SESSION TITLE: The Matrix Unraveled: AI, IP Infringement, and Privacy

Laura Clark Fey[1]
Fey LLC, Leawood, KS
lfey@feyllc.com

Navigating the AI Minefield: Legal and Ethical Obligations and Risks and Compliance Strategies[2]

I. Introduction

Eliezer Yudkowsky once stated that "the greatest danger of Artificial Intelligence is that people conclude too early that they understand it." As Artificial Intelligence (AI) technologies continue to proliferate in professional practices and throughout society, it is imperative that professionals take the time to understand key AI technologies available to them, and to develop at least a baseline of knowledge concerning how such technologies work; the benefits and risks of such technologies to them and their clients; and how to implement such technologies in a way that reduces risk.

The McKinsey Global Survey on the Current State of AI, conducted in April of 2023, confirms the explosive growth of usage of generative AI (Gen AI) technologies in organizations. One-third of survey respondents advised that their organizations are already using Gen AI technologies regularly in one or more business functions. Experimentation with Gen AI technologies is common. Seventy-nine percent of survey respondents asserted that they have had at least some exposure to Gen AI, either for work or outside of work, and 22 percent say they are regularly using it in their own work.

Survey respondents asserted that they expect new AI capabilities to transform their industries. As noted by McKinsey, Gen AI has "captured interest across the business population: individuals across regions, industries, and seniority levels are using Gen AI for work and outside of work." With the recent public release of Gen AI technologies, it is not surprising that AI experimentation and broader usage of a variety of AI technologies (including but not limited to Gen AI technologies) is increasingly common. Professionals, of course, are among the many types

[1] Laura Clark Fey, one of the first twenty-seven U.S. attorneys recognized as Privacy Law Specialists (IAPP), leads Fey LLC, a global data privacy, AI and information governance law firm. Laura is a member of the inaugural class of IAPP Fellows of Information Privacy, a Certified U.S. and European Information Privacy Professional, and a Certified Information Privacy Manager. Laura teaches Global Data Protection in the Age of AI at the University of Kansas School of Law and International Issues at Baylor Law School. Laura is Chair of the DRI Center for Law and Public Policy's Data Privacy and Protection Working Group; a member of the DRI Center for Law and Public Policy's AI Working Group; and immediate Past-Chair and current member of DRI's Cybersecurity and Data Privacy Committee. She is also a member of IADC.

[2] Laura would like to thank Fey LLC Associate Attorney, Blake Lines, and Law Clerk, Austin Polina, for their valuable assistance and insights in developing this paper.

of workers actively implementing AI and Gen AI technologies. For example, attorneys are now utilizing AI technologies to review, analyze, draft, and even negotiate contracts. Architects are utilizing AI technologies to make more efficient and environmentally friendly design decisions. Insurance companies are using AI to help with underwriting, fraud detection, and customer service activities. And financial professionals are using AI to perform data analysis, portfolio management, and market research.

With the large increase in AI usage by professionals, it is critical for professionals to think about not only the benefits of AI technologies, but also the legal, ethical, and business risks that accompany such technologies. Risks posed by AI technologies include hallucination risks (*i*.e, risks that tools will generate content that looks convincing, but has no basis in fact); risks posed by training data sets that are biased, contain propaganda, hate speech, or otherwise dubious content; risks posed by lack of transparency concerning the data used to train the AI tool and the how and why of AI decision-making; risks posed by limitations in logical reasoning capabilities; risks posed by the lack of internal moral compasses in AI technologies; manipulation risks; deepfake risks; and cybersecurity and confidentiality risks.

This paper has been prepared to assist professionals in developing a deeper understanding of these and other risks posed by using (and refraining from using) AI technologies, and to provide compliance and risk-reduction strategies. The first substantive section provides a high-level explanation of AI technologies. The second substantive section addresses key AI legal risks. The third substantive section addresses key AI ethical obligations for lawyers. The fourth substantive section addresses AI ethical obligations for other professionals. The paper concludes with 15 best practice recommendations for professionals to implement in furtherance of reducing those risks.

