



©Shutterstock.com/boasalt

Artificial Intelligence and Tort Liability: The Evolving Landscape

As companies increasingly integrate artificial intelligence (AI) into their products and systems, the potential for AI to cause injury and property damage continues to grow. Companies and their counsel should consider how traditional tort principles intersect with AI technology, and implement policies and practices that guide the prudent use of AI to minimize liability risk.



STEPHANIE E. NIEHAUS

PARTNER
SQUIRE PATTON BOGGS (US) LLP

Stephanie has a varied litigation practice with an emphasis on complex product liability and mass tort matters, and has a particularly deep understanding of multi-plaintiff matters. She has considerable trial and other in-court experience, and also routinely provides strategic advice to clients seeking to avoid or minimize the risk of litigation. Stephanie has a special interest in the tort and other legal implications of emerging AI technologies and speaks frequently on those issues.



HUU NGUYEN

PARTNER
SQUIRE PATTON BOGGS (US) LLP

Huu focuses his practice on commercial and corporate transactions in the technology and venture space, and counsels and assists clients with AI and autonomous vehicle matters, licensing, strategic relationships, financial regulatory matters, privacy and security matters, cyber law, and intellectual property rights matters. Previously, he was an AI programmer and a research scientist. Huu is a vice-chair of the American Bar Association's Artificial Intelligence and Robotics Committee and a co-editor of the FinTech Law Report newsletter published by Thomson Reuters.

In a rising trend, consumer product manufacturers are incorporating autonomous AI in everything from personal assistants to household appliances. AI, also known as cognitive computing or machine learning, typically refers to computer technology that simulates human intelligence, including abilities such as problem solving and learning. As the AI incorporated in everyday products evolves from semi-autonomous to fully autonomous functionality, so too does a product's ability to act independently of a human operator.

Although the use of AI technology ultimately may increase overall safety by, for example, taking over hazardous tasks that are currently handled by humans, AI's ability to act autonomously raises novel legal issues. An overarching question is how to assign fault when the use of an AI product results in injury or other damage.

Litigants and courts have begun to test the application of traditional legal theories to injuries involving AI products, such as self-driving vehicles and workplace robots. Several recent disputes illustrate how principles of tort liability and employer liability for workplace injuries can be applied to cases involving AI, while others test the bounds of those principles and highlight the need for the law to evolve with the new technologies. Companies and their counsel should understand how traditional tort principles might apply to AI-enabled products and systems, and implement certain best practices to reduce potential liability risk.

PRODUCT LIABILITY PRINCIPLES

Product liability law determines who is at fault when someone is injured by a product. It is generally based on state common and statutory law, including theories of:

- **Negligence.** Negligence claims seek to impose liability on a defendant that fails to meet the standard of care that a reasonable company (or person) should have exercised under the circumstances. The plaintiff typically alleges that the defendant product manufacturer or seller:
 - negligently designed or manufactured the product; or
 - provided inadequate warnings or instructions on the product label to notify consumers about safe uses of the product.
- **Breach of warranty.** Warranty claims are based on the contractual relationship between the plaintiff and a defendant product seller, and typically rely on state law versions of Article 2 of the Uniform Commercial Code (UCC). The plaintiff's warranty claim may allege the breach of:
 - an express warranty, where the plaintiff must prove that the defendant made a false, material, factual statement about the product and the plaintiff relied on that statement;
 - an implied warranty of the product's merchantability, where the plaintiff must prove that the product was unsuitable for the ordinary purposes for which the product is used; or
 - an implied warranty of the product's fitness for a particular purpose, where the plaintiff must prove that the product was required for a special purpose, the plaintiff relied on the defendant's skill or judgment in selecting the product for that purpose, and the product could not serve the special purpose.

- **Strict liability.** Although strict liability varies by jurisdiction, most states have adopted the basic concepts of Section 402A of the Restatement (Second) of Torts. Under Section 402(A), a defendant who sells a product in a defective condition that is "unreasonably dangerous" may be liable for physical harm or property damage even if:

- the defendant exercised all possible care in the preparation and sale of the product; and
- the consumer did not enter into any contractual agreement with the defendant.

Section 402(A) applies only if the product reaches the user without a substantial change in the product's condition from when the product left the defendant's control, although some courts and legislatures hold manufacturers accountable for injuries attributable to foreseeable modifications by the user or a third party. The Restatement (Third) of Torts modifies this standard, but only a few states have adopted it.

