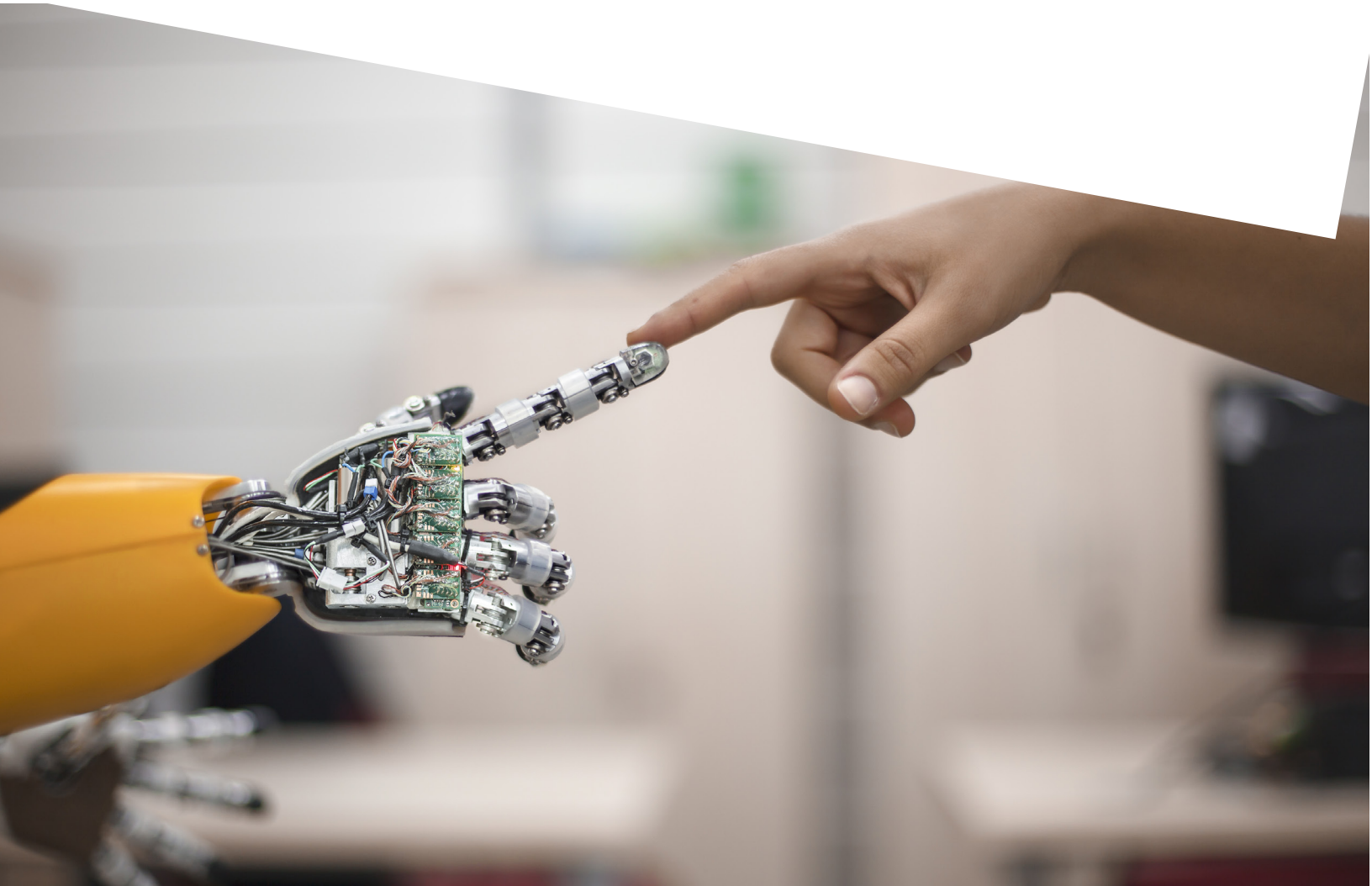
ADG Insights

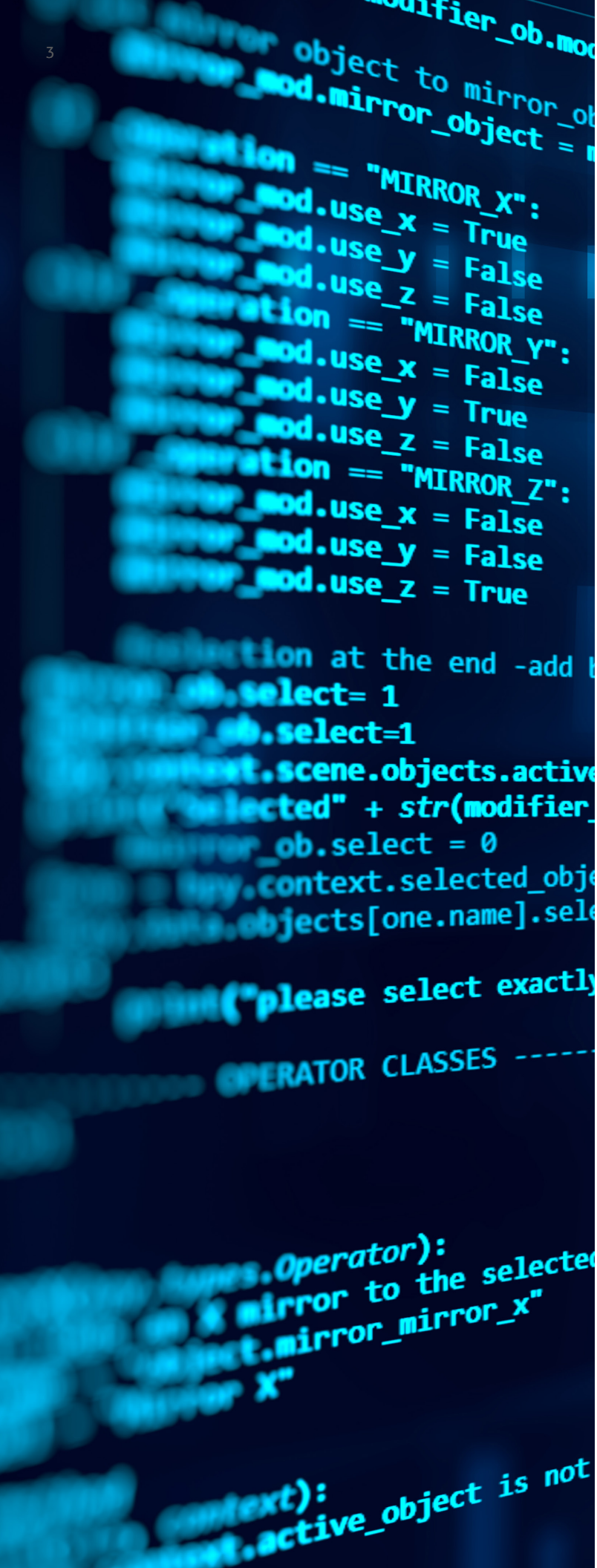
Artificial Intelligence

May 2018

Hogan Lovells

Contents





I. Introduction

Virtually every industry is being reshaped by the use of Artificial Intelligence and advanced machine-learning (collectively, AI). This is especially true for the Aerospace, Defense and Government Services (ADG) industry. AI presents significant opportunities for new products, new capabilities, and efficiencies for companies operating in this high-technology industry sector. ADG companies are leveraging AI for a wide variety of applications, including big data analytics, drones and autonomous vehicles, launch and space vehicles, advanced manufacturing, and more. AI is being used for the optimization of manufacturing processes (as part of Industrial Internet of Things [IoT], Digital Thread, and Digital Twin initiatives), smart maintenance, flight operations optimization, training, and even virtual assistants for pilots and crew.

The use of AI, however, brings with it significant new legal challenges in almost every area of the law, including export controls, data privacy, cybersecurity, products liability, intellectual property, and contract law.