II. What are AI Technologies?

Although there has been a significant increase in attention to AI technologies, especially Gen AI, during the past year, AI technologies have been around since the 1950s. The term "artificial intelligence" was first coined in 1956, when the first AI conference took place at Dartmouth College. Since then, a wide variety of AI innovations have been theorized, developed, and implemented, with some of the most recent innovations being technologies utilizing Gen AI, such as ChatGPT.

The National Institute of Standards and Technology (NIST) uses the following definition of AI: "(1) A branch of computer science devoted to developing data processing systems that performs functions normally associated with human intelligence, such as reasoning, learning, and self-improvement. (2) The capability of a device to perform functions that are normally associated with human intelligence such as reasoning, learning, and self-improvement." AI technologies are used to recognize patterns, reach conclusions, make informed judgments, optimize patterns, predict behaviors, and automate repetitive functions. *See* AI in the Workplace, Thomson Reuters. Examples of familiar AI technologies include image recognition technologies; voice-controlled virtual assistants, like Amazon's Alexa; language translation programs; smart home devices; smart watches; tax preparation software; and chatbots.

AI technologies have gradually permeated our personal and professional lives. But there has been a huge leap forward in AI technologies in recent years with the development of Gen AI

technologies, such as ChatGPT and Stable Diffusion. Gen AI is a term describing algorithmic models that have been trained to generate new data, including texts, images, and sound. Gen AI technologies have been made possible in recent years primarily because of significant advances in machine learning capabilities, significantly increased computing power, significantly increased content accessible through the Internet, and significantly decreased costs for collecting and storing training data used for Gen AI technologies. Among other things, Gen AI technologies can write essays and legal briefs; write software code; take notes during meetings; engage in dialogue/discussions with users; create images from text prompts; and create video clips based on images.

AI technologies including Gen AI, are already serving a variety of functions for professionals. For example, lawyers are using AI technologies to, among other things, conduct legal research; prepare memoranda; analyze court decisions and predict outcomes; draft pleadings and briefs; review briefs and identify key relevant authorities not referenced in briefs; respond to eDiscovery requests; draft wills; analyze contracts; and even negotiate contracts through chatbots. AI technologies will continue to advance at increasingly rapid rates. AI, particularly Gen AI, is widely expected to have a very significant impact on all industries.

Gen AI will have a particularly significant impact on professionals performing knowledge work. As McKenzie has noted, "Generative AI is likely to have the biggest impact on knowledge work, particularly activities involving decision making and collaboration, which previously had the lowest potential for automation." Another recent study, which was conducted by researchers at Princeton University, the University of Pennsylvania, and New York University, concluded that, among the "most-exposed" industries to new AI technologies were securities, commodity contracts, and other financial investments and related activities; legal services; insurance and employee benefit funds; and agencies, brokerages, and other insurance related activities." A report conducted by Goldman Sachs estimated that up to 44% of legal work could ultimately be automated by AI.

It will be increasingly critical for professionals to develop a good understanding of current and evolving AI technologies that can be used for the benefit of both their companies and their clients. Professionals should have knowledge not only of how AI technologies work, but also the benefits and risks of using such technologies, and key actions necessary to reduce legal, ethical, and business risks posed by such technologies.

III. Overview of Key AI Legal Obligations and Risks

This section addresses key legal obligations and risks that professionals should consider before implementing AI technologies. This list is not exhaustive.

A. Contractual Risks

Professionals should carefully consider AI-related obligations and risks arising from their agreements with the companies providing their AI technologies. Before entering into agreements with such providers, professionals should carefully analyze key contractual terms, including ownership/IP clauses, disclaimers and warranties, limitations on liability, risk-shifting (*e.g.*, indemnity), insurance, service performance characteristics (*e.g.*, severity levels and circumstances

under which the AI provider will not be liable for outages or performance issues), prohibitions and restrictions imposed on users, privacy and legal compliance, and usage-related terms.