For any of the traditional theories of liability, a plaintiff's claim typically rests on an allegation that a product was defectively designed, manufactured, or labeled. The same product defect can form the basis for multiple claims under different theories. This includes "failure to warn" claims, which can form the basis for claims sounding in negligence, breach of warranty, and strict liability. (While joint and several liability may be relevant when asserting these theories, it is beyond the scope of this article.)



Search [Product Liability Claims, Defenses, and Remedies](#) for more on the traditional product liability causes of action.

A recent case, *Cruz v. Raymond Talmadge d/b/a Calvary Coach*, involved a common AI-driven product: a GPS device. In *Cruz*, the plaintiffs were injured, some critically, when a bus in which they were riding struck an overpass. At the time of the accident, the bus driver was using two GPS devices manufactured by different companies. The plaintiffs brought claims against those GPS manufacturers based on traditional theories of negligence, breach of warranty, and strict liability.

The plaintiffs alleged that the devices were defectively designed because they:

- Directed the driver to follow a route that required him to drive the bus under an overpass that was too low for the vehicle.
- Failed to warn the driver of the dangerous situation created by driving underneath an overpass with inadequate clearance.

The plaintiffs claimed that their injuries were foreseeable because "[i]t is a well-known fact that faulty directions onto height restricted roadways by GPS devices have resulted in numerous bridge strikes," and that feasible alternative designs existed because the device manufacturers "possessed the data necessary to provide information to users regarding height restriction." (Am. Compl. ¶¶ 54, 58, *Cruz v. Raymond Talmadge d/b/a Calvary Coach*, No. 1584-0222, 2015 WL 13776213 (Mass. Suffolk Cty. Super. Ct. Sept. 25, 2015).)

The *Cruz* plaintiffs based their claims on traditional product liability principles. Given the semi-autonomous nature of the

GPS devices at issue, the plaintiffs' claimed injuries could be traced back to:

- Design components that were developed by specific companies and substantially unchanged from the time the devices left the companies' control.
- The alleged failure of the companies to adequately warn about foreseeable dangers of their products.

However, appropriate application of product liability concepts is less straightforward when the product at issue incorporates more fully autonomous AI technology. Specifically, it is unclear how the law should assign liability for AI that learns and makes decisions on its own, and whether analytical elements like the foreseeability and substantially unchanged standards that underpin the traditional tort framework remain workable in an AI-driven world.

Another recent case, *Nilsson v. General Motors LLC*, illustrates some of these complexities and hints at how product liability claims may evolve as AI technology develops. In *Nilsson*, a motorcyclist claimed that he was injured when an autonomous vehicle (AV) suddenly veered into his lane and knocked him to the ground. A backup driver was present in the AV at the time of the collision, but the driver was not operating the AV when it crashed.

Although the parties ultimately settled at the pleadings stage, the *Nilsson* pleadings themselves are noteworthy. In his complaint, the plaintiff relied on a theory of general negligence only (and not, for example, defective design or warning), alleging that the AV manufacturer had breached its duty of care because the vehicle itself — and not the backup driver — drove in a negligent manner that caused the plaintiff's injury (Compl. ¶¶ 15-16, *Nilsson v. Gen. Motors LLC*, Jan. 22, 2018 (No. 18-471) (N.D. Cal.), ECF No. 1). Perhaps even more surprising, though, is the manufacturer's admission in its answer that the vehicle itself was required to use reasonable care in driving (Answer ¶ 15, *Nilsson v. Gen. Motors LLC*, Mar. 30, 2018 (No. 18-471) (N.D. Cal.) (stating that "GM admits that the Bolt was required to use reasonable care in driving"), ECF No. 18).

The *Nilsson* pleadings implicate several novel issues. Where fault cannot be traced directly back to a human actor (because, for example, the AI has learned and can make decisions on its own), the law must determine whether to consider the AI product to be the actor and, if so, the applicable standard of care governing the AI (for example, a reasonable human versus

a new "reasonable machine" standard). Similarly, an AI product that is intended to "behave" of its own accord creates new dimensions for the concept of foreseeability, raising questions about not only what is foreseeable for AI, but also whether humans might eventually be held to a different standard, especially in cases where AI was available to perform the task.

