Online Lenders Alliance

How is AI/ML Changing Compliance?

July 16, 2024

James Gatto
AI Team Leader
Sheppard Mullin

Kelly Truesdale
Associate
Mayer Brown

COMPLIANCE UNIVERSITY

Speaker Bios

James Gatto

AI Team Leader

J.D., Georgetown University Law Center, 1988

B.E., Electrical Engineering (Physics minor), Manhattan College, 1984

Former U.S. Patent Examiner

jgatto@sheppardmullin.com

703-989-9288

I am passionate about the intersection of disruptive tech, law and business

35 years of business-focused, legal advice on all aspects of intellectual property strategy, technology transactions, technology-related regulatory issues and litigation, especially ones driven by new business models and/or disruptive technology.

- **Artificial intelligence** (training, policies, IP, regulatory) 20+ years
- **Open Source** (audits, diligence, license issues, policies) 20+ years
- **Blockchain** (blockchain games, crypto/NFTs, metaverses, digital art) 12+ years
- **Interactive entertainment** (games, AR, VR, fantasy sports, esports) 15+ years

Some Recent AI Activity

- Adjunct Professor, Ole Miss Law School “Legal Issues with AI”
- Invited Speaker, Korean Copyright Office “AI and Open Source”
- Speaker, US Copyright Office Listening Session on AI Authorship
- Speaker, USPTO Listening Session on AI Inventorship Issues
- ABA-IPL AI/Machine Learning (AI/ML) Task Force – appointed member
- AIPLA AI Subcommittee, co-leader
- Member, Artificial Intelligence Committee, International Technology Law Association
- Member, NIST Generative AI Public Working Group

Speaker Bios

Kelly Truesdale

J.D., Georgetown University Law Center

M.S., Computer Science, Georgia Institute of Technology

I.M.B.A., University of South Carolina

B.S., Computer Science, Florida Institute of Technology

ktruesdale@mayerbrown.com

202-263-3294

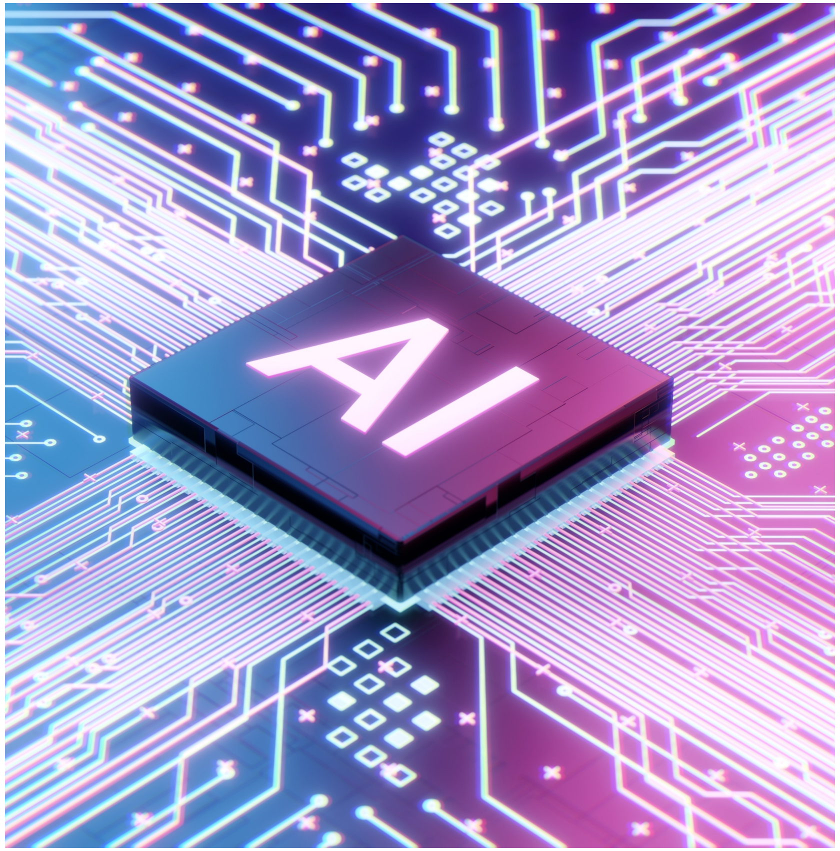
Focuses on advising financial institutions, fintechs and technology-focused firms on M&A, corporate and other transactional matters, as well as regulatory and product considerations related to payments, digital assets and other innovative technology applications in financial services.

- **Mortgage transactions** (whole loans, MSRs, servicing agreements)
- **Payments regulatory** (funds transfers, ACH, RTP and card network rules)
- **State money transmission laws** (application and compliance)
- **BSA/AML compliance** (CIP/KYC requirements and compliance)

