

Artificial Intelligence Key Legal Issues

A Practical Guidance® Practice Note by Daniel J. Barsky, Holland & Knight LLP



Daniel J. Barsky
Holland & Knight LLP

This practice note provides an overview of the primary and emerging legal issues relating to the acquisition, development, and exploitation of artificial intelligence (AI). Issues addressed include those involving general commercial contracts, consumer products, products liability, intellectual property (IP), privacy and data security, bankruptcy, antitrust, and employment. The practice note discusses key issues that businesses should consider in areas where AI technology is germane.

For related content, see [Generative Artificial Intelligence \(AI\) Resource Kit](#), [Intellectual Property & Technology Fundamentals Resource Kit](#), and [Intellectual Property Licensing Resource Kit](#).

Defining Artificial Intelligence

Understanding the basic types of AI, and the main elements comprising AI, is a necessary first step in understanding the application of AI in commerce and the resulting legal issues.

What is AI? AI is computer software that is programmed to execute certain algorithms (computer code programmed to perform particular tasks) to recognize patterns in large volumes of data. From those patterns, the AI is programmed to reach conclusions, predict future behavior and patterns, make informed judgments based thereon,

and as a result, provide the requested output. Common examples of AI include:

- Image recognition technology (such as that which is used by Apple iPhones)
- Industrial robotics (such as Denso and Motoman)
- Voice control assistance technology (such as Google Home and Amazon Echo)
- Speech-to-text conversion programs
- Language translation programs
- Smart watches (i.e., fitness trackers)
- Logical AI programs (such as online tax prep software) –and–
- Chatbots (such as ChatGPT)

AI is generally classified into seven different types in two categories. The first four types are categorized based on functionality:

1. **Reactive Machines.** The oldest form of AI systems; they lack memory and therefore cannot use previous experience to inform present actions and improve their operation. Reactive Machines can only be used to automatically respond to a specific set of inputs. An example is IBM's Deep Blue chess machine.
2. **Limited Memory.** These are Reactive Machines that have, as the name suggests, limited memory. The AI can use the memory to store prior data and predictions and use that data to make better predictions going forward. Most current AI tools are Limited Memory tools.
3. **Theory of Mind.** A theoretical type of AI that is currently being developed. In this type of AI, the AI begins to interact with the thoughts and emotions of

the human user. For example, if you yell at Siri, Siri does not understand you are mad, but a Theory of Mind-based Siri would understand the emotion behind the words you are speaking.

4. **Self-Aware.** A hypothetical type of AI that is entirely self-aware. Think of Skynet from the Terminator movies.

The remaining three types of AI are categorized based on their capabilities:

1. **Narrow AI.** All existing AI—no matter how impressive it seems—falls within this category. These are AIs that can only perform a specific task autonomously. In other words, they can do nothing more than what they have been programmed to do.
2. **General AI.** AI that is designed to learn, think, and perform at levels and in ways similar to humans. General AI will be able to independently build itself, as opposed to requiring direct programming by humans.
3. **Super AI.** A hypothetical state of AI where the AI's powers substantially exceed those of humans.

There are four main elements comprising AI:

1. **Machine Learning.** Machine learning is the use of algorithms and statistical models to allow the AI to learn from the input data and make predictions and decisions based on what it has learned. An example of this is ChatGPT.
2. **Natural Language Processing (NLP).** NLP refers to the ability of AI to understand and process human language (both speech and text). An example of NLP is Siri.
3. **Machine Perception.** Sometimes referred to as “computer vision,” involves teaching machines to interpret and understand environmental inputs, such as visual information from images or videos, allowing them to recognize patterns, objects, and people. An example of this is photo tagging software.
4. **Machine Control.** Machine control refers to the ability of AI to control physical machines (such as robots) to perform physical tasks, such as autonomous driving vehicles.

The term machine does not necessarily mean a mechanical process. It refers, instead, to the artificially intelligent system, which may take any number of forms. It may be wholly intangible, such as computer software, and it may be incorporated into a simple machine to perform a task like a robotic vacuum cleaner. It may, alternatively, be part of a network of systems to operate a more complex device like the steering control system of a driverless car. For more information regarding AI in e-commerce, see [Artificial Intelligence and Automation in E-Commerce](#).

The application and scope of AI has grown exponentially in the past decade and this trend is expected to continue at a rapid pace, as seen in recent months with AI tools rapidly expanding for general public use.

AI and General Commercial Contracts

Businesses that exploit AI have the option of either developing their own AI (either in-house or with a third party) or licensing it from a third party, or a combination of the two. Most companies, even when developing their own AI, will license some AI from other sources; APIs for AI are becoming more prevalent. As with most IP license agreements, pay attention to the critical transaction terms below.

Representations and Warranties

A licensee should ensure that it receives, at a minimum, the following representations and warranties from the licensor of the applicable AI:

- **Right to contract and license AI.** A licensor should have and continually maintain the right to enter into the license agreement and license the AI, including all elements contained therein. Licensors typically seek a correlative representation and warranty, providing that the licensee is entitled to enter into the contract without violating any agreement, law, and/or any third-party right of any kind (i.e., that may arise out of its exploitation of the AI in a manner that is unauthorized by the licensor or when combined with materials or information not provided or approved in advance by the licensor).
- **Noninfringement.** Given the fluctuating state of case law pertaining to AI and intellectual property infringement, a licensee should ensure it negotiates a representation and warranty that the licensor's software does not infringe the intellectual property rights of any third parties. Additionally, as noted below, this representation and warranty should be exempt from any limitations of liability.
- **Ownership.** A licensor should represent and warrant that it is the owner of the licensed AI and that it is the entity responsible for the creation of the AI.
- **Compliance with data privacy laws.** In addition to a general “compliance with all laws” representation and warranty, a specific representation and warranty that the licensor has complied with all applicable data privacy laws, rules, and regulations should be included. With the continuously evolving patchwork of data privacy laws

in the United States, and data privacy a contentious issue in AI (particularly in the way the AI algorithms are trained and the data used in that training), data privacy compliance is a complicated issue with, potentially, substantial liability associated with it. Therefore, a negotiated representation and warranty with respect to data privacy compliance is recommended.

- **Disclaimers and warranties.** The licensed AI should function as contemplated without defect of any kind that could cause loss, injury, or death. Most licensors will seek to include a limited warranty addressing malfunction and the corresponding loss or injury, with remedies that are exclusive in nature. Additionally, note that subject to applicable state law, many warranties can be disclaimed in an agreement, including certain implied warranties, such as the implied warranties of merchantability, fitness for a particular purpose, title, and infringement. As such, licensor's counsel should ensure that the agreement's governing law supports whatever agreed-upon disclaimers are included in an agreement. For warranty and disclaimer clauses, see [Product Warranty and Disclaimer Clauses](#) and [Disclaimer of Express Warranties Clauses](#).

In addition to the more traditional representations and warranties outlined above, a licensee should consider requesting a representation and warranty from licensor addressing how the AI was trained and the sources of data used in that training.