Because these issues are treated differently in different countries, the cross-border issues in a developing legal and regulatory landscape are extremely complex. In some cases, the rapidly changing landscape may also challenge your ability to achieve certain contract goals.

II. AI in the ADG Industry

The below presents two examples of areas in which AI is currently being utilized in the ADG industry.

A. AI in Unmanned Aircraft Systems (UAS or drones)

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. For instance, below are several AI-enabled advancements in UAS.

- **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 fly 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 the way humans do. AI software is enabling drones to fly autonomously, even in dark, obstacle-filled environments or beyond the reaches of GPS or other methods of connectivity.
- **Real-time data analytics**: AI is also allowing drones to collect and process huge volumes of data in real-time. Aerial imagery analysis that would take humans hours, days, or weeks is being streamlined and automated by AI. Moreover, AI is able to determine what kind of data and images are important enough to collect, further streamlining the analytical process
- **Swarm technology**: AI technology is also enabling interconnected swarms of tens or hundreds of drones to operate entirely autonomously. AI integrates the data collected by each member of the swarm, generating a deep level of situational awareness, and AI enables the swarm to change its configuration to complete the mission if any one drone is lost.

B. AI in the space and satellite industry

The space and satellite industry presents a quintessential use case for AI. The industry requires machine intelligence and assistance to launch, operate, maintain, control, repair, and ensure achievement of the mission. Some examples of potential AI applications are listed below.

- **Remote sensing and monitoring** of a broad array of potential targets, including environmental changes, dark ships, national security monitoring, 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 increasingly complex satellite-to-satellite handoffs between satellites in different orbits.
- **Robotics** in space employed for mission extension vehicles, space docking, satellite health monitoring, manned space vehicles support (including health, safety, medical, analytics, and repair). Automated transport vehicles also employ AI-enabled robots that make their own decisions to explore, learn, identify, carry out repairs and adapt during missions.
- **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.
- **Remote missions** to Mars and beyond (and a broad variety of information transit, maneuvers, and return).

III. Legal issues that will shape your company's ability to capitalize on AI

A. 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 not designed with AI in mind, 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, an appreciation of the government's interests intended to be served by the export control regime, extensive experience with export control requirements, and the creativity to develop solutions that address the government's interests in a way that does not unnecessarily impair commerce.

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.

UAS and drones

As noted previously, the drone industry is adopting 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 be subject to the highly restrictive controls applicable to drones.

B. 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, contravenes 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. Indeed, part of what makes AI such an important leap forward is its ability to find relevance in information not previously understood to be relevant.

Fractured U.S. privacy laws

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 Privacy Act of 1974 applies to systems of records maintained by or on behalf of the U.S. government and restricts the use of covered Personally Identifiable Information to authorized users.

The General Data Protection Regulation

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 may be covered. The GDPR requires data controllers to provide individuals with privacy notices. For example, where data processing involves "automated decision-making, including profiling," the privacy notice must include "meaningful information about the logic involved." Since "the logic involved" might itself emerge as a result of the application of AI to massive data sets, setting out "the logic involved" prior to the application of AI to the data sets might be all but impossible. 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 of AI, especially as the uses of AI outputs 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, informed by a sophisticated understanding of the applicable legal requirements.

Cybersecurity

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. To the extent AI data includes Covered Defense Information or Controlled Unclassified Information, the company would need to ensure that the data is protected consistent with the regulatory requirements located at 48 CFR 252.204-7012 and 48 CFR 52.204-21.

C. Product liability

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-specific legislation, regulations, and standards are needed. In the EU, 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 statutory landscape applicable to products. The existing product laws and standards would need to be considered in relation to the product's features and functionality 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 whether, and under what circumstances, AI incorporated into a tangible object, such as an autonomous vehicle, is subject to strict liability.