Professionals also should consider risks arising from their agreements with other third-party service providers and with their clients. Professionals should consider risks arising from their agreements with third-party service providers that are currently using or will or may be using AI technologies moving forward. Professionals also should consider any AI-related contractual risks arising from their current client agreements (including any limitations or restrictions placed on AI usage). Professionals should take such limitations and restrictions into account in making decisions with respect to AI usage. Professionals should update their client agreements to incorporate terms designed to reduce AI-related risks. For example, to reduce both legal and ethical risks, professionals should incorporate terms into their client agreements addressing (and obtaining agreement to) their usage of AI technologies.

B. Statutory and Regulatory Risks

Professionals also should identify and develop a plan to address their AI-related statutory and regulatory obligations and risks. Although there are no comprehensive AI laws currently in effect in the U.S., it is important to be aware that some cities and states have already passed targeted AI laws. For example, in 2018 California passed the Bolstering Online Transparency Act, which makes it unlawful to use a bot to communicate or interact online with a California resident in order to incentivize the sale or transaction of goods or services (or to influence a vote in an election). As another example, in 2021, Illinois passed the Artificial Intelligence Video Interview Act, which imposes a number of obligations on organizations using AI to analyze video interviews. A final example at the city level is New York City's Local Law 144, which requires, among other actions, independent bias audits of AI-enabled technologies used to "substantially assist or replace discretionary decision making for making employment decisions," including hiring and promotion decisions. Professionals should keep abreast of rapidly developing legislation at all different levels (*i.e.*, from cities to countries and regions). It is noteworthy that, according to Stanford University's Artificial Index Report 2024, to date, 148 AI-related bills have been passed by 32 countries. More will be coming.

Professionals also should identify obligations and risks affecting their AI usage that arise from other types of laws and regulations, including privacy laws and regulations; unfair and deceptive trade practices acts and other consumer protection laws; bias and discrimination laws; and competition laws. For example, comprehensive privacy laws, including those passed in the European Union and in multiple U.S. states, may impose obligations relevant to AI implementation and usage, including but not limited to notice obligations, consent/lawful bases for processing obligations; automated processing/profiling-related obligations; privacy by design and default obligations; data minimization and purpose limitation obligations; security obligations; data breach notification obligations; and obligations relating to cross-border transfers. In addition to comprehensive privacy laws, there are sector-specific and data-specific data privacy laws (*e.g.*, HIPAA, FCRA, GLBA, COPPA) that may also impose obligations on professionals implementing AI technologies. With respect to consumer protection laws, it is noteworthy that in April of 2023, the Federal Trade Commission, Equal Employment Opportunity Commission, Department of Justice, and the Consumer Financial Protection Bureau issued a joint statement pledging to enforce

federal laws governing civil rights, fair competition, consumer protection, and equal employment opportunities to "promote responsible innovation" in the context of automated decision-making and AI systems used by public and private organizations.

C. Intellectual Property, Trade Secret, and Confidentiality Risks

AI, particularly Gen AI, is giving rise to novel IP issues. Because the data that is used to train AI systems often includes a lot of third-party intellectual property (*e.g.*, patents, trademarks, and copyrights for which specific authorization has not been obtained), AI outputs may infringe upon IP rights. Numerous cases asserting copyright violations have already been filed against Gen AI developers. Concerns have even been raised about whether users of AI-produced outputs that infringe upon IP rights may also be liable for using such outputs. In addition to considering risks that may arise from using such AI outputs, professionals inputting any IP, trade secrets, or other confidential data into AI technologies will need to take care to protect their organizations' and their clients' IP; to protect the proprietary nature of any trade secrets that are input into AI systems; and to protect the confidentiality of any confidential information input into such systems through their selection of AI technologies capable of protecting such information and appropriate implementation of such technologies.