From the licensor's standpoint, the licensee should be required to represent and warrant that licensee will only use the licensed AI for the purposes specifically set forth in the license agreement. Licensee's use of the licensed AI for purposes beyond the scope permitted in the license can result in liability for both licensee and licensor.

For representations and warranties clauses, see [Representations and Warranties Clauses](#).

Indemnification

An indemnification provision, also known as a hold harmless provision, is used to shift potential liability from one party to the other. Each party should ensure that the other party indemnifies, defends, and holds it (and its affiliates, employees, and representatives) harmless from and against any third-party loss, cost, or damage arising out of a breach of its contractual obligations or applicable law, and/or its negligence or willful misconduct. The indemnity should be tailored to each party's specific needs. For example, an indemnification can be restricted to particular third-party claims (i.e., breach of warranty), or limited to circumstances where a lawsuit has already been filed or a

final judgment has already been rendered. Indemnifying parties generally control the defense of a claim since they are the ones paying for it, but this is a point that must be negotiated. Oftentimes notice of a claim or potential claim is required; the notice requirement protects the indemnifying party from having to defend against a claim where it has been materially prejudiced by the indemnified party's delay in providing the indemnifying party with all requisite information about its existence and subject matter. Settlements most commonly require the approval of the indemnified party since its interests are directly at stake. If the parties wish for the indemnification to cover attorney's fees, this should be expressly provided, as the courts of most jurisdictions will generally exclude their recoverability otherwise.

With respect to AI-related license agreements, the indemnification should most certainly cover any breach of the agreement, including the representations and warranties regarding noninfringement and functionality. If the licensee is permitted to sublicense the AI to a third party, licensee's counsel should use best efforts to ensure that the indemnification extends to any loss, cost, or damage incurred by any such third party (and their licensees and users). This can be handled by simply having the indemnified party include each party's licensees and assigns (in addition to their officers, directors, employees, agents, affiliates, and partners). For additional information on indemnifications generally, see [Indemnification Provisions in Commercial Contracts](#).

Limitation of Liability

A limitation of liability provision limits a party's financial exposure if a claim is made or a lawsuit is filed. It can be used to exclude one or both parties' liability for specific types of damages, such as indirect (including punitive damages, an otherwise standard tort remedy), consequential, and incidental, among others. It can also include a liability cap, often expressed as a multiple of fees paid in accordance with the agreement by one party to the other party, either during a specific time period or over the lifetime of the agreement. Ensure that the clause is appropriately tailored to meet its client's needs given the specifics of the deal in question. For example, a limitation of liability clause can apply to the agreement as a whole, or, alternatively, only to specific terms. Exceptions can be carved out, such as making the limitation not applicable to either party's indemnification obligations. Additionally, limitations of liability can be mutual or one-way and can also incorporate a "statute of limitations" restricting the time period within which a claim for indemnity must be made.

In an AI license agreement, the risks associated with equipment or system failure can be disastrous. For instance, highly sensitive personal information can be exposed to downstream users which would subject the business to a lawsuit that could very likely be ruinous, particularly if a class action ensued as a result and, therefore, excluding data privacy matters from a limitation of liability should be considered by a licensee. Additionally, as noted above, liability for intellectual property infringement is uncertain and represents a substantial risk for licensees, who should consider excluding liability for intellectual property infringement from a limitation of liability. For additional guidance on limitation of liability, see [Risk Allocation in Commercial Contracts](#).

Insurance

Agreements often incorporate insurance obligations requiring one or both of the parties to obtain and maintain adequate insurance coverage. This serves to protect each party from the other party's inability to satisfy its financial liabilities under the applicable agreement (including its indemnification obligations). The types and minimum levels of insurance required depend upon the parties' needs, although general liability, employer's liability, and worker's compensation insurance are most commonly requested. Liability insurance policies cover amounts that an insured must pay to third parties for property damage or personal injury for which the insured is liable. There are an infinite number of ways that AI systems can cause damage, injury, or simply fail, and the ensuing loss could be enormous. As such, coverage levels should be high enough to account for these risks. Additionally, insurance coverage should be considered to back up a party's indemnity obligation; after all, an indemnity is only as good as the indemnifying party's ability to make payment pursuant to the indemnity provision. For insurance clauses, see [Insurance Clauses](#).

Escrow

Because most current AI tools are embodied as software, as with any other software-related agreement, consideration should be given as to whether an escrow of the AI software should be included. Software escrows are generally used to ensure that, if something happens to the licensor of the software (such as a bankruptcy or assignment for the benefit of creditors), the licensee will have access to the software's source code, allowing the licensee to continue operating the software after the licensor has ceased operating. Additionally, because AI tools are driven by the datasets used to train the AI models, consideration should be given to requiring an escrow of the underlying dataset itself and not just the source code of the AI tool. See, e.g., [Source Code Escrow Clauses \(Software License Agreement\) \(Pro-Licensee\)](#).

Service Level Agreements

Many popular AI tools are offered as Software as a Service (SaaS) and are therefore not distributed and hosted locally on the customer's hardware. As with any SaaS agreement, a Service Level Agreement should be negotiated and included as part of the contracting documents. See, e.g., [Cloud Computing Service Agreement \(Pro-Customer\)](#).

Updates

As noted above, AI tools are driven by large datasets that the AI algorithms are trained on. Those datasets have a cutoff date and the AI is therefore unaware of, and cannot utilize, any information that came into existence after the cutoff date. For example, ChatGPT-3, a popular AI tool, has a dataset cutoff date of September 2021 (the exact date is not public information). Therefore, if you ask ChatGPT-3 a question such as "who won the 2022 World Series," it is unable to respond. When negotiating a contract for an AI system, data cutoff dates, whether there will be updates to the dataset, the timing of those updates, and the delivery of those updates are all topics that should be negotiated and included in the contracting documents.

Consumer Products

The Internet of Things (IoT) is a network of devices that communicate with each other through networks like the internet. From toaster ovens to thermometers, industrial and consumer home devices are having chips placed into them to collect, store, and communicate data with each other through the internet. By combining these electronically connected devices with computerized systems, individuals and businesses can now readily gather a wealth of valuable information. This data is used with AI to predict behavior, such as changing thermostat temperatures based upon a prediction of when occupants of a home may be present or absent, or asleep or awake. In this way, AI has permeated consumer devices. IoT devices can be found in almost every industry, including:

- Healthcare (e.g., implantable medical devices)
- Fitness (e.g., wearable fitness trackers)
- Transportation (e.g., self-driving vehicles and technology that controls streetlights)
- Home consumer products (e.g., gadgets that control televisions, alarm systems, thermostats, appliances, and lighting systems)
- Agriculture (e.g., technology that measures soil and water conditions and automates fertilization) –and–
- Toys (e.g., dolls that record, remember, and respond to a child's voice)

Computers, laptops, and tablets are not considered IoT devices, although they regularly communicate with such devices and are, generally, an integral part of their functionality. IoT devices all include a physical product, software, and internet or cloud connectivity. As such, it is sometimes unclear whether a specific IoT device is a product, a service, or a combination of both. Products (and hybrid product/services) are subject to product liability legal standards that generally include the potential for the manufacturer to be strictly liable for damages. Pure services, however, are not subject to the same, stringent standards. Software as a Service technology that incorporates AI is considered a pure service, at least from the vantage point of the customer or end user. However, a service provider may have a valid product liability claim against the software's manufacturer. In other words, multiple warranties may apply to an IoT device. Product liability is discussed in further detail, below. For more information on the subject matter, see [Internet of Things Key Legal Issues](#).