When looking to launch a new AI product, companies will need to:

- identify appropriate safety and other product standards;
- determine the application of relevant product laws in circumstances where the laws could not possibly have envisioned the technology in question (and where the relevant guidance or case law is scarce or especially challenging to apply); and
- conduct 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 product liability questions 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 a product is 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? What types of injuries would be 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, or the company or even government entity that chose the external environment from which the product learned the unsafe behavior? These are the types of questions that manufacturers will need to grapple with in order to assess litigation risks associated with marketing new AI products.

Depending on the use of the AI, statutory, contractual, and common law protections may be available to mitigate certain risks relating to companies that do business with the U.S. government. These protections include:

- **The Government Contractor Defense:** The common law Government Contractor Defense allows contractors to avoid tort liability for harm caused by products manufactured in conformity with reasonably precise specifications either supplied or approved by the government.
- **Safety Act Protections:** This statute was enacted as part of the Homeland Security Act of 2002 with the purpose of encouraging the development of anti-terrorism products and services by providing liability protections for sellers (and purchasers) of qualified anti-terrorism technologies. Covered technologies include any product or service that is used for the specific purpose of preventing, detecting, identifying,

or deterring acts of terrorism or limiting the harm such acts might otherwise cause.

- **Public Law 85-804, Indemnification for Unusually Hazardous Activities:** This statute permits indemnification when a contractor is exposed to risks that are unusually hazardous or nuclear in nature and for which insurance coverage is not available at a reasonable cost.
- **10 U.S.C. § 2354, Indemnification of R&D Contractors:** Under 10 U.S.C. § 2354, the Department of Defense may indemnify research and development contractors for "[c]laims (including reasonable expenses of litigation or settlement) by third persons, including employees of the contractor, for death, bodily injury, or loss of or damage to property, from a risk that the contract defines as unusually hazardous." Identical authority was extended to the HHS pursuant to 42 U.S.C. § 241(a)(7), which grants the Secretary of the HHS authority to "enter into contracts, including contracts for research in accordance with and subject to the provisions of law applicable to contracts entered into by the military departments under [10 U.S.C. § 2354]." Both indemnification authorities, however, are subject to the availability of appropriated funds.
- **FAR 52.246-24, Limitation of Liability-High Value Items:** This contract clause implements the U.S. government's long-standing policy to limit a contractor's liability for the post-acceptance loss or damage to property of the government.
- **FAR clause 52.228-7, Insurance Liability to Third Persons:** Pursuant to this contract clause the government agrees to reimburse the contractor for certain liabilities to third persons not compensated by insurance or otherwise. These liabilities must arise out of the performance of the contract, whether or not caused by the negligence of the contractor's agents, servants, or employees, and must be represented by final judgments or settlements approved in writing by the government.

D. Intellectual property

Who owns patents and copyrights for AI output?

Through patents and copyrights, governments grant 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? This may prove difficult if the way the new solution is carried out is entirely obscured.

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?

Difficulties establishing trade secret protection for AI

Trade secret law, another traditional field of IP, raises a different, but equally challenging set of issues. To be protected, 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.

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.

Who owns the data needed for and created by AI?

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.

IP considerations unique to U.S. government contractors

By operation of law, the U.S. government typically gains substantial rights in IP developed with government funds, as well as enhanced rights to "mixed-funding" IP (public/private). A company that is developing or reducing to practice technology involving AI should be mindful that the government typically gains substantial rights when the government funds the development. A contractor may be able to negotiate special rights in certain circumstances, including when the agreement with the government is in the form of an "Other Transaction Agreement."

Drafting contracts to address AI

Contracts that address rights to AI should allow for flexibility to address a changing technology and regulatory landscape. Like all contracts, contracts involving AI must contain all necessary terms and reflect the company's strategy. To identify these, drafters should inventory the knowns and unknowns of the technology and develop a contractual roadmap that will contain sufficient flexibility to change course based on technological, regulatory, and other developments.

Care must be taken to consider

- how any new regulatory system is likely to operate;
- what flexibility is needed (or can be provided) in the contract; and
- how unknown and possible (or probable) risks are taken into account.

Acquisition strategies should address

- 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, and most favored nations provisions); and
- appropriate decision mechanisms with off-ramps to protect the parties against situations too far from the envisioned business model.

