wiley

Keeping Pace with Emerging Tech Developments Including AI

Prepared for The Association of Corporate Counsel National Capital Region In House Paralegal Institute 2023

Duane Pozza & Kat Scott

June 20, 2023

What We're Discussing Today

- What is AI?
- What are the potential beneficial uses of AI?
- What are the key potential risks of AI?
- Who in the government is interested, and what are the key legal and regulatory developments in response to AI?
- What are the tools and best practices for organizations to leverage AI and manage risks?
- What is the legal and regulatory landscape like for other emerging technologies (e.g., blockchain and NFTs)?

Artificial Intelligence 101

What is AI?

- Involves capacity to learn
- Generally based on large data sets

"AI is the ability of a computer system to solve problems and to perform tasks that would otherwise require human intelligence." *Interim Report of National Security Commission on AI (2019)*

Potential Use Cases

- Predictive analytics
- Pattern recognition in large data sets
- Cybersecurity and fraud defense
- Voice interaction
- Detecting deepfakes
- Automated diagnostics and maintenance
- Object recognition and imagery analysis
- ***Buzzwords:*** AI, ML, algorithms, natural language processing, generative AI

Key AI Risks/Principles

- Bias
- Explainability
- Accountability
- Privacy
- Security & Safety
- Transparency

Key AI Risk/Principle: Explainability

Key Issues

- When do you need to explain how AI reached a conclusion? And can you?
- Who is your audience?
- Explainability requirements in practice: credit decisions and adverse action notices

Resources & Best Practices

- NIST's Four Principles of Explainable Artificial Intelligence:
  - Explanation
  - Meaningful
  - Explanation Accuracy
  - Knowledge Limit

Key AI Risk/Principle: Bias

- **Key Issues**
  - Mitigating harmful AI bias
  - Biased data sets vs. algorithmic bias
  - Sector-specific laws: credit, housing, employment
  - FTC: “data abuses” and “algorithmic fairness”
  - Third party testing proposals
- **Resources & Best Practices**
  - ***NIST research***
    - Towards a Standard for Identifying and Managing Bias in Artificial Intelligence
    - Managing AI/ML Bias in Context
  - ***FTC guidance***
    - Don’t discriminate based on protected classes.
    - Focus on inputs as well as outcomes.
    - Ensure AI models are validated and revalidated to ensure that they work as intended, and do not unlawfully discriminate.
    - Ask questions before using algorithm.
      - How representative is your data set?
      - Does your data model account for biases?
      - How accurate are your predictions based on big data?
      - Does reliance on big data raise ethical or fairness concerns?

Key AI Risks/Principles: Privacy and Security & Safety

Privacy

- Are there privacy risks unique to AI?
- Federal Trade Commission (FTC)
  - Enforcement: Focus on deception – what is said in privacy policy?
  - Rules: Commercial surveillance and data security ANPR
- State privacy laws
  - Omnibus privacy laws in VA, CO, and CT create "opt-out" right for automated profiling in furtherance of legally significant decisions
  - Forthcoming rulemaking in CA to establish access and opt-out rights
- What's next? Congress?

Security & Safety

- Are there security and safety risks unique to AI?
- AI faces a range of cybersecurity threats – which pose both operational risk and legal risk in case of an incident
- Physical safety issues
- Reputational risks and IP-related issues

Key AI Risks/Principles: Accountability and Transparency

Accountability

- Who is accountable for making sure nothing goes wrong with AI?
- Multiple participants in AI lifecycle: software developers, product developers, downstream operators
- Human involvement/accountability

Transparency

- When do you need to disclose that AI is being used?
- State law examples
  - California Bot Disclosure Law: automated bots cannot mislead consumers about artificial identity, to incentivize sales or influence electoral vote
  - Illinois Artificial Intelligence Video Review Act: employers using AI analysis of job applicant-submitted videos must provide notice, obtain consent, and more

AI Risks/Principles in Practice

- Potential tension between principles (e.g., explainability and security)
- Tension with traditional privacy principles (e.g., purpose specification and avoiding secondary use)
- Standards and measurements continue to be developed
- Will there be clear rules and guidance on issues like bias?