Products Liability

No statutes currently address the injuries and loss that can be caused specifically by the use of AI. As such, courts generally apply traditional legal theories to their use when determining who is at fault when an AI product causes injury, loss, or damage. This area of law is evolving as AI permeates products.

Product Liability Legal Theories

Product liability law is based upon the theories of negligence, breach of warranty, and strict liability.

Negligence

The elements of the tort of negligence for product liability are the same as for any other negligence tort. A plaintiff must establish the following:

- The defendant owed plaintiff a duty of a minimum standard of care that a reasonable person should have exercised under the particular circumstances. Examples include negligent product design or inadequate instructions or warnings regarding the safe use of the product.
- Defendant breached this duty by failure to meet the standard of care.
- The breach of the standard of care caused injury or damage to the plaintiff.

In product liability cases, those who provide the product owe a standard of care to each person reasonably

affected by the product. Privity of contract is therefore not necessary. Additionally, a plaintiff asserting a negligence claim does not have to be directly engaged with the defective product. A plaintiff may be a witness or a bystander that is affected by the product defect. Breach of the duty of care can occur in many stages in the supply chain. The duty can be breached in the design, manufacturing, testing, assembly, distribution, and/or sale of the product. A claim premised upon a negligence theory of product liability may also include failure of the duty to warn, a failure to provide an adequate warning, or a failure to warn of defects which become known after the product has been placed into circulation. Note that a party could have a claim for failure to warn in addition to strict liability.

Breach of Warranty

A plaintiff could claim breach of warranty for a product purchased or procured from the defendant based upon the terms of the parties' sales agreement. To have standing to assert a breach of warranty claim, there must generally be privity of contract, meaning that only those parties to an agreement will have any enforceable rights and/or obligations under that contract. In other words, a party who is not provided a warranty as a purchaser or lessor pursuant to a sales or lease agreement generally may not bring a claim for breach of warranty. Courts have routinely rejected warranty claims when there is no privity between the plaintiff and the defendant that sold the item, although a claim may still be permitted when the plaintiff's claim involves personal injuries. As such, a consumer that obtains goods from a seller that is distributing the merchandise on behalf of another party should ensure that it receives a warranty (or pass-through warranty, as applicable) so that it has adequate recourse if necessary, particularly since the risks associated with AI-related malfunction are high.

Warranties may be either express or implied. An express warranty is an affirmative promise or guarantee about the quality or features of the goods being sold by a seller, which becomes part of the basis of the bargain that the goods will conform to the seller's affirmation or promise. Generally, express warranties are statements and promises, which can be written or oral, voluntarily made by the seller regarding its goods. Implied warranties are automatically made whenever goods are sold. Implied warranties are created by law and guarantee that the goods acquired by buyers will meet certain minimum standards. The seller is not required to make any statement or engage in any conduct for an implied warranty to exist, nor does there need to be any intent between the parties to create an implied warranty. The two primary implied warranties are the implied warranty of merchantability (i.e., that the

goods are fit for the ordinary purposes for which they are intended) and the implied warranty of fitness for a particular purpose (i.e., that the goods are fit for the particular purpose for which the buyer is acquiring them and the seller has reason to know what, exactly, that is). For more information on express and implied warranties, see [Uniform Commercial Code Article 2 Express Warranties](#) and [Uniform Commercial Code Article 2 Implied Warranties](#).

Strict Liability

The elements for a claim of strict liability in product liability are:

- The product was sold in an unreasonably dangerous condition
- The product would reach the consumer without alteration or correction of that condition (it is expected that the product will be sold without any defect)
- The product caused injury or damage to the plaintiff

Assume that a strict liability claim is available against a manufacturer for defects. The standard may be as simple as a failure to meet the consumer's reasonable expectations. A strict liability claim is certainly available for any inherently dangerous product, such as an AI-driven autonomous automobile. Any hazardous defect or failure in a dangerous product must be removed prior to the product being sold to avoid a strict liability claim. Fulfilling the duty to warn after the fact, which may be a defense to a negligence claim, does not avoid a claim for strict liability.

A plaintiff may also claim strict liability if there is a hazardous defect in the design or in the packaging of a product. Though it might seem that there is a bright line separating claims for strict liability from the others, note that the condition of the product itself gives rise to strict liability. In that sense, most parties in a supply chain are subject to liability, this includes the designer, the materials manufacturer, the assembler, the packager, the reseller, and the merchant. The strict liability claim for a product defect is ultimately grounded in public policy. Accordingly, claims based on the premise that the risk of the product outweighs the value of the product to society are found in the strict liability theory of product liability. Note, however, that each state treats strict liability claims in its own way and as such, you should understand well the laws applicable to the contract at hand. For instance, some jurisdictions do not impose liability on a product's seller if such seller does not alter or modify the item. Most states, however, have adopted [Section 402A of the Restatement \(Second\) of Torts](#), which provides that whomever sells a product in a defective condition which is, therefore, "unreasonably dangerous," may be liable for property damage or physical harm despite the exercise of due care

otherwise and/or a lack of privity of contract between the seller and the consumer. For further guidance on applicable state products liability law, see [Products Liability State Law Survey](#).

AI-Related Product Liability Cases

Cruz v. Talmadge

In *Cruz v. Talmadge*, 244 F. Supp. 3d 231 (D. Mass. 2017), the plaintiffs were injured (some killed) when the bus that they were on struck an overpass. The plaintiffs sued the manufacturers of the two GPS devices (a popular AI item) that were guiding the driver under the theories of breach of warranty, strict liability, and negligence. They claimed the devices were defective in that (1) they did not lead the driver to an alternate route to avoid the low overpass; and (2) they did not warn the driver of this unreasonably dangerous situation, despite the fact that the device's manufacturers had the requisite data to provide users with information about height restrictions. Additionally, the plaintiffs successfully argued that the accident was foreseeable in that many an accident of a substantially similar nature had taken place over the years.

Nilsson v. General Motors, LLC

In *Nilsson v. General Motors LLC*, Case No. 4:18-cv-00471 (N.D. Cal. June 26, 2018), plaintiff, an injured motorcyclist, was hit by an autonomous vehicle (AI-controlled car) when it swerved into his lane on a highway. A backup driver was in the car at the time of impact but was not operating the vehicle. The plaintiff sued the manufacturer solely on the theory of negligence, arguing that the vehicle itself (and not the backup driver) drove negligently (i.e., that the car did not use reasonable care when driving). The manufacturer, General Motors, surprisingly admitted that the car (known as the Bolt) was, in fact, required to meet this threshold. The case settled before going to trial, yet it raised several novel issues, including the following:

- When fault cannot be attributed to a particular person or persons, a court must decide how to apply the "reasonable care" standard to a nonhuman actor (i.e., how to establish a "reasonable machine" standard).
- Where an AI product acts autonomously, a court must establish how foreseeability is determined.
- If products themselves can be held liable, then it is ambiguous as to who should be responsible for the injury or damage that they cause.

