Artificial Intelligence Key Legal Issues

Go to: Defining Artificial Intelligence | AI and General Commercial Contracts | Consumer Products | Products Liability | Intellectual Property Issues | Privacy and Data Security Issues | Bankruptcy Issues | Antitrust Considerations | Employment Issues | Related Content
Maintained

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

Defining Artificial Intelligence

Understanding what artificial intelligence (AI) is and some of its effects on society are necessary first steps in understanding some of the legal risks arising from its application in commerce. There are four main elements comprising artificial intelligence:

- Machine processing
- Machine learning
- Machine perception
- Machine control

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.

AI is computer software that is programmed to execute certain algorithms (i.e., sets of code that are programmed to perform particular tasks) to recognize patterns in large volumes of data, reach conclusions from such patterns, predict future behavior and patterns, make informed judgments based thereon, and as a result, optimize business practices, among other things. 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)

The application and scope of AI has grown exponentially in the past decade and this trend is expected to continue at a rapid pace.

AI and General Commercial Contracts

Businesses that exploit AI have the option of either developing their own AI 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. As with most IP license agreements, pay attention to the key transaction terms below when licensing AI and its component parts (including software, for example).

Representations and Warranties

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

- **Right to contract and license AI.** A licensor should have and maintain the right to enter into the license agreement and license the AI, including all elements contained therein, without violating any agreement, law, and/or third-party right of any kind (particularly, any IP right). Licensors 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).
- **Disclaimers and warranties.** The licensed materials (i.e., the 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 Disclaimers Clauses and Disclaimer of Express Warranties Clauses.

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 costs 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 the client'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. 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. 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. They can also incorporate a statute of limitations.

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. 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 depends 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. For insurance clauses, see Insurance Clauses.

Consumer Products

With the advent of the Internet of Things (IoT), AI has proliferated in the consumer products market. 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. The IoT is a network of devices that talk to each other through the web. By combining these electronically connected devices with computerized systems, individuals and businesses can now gather a wealth of valuable information quite readily. 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)
- 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 as to whether a specific IoT device is a product and/or a service. 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/end user if there is a claim. The service provider,

however, could very well 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.

Product Liability Law – 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 either be 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 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, it 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. Raymond Talmadge d/b/a Calvary Coach

In Cruz v. Raymond Talmadge d/b/a Calvary Coach, 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 alternative 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 has 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.

David Vladeck, in "Machines Without Principles: Liability Rules and Artificial Intelligence," 89 Wash. L. Rev. 117 (2014), argues that this burden should rest squarely on the manufacturer's shoulders.

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 patent is usually 20 years commencing on the date that the application for the patent was filed. In certain situations, term extensions may be available. 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 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
- 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 data sets, 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).

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 is regularly used in a business which provides its owner with an opportunity to obtain an economic advantage over the competition. It can be a valuable form of IP protection for 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 U.S. Economic Espionage Act of 1996 (18 U.S.C. § 1831 et seq.), which amends the Defend Trade Secrets Act of 2016 (DTSA). 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
- 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 economic value from the information's confidentiality.
- The business owner makes ongoing, reasonable efforts to preserve the information's secrecy. Examples of such efforts including 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 non-disclosure 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. One of the greatest advantages of trade secret protection is that it can last indefinitely. Additionally, unlike patent or copyright protection (as discussed below), there is no application or registration process, and the information's owner is not required to publicly disclose the protected data. Significant and ongoing efforts, however, are required to protect the proprietary nature of the information to maintain trade secret protection, which is no small feat. This effort is 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.

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, though beneficial, is not required for copyright protection, as a copyright automatically vests with the author (or, if the work is a "work made for hire," the employer). For information on works made for hire, see Works Made for Hire and for guidance on copyright registration, see Registration of Copyrights. Note that 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)). It remains unclear, however, as to 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.

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 (see 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. However, copyright owners are required to re-register their protected IP regularly. 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.

Privacy and Data Security Issues

An AI system generally relies heavily on large volumes of data. It is this information that the system then processes to reach conclusions, improve business practices, and predict future patterns. 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. Again, ensure that his or her client use encryption wherever possible, password protect all proprietary digital information, require employees and agents to execute NDAs, and provide confidential information only to those who require it and on a just-in-time basis.

Applicable Laws Generally

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 (C.C.P.A.), Cal. Civil Code § 1798.100 et seq., where applicable). For information about the GDPR and the C.C.P.A., see General Data Protection Regulation Fundamentals (EU GDPR) and CCPA Compliance: Comparing Key Provisions of the GDPR and CCPA. 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, 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 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) issues 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:
    - o Inform job applicants that AI will be used to analyze their videos.
    - o Explain how their AI program works and exactly how the applicant will be evaluated.
    - o Obtain the applicant's prior consent.
    - o Share the videos only with those individuals required to evaluate the applicant.
    - o Destroy all copies of the video within 30 days after an applicant's request therefor.

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. 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 requiring 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 his or her 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, 11 U.S. Code Title 11, 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 (see 11 U.S.C. § 101(35A))

Note the exclusion of trademarks, service marks, and trade names.

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:
    - o 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 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. For more information regarding antitrust law, see Antitrust Law Fundamentals. 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.

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 actually eliminated. 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 his or her 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. The OSHA also provides guidelines for robotics safety. See Guidelines for Robotics Safety, OSHA Instruction STD 01-12-002 (1987). Under the OSHA, a covered employer utilizing robotics—like any other employer the 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 the 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. See Nanette Byrnes, As Goldman Embraces Automation, Even the Masters of the Universe Are Threatened, MIT TECHNOLOGY REVIEW (Feb. 7, 2017).

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

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
- CCPA Compliance: Comparing Key Provisions of the GDPR and CCPA
- Privacy and Data Security Considerations When Negotiating or Reviewing a Transaction or Agreement
- OSH Act Requirements, Inspections, Citations, and Defenses

Antitrust

- Antitrust Law Fundamentals

Corporate Counsel

- Trade Secret Fundamentals
- Criminal Background Checks: Key Analyses and Considerations

Data Security & Privacy

- General Data Protection Regulation Fundamentals (EU GDPR)
- CCPA Compliance: Comparing Key Provisions of the GDPR and CCPA
- 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

Labor & Employment

- Defend Trade Secrets Act (DTSA) Fundamentals

Templates

Commercial Transactions

- Representations and Warranties Clauses
- Product Warranty and Disclaimers Clauses
- Disclaimer of Express Warranties Clauses
- Insurance Clauses
- Privacy Policy (UK GDPR)

Labor & Employment

- Confidentiality Agreement with Employee (Unilateral)

Current as of: ***09/29/2021***