D. Bias and Discrimination Risks

One of the most significant risks professionals should consider when using AI technologies is the potential for AI technologies to produce outputs that are biased or discriminatory. AI technologies are only as good as the data on which they are trained. The data set and the algorithms used by such technologies have the potential to exacerbate prior discriminatory practices. Because of the lack of transparency in many AI technologies (*i.e.*, no visibility into why an AI technology made the decision/prediction it made), it can be difficult to defend decisions alleged to be biased or discriminatory that were made based on output from such AI technologies. These risks are particularly high in the context of AI technologies assisting with employment-related decisions, including screening candidates, interviewing candidates, hiring new employees, and promoting employees. In addition to the risks that Gen AI technologies might produce outcomes that are biased or discriminatory, professionals should be aware of the risk that users of Gen AI technologies or cyber criminals could manipulate such technologies to produce prejudiced outputs.

E. Antitrust Risks

Professionals should also consider potential antitrust risks that may arise in connection with certain AI usages. This is an area of law that is starting to garner more and more attention. For example, AI algorithms used to set prices could be alleged to result in price-fixing agreements among competitors. As AI advances, antitrust risks also could arise from AI systems, alone or together with other AI systems, reaching anticompetitive decisions. For example, AI systems could arrive at a conclusion that colluding with a competing AI system is appropriate in furtherance of the goal of maximizing profits. Concerns have also been raised by the FTC that Gen AI technologies could be concentrated in a small number of organizations, which would threaten innovation and competition.

F. Risks Arising from Malicious Actors Using AI Technologies

A final legal risk to consider is a risk arising not from professionals' usage of AI technologies, but from malicious actors using AI technologies, specifically Gen AI technologies. Such technologies are and will continue to be used by malicious actors for a host of bad purposes—including bypassing security measures through the creation of deepfakes; conducting social engineering scams; implementing ransomware attacks; and producing and spreading misinformation and disinformation. In addition to the business risks posed by such malicious activities, if such actions resulted in personal data breaches, the actions of such bad actors could result in data breach litigation and regulatory actions being filed against professionals' organizations. As a related point, trial lawyers should expect increased evidentiary challenges with respect to audio, video, and texts that either are deepfakes or are falsely alleged to be deepfakes.

IV. Key AI Ethical Obligations and Risks for Lawyers

This section of the paper examines how lawyers' use of AI technologies is governed by the ABA Model Rules of Professional Conduct (ABA Model Rules). Although the ABA Model Rules have been accepted in their entirety in many states, there are some states where lawyers' ethical duties may differ. Lawyers should review the specific ethical rules and related guidance in the jurisdictions in which they practice. The following sets forth key ABA Model Rules lawyers should consider as they select and implement (or not) AI technologies.

A. ABA Model Rule 1.1: Competence

First, lawyers should consider their duty of competence. Under ABA Model Rule 1.1, all lawyers are required to provide competent legal representation to their clients. Competent representation requires lawyers to not only "use methods and procedures meeting standards of competent practitioners," but also "to keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology." *See* ABA Model Rule 1.1, Comments 5 and 8.

The rise of AI technologies, including Gen AI technologies, has significantly increased the challenges of meeting technology-related competence obligations. Lawyers must develop a reasonable understanding of both the benefits and the risks of using AI technologies in their practices.

B. ABA Model Rule 2.1: Advisor

Second, lawyers should consider their duties as advisors. Under ABA Model Rule 2.1, "a lawyer shall exercise independent professional judgment and render candid advice." In doing so, a lawyer "may refer not only to the law but to other considerations such as moral, economic, social, and political factors, that may be relevant to the client's situation." *See* ABA Model Rule 2.1.

AI technologies should only be used to help aid lawyers in making decisions, and not as a substitute for a lawyer's independent professional judgment. Because the practice of law is often a time-sensitive practice and AI technologies can be highly efficient at performing certain tasks, it may be tempting for lawyers to rely solely upon AI outputs to prepare pleadings, agreements, documents and other deliverables to meet court, client-driven, or internal deadlines. However, AI technologies: (1) are not human, and cannot give adequate consideration to the moral, economic, social, and political factors that lawyers may consider when making arguments to the court or in giving advice to their client; and (2) can be prone to making mistakes and providing inaccurate outputs.