The downstream consequences of these decisions are significant. Moreover, if products themselves can be liable, it is unclear who compensates injured parties. At least one commentator has suggested that the common law doctrine of *res ipsa loquitur* might be appropriate in these circumstances, shifting the burden to manufacturers and providing claimants with an avenue for relief (see generally David C. Vladeck, *Machines Without Principles: Liability Rules and Artificial Intelligence*, 89 Wash. L. Rev. 117 (2014)).

EMPLOYER LIABILITY PRINCIPLES

The workplace provides another fertile area for AI tort litigation. Workplace robots in particular have been the subject of suit for many years. Like product liability cases, as technology improves and AI becomes more autonomous, employment-related AI cases potentially raise novel questions about the continued viability of traditional approaches to the workers' compensation bar and employer intentional torts. For example, the concept of an intentional tort is untested in any case involving AI, so it remains an open question whether an employer can be held to have acted intentionally where any "intent" effectively rests with the AI.

In most states, workers' compensation benefits are typically an employee's exclusive remedy for a workplace illness, injury, or death. Employees therefore are generally precluded from asserting negligence claims against their employers unless the employer acted intentionally (as defined by state law). At the same time, most workers' compensation laws do not preclude claims against third-party tortfeasors, leaving open claims against manufacturers and suppliers.



Search [Workers' Compensation: Common Questions](#) for more on workers' compensation laws, including information on compensable injuries, compensation benefits, and leaves of absence.

For example, in *Hills v. Fanuc Robotics America, Inc.*, the plaintiff brought suit in connection with injuries caused by a workplace

An AI product that is intended to "behave" of its own accord creates new dimensions for the concept of foreseeability, raising questions about not only what is foreseeable for AI, but also whether humans might eventually be held to a different standard.

robot. The plaintiff had attempted to disable the robotics system to clear a jam in a conveyor belt at a Winn Dixie grocery store. While the plaintiff was clearing the jam, the robotics system suddenly activated and pinned the plaintiff to the conveyor belt, causing his injuries. The plaintiff claimed that both the robot and a safety light curtain separating the system from the conveyor belt (and intended to protect employees from accidental proximity to the robot while it was operating) malfunctioned. He brought claims against the manufacturers of both products as well as the designer of the automated palletization system that integrated the products. (First Suppl. & Am. Compl. ¶¶ 5-7, *Hills v. Fanuc Robotics Am., Inc.*, Apr. 3, 2008 (No. 04-2659) (E.D. La.), ECF No. 60.)

The plaintiff also sued his employer, the grocery store, claiming that it was vicariously liable because one of the store's managers disabled the malfunctioning safety light curtain and instructed employees to place the robot on hold, rather than stopping the robot entirely, if they needed to approach it. These actions allegedly violated standard operating policies for the robot, safety light curtain, and automated palletization system. (Pet. for Damages ¶¶ 24-27, 31, *Hills v. Fanuc Robotics Am., Inc.*, Aug. 13, 2004 (No. 2004-11694) (La. Civ. Dist. Ct., Orleans Parish).)

After settling with the robot manufacturer, the plaintiff ultimately prevailed at trial on his claims against the palletization system manufacturer and the light curtain manufacturer. Notably, the robot manufacturer was not found to be at fault for the plaintiff's injuries. Instead, the jury found that the employer was 65% responsible, the designer of the automated palletization system was 25% responsible, and the light curtain manufacturer was 10% responsible for the plaintiff's injuries. (Judgment, *Hills v. Fanuc Robotics Am., Inc.*, July 16, 2010 (No. 04-2659) (E.D. La.), ECF No. 253.)

In another case, *Holbrook v. Prodomax Automation Ltd.*, a robot unexpectedly entered an area where an auto parts worker was performing her duties. While attempting to place an unnecessary part on a fixture, the robot pinned the worker and crushed her skull. The worker died from her injuries.