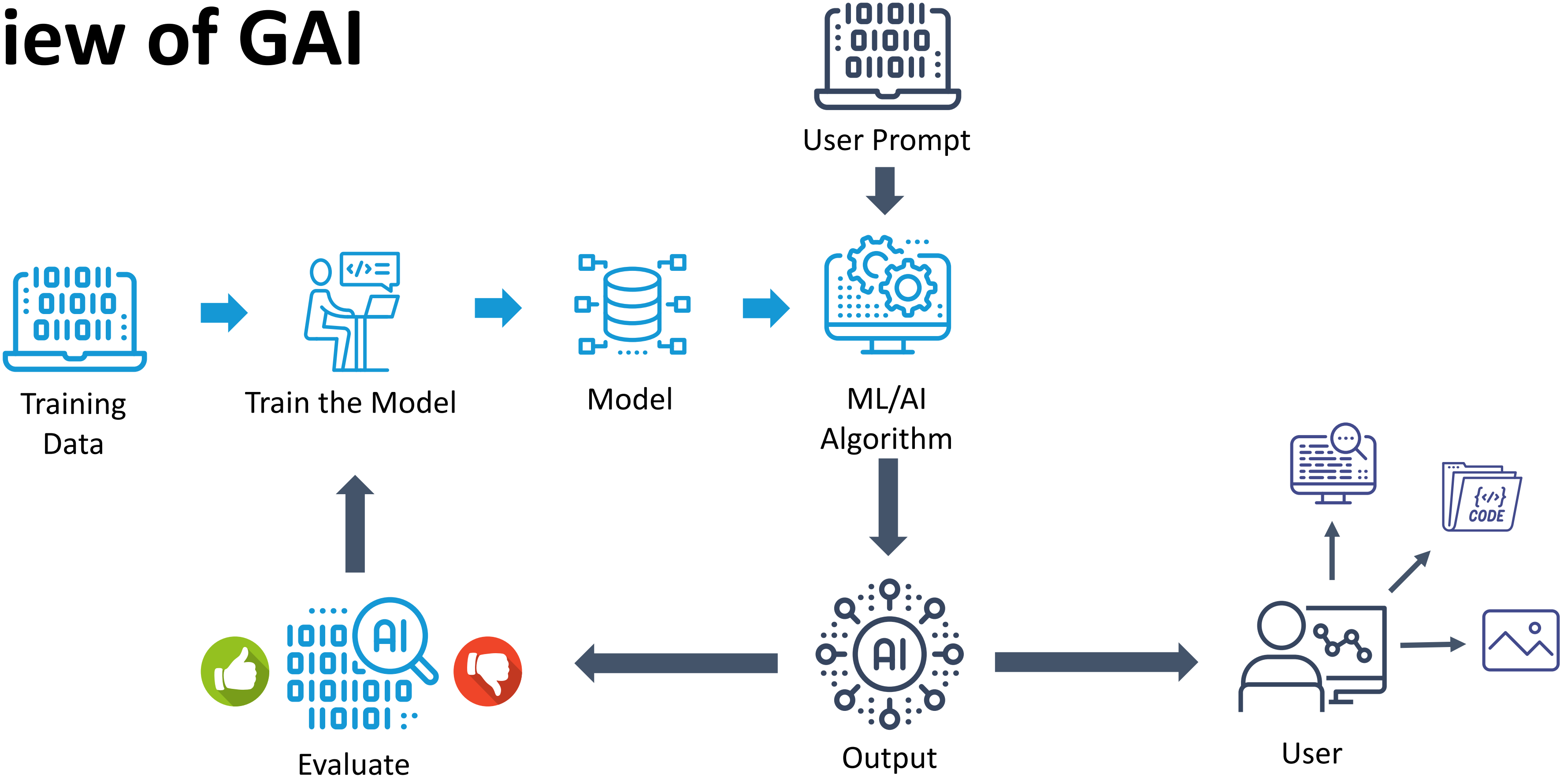
Prior to law school, worked as a software engineer developing APIs and data processing and analysis pipelines.

Agenda

- An overview of AI
- Uses of AI in Lending
- General Legal Issues with AI
- Legal and Compliance Issues – Specific Issues
- Overview of Regulatory and Legislative Framework
- How to Manage AI Legal Risk and Compliance



Overview of GAI



AI Models

- Foundation models – pretrained Large Language Models (LLMs) trained on billions+ parameters
- Fine Tuning – customizing foundation models by training on data (may be your data) to generate specialized results – specific tasks or domains (e.g., law, medicine, etc.)
- Retrieval Augmented Generation (RAG) – augments the capabilities of an LLM by adding an information retrieval system to constrain outputs based on your enterprise/specialty content

Overview of AI

Artificial Intelligence (AI)

Machines with human-inspired capabilities including:

Communication

Perception

Planning

Reasoning

Knowledge representation

Move and manipulate objects

Learning

Machine Learning (ML)

Machines use data to generate output that is:

Descriptive – explain what happened

Predictive – predict what will happen

Prescriptive – make suggestions about what action to take

Generative AI (GAI)

AI used to generate new:

Text

Images

Code

Video

Audio

Other content

Sample Legal Issues by "Role" in AI

Obtaining Data

Proper acquisition of data
Right to use
Compliance with any terms Infringement

- Copyright/TM
- Privacy/BIPA
- NIL – right of publicity
- Other

Training Models

All of the data issues +
Responsible AI –

- Transparency
- Explainability
- Bias/Discrimination ("BAD")
- Accuracy

Providing AI Tools

All of training issues +
Patent Infringement
Liability for Outputs

- Defamation
- Deep Fakes
- Indemnity

FTC/Agency Regulations

- False Advertising

Using Tools

Infringement

- Copyright/TM
- Privacy/BIPA
- NIL – right of publicity
- Other

Indemnity?
IP protection

- Copyrightability

Ownership of Output
Hallucinations
Deepfakes
BAD Output
BAD Use
Other

Using Output

All of Using Tools Issues +
Lack of awareness how deliverables were generated

Applications of AI/ML in Lending

- Business Operations
  - Process automation (IT, HR, etc.)
- Product Development
  - Code generation (Copilot)
  - Testing and validation
- Evaluating Creditworthiness
  - Utilize additional data sources
  - Credit risk modeling
- Loan Processing
  - Document analysis
  - Approval workflow automation
  - Fraud detection
- Marketing
  - Segmentation and targeting
  - Cross-selling
- Customer Service
  - Chatbots and virtual assistants

General Legal Issues with AI

- Obtaining data – proper access
- Training AI – right to use data
- Developing AI – Responsible AI (accuracy, transparency, avoid bias and discrimination)
- Deploying/Using AI
- Handling inputs/outputs
- Liability and Indemnity