For additional guidance on product liability and product liability claims, see [Product Liability Claims, Defenses, and Remedies](#) and [Product Liability Claims Preemption and Mitigation](#).

Intellectual Property Issues

The creation, sale, license, and use of AI, along with its related technology, presents IP issues with respect to ownership and infringement. Specifically, IP is protectable through patents, trade secrets, and copyrights.

Patents

A patent for an invention is a property right grant to the inventor (with whom it originally vests, see 35 U.S.C. § 100(f)) and is issued by the U.S. Patent and Trademark Office (USPTO). The term of a new utility patent is 20 years commencing on the date that the application for the patent was filed plus any extensions that may be available, less any terminal disclaimers. For a new technology to be patent eligible, consult Section 101 of the U.S. Patent Act (35 U.S.C. § 101), which requires an invention to be novel, non-obvious, and accompanied by a sufficiently detailed written description of its structure and functionality to enable a person of ordinary skill to make and use the full scope of the particular invention. See 35 U.S.C. § 112. Abstract ideas that do not demonstrate at least one inventive concept are not patentable. See *Diamond v. Chakrabarty*, 447 U.S. 303 (1980); see also *Alice Corp. Pty. Ltd. v. CLS Bank Int'l.*, 134 S. Ct. 2347 (2014). For further guidance, see [USPTO Revised Patent Subject Matter Eligibility Guidance](#), 84 Fed. Reg. 50 (Jan. 7, 2019) and [USPTO Patent Subject Matter Eligibility Guidelines 2019](#). The requirements of *Alice Corp.* will apply to inventions that claim AI within the scope of the patent.

The USPTO uses the designation Class 706 (Data Processing: Artificial Intelligence) to classify inventions that exploit or incorporate AI. Note that while patents are valuable tools to protect IP, they do present certain risks, including:

- The application process generally takes several years during which there is no recourse against infringers – and–
- The process requires public disclosure of the invention (i.e., the inventor is required to divulge valuable trade secrets)

Additionally, AI is being used, more and more, to create patentable inventions on its own. For instance, AI has already been known to develop novel and valuable datasets, computer codes, and improved apparatus. The Patent Act, however, pursuant to 35 U.S.C. § 100(f), requires all inventors to be individuals, and natural persons (i.e., not corporations). See the USPTO's [Manual of Patent Examining Procedure](#) (MPEP) (MPEP § 2137.01); see also *Beech Aircraft Corp. v. Edo Corp.*, 990 F.2d 1237 (Fed. Cir. 1993).

Thaler v. Vidal

Computer scientist Stephen Thaler has been challenging the USPTO's position that AI cannot serve as an inventor. Thaler founded Imagination Engines, Inc. and created an advanced artificial neural network technology named the Device for the Autonomous Bootstrapping of Unified Sentience, or DABUS for short. Thaler has described DABUS as “a collection of source code or programming and a software program.” *Thaler v. Vidal*, 43 F.4th 1207, 1209 (Fed. Cir. 2022). DABUS has allegedly created artwork and two inventions, a “Neural Flame” and a “Fractal Container.” Thaler filed patent applications for both alleged inventions and listed DABUS as the sole inventor on both. The USPTO “concluded both applications lacked a valid inventor and were, hence, incomplete” and subsequently denied both applications on the ground that “a machine does not qualify as an inventor.” *Thaler*, 43 F.4th at 1210. Thaler sought judicial review of the USPTO's decision, which was upheld. *Id.* Thaler then sought review by the Federal Circuit, which determined that “an ‘inventor’ must be a human being . . . ” *Thaler*, 43 F.4th at 1212. Thaler then sought review at the U.S. Supreme Court, which denied review on April 24, 2023.

Thaler has sought registration of the alleged inventions created by DABUS in other countries and jurisdictions as well, including the United Kingdom, European Union, South Africa, and Australia. In the United Kingdom, Thaler's patent applications were rejected by the UK Intellectual Property Office on the grounds that the inventor must be a human or a company rather than a machine. Thaler appealed his case to the UK's Supreme Court, which heard arguments on March 2, 2023; a decision remains pending. Thaler's applications in the European Union, Australia, and Germany have also been rejected on similar grounds. However, Thaler's applications in South Africa were allowed. The patentability of AI-created inventions must therefore be considered on a country-by-country basis.

Another issue may arise when an AI system itself infringes a third-party IP right. Courts are split as to whether liability rests with the AI's owner at the time of infringement or its program developer. For additional guidance on patent infringement and patents generally, see [Patent Litigation Fundamentals](#) and [Patent Fundamentals](#).

Trade Secrets

A trade secret is information that a person or company makes a reasonable effort to protect and which derives independent economic value. Trade secret protection can be a valuable way to protect AI (such as algorithms or source code), and may include a pattern, compilation, device, program, formula, technique, process, or method. Trade secrets are protected under the Defend Trade Secrets

Act of 2016 (DTSA), which amends the U.S. Economic Espionage Act of 1996 (18 U.S.C. § 1831 et seq.). This statute (1) creates a private cause of action for trade secret misappropriation and (2) grants legal immunity to corporate whistleblowers. Most states maintain their own trade secret statutes as well, primarily modeled on the Uniform Trade Secrets Act (UTSA), a model law published by the Uniform Law Commission in 1979 and adopted by 48 states, which:

- Defines the types of information entitled to trade secret protection
- Sets forth a private cause of action for misappropriation –and–
- Provides remedies for misappropriation, including injunctions, monetary damages, and, in some instances, reasonable attorney’s fees

For additional guidance, see [Defend Trade Secrets Act \(DTSA\) Fundamentals](#).

Generally, trade secret protection applies liberally to information that meets the following criteria:

- The information is not generally known outside of the business’ organization and control.
- The business owner derives business advantage and/or independent economic value from the information’s confidentiality.
- The business owner makes ongoing, reasonable efforts to preserve the information’s secrecy. Examples of such efforts include password protecting digital information, keeping physical information under lock and key, providing information solely to those individuals requiring it to perform their job functions, requiring employees and agents to execute nondisclosure agreements (NDAs), establishing and enforcing written policies governing access to and use of trade secrets, and using data loss prevention software and encryption services wherever applicable. For a sample NDA, see [Confidentiality Agreement with Employee \(Unilateral\)](#).

Most forms of AI are potentially protectable as trade secrets, as their owners will most certainly use ongoing, reasonable efforts to guard their technological know-how to profit from their proprietary knowledge and the resultant work product, particularly the algorithms, the datasets, and how the algorithms are trained on the datasets. One of the greatest advantages of trade secret protection is that it lasts indefinitely, so long as the trade secret is not publicly disclosed. Additionally, unlike patent or copyright protection (discussed below), there is no application or registration process as a prerequisite to enforcement, and the owner of the trade secret is not required to publicly disclose the trade secret. Significant and ongoing efforts,

however, are required to protect the proprietary nature of the information to maintain trade secret protection, efforts that are not required for patent or copyright protection. For more information on trade secrets generally, see [Trade Secret Fundamentals](#) and [Trade Secret Misappropriation: Elements, Remedies, and Defenses](#).