In its complaint, the worker's estate asserted traditional claims of negligent or defective design, defect in manufacture, failure to warn, negligence, and *res ipsa loquitur* against the companies that manufactured the robot and its controllers, tooling, fixtures, and safety devices. The plaintiff also asserted claims against these same companies based on their installation, integration, engineering, and servicing of the robot and its safety devices, which the complaint defines as the robot's "automation system." (First Am. Compl. ¶¶ 20-21, *Holbrook v. Prodomax Automation Ltd.*, July 24, 2018 (No. 17-219) (W.D. Mich.), ECF No. 43.) The plaintiff did not sue the worker's employer, likely due to Michigan's workers' compensation bar. The case remained pending as of press time.

Taken together, these cases suggest that where there is a viable avenue for tort recovery against a manufacturer, an employee plaintiff might elect not to sue the employer to avoid having a jury apportion fault against it. However, it may be harder to obtain third-party discovery from a non-party employer.

BEST PRACTICES TO MINIMIZE AI-RELATED TORT LIABILITY

While the legal framework governing tort liability related to AI-enabled products and systems continues to evolve, companies using AI technology should adopt an AI policy that incorporates certain best practices to guard against liability risk and ensure the company is prepared for potential litigation. An AI policy may be integrated with a company's privacy and data security policies, as AI typically revolves around the collection, analysis, and interpretation of data. There may be other places for separate or supplemental policies concerning the use of AI, such as physical safety and security policies or as part of a crisis management plan, especially where an AI tort has the potential to become a company crisis.

A comprehensive AI policy can incorporate both technical and narrative elements, and support a company's showing that its operation of an AI product or system was safe, appropriate, and responsibly designed and deployed. This proactive step can help guard against later claims concerning the reasonableness of a company's AI-related conduct.

Although industry groups, such as the Institute of Electrical and Electronics Engineers (IEEE), and technology leaders have proposed AI policies (see, for example, Microsoft Corp., *FATE: Fairness, Accountability, Transparency, and Ethics in AI*, available at microsoft.com), no AI industry gold standard has yet emerged. Moreover, while there is some information on physical robot safety in the workplace under the Occupational Safety and Health Act and related regulations (Guidelines for Robotics Safety, Directive STD 01-12-002 (Sept. 21, 1987), available at osha.gov), no guidance has emerged on the use of AI generally. Therefore, companies should apply broad principles when developing AI policies and address:

- Safety standards for the AI-enabled product or system.
- Ethical considerations guiding the company's AI use.
- Oversight and reporting abilities regarding the AI-enabled product or system.
- Relevant third-party relationships affecting the company's AI use.

An AI policy embodying these principles can not only guide the content of other internal policies and procedures but also aid the creation of external notices that address and explain the company's AI use. Companies may also publicize ethical standards, information security protocols, and tort incidence or crisis response plans, where appropriate. However, companies and their counsel should be aware that regulators and plaintiffs' attorneys may scrutinize policies, so a company should not include commitments in any policies or notices that it is unprepared to meet.



Search [Developing a Legal Compliance Program](#) for information on key points to consider when developing, implementing, and maintaining a legal compliance program.

Search [Corporate Crisis: Board Preparation and Response](#) for information on the components of an effective crisis management plan.

The Intersection of AI and Tort Law: A Hypothetical Example

Startup, Inc., a new company, provides transportation for its employees to and from its state-of-the-art campus using Startup's highly publicized, fully autonomous self-driving company buses. In its press release announcing the company's adoption of the buses, Startup stated that the buses were intended to lower traffic congestion and provide a safe way for its employees to get to work.

The Startup buses were manufactured and designed by a separate company, Bus Corp., as part of its efforts to commercialize self-driving vehicles for public transportation. Central to the design of the buses is GPS software that guides the buses on their various routes. The GPS software was designed and manufactured by another company, CarGPS LLC. The automated bus system is operated and maintained by Daily Maintenance Inc., which contracts with Startup. The manual for the GPS software (published by CarGPS) instructs that the software must be updated on a regular basis but is silent on the frequency of these updates. In any case, Daily Maintenance is not required to perform the updates as part of its contract with Startup.

Although Startup does not require its employees to ride the buses to and from work, nearly all employees do so because of the remote location of Startup's campus and what employees assume is an intentional lack of parking at the campus.

Several months after Startup's announcement about the buses, one of the Startup buses struck an overpass that was too low for the bus to clear, injuring several employees riding the bus, some permanently, and causing the uninjured employees to witness their colleagues' trauma.