Data Issues

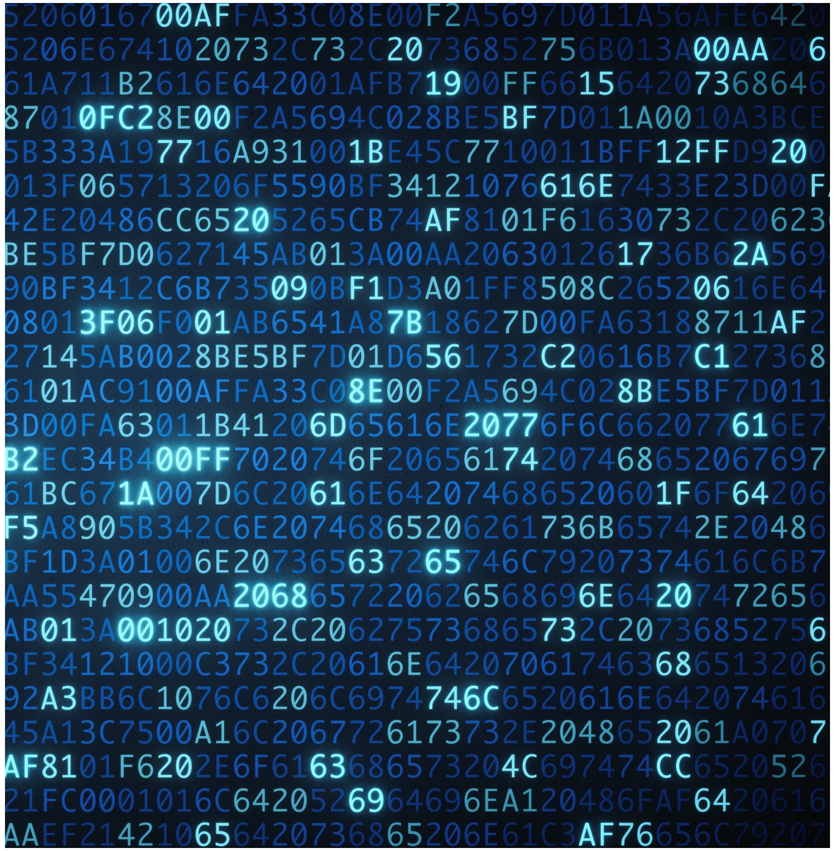
Issues with Data for Training AI Models

- Need right to **acquire** the data
- Need right to **use** the data for training
- Training on copyrighted content can infringe
  - Fact Dependent – content types, content sources, licensed or otherwise permitted use
  - If infringement, is fair use a defense?
  - Google Books case v. Ebooks case

Some Other Potential Issues With Data for Training AI Models

Need to consider data sources, data types, permissions

- Websites
  - Web scraping
- Images/creative works
  - Creative commons – license to use but some limitations (e.g., no commercial use, no derivatives, etc.)
- Right of Publicity – if content contains celebrity NIL, can you use?
- Privacy – if content contains PII/Biometric info, can you use?
- Open source (code, data) – often license to use but compliance obligations (e.g., copyright, attribution)



Just Because It’s “Your” Data ≠ Right To Use

- Many companies have troves of valuable user data
- Want to use to train AI
- Use of customer data that exceeds use permitted by the privacy policy/terms in effect at the time the data was collected could be problematic

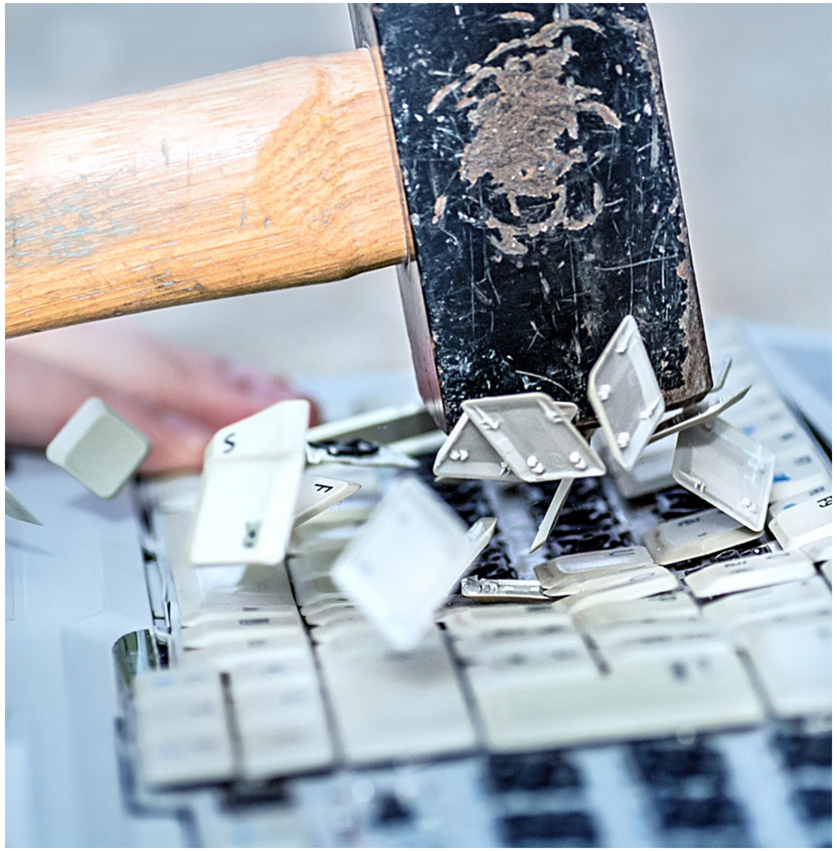
Legal Considerations When Using Consumer Data To Train AI

- Merely changing TOS/PP to permit use of previously collected data may not work

FTC Warns About Changing Terms of Service or Privacy Policy to Train AI on Previously Collected Data

2022 FTC Settlement with Everalbum

- *Everalbum* – FTC enforcement for unauthorized use of images collected for one purpose (online photo albums) but used for another (train facial recognition technology)
- Result: “Algorithmic disgorgement”
  - Penalty for improperly using data to build algorithmic systems like AI/ML models
  - Required to destroy ill-gotten data and the models/algorithms derived from it



