Legal Reasoning

Counseling clients on managing the risks of artificial intelligence.

WRITTEN BY **SHAWN E. TUMA** AND **KRISTEN PETRY**

> "Success in creating AI would be the biggest event in human history. Unfortunately, it might also be the last unless we learn how to avoid the risks." —Stephen Hawking

Artificial intelligence is here and, though still in its infancy, it has taken the world by storm. We are living in a time that will go down in history as the dawn of a new age—the artificial intelligence age—which will have as profound of an impact on society as did its predecessors, the Iron, Industrial, Computer, and Information ages. As AI matures, it is primed to reshape every sector of the worldwide economy at an exponential rate. Unfortunately, as rapidly as AI's capabilities advance, so too do its risks. Heeding Hawking's warning, figuring out how to manage those risks may be humanity's most important challenge.

For the lawyer advising clients in an area such as AI, this poses two distinct challenges. First, we must have a basic understanding of the technology itself as well as its risks through its operational application. Second, we must be prepared to advise our clients about the legal aspects of how this technology may impact them and what they can do to help manage the associated risks, technologically and legally.

COUNSELING CLIENTS ABOUT AI REQUIRES LAWYERS TO USE LEGAL REASONING

The law always struggles to keep up with the rapid advancement of technology. That was the same for the previously mentioned ages as it is for AI. Federal and state legislatures are proposing and debating laws that will help govern this societal shifting technology but very little meaningful law has been enacted. The courts are addressing issues as they come before them, but, by design, the common law method works slowly and methodically, as though painting a masterpiece dot by dot on the canvas. Federal and state regulatory agencies have made some progress; however, their attention is focused on only the narrow interests of their respective agencies and have implemented little in the way of guidance for others.

Given this situation, what are we as lawyers to do when our clients come to us with questions about how they can manage the legal and regulatory risks surrounding this innovative technology? The answer is simple, though not necessarily easy: We are to do what we have always done before when leading the way into unchartered territory. We are to look to the guidance and principles that are known and binding, then, to those that are persuasive, and then, using logic and reason, analyze our way toward a conclusion that is our best prediction of what we *think* the outcome should be based upon the best available information. And ironically, this is how we earn our keep as lawyers, for any lay person—or AI—can regurgitate the text of a statute or regulation but, at least for now, it is we as lawyers who are best suited for legal reasoning.

NIST'S ARTIFICIAL INTELLIGENCE RISK MANAGEMENT FRAMEWORK IS GUIDANCE FOR NAVIGATING THE AI JOURNEY

Fortunately, we are not starting from a blank slate. The National Institute of Standards and Technology, or NIST, and the U.S. Department of Commerce published the Artificial Intelligence Risk Management Framework, or AI RMF,[1] to assist individuals and companies in evaluating and mitigating risks at every stage of the AI life cycle. While compliance with NIST frameworks such as the AI RMF is only mandatory for federal government agencies and their contractors, they are powerful persuasive guidance for all organizations.

Functionally speaking, the AI RMF was designed to provide guidance for all organizations and individuals that have a role in the design, development, deployment, and use of AI. From a legal guidance perspective, the AI RMF is a framework and not intended to be a law or regulation for all; however, it addresses many of the issues that we see as developing legal issues and over time will come to be used as an example of the appropriate standard of care for such issues by attorneys and regulators in future litigation. Currently, the AI RMF represents one of the most comprehensive governance strategies for defining and addressing AI risks, and it is a great place to begin legal analysis.

OVERVIEW OF THE NIST AI RMF

The "goal of the AI RMF is to offer a resource to the organizations designing, developing, deploying, or using AI systems to help manage the many risks of AI and promote trustworthy and responsible development and use of AI systems."[2] The intended audience is "'those who play an active role in the AI system lifecycle, including organizations and individuals that deploy or operate AI'" referred to as AI Actors.[3]

The AI RMF recognizes that enterprise risk management is critical to responsible AI development and use. Creating and implementing trustworthy AI requires input from multiple stakeholders, including information technology personnel, C-suite executives, risk management personnel, legal services, affected organizational departments, and end users. For AI systems to be perceived as trustworthy, they should have the following characteristics: "valid and reliable, safe, secure and resilient, accountable and transparent, explainable and interpretable, privacy-enhanced, and fair with harmful bias managed."[4]

Because we cannot manage what we do not know exists, individuals and companies must be able to identify the risks posed by AI to develop a comprehensive governance strategy. The AI RMF groups the risks into three distinct categories: (1) Harm to People, (2) Harm to an Organization, and (3) Harm to an Ecosystem.[5] Some examples include harm to civil liberties (people), physical or psychological safety or economic opportunity (people), harm to a group such as discrimination (people), harm to democratic participation or educational access (people), harm to business operations or reputation (organization), and harm to the global financial system, supply chain, or natural resources (ecosystem).[6] Due to the ongoing and evolving nature of AI risk, AI risk management should be continuous, timely, and performed throughout the AI system life cycle to remain effective.

