of proprietary rights also bears mentioning: ownership of data. Data is increasingly recognized as valuable in its own right. Yet it doesn't always fit easily within the traditional IP doctrines. With the increased processing complexity and speed of AI systems, data, particularly large data sets, are an ever-more important consideration.

## Infringement

On the flip side, if an AI system comes up with a technical solution that happens to infringe on third parties' patent rights, or develops art or music that has too-uncanny similarities to known, existing works, who is the infringer? Can the AI system infringe a patent or a copyright?


Celine Crowson
Partner, Washington, D.C.
T +1 202 637 5703
celine.crowson@hoganlovells.com

Dr. Christian Mammen
Partner, San Francisco
T +1 415 374 2325
chris.mammen@hoganlovells.com

Audrey Reed
Partner, Washington, D.C., New York
T +1 202 637 6626
audrey.reed@hoganlovells.com

# Telecommunications

The data analytics and processing performed in most AI applications will require access to sophisticated computer hardware and software and high-capacity, low-latency communications network connections. For many AI applications, the most immediate communications link to the user device will be a wireless link, either terrestrial or satellite, because the user device collecting, processing, storing, and sending the data will be in motion. Because most AI users will not be in a position to build their own private communications networks, they will have to rely mainly on mobile connectivity provided by third-parties, including commercial terrestrial wireless and satellite operators. The communications networks of these providers will need to be high-capacity, ubiquitous, secure, and reliable.

Depending on the requirements or sensitivity of the particular AI application, AI users will need to establish redundancy measures to ensure that their AI applications will be maintained at a high quality and reliability level when a primary communications link is temporarily unavailable. The user device hardware that will be collecting, processing, storing, and transmitting the AI data (including on-board sensors and on-board radio communication devices) may themselves be subject to government radio frequency exposure, emissions, and other limits.

Care will need to be taken in procurement of the communications network capacity and equipment necessary to support these business objectives through service contracts with third-party providers and engagement with government regulators. Relatedly, issues will need to be borne in mind with respect to government regulation of communications law, spectrum policy, licensing, equipment, network construction, and service quality and reliability issues. And companies will also need to comply with calling and texting laws (such as the U.S. Telephone Consumer Protection Act) to the extent they incorporate these platforms into their AI activities.


Michele Farquhar
Partner, Washington, D.C.
T +1 202 637 5663
michele.farquhar@hoganlovells.com

Ari Fitzgerald
Partner, Washington, D.C.
T +1 202 637 5423
ari.fitzgerald@hoganlovells.com

Mark Brennan
Partner, Washington, D.C.
T +1 202 637 6409
mark.brennan@hoganlovells.com

Trey Hanbury
Partner, Washington, D.C.
T +1 202 637 5534
trey.hanbury@hoganlovells.com

Alexander Maltas
Partner, Washington, D.C.
T +1 202 637 5651
alexander.maltas@hoganlovells.com

Tony Lin
Counsel, Washington, D.C.
T +1 202 637 5795
tony.lin@hoganlovells.com

# Media Regulation

Freedom of expression is one of the pillars of democratic society because without it, no other right could exist. AI can have adverse effects on freedom of expression because it can anticipate the kind of information that you like and simply feed you more of the same. This is called the filter bubble effect, which can lead to increasing polarization of society and the absence of democratic debate.

This bubble effect is a hard problem to solve, but the problem is broader than just a debate about AI. This issue instead relates to how the state should intervene to help make sure the marketplace of ideas functions properly. Generally, the state is the last person stakeholders would want to intervene in a marketplace of ideas because the state is, for many people, the most dangerous monopolist.

In the age of analog television and radio, media regulators helped ensure that citizens received a diverse set of viewpoints on topics of interest to the public. In the digital age, providing viewpoint diversity is much more difficult given the diversity of content available. How do you encourage citizens to explore all areas of a vast public library? Many countries are looking at how public service broadcasters can fulfill their public service role in an online environment. The regulatory debate should center on the future of media regulation, not on the regulation of AI.

# Antitrust

AI has consequences that go far beyond the direct purpose of the technical devices themselves. The same technology can have totally different outcomes when introduced into different contexts. Algorithms may facilitate perfect competition or they may facilitate collusion. For instance, some algorithms make markets more transparent and dynamic and thus have pro-competitive effects. On the other hand, AI using algorithms that implement collusive structures by monitoring and punishing deviation by any competitor without the need for explicit communication raise antitrust concerns. Detecting the difference between the pro-competitive and anticompetitive algorithms is, however, not an easy task.