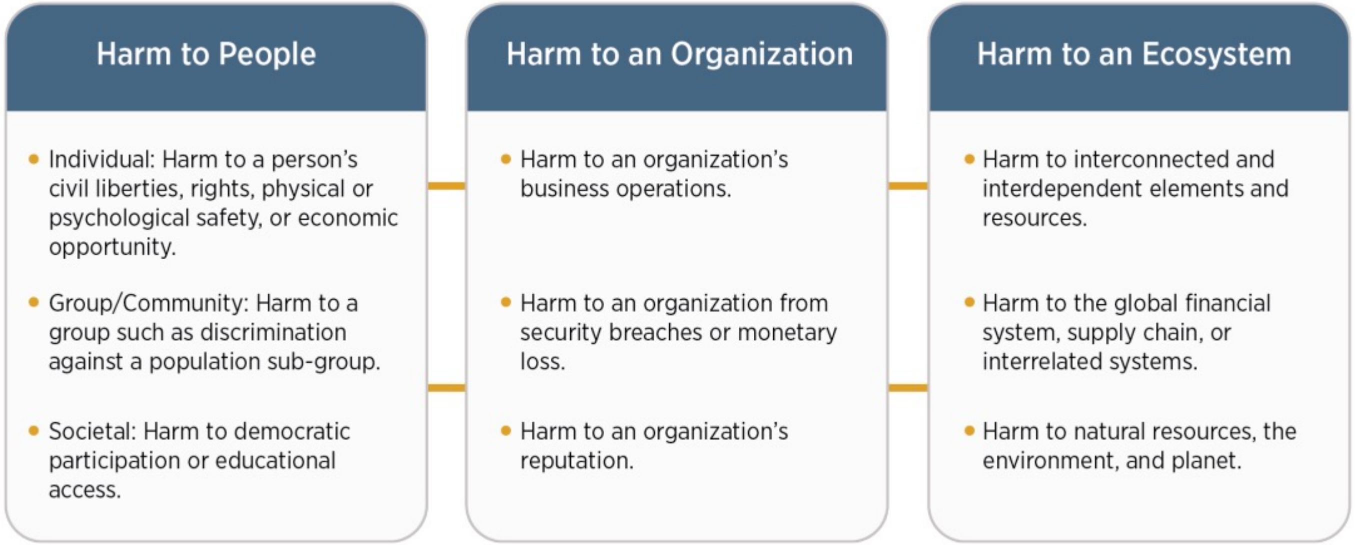
What is Responsible AI?

Responsible AI refers to a set of principles that guide the:

- **Design**
- **Development**
- **Deployment**
- **Use**

of AI systems

Responsible AI



Harm to People

- Individual: Harm to a person's civil liberties, rights, physical or psychological safety, or economic opportunity.
- Group/Community: Harm to a group such as discrimination against a population sub-group.
- Societal: Harm to democratic participation or educational access.

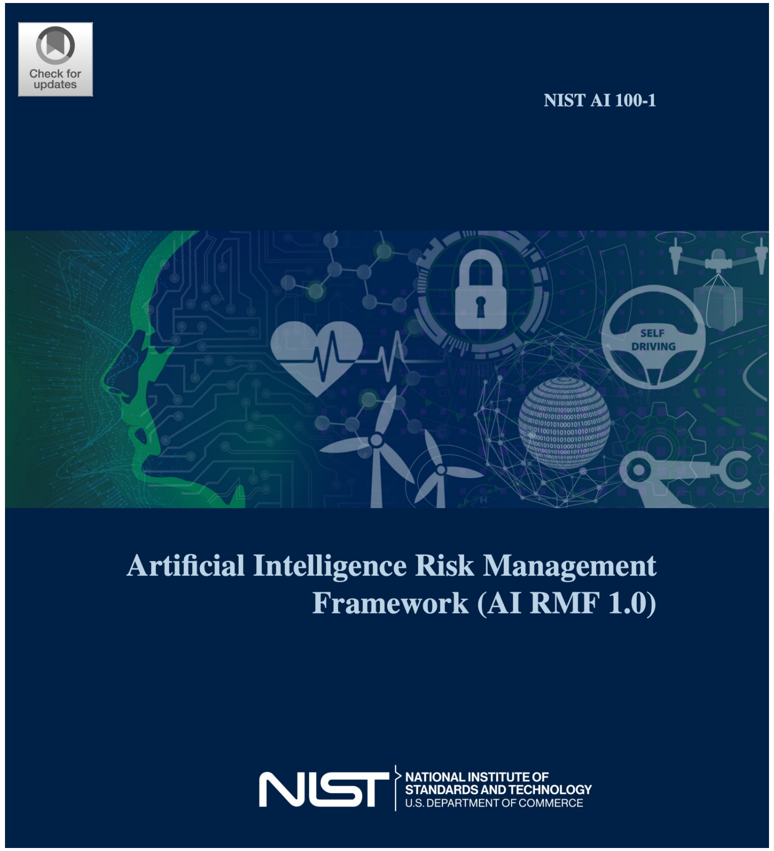
Harm to an Organization

- Harm to an organization's business operations.
- Harm to an organization from security breaches or monetary loss.
- Harm to an organization's reputation.

Harm to an Ecosystem

- Harm to interconnected and interdependent elements and resources.
- Harm to the global financial system, supply chain, or interrelated systems.
- Harm to natural resources, the environment, and planet.

Fig. 1. Examples of potential harms related to AI systems. Trustworthy AI systems and their responsible use can mitigate negative risks and contribute to benefits for people, organizations, and ecosystems.



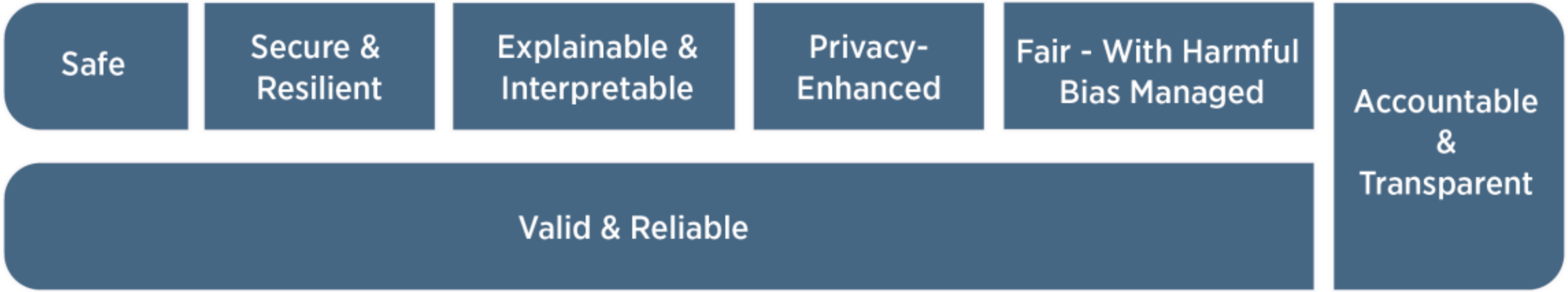
Check for updates

NIST AI 100-1

Artificial Intelligence Risk Management Framework (AI RMF 1.0)