Immediately before the accident, a passenger noticed the upcoming overpass and attempted to engage the brakes before

the vehicle hit the overpass. However, the bus was designed to slow down gradually unless it detects an emergency. The Bus Corp. user manual stated that a backup driver should monitor the bus and take over in emergencies, but it did not clearly state that a backup driver must engage the emergency brake, rather than the regular brake, to quickly override the autonomous operation of the bus. In any case, there was no backup driver riding the bus at the time of the collision.

During the crash, the bus recorded information from its external sensors (such as cameras showing that the overpass was clearly too low), but it did not record information from its internal sensors (such as the GPS signals). After learning of the accident, Startup's counsel engaged experts to investigate the faulty AI and supervised their technical work. These experts inspected the GPS software by running the version that was operating at the time of the crash. During that inspection, the GPS signal did not show that the overpass was too low. However, because the GPS information was not recorded at the time of the crash, it is difficult to show how the bus used the faulty GPS signal.

As part of its vendor management policies, Startup states that it understands the risks of accidents posed by autonomous devices and requires all devices provided and used by its vendors to be safe. Startup required Bus Corp and CarGPS to agree to this safety policy in their contracts. However, Startup has never audited its vendors for safety and no one at Startup understands how the buses operate.

This hypothetical scenario presents a fact pattern similar to those in the *Cruz* and *Hills* cases. The employee-plaintiffs involved in the crash may make similar arguments about liability and assert claims against:

SAFETY STANDARDS

Safety should be a primary consideration in the use of AI. Safety extends beyond minimizing the risk of injury to people and property, and includes minimizing the risks of cyber or privacy intrusion, data loss, and other violations of law.

Before incorporating AI into a product or system, a company should, at a minimum:

- Confirm that the AI product or system was designed according to specifications that promote safety.
- Confirm that the AI product or system was developed and manufactured to be safe.
- Provide clear instructions for safely using the AI product or system.

- Consider incorporating failsafe systems that trigger human intervention and oversight.
- Warn users of the dangers of using the AI product or system.
- Have a recall procedure in place to recall products, where appropriate.

A company should also consider whether to implement additional safeguards to protect against improper or illegal, but foreseeable, uses of the AI product or system.

For example, a company using an automated drone to deliver goods should place safety guides (such as electronic markers, safety lights, or cones) on the streets to help the drone avoid the paths of people and cars. Even if someone were to move the guides, the drone should be designed to properly detect and navigate around people, buildings, cars, and other objects. A company using a vendor for this type of drone should require

■ **Startup.** The plaintiffs could assert claims against Startup in its capacity as:

- an employer, by alleging that it acted with reckless indifference to the safety of its employees in selecting and deploying the particular model of self-driving bus for use by its employees; or
- a product seller, depending on the level of control it had over, and the contractual agreements governing, the design, manufacture, and maintenance of the buses.

■ **Bus Corp.** The plaintiffs might assert claims against the bus manufacturer alleging that the bus itself was:

- negligent, because the bus should have used common sense reasoning to override the GPS instructions and avoid driving under the overpass given that its sensors could clearly see that the overpass was too low (similar to the plaintiff's argument in *Nilsson* that the car itself was negligent);
- defectively designed or manufactured; or
- accompanied by defective warnings or instructions.

■ **CarGPS.** The plaintiffs might claim that the GPS software was:

- defective or unsuitable for its intended purpose, namely to direct buses on relevant roadways; or
- negligent, because it should not have directed the bus to follow a route that would require the bus to drive under an overpass that was too low for the vehicle, it should have provided a warning of the dangerous situation, or, under *res ipsa loquitur* principles, it must be defective because, among other things, the GPS signal directs the routes of the buses and the signal is under the exclusive control of CarGPS.

■ **Daily Maintenance.** The plaintiffs might claim that Daily Maintenance was negligent because it did not:

- properly operate and maintain the bus; or
- place a backup driver on the bus who would have avoided the accident.

Assuming all elements for negligence or product liability are met, each potential defendant likely shares some liability for the employees' injuries. There may be comparative liability between the parties, with the exception of Startup itself, which would probably benefit from the applicable workers' compensation regime.