It appears likely that the law will recognize as enforceable trade secrets that are created by AI. Unlike patents and copyrights, there is no legal requirement that a trade secret be created by an individual. Moreover, a trade secret created by AI (such as a proprietary pricing model) facially satisfies all requirements to be protectable as a trade secret: it is not generally known by third parties, it can derive independent economic value, and the party operating the AI that created the trade secret can take commercially reasonable measures to protect the secrecy of the trade secret.

Copyrights

A copyright protects an original work of authorship that has been fixed in a tangible medium of expression. Common works of authorship include literary, musical, and dramatic works; motion pictures; and sound recordings. Registration in the U.S. Copyright Office is not required to obtain a copyright. However, registration (or preregistration) is a necessary condition precedent to bringing and maintaining a civil action against a third-party infringer. Copyrights automatically vest with the author or, if the work is a “work made for hire,” with the employer of an employee who creates the work in the ordinary scope of their employment. It is important to note that the “work made for hire” doctrine does not apply to independent contractors, except in limited circumstances. For information on works made for hire, see [Works Made for Hire](#) and for guidance on copyright registration, see [Registration of Copyrights](#). See also [Copyright Fundamentals](#).

Pursuant to the Copyright Act, the following are eligible for copyright protection:

- Literary works (which can include catalogs, directories, computer databases, and computer programs)
- Musical works, including any accompanying words
- Dramatic works, including any accompanying music
- Pantomimes and choreographic works
- Pictorial, graphic, and sculptural works
- Motion pictures and other audiovisual works
- Sound recordings
- Architectural works

17 U.S.C. § 102(a).

As such, copyright protection is available for some types of AI, including source code and the visual elements of an AI computer program, provided they are fixed in a tangible medium of expression. See *Sega Enters. v. Accolade, Inc.*, 977 F.2d 1510 (9th Cir. 1992). Note, however, that the functional aspects of such copyrightable materials, including, the formatting, logic, algorithms, hardware, or system designs, are not copyrightable.

The requirements for obtaining copyright protection are less stringent than those required for obtaining patent protection. Additionally, to prevail on a copyright infringement claim, a plaintiff must be capable of proving actual copying (something that is not required to prevail on a patent infringement claim), and such copying cannot fall under the fair use exception. For more information on fair use, see [Fair Use Considerations](#) and for additional guidance on copyrights generally, see [Copyright Fundamentals](#).

Thaler's A Recent Entrance to Paradise

As with patents, there has been an ongoing dispute, led by Thaler and his DABUS AI, whether AI can be an “author” and whether AI can own copyrights in the “works” it creates. While the U.S. Copyright Act (17 U.S.C. §§ 101–180) (Copyright Act) does not define the term “author,” the U.S. Copyright Office, along with most courts, have determined that authors must be human (see *Naruto v. Slater*, 888 F.3d 418 (9th Cir. 2018)). In 2018, Thaler sought copyright registration for an image created by DABUS in 2014, titled “A Recent Entrance to Paradise.” As with the patent applications, Thaler listed DABUS as the author of the work on the application filed with the U.S. Copyright Office (USCO). Thaler claimed that the artwork was “autonomously created by a computer algorithm running on a machine” and claimed it was a work made for hire; Thaler did not assert that the artwork was created with contribution from a human author. The USCO refused registration on the basis that human authorship was required. Thaler sought reconsideration and the U.S. Copyright Review Board upheld the USCO’s decision, determining that an author must be human. Additionally, the Review Board rejected Thaler’s argument that the artwork was a work made for hire because “[a] work made for hire must be either (A) prepared by ‘an employee’ or (B) by one or more ‘parties’ who ‘expressly agree in a written instrument’ that the work is for-hire.” The Review Board determined that DABUS was not an employee and, as a “creativity machine,” DABUS could not enter into a binding legal contract.

Zarya of the Dawn and Mixed Human/AI Works

There remains the question of how much computer or AI involvement in the creation of a work renders the work

ineligible for copyright protection. Computers have long been used as tools by artists when creating works, from programs like Adobe’s Photoshop used by photographers to retouch and enhance photographs, to digital artists whose works are created entirely using computer tools. None of the foregoing works have been denied copyright registration on the same basis that Thaler and DABUS were denied registration. Additionally, many AI tools can accept a wide variety of user control in the input, from the simple request to create “a drawing of a car” to the increased user control for “an F1 style racecar” to the still more user control to “use this drawing I made to create an F1 style racecar driving on a track with Sir Jackie Stewart as the driver.” How much AI use in creating a work is too much, and how much control a human must exert over the AI tool to be eligible for copyright protection, remain open legal questions. While it is clear that works created entirely by humans with no AI input can be registered as copyrights, and works created entirely by AI with minimal human input are ineligible for copyright protection, the line where a work shifts from protectable to non-protectable remains elusive at this time.

Guidance does exist for mixed works created by both human and AI authors. Kristina Kashtanova applied to the USCO for registration of a copyright in her comic book titled *Zarya of the Dawn*. *Zarya of the Dawn* was created by Kashtanova, who used the Midjourney AI technology to create the artwork contained within the comic. Kashtanova applied to the USCO for a copyright registration, listing only herself as the author of the work. The USCO granted Kashtanova a copyright registration. Subsequently, the USCO sought more information from Kashtanova regarding the authorship of the work. The USCO ultimately cancelled a portion of Kashtanova’s copyright registration; Kashtanova received a copyright registration for the text of the work as well as the selection, coordination, and arrangement of the work’s visual elements. However, the visual elements themselves—which were created by the Midjourney AI were cancelled from the registration certificate. Therefore, copyright registration certificates can be received for the human-created portions of a work that contains mixed human/AI elements.

Infringement

Another open question is the issue of infringement of third-party intellectual property. As noted above, AI tools are ‘trained’ on large datasets. In the case of artwork-generative AI tools, the training datasets typically consist of information scraped from the internet or other sources. This means that AI tools are almost always trained substantially, or entirely, on works created by others, which raises the question—are the outputs of AI tools derivative works of

the third-party works the AI model was trained on? While there is no definitive answer yet, there is ongoing litigation on this topic. These lawsuits are currently in an early stage and have not yet produced any notable decisions.

Finally, it remains unclear whether AI-generated work is owned by the applicable software programmer or another party, such as the person who inputted data into the AI system to generate the work in the first instance. This is yet another open question that will be determined as litigation progresses.

For a discussion of copyrightability of generative AI in the U.S. and Europe, see [Generative AIs Challenged By Copyright and Related Rights: A Comparative Approach in European and U.S. Law](#).