Key Government Actors and Workstreams

Federal

- White House
- Federal Trade Commission (FTC)
- NTIA
- Financial Regulators
- National Institute of Standards and Technology (NIST)
- Congress

States

- Legislation targeting specific AI use cases

International

- European Commission: Proposed AI Act
- Organization for Economic Cooperation and Development (OECD) AI Principles
- US-Led International Ventures

Perils for AI on Legal, Regulatory, and Policy Fronts

- AI legal framework is developing in real time
- This poses challenges for AI developers and companies
- Lawsuits and regulatory actions look backwards – so what companies do now will be under scrutiny in the future
- Companies also must be ready for patchwork of rules
- AI governance can often help solve legal problems

NIST AI Risk Management Framework (AI RMF)

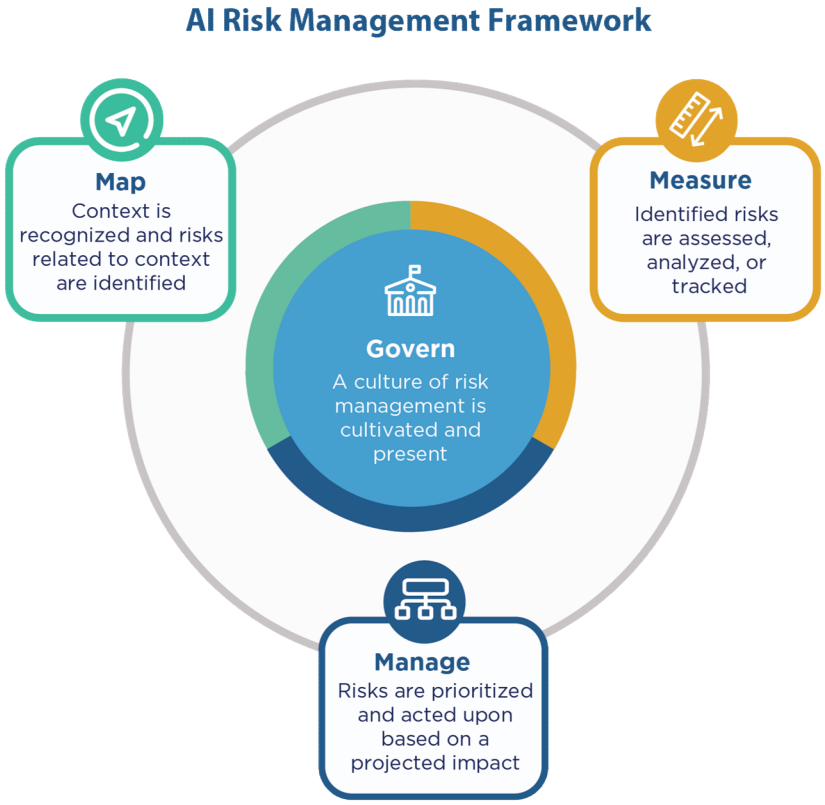
- A risk management resource for organizations designing, developing, deploying, or using AI systems
  - Provides voluntary guidance and risk management practices
- Frames AI related risks
  - 7 “trustworthy AI characteristics”
- Outlines the AI RMF “Core”
  - 4 “Functions,” along with “Categories” and “Subcategories” that help organizations address AI system risks as a practical matter

AI RMF: Trustworthy AI Characteristics

- Valid and reliable
- Safe
- Secure and resilient
- Accountable and transparent
- Explainable and interpretable
- Privacy enhanced
- Fair – with harmful bias managed

AI RMF: 4 Functions

- Govern: recommendations concerning high level processes and organizational schemes for fostering a culture of risk management throughout an organization
- Map: recommended methods for contextualizing and identifying AI system risks
- Measure: recommendations for assessing, analyzing, and tracking identified AI risks
- Manage: recommendations for allocating resources and prioritizing AI system risks



Some Developing Best Practices

- Consider corporate or industry-wide principles and policies
  - Establish generative AI policies
- Ensure review processes throughout lifecycle of AI
- Adopt risk-based approach to identify and proactively mitigate risks
- Establish clear responsibility and accountability within organization
  - Ensure both technical and non-technical personnel are engaged
- Establish incident response protocols and training
- Pay attention to “informal” guidance from regulators like the FTC

Blockchain and NFTs

- Blockchain technology
  - Allows transactions to be recorded in verifiable way
  - Decentralized vs. centralized blockchains
  - Issues include privacy and IP protection
- Non-fungible tokens (NFTs)
  - Digital assets - but not cryptocurrencies
  - Can be used for marketing purposes
- How will technology and tokens be regulated?
  - Significant recent SEC activity

wiley

Questions? Contact Us.

Duane Pozza
dpozza@wiley.law
202.719.7533

Kat Scott
kscott@wiley.law
202.719.7577