Regardless of how the litigation may progress, Startup (and the other companies) should revise its AI policies and practices in light of the accident. With a properly implemented AI policy, Startup should, at a minimum:

- Understand the operations and risks of the AI and operate it safely.
- Ensure that backup drivers are present on the buses and that they are trained on the emergency procedures in the Bus Corp. user manual.
- Require vendors to provide clear and comprehensible instruction manuals.
- Audit Daily Maintenance and require it to update the GPS software on a consistent basis.
- Require Bus Corp. to ensure that the buses record and retain all applicable data, including GPS information, consistent with Startup's retention policy so that Startup can understand any faulty AI operation in the future.

the vendor to put safeguards in place that anticipate pedestrian behavior, to the extent it is technically feasible and foreseeable (see below *Third-Party Governance*).

Additionally, as the *Hills* case demonstrates, a company must anticipate potential failures in safety mechanisms. In the drone example, a company should take into account that while the company policy and user manual might require all drones to be deactivated before the guides may be moved, it is foreseeable that company employees or the public may accidentally (or intentionally) move the guides without first deactivating the drones.

ETHICAL CONSIDERATIONS

A company should consider how its use of AI fits with its core values. The needs and viewpoints of a company's stakeholders should guide the company's AI use, including its creation of

products or systems that rely on AI. Where possible, a company should maximize the societal benefit of its AI use. Besides the importance of having ethical policies in place, this approach can help the company show its AI use in a sympathetic context if it is faced with litigation.

To craft a socially responsible AI policy, a company might consider whether and how its AI use:

- Promotes interests of diverse stakeholders. For example, if the company manufactures children's educational games that use AI, it should consider what values educators, administrators, and students want the AI to embody.
- Aligns with the ethical codes and core values of the company. For example, the company should consider whether the AI eliminates bias from routine processes or potentially reinforces bias through its data and machine learning operations.

OVERSIGHT AND CONTROLS

A company's procedures for oversight and control of its AI is a critical component of both a corporate compliance program and a defensive litigation strategy. These procedures should incorporate both technical product controls and legal and corporate policy safeguards.

An effective oversight and control program should address:

- **The delineation of responsibility for AI.** For example, a company should consider whether to:
 - require its Chief Technology Officer or cyber experts to manage AI issues;
 - appoint a single officer, director, or manager to oversee the company's AI program; or
 - entrust AI governance to a committee or task force.

A company's decision will be based on the importance of AI to the company and the size and maturity of the company's IT team.

- track updates to AI software (for example, confirming that customers applied any patches, updates, or upgrades as required by the AI's user manual).

- **Records retention protocols.** A company must determine how its records retention policy should address the storage of AI information, including whether the AI must be designed to retain certain types of records, such as when accidents occur, and how long the records should be retained. (For more information, search [Records Management Toolkit](#) on Practical Law.)

- **The role of counsel concerning AI use.** A company's AI oversight procedure should define counsel's role. Structuring an active role for counsel can help to protect the attorney-client privilege and ensure compliance with applicable regulations and laws. During a potential litigation involving an AI product or system, counsel should aim to protect the attorney-client privilege by directing and supervising technical experts' investigations into the malfunctions of the AI.

A company must determine how its records retention policy should address the storage of AI information, including whether the AI must be designed to retain certain types of records, such as when accidents occur, and how long the records should be retained.

- **The specific type of AI and its operation.** At a minimum, a company must understand its AI use to gauge the risk of potential torts that may be committed by or with the AI (for example, assessing how predictably the AI will behave). This includes determining whether the AI:
 - is semi-autonomous or fully autonomous;
 - incorporates machine learning or is static; and
 - interacts with people, whether employees or consumers.
- **Audit schedules and capabilities.** A company's AI use should be audited regularly to ensure that the company has an up-to-date understanding of how its AI is operating. A company should:
 - periodically confirm that the AI is serving its purpose and has not inadvertently introduced bias or other undesirable behaviors, which is particularly important to monitor if the AI incorporates a machine learning system;
 - ensure that the AI records information on judgments and decisions the AI makes so that they are available for analysis (for example, as part of a data forensics examination during litigation); and