Privacy and Data Security Issues

As noted above, an AI system generally relies heavily on large volumes of data. Much of the data being exploited includes customer and user personal information, including some highly sensitive data, such as individual financial and/or health records. Such exploitation raises important privacy and data security issues. Extra precautions must be taken to ensure that this information is protected from unauthorized use and disclosure. To mitigate risk, in addition to ensuring compliance with data privacy laws (discussed further below), ensure that encryption is used wherever possible (both when data is in transit and at rest), password protect all proprietary digital information, require employees and agents to execute NDAs (and any other agreements that may be necessary, such as Business Associate Agreements), and provide confidential information only to those who require it and on a just-in-time basis.

Applicable Laws

All applicable laws governing privacy and data protection must be adhered to (such as the DTSA), including those that apply solely to specific types of data. For example, healthcare information is subject to the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act, information respecting children may be subject to the Children's Online Privacy Protection Act, and certain financial information may be subject to the Gramm-Leach-Bliley Act (GLBA) or the Fair Credit Reporting Act (FCRA). Additionally, whenever personal information is processed, a business should ensure that the appropriate privacy addendums are entered into (including those addressing the EU General Data Protection Regulation (GDPR),

Regulation (EU) 2016/679, and the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), Cal. Civil Code § 1798.100 et seq., where applicable). For information about the GDPR and the CCPA, see [General Data Protection Regulation \(GDPR\) Overview Resource Kit](#) and [CCPA/CPRA Compliance: Comparing Key Provisions of the GDPR and CCPA/CPRA](#). For additional guidance on privacy and data security generally, see [Privacy and Data Security Considerations When Negotiating or Reviewing a Transaction or Agreement](#) and for general information on data protection and privacy internationally, see [Data Protection and Privacy in International Jurisdictions](#).

AI-Specific Laws

The United States does not currently maintain any federal statutes specifically regulating privacy and automated decision-making in general. Nevertheless, some U.S. laws generally govern AI and automated decision-making, including the following:

- **The Fair Credit Reporting Act (FCRA) (15 U.S.C. § 1681 et seq.).** This act serves to promote the fairness, accuracy, and privacy of consumer information included in the records of consumer reporting agencies.
- **FTC guidance.** In April of 2020, the Federal Trade Commission (FTC) issued guidance (FTC guidance) with respect to a business's use of AI for machine learning technology and automated decision-making. The FTC guidance includes best practices for managing consumer protection risks arising from the exploitation of AI. Among other things, the guidance provides that AI algorithms should be transparent, fair, explainable, and empirically sound.
- **The Illinois Artificial Intelligence Video Interview Act of 2020 (820 ILCS 42/1).** This statute addresses the use of AI in the hiring context, and requires employers who exploit it to analyze video job interviews to do the following:
 - Inform job applicants that AI will be used to analyze their videos.
 - Explain how their AI program works and exactly how the applicant will be evaluated.
 - Obtain the applicant's prior consent.
 - Share the videos only with those individuals required to evaluate the applicant.
 - Destroy all copies of the video within 30 days after an applicant's request therefor.

While there are no AI-specific laws or regulations currently enacted in the United States, it is likely that rulemaking and legislation will begin to appear. If, as has happened

with data privacy in the United States, the legislative and rulemaking process takes place at the state, as opposed to federal level, creators and users of AI will be faced with a multistate patchwork of rules and laws to follow.

The European Union is already working on AI-specific rules and regulations. On September 28, 2022, the European Commission adopted two proposals “to adapt liability rules to the digital age, circular economy and the impact of global value chains.” The proposals modernize existing rules on strict liability of manufacturers for defective products and propose harmonizing national liability rules for AI, “making it easier for victims of AI-related damage to get compensation.”

AI-Specific Challenges

The exploitation of AI creates certain challenges when trying to comply with data protection and privacy principles. For instance, data protection laws generally require a business to only collect, store, and use whatever personal information is absolutely necessary to achieve the stated purposes of such data’s processing. After such use, the data should be purged from the business’ database. However, companies that exploit AI will face challenges meeting these obligations, particularly since AI usually involves collecting as many data points as practically possible for the most informed outcome and storing that data, both the training data and the output data. This is particularly true with wearable technology. Best practices include de-identifying the data wherever possible, including through the use of encryption and pseudonymization (otherwise known as anonymization) techniques.

Furthermore, FTC guidance requires businesses to explain their algorithmic decision-making processes to individuals. This can pose a problem when such disclosure requires the entity to reveal proprietary information (including trade secrets). Additionally, businesses are restricted to processing personal information pursuant to their disclosed purpose(s) only, yet it is near impossible to accurately predict what, exactly, the AI algorithms will learn and what resultant data will be gathered. New information can, therefore, be exploited for new purposes that were never originally disclosed to the consumer at the time of their disclosure. Best practices include regularly auditing the company’s use of personal information to ensure that such use is consistent with the purposes disclosed to the consumers when collecting their data. If such use is not consistent, a business should promptly update all of its privacy policies to account for the new purpose(s) and, where necessary or appropriate, obtain new consent (particularly for highly sensitive data) and de-identify the information as much as

possible. For a sample privacy policy, see [Privacy Policy \(UK GDPR\)](#).

Finally, employers that exploit AI recruiting and screening tools must ensure compliance with their applicants’ privacy rights, including, by way of example, those addressing password privacy, salary history bans, and biometric privacy laws.

Bankruptcy Issues

Under the U.S. Bankruptcy Code, IP includes the following:

- Copyrighted works of authorship and mask works protected under the U.S. Copyright Act
- Trade secrets
- Patent applications and patented inventions protected under the U.S. Patent Act
- Plant varieties

11 U.S.C. § 101(35A). Note the exclusion of trademarks, service marks, and trade names, which are treated differently in bankruptcy court.

Pursuant to Section 365 of the Bankruptcy Code, a debtor in bankruptcy is entitled to assume, assign, or reject executory contracts (subject to court approval). Courts generally define executory contracts as contracts on which performance is due to some extent on both sides. As such, they can be assigned by a debtor in bankruptcy despite any anti-assignment language in the applicable agreement. See 11 U.S.C. § 365(f)(1).

Note that IP licenses (including AI licenses) are typically considered executory contracts, as both the licensor and the licensee generally maintain significant ongoing obligations under the agreement’s terms. A debtor’s right to reject unfavorable AI licenses, for example, can have a huge impact on the party’s creditors. Section 365(n) of the Bankruptcy Code, however, provides creditor-licensees with special protections if a debtor rejects an IP license. Specifically, such creditors may:

- Treat the license agreement as fully terminated and collect rejection damages (which, unfortunately for the creditor, are mere pennies on the dollar) –or–
- Retain its rights under the license agreement, subject to payment of all royalties due to the debtor/licensor, and further subject to the creditor’s provision of:
 - A waiver of any rights to set off any future or past royalties against damages arising out of the debtor’s rejection of the agreement

- o A waiver of any administrative claim that it may have against the debtor's estate arising from the debtor's performance under the applicable license agreement

Additionally, anti-assignment provisions are not applicable to the debtor in bankruptcy (subject to court approval). However, pursuant to 11 U.S.C. § 365(c)(1), a debtor is not permitted to assign or assume an executory agreement if applicable law excuses a party to the agreement (other than the debtor) from rendering performance to or accepting performance from an entity other than the debtor and this party does not consent to the assignment or assumption.