C. ABA Model Rule 1.5: Fees

Third, lawyers should consider their obligations to refrain from charging unreasonable fees or expenses. ABA Model Rule 1.5 prohibits lawyers from charging or collecting an unreasonable fee, or an unreasonable amount for expenses from the client. Comment 1 to ABA Model Rule 1.5 states that lawyers may only "charge fees that are reasonable under the circumstances."

Lawyers desiring to charge their clients for the expenses of implementing AI technologies should consider whether such expenses are reasonable. Lawyers should also consider the impact of decisions to use, or not use, AI technologies on the reasonableness of their fees.

D. ABA Model Rule 1.4: Communication

Fourth, lawyers should consider their duty to communicate with their clients. ABA Model Rule 1.4 states that "a lawyer shall reasonably consult with the client about the means by which the client's objectives are to be accomplished." ABA Model Rule 1.4 also states that "a lawyer shall promptly inform the client of any decision or circumstance with respect to which the client's informed consent . . . is required."

Regarding ABA Model Rule 1.4 and the use of AI technologies, the ABA stated in ABA Resolution 112 that lawyers should get informed consent from clients before using AI technologies. Lawyers need to communicate adequate information to allow clients to make informed decisions about the use of AI technologies. Lawyers may also need to communicate with clients when they do not plan to use AI technologies, especially if such technologies are reasonably available and might benefit the client.

E. ABA Model Rule 1.6: Confidentiality

Fifth, lawyers should consider their duty of confidentiality. Per ABA Model Rule 1.6, lawyers shall "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Factors to be considered in determining whether a lawyer's efforts are reasonable include: (a) the sensitivity of the information disclosed; (b) the likelihood of disclosure if additional safeguards are not set; (c) the cost to set additional safeguards; (d) the difficulty in setting safeguards; and (e) the extent to which the safeguards adversely affect the lawyer's ability to represent the client. See ABA Model Rule 1.6, comment 18.

The use of AI technologies in the legal profession may risk violating client confidentiality. The most obvious risk would be that a lawyer may input confidential client information directly into a third-party AI technology, thus disclosing confidential information to the third-party AI technology provider without client consent. A related risk is posed by the fact that many third-party AI technologies, as implemented, retain all inputs and outputs to help train and develop their AI algorithms. Thus, confidential client information could end up being provided to other users of such AI technology.

F. ABA Model Rule 1.15: Safekeeping Client Property

Sixth, lawyers should consider the related obligation of safeguarding client property. ABA Model Rule 1.15 states that "a lawyer shall hold property of clients or third persons that is in the lawyer's possession in connection with a representation separate from the lawyer's own property." Comment 1 to ABA Model Rule 1.15 states "a lawyer should hold property of others with the care required of a professional fiduciary."

In ABA Formal Opinion 483, the ABA emphasized that client property includes client files stored both physically and electronically. Lawyers have a duty to safeguard client information under both Model Rule 1.6 (a duty of confidentiality) and Model Rule 1.15. This further highlights the importance of lawyers being cautious about inputting client information into AI technologies, and confirming such technologies are reasonably designed and implemented to protect the confidentiality of client information on an ongoing basis.

G. ABA Model Rule(s) 1.7 & 1.9: Conflict of Interest

Seventh, lawyers should consider their obligation to avoid conflicts of interest. The conflict of interest rule relevant to current clients is ABA Model Rule 1.7, which states that "a lawyer shall not represent a client if the representation involves a concurrent conflict of interest. A concurrent conflict of interest exists if the representation of one client will be directly adverse to another client." ABA Model Rule 1.7 goes on to state that even if there is a conflict of interest, the lawyer can represent each client if, "(1) the lawyer reasonably believes that the lawyer will be able to provide competent and diligent representation to each affected client; (2) the representation is not prohibited by law; (3) the representation does not involve the assertion of a claim by one client against another client represented by the lawyer in the same litigation or other proceeding before a tribunal; and (4) each affected client gives informed written consent." One scenario where a violation of Model Rule 1.7 could be inadvertently violated by an AI technology would be if a conversation between a law firm's AI chatbot and a potential new client gave rise to an attorney-client relationship with an individual who is adverse to a client already represented by the lawyer or the lawyer's firm.