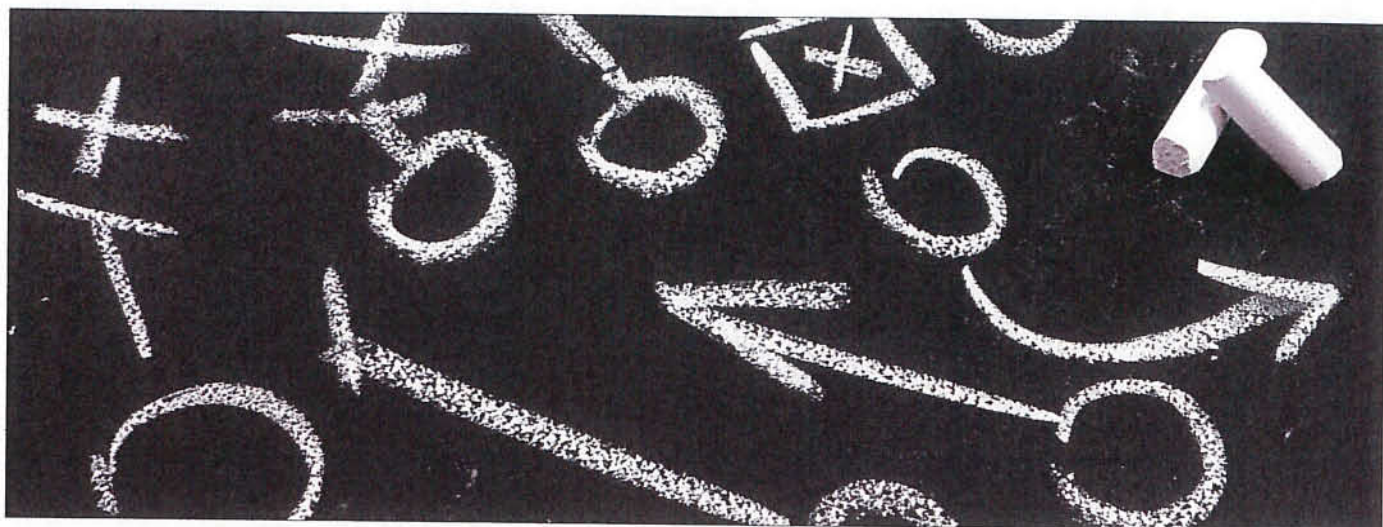
THIRD-PARTY GOVERNANCE

In many cases, a company's use of AI will involve contracting with vendors to develop or implement an AI system. A best practice is for the company to manage AI vendor relationships as if the company itself were developing the AI. This means that a company selecting an AI vendor should consider whether the vendor has processes in place to comply with the company's AI principles and serve the company's core values concerning AI use.

A company's general supply chain policy may refer to its AI policies or ethical policies to ensure vendors also responsibly use and deploy AI. Moreover, the company should have consistent AI-related requirements and enforce its policies.



Search [Developing a CSR Supply Chain Compliance Program](#) for information on key points to consider when developing and implementing a corporate social responsibility (CSR) supply chain compliance program.



Final Pretrial Order Under FRCP 16(e): Overview

This Practice Note provides guidance for counsel on how to prepare a proposed final pretrial order (or pretrial stipulation) under Federal Rule of Civil Procedure (FRCP) 16(e) for use in a federal civil trial. It also discusses the consequences of failing to include required items in a final pretrial order and the circumstances under which a party may seek to modify a final pretrial order after it is issued.

Practical Law Litigation

The final pretrial order that a court issues under FRCP 16(e) is one of the most important documents in a case headed for trial. The final pretrial order supersedes all previous pleadings and provides the court and counsel with a roadmap for trial (see *Rockwell Int'l Corp. v. United States*, 549 U.S. 457, 465 (2007); *Friedman & Friedman, Ltd. v. Tim McCandless, Inc.*, 606 F.3d 494, 498 (8th Cir. 2010)).

This Note addresses key considerations for counsel when preparing a proposed final pretrial order, including:

- The basic procedure for negotiating, drafting, and filing a final pretrial order.
- The information that courts typically require counsel to include in a final pretrial order.

- The consequences of failing to include required information in a final pretrial order.
- The standard that a party must meet for a court to modify a final pretrial order after it is issued.



Search [Final Pretrial Order Under FRCP 16\(e\)](#) for a sample proposed final pretrial order, with explanatory notes and drafting tips.

BASIC PROCEDURE FOR PRETRIAL ORDERS

The basic procedure for preparing a final pretrial order generally is similar across federal district courts, although the exact procedure and required contents may vary depending on the rules of the applicable district court and presiding judge.