Overall, a practical, comprehensive governance strategy will address the risks of AI at each stage of its life cycle—design, development, deployment, and use. The AI RMF recommends the use of four high-level functions to manage AI risks: Govern—cultivating and presenting a culture of risk management; Map—identifying, assessing, tracking, and analyzing risks; Measure—prioritizing and acting upon a projected risk impact; and Manage—recognizing the context of related risks.[7]

KEY GUIDANCE FOR LAWYERS FROM THE NIST AI RMF

NIST provides several hundreds of pages of guidance for using the AI RMF, and much of it is related to legal functions, so an article of this nature can only paint with very broad strokes. Initially, the focus for many lawyers counseling clients on these issues will likely be Part 2: Core and Profiles, within the Govern function.[8] The Govern category focuses on understanding, managing, and documenting policies, processes, procedures, and practices, which are roles that fit well within the attorney's core skill set. A high-level review of that category, as well as key provisions of the *NIST AI RMF Playbook*[9] addressing the other categories, provides some key areas to focus on when counseling clients.

- Ensure that you have a thorough understanding of the client, the nature of their business, their business environment, activities, information, and relationships to other parties.
- Ensure that you and the client both have a clear understanding of what the client's objectives are for using AI and its intended uses. Each client's needs will be unique and must be understood at the outset.
- Ensure that you and your client engage in a thorough analysis of any existing legal and regulatory requirements involving AI that pertain to that particular client and that such requirements are understood, managed, and documented by the client.
- Ensure your client recognizes the need to develop, understand, manage, document, and effectively implement policies, processes, procedures, and practices for much of its work as it relates to AI and, where appropriate, that such policies are transparent. Examples may include policies, processes, procedures, and practices:
  - Mapping, measuring, and managing of AI risks across the organization.
  - Connecting AI governance to existing organizational governance and risk controls.
  - Aligning to broader data governance policies and practices, particularly the use of sensitive or otherwise risky data, such as personal information.
  - Establishing whistleblower policies to facilitate reporting of serious AI system concerns.
  - Detailing and testing incident response plans.
  - Determining the needed level of risk management activities based on the organization's risk tolerance and addressing the risk management process as a whole.
  - Addressing the decommissioning and phasing out of AI systems.
  - Addressing third-party and vendor management protocols and due diligence related to using third-party's AI systems or engaging in business or sharing data with parties that use AI systems and how that may impact the client.
  - Providing appropriate education and training to all

stakeholders and end users, including employees or consumers.

- Ensure the client understands that insurance is a critical risk management tool and that it must specifically obtain coverage for AI, data, and cyber-related risk or else they may not be covered by default.
- Finally, ensure the client understands that due to the evolving and uncertain nature of technology and its uses, the business environment, the legal and regulatory environment, and the client's own activities, the advice you are providing is not absolute but is your best analysis of what the rules are at this time and that could change quickly. **TBJ**

NOTES

1. *Artificial Intelligence Risk Management Framework (AI RMF 1.0),* National Institute of Standards and Technology (2023) (NIST AI 100-1), U.S. Department of Commerce, https://doi.org/10.6028/NIST.AI.100-1.
2. *Id.* at p.2.
3. *Id.* at p.2.
4. *Id.* at p.12.
5. *Id.* at p.5.
6. *Id.* at p.5.
7. *Supra* note 1.
8. AI RMF at p.20.
9. *NIST AI RMF Playbook,* National Institute of Standards and Technology, U.S. Department of Commerce, https://airc.nist.gov/AI_RMF_Knowledge_Base/Playbook.

SHAWN E. TUMA
is an attorney widely recognized in data privacy and cybersecurity law, areas in which he has practiced for well over two decades. He is co-chair of the Data Privacy, Cybersecurity, and AI/Emerging Tech practice groups at Spencer Fane and works primarily in the firm's Collin County office, where he also serves as office managing partner. Tuma is a past chair of the State Bar of Texas Computer & Technology Section.

KRISTEN PETRY
is an attorney with Spencer Fane and a member of the firm's Health Care, Data Privacy, Cybersecurity, and AI/Emerging Tech practice groups. Her practice includes guiding clients in the health care industry, where she navigates simple and complex litigation and compliance issues. Petry has defended large hospital systems and individual health care providers, including physicians, nurses, therapists, dentists, and chiropractors. She also has experience advising clients on federal regulations, including HIPAA and 42 CFR Part 2.