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Trustworthy AI



Safe

Secure & Resilient

Explainable & Interpretable

Privacy-Enhanced

Fair - With Harmful Bias Managed

Accountable & Transparent

Valid & Reliable

Fig. 4. Characteristics of trustworthy AI systems. Valid & Reliable is a necessary condition of trustworthiness and is shown as the base for other trustworthiness characteristics. Accountable & Transparent is shown as a vertical box because it relates to all other characteristics.

Commitment to AI Ethics and Diversity – Responsible AI

- Accountability – external engagement; internal governance for product and development activities
- Reliability – alignment of expectations for output and performance
- Transparency – understanding of terms and intended use of products; data used to train AI models; privacy and security
- Explainability – understanding of criteria used and output
- Fairness – design and impact promotes positivity and inclusion
- Sustainability – consideration of impacts on society, economy, environment
- Diversity – diverse AI teams and datasets

Why is the NIST Voluntary Framework Important?

CO AI law imposes obligations on **developers** and **deployers** of AI systems and provides an affirmative defense if the developer or deployer:

i) has implemented and maintained a program that complies with **a nationally or internationally recognized risk management framework for artificial intelligence systems that the bill or the attorney general designates**; and

ii) the developer or deployer takes specified measures to discover and correct violations

[Colorado Introduces an AI Consumer Protection Bill]()

NIST RMF Updates (drafts)

- NIST published for comment four draft publications to help improve the safety, security and trustworthiness of AI systems
- Two provide guidance to help manage the risks of generative AI and are designed to be companion resources to the (AI RMF) and Secure Software Development Framework (SSDF)
- The third offers approaches for promoting transparency in digital content
- The fourth proposes a plan for developing global AI standards
- For more information on these four new publications see *NIST Updates AI RMF as Mandated by the White House Executive Order on AI*

Handling Inputs and Outputs

- Inputs/Outputs
  - Confidentiality
  - Ownership
  - License
- Typically addressed in TOS/License
  - Different terms for different versions (free vs. enterprise)

IP Issues

IP Protection Limited for GAI Output

Copyright guidance

- Output of GenAI typically not protectable!
- Copyright can protect only material that is the product of human creativity

Patent guidance

- AI tools can be patented – 20% of all current patent filings are AI-related
- AI-assisted inventions are not categorically unpatentable
- Focus of inventorship analysis on whether significant human contributions

Ownership and Protectability of GAI Output

- Terms of Use for different tools treat ownership differently
- Some grant ownership, some don’t, some don’t address
- Some require license grant to tool provider
- Some recognize another user’s prompt may generate same output and they own too
- Copyright Protection for output of GAI is limited – not human authorship

Liability and Indemnity

Liability

- Who is liable if output infringes?
  - Tool provider
  - User
- Indemnity – varies per tool and version
  - Some free versions **user indemnifies** tool provider!
  - Some enterprise versions, tool provider indemnifies
  - Some indemnities have preconditions

Sample Indemnity Issue

- Microsoft does not make any warranty or representation of any kind that any material created by the Online Services does not infringe …
- **You agree to indemnify** and hold harmless Microsoft … arising from or relating to your use of the Online Services, including **your subsequent use of any content** from the Online Services

Copilot Copyright Commitment

Exception: Covers potential infringement by use of output of Microsoft's Copilots and Azure OpenAI Service for paid versions of Microsoft commercial Copilot services, Bing Chat Enterprise, Microsoft 365 Copilot and GitHub Copilot.

- Must implement required "guardrails and mitigations" to be eligible (many companies are not aware of this!)
- If a customer tenders a claim for defense, the customer will be required to first demonstrate compliance with all relevant requirements

Sample FTC Enforcement

FTC Investigation of OpenAI

Determining whether OpenAI "engaged in unfair or deceptive privacy or data security practices or engaged in unfair or deceptive practices relating to risks of harm to consumers"

- FTC is investigating OpenAI over possible consumer harm through its data collection and the publication of false information.
- FTC sent a 20-page letter that requests documents related to developing and training its large language models, and data security issues.
- FTC wants detailed information on how OpenAI vets information used in training its AI models and how it allegedly prevents false claims from being shown to ChatGPT users. It also wants to learn more about how APIs connect to its systems and how data is protected when accessed by third parties.

FTC Investigation of OpenAI

Examples of Types of Information Being Sought by FTC About AI Products:

How Marketed	Process to Correct “Hallucinations”
How You Ensure Ads/Reps are clear	Process for Retraining/Refining Models
Research Tests re: accuracy of Products	Process of Reinforcement Learning Through Human Feedback
How You Use Info Retained or Collected	Policies and Procedures to Assess Risk
Data Used to Train and How Collected	Policies to Protect PII
How you Review Data Used to Train	Policies to Delete PII if Requested
How do you manage bias	Policies re: Accuracy of Statements About Individuals

Legal and Compliance Issues – Specific Uses

AI Bias With Employment

EEOC

- May 2023 – Assessing Adverse Impact in Software, Algorithms, and Artificial Intelligence Used in Employment Selection Procedures Under Title VII of the Civil Rights Act of 1964
- September 2023, settled its first AI-based hiring discrimination case against iTutorGroup Inc. for using recruitment software that automatically rejected older applicants

New York City Law – requires employers to provide notice about the use of an AI system, offer them an opt out, and audit any such systems for bias – see here for more

NY AI Laws Going Live Next Month | Sheppard Mullin Richter & Hampton LLP - JDSupra

New York State Law – would limit employers' ability to use electronic monitoring and automated employment decision tools – see here for more