Lawyers should also be cognizant of the conflicts of interest rule relevant to former clients, ABA Model Rule 1.9 , which states, "a lawyer who …or whose present or former firm has formerly represented a client…shall not thereafter: (1) use information relating to the representation to the disadvantage of the former client except as…Rules …permit or require…or when the information

has become generally known; or (2) reveal information relating to the representation except as…Rules …permit or require." Comment 9 to ABA Model Rule 1.9 states that the conflict can be waived if the former client gives informed consent, which must be confirmed in writing. A situation where this rule could be implicated would be if a lawyer utilized an AI technology that, in its output, utilized a former client's confidential information that had previously been input into the technology to the disadvantage of such former client.

H. Responsibilities of a Partner or Supervisory Lawyer (ABA Model Rule 5.1)

Eighth, under ABA Model Rule 5.1: "A partner in a law firm [or supervisory lawyer] . . . shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct." Supervisory lawyers must make reasonable efforts to "establish internal policies and procedures designed to provide reasonable assurance that all lawyers in the firm will conform to the Rules of Professional Conduct." See ABA Model Rule 5.1, comment 1. A lawyer is responsible for "another lawyer's violation if: (1) the lawyer orders or…ratifies the conduct involved; or (2) the lawyer is a partner… [or] has direct supervisory authority over the other lawyer and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action." *See* ABA Model Rule 5.1.

Partners and supervisory attorneys should confirm that their firms have appropriate measures in place to help ensure ethical compliance in connection with the firms' AI technology usage, including the selection and implementation of appropriate AI technologies, and the implementation of appropriate AI policies, training, and oversight. Supervising lawyers also should take reasonable actions to oversee and remediate any potential harm caused by AI usage by a lawyer they are supervising.

I. Responsibilities Regarding Nonlawyer Assistance (ABA Model Rule 5.3)

Ninth, lawyers directly supervising nonlawyers must ensure nonlawyers are using AI technologies in accordance with ABA Model Rules. Per ABA Model Rule 5.3: "A lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer." Nonlawyers include not only parties employed by lawyers at the firm, but also third parties outside of the firm who are hired to assist in rendering legal services to the client. See ABA Model Rule 5.3, comment 3.

It is worth noting that, in 2012, the ABA changed the title of ABA Model Rule 5.3 from "Responsibilities Regarding Nonlawyer Assistants" to "Responsibilities Regarding Nonlawyer Assistance," presumptively, so the rule could cover non-humans. Thus, lawyers are not only responsible for supervising their law clerks, paralegals, and other employees, but also their independent contractors using AI technologies and their AI vendors/technologies.

J. Unauthorized Practice of Law (ABA Model Rule 5.5)

Tenth, ABA Model Rule 5.5 states that "a lawyer shall not practice law in a jurisdiction in violation of the regulation of the legal profession in that jurisdiction or assist another in doing so."

Comment 2 to ABA Model Rule 5.5 reiterates that "a lawyer may not assist a person in practicing law in violation of the rules governing professional conduct in that person's jurisdiction."

Lawyers who use AI technologies in the practice of law without applying their own, independent judgment in reviewing, revising, and approving deliverables that are created using such AI technologies risk assisting such AI technologies in the unauthorized practice of law. Lawyers using such AI technologies should supervise the use of such technologies and should conduct their own independent review of the outputs of such technologies.