In addition, drafters should include provisions that address the impact of a changing regulatory landscape on the parties' deal. As noted, AI raises novel product liability, data privacy, intellectual property, and other legal questions. When drafting contracts for deals involving AI, drafters should consider including provisions that allocate the responsibilities and costs for compliance with future laws, as these costs could be substantial.

Finally, the standard allocation of known or anticipated risks between parties should be enhanced to include separate provisions that allocate unknown risks through contract adjustments or exit strategies. Once there is agreement on the allocation of liabilities and risks, the parties need to support that agreement with appropriate indemnification provisions. 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.

IV. Conclusion

AI and advanced machine-learning are already shaping the ADG industry. To capitalize on these new technologies, companies must grapple with numerous complex and evolving legal challenges.

Authors and contacts

ADG

Michael F. Mason
Partner, ADG Industry Sector Lead
Washington, D.C.
T +1 202 637 5499
mike.mason@hoganlovells.com

ADG

Robert Taylor
Senior Counsel, Washington, D.C.
T +1 202 637 5657
bob.taylor@hoganlovells.com

ADG

Rebecca H. Umhofer
Knowledge Lawyer, Washington, D.C.
T +1 202 637 6939
rebecca.umhofer@hoganlovells.com

ADG

Stacy Hadeka
Senior Associate, Washington, D.C.
T +1 202 637 3678
stacy.hadeka@hoganlovells.com

Space and Satellite

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

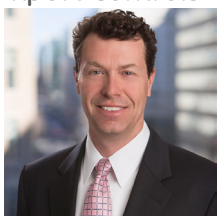
Space and Satellite

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

UAS and Drones

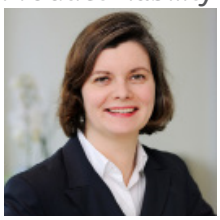
Lisa Ellman
Partner, Washington, D.C.
T +1 202 637 6934
lisa.ellman@hoganlovells.com

Export Controls



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

Product Liability



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

Intellectual Property

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

Hogan Lovells

Aerospace, Defense, and Government Services Industry

We can help you anticipate and deal with the risks before they become problems.

The aerospace, defense, and government services (ADG) industry is changing significantly. Global spending on defense and weapon system platforms is increasing. Governments are procuring analysis and engineering services to address escalating terrorism threats, cybersecurity concerns, and an ever-increasing demand for big data analytics. Commercial space and unmanned vehicle advances have invigorated key sections of the industry. Brexit and the administration change in the U.S. are creating challenges and opportunities across the globe. And, technological advances such as 3-D printing are creating unique opportunities for innovative products, decreased time-to-market schedules, and agile maintenance and repair services.

Our clients demand experience. They need comprehensive and cost-effective support from lawyers who know their business and understand the demands of their industry.

That's where we come in.

Be ready

Our global ADG practice is focused specifically on your needs. Our team includes industry-leading lawyers with corporate, commercial, regulatory, investigations, and litigation experience. We work closely with some of the largest and most established ADG companies in the United States, Europe, and Asia. We advise dozens of middle market businesses, emerging companies, new ventures, global entities, along with investment banks and private equity firms that are active in the industry.

We know, because we've been there

Our clients are also some of the most innovative in the world. They build manned and unmanned aircraft, supply parts, and materials to the aerospace industry, and develop and deliver the technologies essential to defense and national security. Our clients make and provide launch vehicle and satellite services and provide the services and innovations required for homeland security and critical governmental operations.

So let's work together

Together we will tackle the difficult challenges, capitalizing on opportunities, and avoiding pitfalls. We will guide you through government regulatory and procurement hazards and protect your interests in disputes and government investigations. Our industry focus enables us to fully understand your business and the challenges you face. We anticipate emerging issues before they become a problem and we give advice that achieves results.

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
Rio de Janeiro
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar
Warsaw
Washington, D.C.
Zagreb

Our offices
Associated offices

www.hoganlovells.com