Chatbots and Customer Service AI

- Chatbots and virtual assistants
  - One of the most common AI tools encountered by consumers
  - Functionality and sophistication varies widely among implementations
    - Some implementations use LLMs and generative AI to mimic human interactions
    - Other implementations are simple, rules-based engines with defined interactions
  - June 2023 CFPB research report identifies several potential issues
    - Difficulty in understanding consumers' requests and providing accurate, reliable and sufficient information in response; failing to resolve inquiries and limiting consumer access to human intervention
    - Report noted that inaccurate responses or failure to recognize consumers' invocation of rights under federal consumer financial laws risks noncompliance by financial institutions
  - May be impacted by proposed state laws (e.g., UT) on generative AI disclosures
  - Also need to assess legal issues if recording interactions

AI in Lending Decisions

- Creditworthiness and lending decisions
  - AI/ML-based models can incorporate a broad array of data to potentially outperform more traditional credit models
  - Potential for accuracy issues and bias implicates fair lending concerns
    - Fair lending considerations are covered in another session
  - May 2022 CFPB circular and September 2023 guidance confirm that ECOA’s adverse action notice requirements apply when using AI models
    - Complexity or opacity of the underlying model will not excuse noncompliance
    - Adverse action notices must provide accurate and specific reasons for denials
  - Explainability of model outputs is key

AI Code Generators – Open Source Issues

Tainting of proprietary code – if code output from AI generator is under a “restrictive” OS license, the software you are developing must be licensed under OS license and you must make the code available for free

Often results in loss of investment in the software

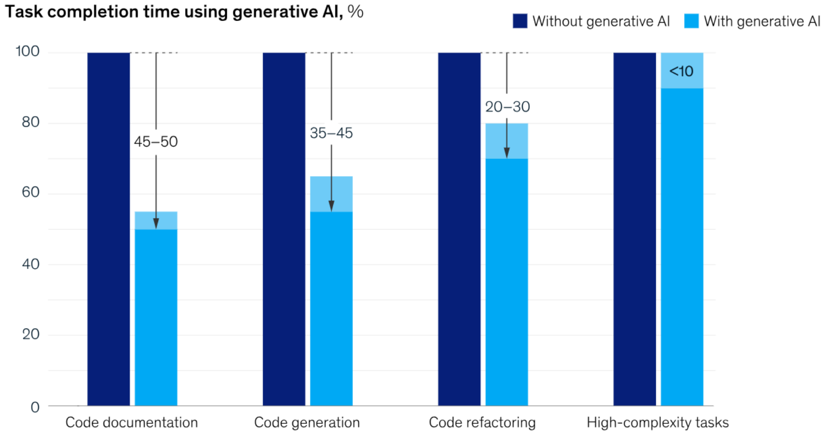
- If Company does not have an OS policy, they need one

  Open Source Software Policies – Why You Need Them And What They Should Include

- If Company does, it needs to update for GenAI

  Solving Open Source Problems With AI Code Generators – Legal issues and Solutions

Generative AI can increase developer speed, but less so for complex tasks.



McKinsey & Company

Overview of Regulatory and Legislative Framework

Equity and Civil Rights Issues in the White House Executive Order on AI

[AI Equity and Civil Rights Issues]

White House AI Executive Order 10/30/23

- Protection of Consumers, Patients, Students and Workers
- Safety and Testing Prior to Launch
- Content Authentication and Privacy
- National Security – Cyber/NS memo
- Responsible AI Use by US Government
- Equity and Civil Rights
- Promote AI Innovation and Competition at Home and Leadership Abroad

The Effects of the Executive Order Will be Far Reaching

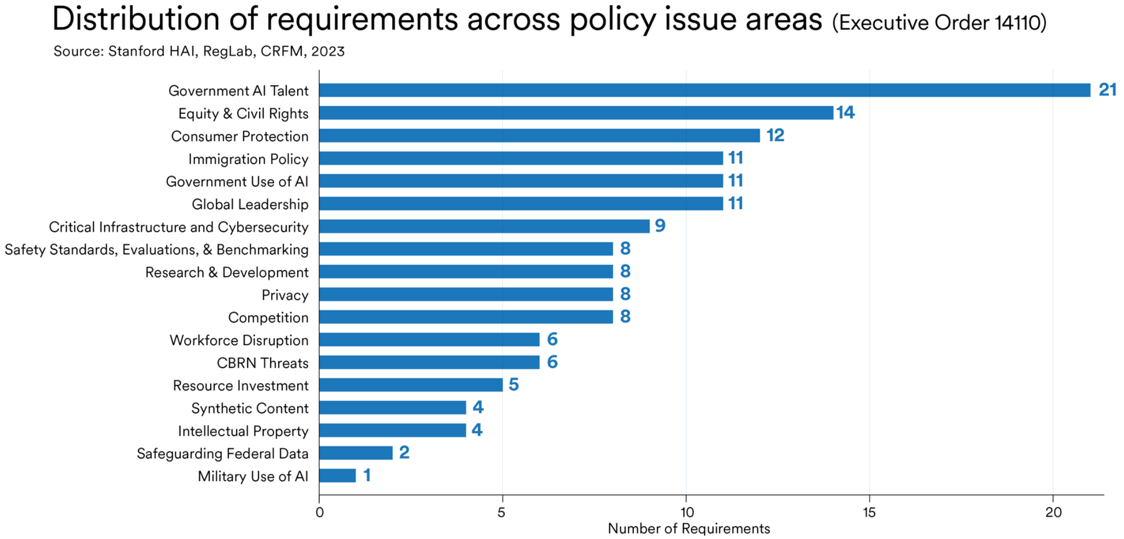
White House Executive Order Ramps Up US Regulation of and Policy Toward AI

- Directs many agencies to take specific actions, including to protect consumers, patients, students and workers and industries; mandates interagency cooperation – **will lead to more regulation and enforcement**
- Calls on Congress to implement **federal privacy legislation**

  American Privacy Rights Act April 7, 2024
- Increase focus on "BAD" AI (**b**iased **a**nd **d**iscriminatory AI) to promote equity and civil rights