K. Misconduct (ABA Model Rule 8.4)

Finally, ABA Model Rule 8.4 states that "it is professional misconduct for a lawyer to: (a) violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so, or do so through the acts of another . . . or (g) engage in conduct that the lawyer knows or reasonably should know is harassment or discrimination . . . in conduct related to the practice of law." Subsection (a) of ABA Model Rule 8.4 encapsulates all other ethical rules because any violation of the previously stated rules is a violation of ABA Model Rule 8.4. Subsection (g) of this rule highlights the importance of lawyers ensuring that the AI technologies they implement do not operate in a manner that results in discrimination or harassment.

V. Ethical Risks for Other Professionals

Other professionals should review any and all ethical rules and guidance applicable to their use of AI technologies, as well as any applicable state laws or regulations governing their profession. Key ethics rules that may be applicable include rules requiring fairness; transparency; accountability; legal compliance; security; confidentiality; client communication; conflicts of interest; and competence.

Additionally, all professionals should consider their obligations under any AI code of ethics implemented by their organizations. Such AI ethics codes and AI policies are important in establishing guidelines for responsible uses of AI technologies.

VI. Best Practices to Reduce the Legal and Ethical AI Risks

To help reduce the legal and ethical AI risks addressed above, we are providing 15 best practices recommendations professionals should consider implementing:

1. Implement strong AI governance policy and processes, including appropriate training on such policies and processes for your firm/company; and ensure processes are in place to oversee usage of AI technologies.
2. Develop a reasonable understanding of key AI technologies that would be beneficial to you and/or your clients, including their capabilities and limitations, and the benefits and risks of implementing such technologies.
3. Implement risk-based AI vendor management practices governing AI vendor selection, contracting, technology implementation, auditing, and offboarding.

4. Carefully consider AI terms, as well as terms that may impact AI usage, in agreements with AI technology vendors; third-party service providers; and clients.
5. Conduct regular audits of AI technologies to help ensure systems are working appropriately, and that AI decisions are non-discriminatory, fair, and empirically sound.
6. Advise clients of AI technologies you will be using in connection with the work you are doing for them (especially if you will be inputting confidential client information into the tool); and obtain informed consent through your client engagement letters or through other agreements to usage of such technologies.
7. Provide other appropriate AI notices and disclaimers.
8. Ensure AI practices meet relevant ethical and professional standards.
9. Develop good prompt drafting skills.
10. Thoroughly review and confirm the appropriateness of all AI outputs (*i.e.*, fact check them), and do not allow AI technologies to replace your professional judgment.
11. Identify potential AI-related disinformation and cybersecurity risks, and develop game plans to help reduce the likelihood such risks will arise and to identify and remediate such risks in the event they do materialize.
12. Implement technology solutions, policies, and practices designed to help ensure applicable privacy obligations are met with respect to implementation of various AI technologies, including but not limited to privacy principles (*e.g.*, data minimization and purpose limitation); privacy by design and default; notice; consent/lawful bases for processing; security; data breach notification; data subject rights; and cross-border transfer limitations.
13. Implement AI technologies, policies, and practices designed to help protect IP, trade secrets, and other confidential information.
14. Confirm appropriate insurance coverage is in place to help protect against potential AI-related claims; ensure application is accurately and completely filled out; and carefully review all insurance terms, including definitions, conditions, exclusions, endorsements, and notification obligations, to help reduce the risk of coverage disputes.
15. Stay on top of laws, regulations, regulatory guidance, ethics rules, opinions and guidance, and best practices that impact your organization's usage of AI technologies.

VII. Conclusion

AI is, of course, here to stay. The impact of AI on professionals is and will continue to be huge. Per the McKinsey Global Survey on the Current State of AI, even though the vast majority of organizations are already implementing one or more AI technologies, including Gen AI technologies, a very significant majority of such organizations do not yet have policies governing Gen AI technology usage, many are not mitigating AI-related cybersecurity risks, and most are not even taking steps to mitigate the most common AI risk—inaccuracy. Professionals implementing these best practices will be ahead of the game.