Finally, pursuant to *Section 363 of the Bankruptcy Code*, a debtor is entitled to buy and sell assets "free and clear" of liabilities. However, courts have generally held that if a debtor is the licensor of a nonexclusive copyright or patent (which are usually used to protect AI), the debtor is not entitled to sell the IP free and clear of those rights retained by the licensees after rejecting the agreement in question. See *In re Dynamic Tooling Sys., Inc.*, 349 B.R. 847 (Bankr. Kan. 2006). As such, the non-debtor IP licensees may continue to exploit the licensed IP. For more information regarding license agreements and bankruptcy, see [IP License Agreements: Change of Corporate Control and Bankruptcy Issues](#).

Antitrust Considerations

AI is now being used by many businesses to engage in potentially anticompetitive behavior in violation of applicable law, including, the Sherman Antitrust Act, 15 U.S.C. § 1 et seq., the Clayton Antitrust Act, 15 U.S.C. § 12 et seq., and comparable state statutes. Specifically, AI could be used to facilitate price-fixing arrangements among competitors as well as to reach anticompetitive agreements with other AI systems (each of which are unlawful per se). For instance, the [U.S. Department of Justice obtained a guilty plea](#) from an individual named David Tompkins who, along with several co-conspirators, agreed to fix the prices of certain posters sold online through Amazon Marketplace by adopting specific pricing algorithms for their sale with the goal of coordinating swift changes to their respective prices. The defendants wrote computer code that instructed algorithm-based software to set prices pursuant to this agreement. For more information regarding antitrust law, see [Antitrust Law Fundamentals](#).

Furthermore, AI systems in and of themselves can enter into anticompetitive agreements without human direction or interaction. This can occur when an AI system develops the ability to test and understand market conditions and consumer behavior so that with this information, the system, either alone or in conjunction with another AI

system, will conclude that collusion would be a successful means of maximizing profits.

Employment Issues

The average workplace today relies heavily on AI for recruiting, screening, interviewing, hiring, onboarding, and employee management functions, among other things. Additionally, robots have been developed to perform repetitive tasks under human supervision. For more information, see [Artificial Intelligence and Robots in the Workplace: Best Practices](#).

Recruiting, Screening, Interviewing, and Hiring Employees

AI is being used on a regular basis to sort, rank, and disqualify potential candidates without significant human supervision. This process, however, remains subject to all applicable employment and anti-discrimination laws and AI tools bring inherent risks to this process. For instance, AI tools generally exploit social media, public databases, and the internet in general for information about prospective employees, some of which is off-limits during an interview or on an employment application (such as marital status, political orientation, sexual orientation, race, nationality, or religion). As such, the unconscious bias that affects human recruitment activities is not eliminated and may actually be enhanced. In addition, it is far more challenging to prevail on a discrimination case without human involvement, as there is no way to prove intentional discrimination, or demonstrate how, exactly the AI system made its decision on behalf of a business in the first instance.

However, most discrimination cases rely on circumstantial evidence under the *McDonnell Douglas* burden-shifting analysis, promulgated in 1973 by the U.S. Supreme Court in *McDonnell Douglas Corp. v. Green*, 411 U.S. 792 (1973). Under the *McDonnell Douglas* standard, a plaintiff alleging employment discrimination bears the initial burden to establish a "prima facie case." If the plaintiff satisfies their prima facie burden, the burden shifts to the employer to articulate (not prove) a "legitimate, nondiscriminatory reason" for the adverse employment action. Once the employer has done so, the burden shifts back to the plaintiff to prove that the employer's articulated reason for its actions is a "pretext" for unlawful discrimination. Using this framework may make it far more challenging for an employer to articulate a legitimate business reason behind an AI-driven decision not to hire someone.

Additionally, employers that exploit AI recruiting tools that provide access to criminal records must ensure compliance with applicable law, including the FCRA (15 U.S.C. § 1681)

and comparable state background check statutes. Note, for instance, that AI systems with access to prospective employees' social media account information may arguably qualify as a consumer reporting agency which would trigger certain reporting and disclosure obligations under the FCRA (see 15 U.S.C. § 1681b(b)(2)(A)). Some jurisdictions also impose strict notification requirements on employers who take adverse actions against interviewees based upon background check results. For additional guidance on background checks and corresponding notification requirements, see [Criminal Background Checks: Key Analyses and Considerations](#) and [Fair Credit Reporting Act \(FCRA\) and State Mini-FCRAs: Step-by-Step Guidance for Compliance](#).

Finally, as mentioned earlier in this practice note, employers that exploit AI recruiting and screening tools must ensure compliance with their applicants' privacy rights and applicable privacy laws, including those addressing password privacy, salary history bans, and biometric privacy laws, to name a few.

AI Robots in the Workplace

AI-powered robots (such as floor cleaners, autonomous carts, and drones) are being mass produced for use in the workplace. Their use raises many concerns, several of which are discussed below.

Safety and Accident Issues

Employers are responsible for providing a safe working environment, and in connection therewith, are subject to statutes including the Occupational Safety and Health Act of 1970 (OSHA), along with a host of state and local laws that similarly govern workplace health and safety obligations.

There are currently no OSHA standards specifically for the robotics industry. However, the OSHA highlights general standards and directives applicable to employers utilizing robotics. See [Robotics, Standards, Occupational Safety and Health Administration, Safety and Health Topics](#). OSHA also provides guidelines for robotics safety. See Guidelines for Robotics Safety, OSHA Instruction STD 01-12-002 (1987). Under OSHA, a covered employer utilizing robotics—like any other employer OSHA covers—must conduct a “hazard assessment,” in which it reviews working environments for potential occupational hazards. See 29 C.F.R. § 1910.132(d). An employer that identifies a hazard must implement a “hazard control,” in the following order of preference, hazard elimination, hazard replacement, engineering controls, administrative controls, or personal protective equipment. See [OSHA Recommended Practices for Safety and Health Programs, Hazard Prevention and Control](#). With this legal

framework as background, consider taking the following actions to mitigate the risk of employee exposure to hazards and legal actions associated with robots:

- Enlist the assistance of an OSHA-trained attorney to assist at the outset of implementation
- Have the employer develop a basic understanding of the robot's potential hazards and preventative measures the employer can take should the robot malfunction, such as the steps for shutting it down –and–
- Know who to contact (i.e., which engineers to enlist) when a robot misbehaves (This is particularly important as the cause of many workplace injuries and accidents involving AI-powered robots are not easy to determine and as such, an employer may not be capable of satisfying OSHA or other regulatory agencies that it has taken the proper steps to prevent a deleterious incident from happening again.)

For more information on complying with OSHA generally, see [OSH Act Requirements, Inspections, Citations, and Defenses](#).

Mass Layoffs; Employee Termination

Thanks to recent technological advances, AI algorithms and robots are developing the sophistication to displace human employees, causing many employers to engage in mass layoffs and reductions in force. For instance, Goldman Sachs recently laid off nearly 600 equity traders whose work has largely been supplanted by automated trading programs and a team of computer engineers.