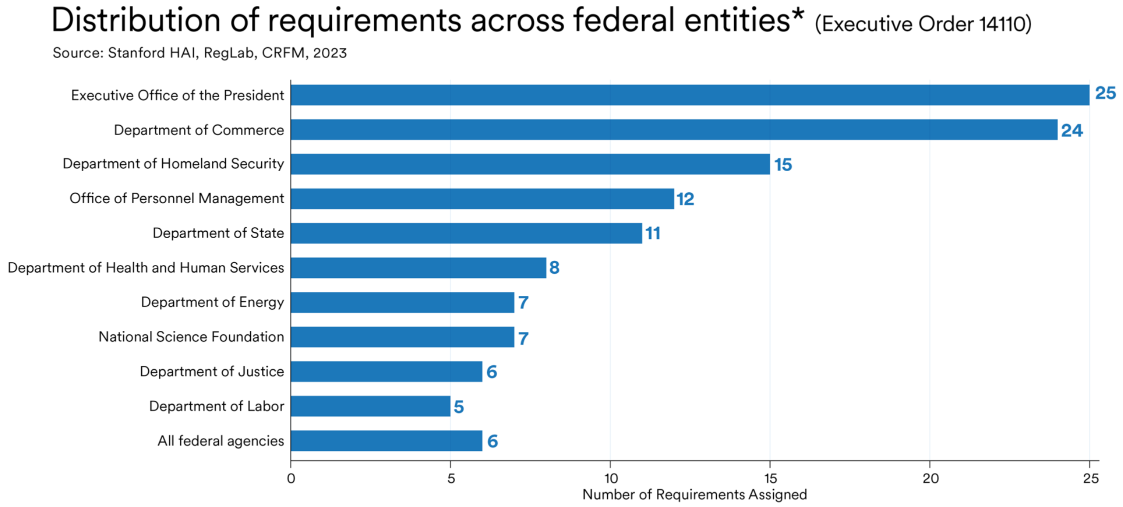
  Equity and Civil Rights Issues in the White House Executive Order on AI
- Create programs and provides resources to enhance US leadership in innovation
- Promote US leadership in coordinating **global regulatory efforts**
- Requires steps to protect US infrastructure from foreign bad actors' use of AI

Tracking The AI Executive Order



Distribution of requirements across policy issue areas (Executive Order 14110)

Source: Stanford HAI, RegLab, CRFM, 2023



Distribution of requirements across federal entities* (Executive Order 14110)

Source: Stanford HAI, RegLab, CRFM, 2023

* Note: Counts reflect only unambiguously assigned requirements—stakeholders may be required to fulfill additional requirements. We only show entities specifically named as responsible for five or more requirements. Requirements that task a Department Secretary "through" the head of sub-agencies fall within the count for the parent-level Department. We also show requirements assigned to all federal agencies as a separate category.

Stanford University

HAI Stanford University Human-Centered Artificial Intelligence

Stanford tracker analyzes the 150 requirements of the White House Executive Order on AI

FTC Guidance on AI

FTC and AI

The FTC has been actively involved in regulating AI and its applications

- Has issued warnings, guidance, policy statements, and engaged in enforcement actions related to AI and potential harms to consumers and competition
- Key Topics
  - Privacy, biometric privacy and security – Rite Aid
  - Accuracy
  - Fairness and non-discrimination
  - Transparency and Explainability
  - Safety and reliability
  - Advertising

FTC and AI

February 2023 – the FTC Division of Advertising Practices updated guidance on the use of AI to caution on:

- Making exaggerated or unsubstantiated claims about their AI products or services
- Promising that your AI product does something better than a non-AI product
- Being aware of the risks of your AI products

April 2023 – FTC guidance on enforcement efforts against AI systems that result in illegal discrimination, such as in credit, employment, housing, or health care

FTC and AI

May 2023 – FTC policy statement on biometric information; FTC will challenge the misuse of biometric information (facial recognition, fingerprints, iris scans, or voiceprints) by AI

May 2023 – the FTC/DOJ charged Amazon with violating COPPA – retained children's **voice recordings** indefinitely and allowed any employee or contractor to access them, even after parents deleted them from their accounts

EU AI Act Overview and Applicability

EU AI Act regarding training data – sample provisions:

- Providers must have "policy to comply with Union copyright law" (Recitals 104 and 107 and Article 53(1)(c) and (d)):
- Use "state of the art technology" to comply with opt outs
- Disclose use of content used for training "… to facilitate ... copyright holders … to enforce their rights" (Recital 107)
- "Any provider ... should comply with this obligation, regardless of the jurisdiction in which the copyright-relevant acts underpinning the training of those general-purpose AI models take place. ... no provider should be able to gain a competitive advantage in the Union market by applying lower copyright standards than those provided in the Union.“ (Recital 106)

Sample Proposed Legislation

- **Generative AI Copyright Disclosure Act** – would require filing in USCO list of all copyrighted works used to train AI models 30 days before public use; applies retroactively to existing AI models disclosure required 30 days after law's effective date (4-9-24)
- **American Privacy Rights Act of 2024** – would create individual federal rights to personal data privacy (4-7-24)
- **Protecting Consumers from Deceptive AI Act** – NIST to develop standards for identifying/labeling AI content; disclosures (3-21-24)
- **Federal AI Governance and Transparency Act** – would establish Federal AI system governance requirements for agencies (3-5-24)
- **AI Consent Act** – requires online platforms to get consumer's express consent to use personal data to train AI models (3-19-24)

Sample Proposed Legislation

- **Protect Victims of Digital Exploitation and Manipulation Act of 2024** – prohibit the production or distribution of non-consensual, deepfake pornography (3-6-24)
- **Restrictions on Utilizing Realistic Electronic Artificial Language ("R U REAL") Act** – requires telemarketers to disclose if they are using artificial intelligence to mimic a human at the beginning of any call or text message (2-1-24)
- **No Artificial Intelligence Fake Replicas And Unauthorized Duplications (No AI FRAUD)** – federal framework to protect Americans' individual right to their likeness and voice against AI-generated fakes and forgeries (1-10-24)