Moreover, the DNA of AI is to take on a life of its own. This raises a difficult question regarding liability for antitrust liability. If there is no or only a weak link between the principal (the human) and the agent (the algorithm), who is on the hook for antitrust infringements? Some antitrust authorities already sent a clear warning message. With the words of the EU Competition Commissioner: “Companies can’t escape responsibility for collusion by hiding behind a computer program.”

One benchmark to hold someone liable under antitrust law for wrongdoing of AI could be whether the human could have been anticipated what the computer did. If it can be anticipated that an algorithm can lead to an anticompetitive action, such infringement by the algorithm will be attributed to the company. This is why businesses using AI (whether created in-house or by third parties) should be well aware of how their algorithms operate. Businesses should make sure that their algorithms comply with antitrust law by design. For compliance officers and legal counsel dealing with AI this means: talk to your technology departments to ensure that software is programmed to prevent any risks of collusion.


Dr. Falk Schöning
Partner, Brussels
T +32 2 505 0911
falk.schoening@hoganlovells.com

Edith Ramirez
Partner, Washington, D.C., Los Angeles
T +1 202 637 5509
edith.ramirez@hoganlovells.com

Logan Breed
Partner, Washington, D.C.
T +1 202 637 6407
logan.breed@hoganlovells.com


For compliance officers and legal counsel dealing with AI this means: talk to your technology departments to ensure that software is programmed to prevent any risks of collusion.

# Export Controls

AI raises new and complex export control issues. Given that AI is a nascent technology that is rapidly evolving, export control rules do not yet impose express, specific restrictions on it. However, AI-related software and technology may be caught under existing rules that were never intended to capture it, resulting in a potential mismatch between the regulatory regime and technology such as machine and deep learning. Accordingly, navigating the U.S. and non-U.S. export controls applicable to AI requires sound judgment and extensive experience with export control requirements.

## Military applications

The International Traffic in Arms Regulations (ITAR) administered by the U.S. Department of State impose stringent restrictions on the export, re-export, temporary import, and brokering of defense articles, technical data, and defense services. As governments and defense companies apply AI to defense projects, including weapons platforms, such technology, software, and AI-enabled hardware may be subject to the strict controls of the ITAR, even where the underlying machine and deep learning technology is based on commercial techniques.

## High performance computing

The rapid evolution and adoption of AI techniques is expected to drive the market for high performance computing in the coming years, with AI platforms consuming more and more computing power. Certain high performance computers, and related software and technology are subject to strict controls under the Export Administration Regulations (EAR) administered by the U.S. Department of Commerce. The export, re-export, and transfer of such hardware, software, and technology may be subject to licensing and other requirements under U.S. and non-U.S. law.

## Space and satellite

Military and commercial space-based systems also are subject to significant export controls under the ITAR and EAR. As the space industry adopts machine and deep learning techniques to assist with launch, operation, maintenance, and other activities, related AI technology, software, and AI-enabled hardware also may be subject to significant control under export control regulations. For more on this, please see our Space and Satellite section on page 10.

## Drones

The drone industry is expected to adopt AI to enhance the operation of drones and other mission critical functions. Military drones are controlled under the ITAR, and certain commercial drones are subject to stringent controls under the EAR depending on their range and duration of flight. To the extent AI is incorporated into drones, such technology, software, and AI-enabled hardware may subject to the highly restrictive controls applicable to drones. For more on this, please see our Unmanned Aircraft Systems (Drones) section on page 4.

Ajay Kuntamukkala
Partner, Washington, D.C.
T +1 202 637 5552
ajay.kuntamukkala@hoganlovells.com

Stephen Propst
Partner, Washington, D.C.
T +1 202 637 5894
stephen.propst@hoganlovells.com

Beth Peters
Partner, Washington, D.C.
T +1 202 637 5837
beth.peters@hoganlovells.com

Aleksandar Dukic
Partner, Washington, D.C.
T +1 202 637 5466
aleksandar.dukic@hoganlovells.com

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ
Silicon Valley
Singapore
Sydney
Tokyo
Warsaw
Washington, D.C.
Zagreb

Our offices
Associated offices

www.hoganlovells.com