In any event, when terminating or laying off employees, the employer should ensure the following:

- That the notification requirements of the Worker Adjustment and Retraining Notification Act (WARN Act) and comparable state statutes (i.e., “mini-WARN Acts”) are complied with.
- That all other employment-related laws are complied with including, by way of example, those related to age discrimination.

For a more detailed discussion about this subject matter, see [Artificial Intelligence and Robots in the Workplace: Best Practices](#).

Employee Benefit Plans

AI is also being used to assist in the management of employee benefit plans and programs. For instance, such technology is routinely being employed to communicate information to plan participants regarding their benefits (including open enrollment and other time-sensitive

information). An employer's biggest concern and area of risk is privacy, and particularly, compliance with HIPAA and comparable state statutes. Health-related AI apps require the user to provide a wealth of highly sensitive personal information, much of which is subject to heightened privacy and data security requirements. Employers using apps that violate applicable privacy and/or data protection laws can be held liable, along with the apps' developers and/or apps' IP owners, for health-related statutory violations, and such violations carry extremely steep penalties. Best practices for an employer include obtaining a broad indemnification from the app's developer and/or owner covering any such violations, and regularly monitoring how their employees' personal information is being used.

Related Content

Resource Kits

- [Generative Artificial Intelligence \(AI\) Resource Kit](#)
- [Intellectual Property & Technology Fundamentals Resource Kit](#)
- [Intellectual Property Licensing Resource Kit](#)
- [General Data Protection Regulation \(GDPR\) Overview Resource Kit](#)

Practice Notes

Commercial Transactions

- [Artificial Intelligence and Automation in E-Commerce](#)
- [Remedies](#)
- [Indemnification Provisions in Commercial Contracts](#)
- [Risk Allocation in Commercial Contracts](#)
- [Internet of Things Key Legal Issues](#)
- [Uniform Commercial Code Article 2 Express Warranties](#)
- [Uniform Commercial Code Article 2 Implied Warranties](#)
- [Products Liability State Law Survey](#)
- [Product Liability Claims, Defenses, and Remedies](#)
- [Product Liability Claims Preemption and Mitigation](#)
- [Trade Secret Misappropriation: Elements, Remedies, and Defenses](#)
- [Privacy and Data Security Considerations When Negotiating or Reviewing a Transaction or Agreement](#)
- [OSH Act Requirements, Inspections, Citations, and Defenses](#)

Antitrust

- [Antitrust Law Fundamentals](#)

Data Security & Privacy

- [Criminal Background Checks: Key Analyses and Considerations](#)
- [General Data Protection Regulation Fundamentals \(EU GDPR\)](#)
- [CCPA/CPRA Compliance: Comparing Key Provisions of the GDPR and CCPA/CPRA](#)
- [Data Protection and Privacy in International Jurisdictions](#)
- [Fair Credit Reporting Act \(FCRA\) and State Mini-FCRAs: Step-by-Step Guidance for Compliance](#)

Insurance

- [Artificial Intelligence and Robots in the Workplace: Best Practices](#)

Intellectual Property and Technology

- [USPTO Patent Subject Matter Eligibility Guidelines 2019](#)
- [Works Made for Hire](#)
- [Patent Litigation Fundamentals](#)
- [Patent Fundamentals](#)
- [Registration of Copyrights](#)
- [Fair Use Considerations](#)
- [Copyright Fundamentals](#)
- [IP License Agreements: Change of Corporate Control and Bankruptcy Issues](#)
- [Defend Trade Secrets Act \(DTSA\) Fundamentals](#)
- [Trade Secret Fundamentals](#)

Templates

Commercial Transactions

- [Representations and Warranties Clauses](#)
- [Product Warranty and Disclaimer Clauses](#)
- [Disclaimer of Express Warranties Clauses](#)
- [Insurance Clauses](#)
- [Privacy Policy \(UK GDPR\)](#)

Labor & Employment

- [Confidentiality Agreement with Employee \(Unilateral\)](#)
-

Daniel J. Barsky, Partner, Holland & Knight LLP

Daniel Barsky is an intellectual property attorney in Holland & Knight's Miami office. Mr. Barsky regularly represents clients in intellectual property (IP), information technology (IT) and data-related licensing and transactional matters, including mergers and acquisitions (M&A), private equity transactions, joint ventures, and multilateral and multinational licensing agreements.

Mr. Barsky's clients call upon him to navigate complex transactions involving IP, IT and data assets. He assists and advises clients with navigating the complexities of transactions involving intangible assets such as patents, trademarks, copyrights, trade secrets and data, brand licensing and distribution agreements, blockchain technology such as cryptocurrency and non-fungible tokens (NFTs), software and technology licensing agreements, and transition services agreements.

Post-closing, Mr. Barsky assists clients with the maintenance and enforcement of their IP and IT portfolios with an eye towards leveraging those portfolios to drive revenue and growth. Mr. Barsky oversees, coordinates and maintains multinational trademark portfolios encompassing thousands of marks registered in more than 100 countries, including the monitoring and enforcement of the portfolios, as well as multinational, anti-counterfeiting activities.

In addition to his transactional and counseling work, Mr. Barsky maintains an active, nationwide IP and IT litigation practice and has represented clients in patent infringement, trademark infringement, anti-counterfeiting, unfair competition, copyright infringement and trade secret theft matters, as well as information technology, data privacy, cyberfraud, data breach and hacking matters, and responses thereto.

Mr. Barsky is an active force and thought leader in South Florida's entrepreneurial and startup community. He regularly represents startup and new business ventures and has helped multiple startups develop, protect, grow, monetize and enforce their IP and other business assets. His work with startups and entrepreneurs includes advising on software license agreements, user agreements, privacy policies, brand clearance, brand protection and monetization strategies, blockchain and NFT questions, and IP registration.

Outside of his law practice, Mr. Barsky helped form, and is a former board member of, Tech Lauderdale, which promotes the growth, connectivity and awareness of the thriving technology ecosystem in Greater Fort Lauderdale and throughout South Florida.

Additionally, Mr. Barsky is an adjunct professor at the University of Miami School of Law where he teaches patent litigation and the university's Startup Practicum, and is the university's faculty supervisor for the U.S. Patent and Trademark Office's (USPTO) Law School Clinic Program. In his various roles at the university, Mr. Barsky works with students and clients in the university's startup practicum to foster the development of the South Florida startup and entrepreneurial community and the professionals that are needed to serve and grow that community.

Mr. Barsky is a registered patent attorney with the USPTO and regularly prosecutes patents, trademarks and copyrights for clients.

This document from Practical Guidance®, a comprehensive resource providing insight from leading practitioners, is reproduced with the permission of LexisNexis®. Practical Guidance includes coverage of the topics critical to practicing attorneys. For more information or to sign up for a free trial, visit [lexisnexis.com/practical-guidance](https://www.lexisnexis.com/practical-guidance). Reproduction of this material, in any form, is specifically prohibited without written consent from LexisNexis.