Dozens of others I am following

State Regulations of AI

- Since 2019, 17 states have enacted 29 bills (as of 12/23) focused on regulating the design, development and use of artificial intelligence
- Sample concerns:
  - Uses of AI (employees, consumers, students, patients)
  - Data privacy and accountability
  - Synthetic content – deep fakes/marking
  - Establishing regulatory and compliance frameworks for Responsible AI systems

Corporate Policies for Managing AI

Some Key Takeaways

- AI governance is critical – need AI governance committee
- Ongoing education is a must
- Develop and implement “role-based” policies including risk management frameworks and AI impact assessments
- Approved only specific tools, versions – specify any conditions of use

Key Steps to Manage AI

What Companies Need to Do to Manage AI

Education

- AI litigation
- Legislation
- New regulations, enforcement actions and guidance
- White House Executive Order and EU AI Act
- State Laws

Develop “Role” Based Policies

- Data Acquisition and Use for AI
- Training AI models (fine tuning and RAGs)
- Developing AI Tools
- Employee use of GenAI
- Use of AI code generators
- Vendors use of AI for company

AI Policies

ONE SIZE
DOES NOT FIT ALL

Checklist for AI Policies

Customize checklists for what to include in a company AI policy based on questionnaire to identify company's use of AI and other factors – *Sample Topics*

- Company Role(s) with AI
  - Data used, training performed, tools developed, employee use, use of 3rd party-developed AI content
- Types of content generated and how used
- Types of tools used by/for company and purpose (e.g., employment decisions, consumer finance, other regulated uses)
- Use of AI code generators by Developers?
- Geographical use
- Other factors

Policies on Training AI

- Need to do a data mapping for what is used to train AI and ensure the right to use the data
- Need to ensure compliance with any restrictions/obligations in any licenses
- Responsible AI – fair, transparent, explainable … test for bias, discrimination
- Truthful advertising
- Many other components of the policy depending on the use cases

Approving Specific Tools – Vetting Vendor

Vendor Diligence

Laws impose obligations on deployers of AI tools – need to understand and conduct legal diligence on your vendors

- AI Tools/AI in Tools
- Individual/enterprise version
- Are inputs and outputs confidential
- License terms?
- Infringement Indemnity? Conditions?
- Responsible AI Development
- Regulatory Compliance

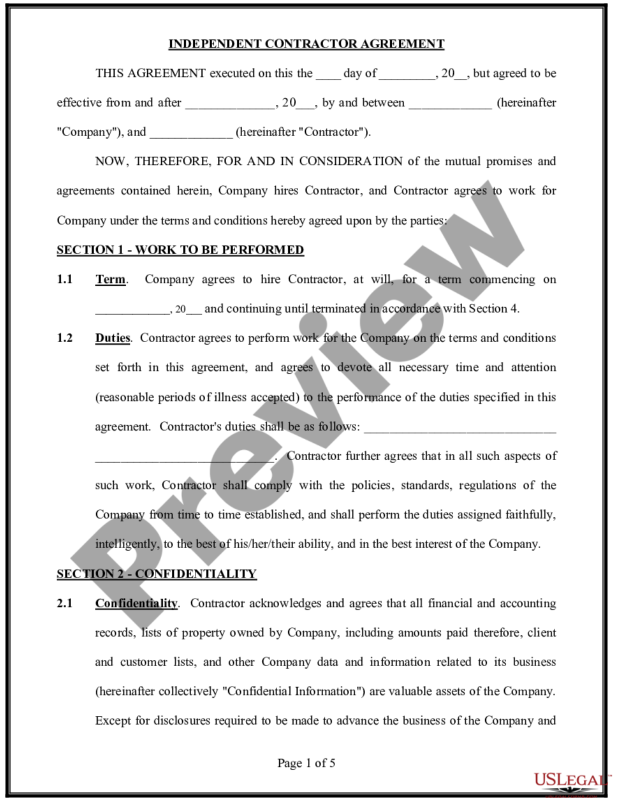
Vendor Vetting and Vendor Management

- Does Vendor have written AI development policy? Ask for copy
- Clear identification of data sources and processing methods?
- Consider whether the vendor has responsible AI use practices and/or policies – follows NIST AI Risk Management Framework and other guidance?
- Evaluation of training data and model design, bias testing methods, bias remediation
- Cybersecurity and confidentiality

Contractor Agreements

Need to consider issues in light of contractor agreements (where content generated for client by third party)

- Prohibit use of GAI?
- Require disclosure?
- Require documentation of use?
- Reps and warranties regarding compliance
- Other issues



INDEPENDENT CONTRACTOR AGREEMENT

THIS AGREEMENT executed on this the ____ day of _________, 20__, but agreed to be effective from and after ______________, 20___, by and between _____________ (hereinafter "Company"), and _____________ (hereinafter "Contractor").

NOW, THEREFORE, FOR AND IN CONSIDERATION of the mutual promises and agreements contained herein, Company hires Contractor, and Contractor agrees to work for Company under the terms and conditions hereby agreed upon by the parties:

SECTION 1 - WORK TO BE PERFORMED

1.1 **Term**. Company agrees to hire Contractor, at will, for a term commencing on ___________, 20__ and continuing until terminated in accordance with Section 4.

1.2 **Duties**. Contractor agrees to perform work for the Company on the terms and conditions set forth in this agreement, and agrees to devote all necessary time and attention (reasonable periods of illness accepted) to the performance of the duties specified in this agreement. Contractor's duties shall be as follows: _______________________________ _____________________________. Contractor further agrees that in all such aspects of such work, Contractor shall comply with the policies, standards, regulations of the Company from time to time established, and shall perform the duties assigned faithfully, intelligently, to the best of his/her/their ability, and in the best interest of the Company.

SECTION 2 - CONFIDENTIALITY

2.1 **Confidentiality**. Contractor acknowledges and agrees that all financial and accounting records, lists of property owned by Company, including amounts paid therefore, client and customer lists, and other Company data and information related to its business (hereinafter collectively "Confidential Information") are valuable assets of the Company. Except for disclosures required to be made to advance the business of the Company and

Page 1 of 5