MARTIN GOLDEN LYONS
— WATTS MORGAN —

Helping Clients Unlock Their Compliance and Technology Initiatives
Heath Morgan, Partner - hmorgan@mgl.law

Creating your AI Policy, AI Committee, and AI Risk Assessment

Creating an AI Policy

1. **Identify Applicable Uses**

- Identify How You Want to Use AI Internally with Your Company and Your Vendors:
    i. Generative AI
    ii. Robotic Process Automation
    iii. Conversational AI
    iv. Machine Learning & Data Collection

    - Identify How Your Employees and Vendors Would Use AI Technology:
        i. How do you imagine your employees using AI?
            - Approval System
            - Access AI Technology
            - Training on AI & Responsible Uses, Prohibiting the Rest
        ii. How do you imagine your employees and vendors using AI?
            - Approval System
            - Approved Access to Data
            - Approved Uses
            - Oversight Process
                - Transparency
                - Right to Delete Data
                - Hallucination Testing

    - Identified Forced Vendor Uses
        i. Identify Software Products that Take Your Data and Train AI:
            - Microsoft Office Co-Pilot
            - Google Docs/Sheets
            - Zoom
            - Adobe
            - Salesforce
            - Apple IOS 18 & Open AI Partnership
        ii. Identify How You Want to Handle Software That Trains AI on Data
            - Prohibit Use
            - Employee Training on Scope of Use
            - Request Confidentiality Agreements from Vendor

2. **Find "Safe" Technology and Uses to Adopt that Avoids Future State & Federal Regulations**
   - Regulatory Trends
     i. CFPB, FTC, and Copyright law have all published AI documents
     ii. 17 States with AI legislation in 2024
     iii. EU AI Act
     iv. CPFB & FTC Dark Pattern Enforcement & Publications
     v. State Data Privacy Laws

   - Key Themes
     i. Protection of Consumer Data
     ii. Transparency of Uses
     iii. Be Mindful of Technology Decisions that Face Consumers
     iv. Consumer Harm

3. **Identify Consumer Uses – How will consumers use this technology in the future of your company?**
   - Consumer Chat Bots
     i. Resolution Bots
     ii. Baiting Bots
   - Debt Settlement Bots
   - Virus Bots
     i. Hackers
     ii. Spam of Systems

4. **Incorporate Data Privacy & Oversight**
   - Protection of Consumer Data
   - Protection of Internal Data
   - Protection of Confidential & Proprietary information
     i. Offensively with Internal Use & Vendor Use
     ii. Defensively with Protections Against Data Scraping
   - Copyright Ownership Issues
   - Other Data Security Considerations:
     i. Neuro Data and other new Data created outside of scope of current privacy laws
     ii. Authentic Data vs. Synthetic Data
     iii. Local Data v. Cloud Data
     iv. What Country is Data located in & What are their AI laws?

Heath Morgan, Partner - hmorgan@mgl.law

Create an AI Committee

1. **Establish Committee Members**
   a. Employees/Advisors with technology background
   b. Employees/Advisors with future forward mindset
   c. Outside Experts & Advisors

2. **Establish Which Technology to Engage and Prohibit**
   a. If you don't have this in policy right now, employees & vendors could be using this without your knowledge
   b. How to interact with consumer bots
   c. Risk Assessment for any new Technology
   d. Categorize AI Technology

3. **Recurring Meetings**
   a. Keep up with technology changes
   b. Meet on AI developments
      v. Internal AI integration
      vi. External Vendor Updates

Conduct a Risk Assessment on AI Technology

1. **Categorize the type of Technology**

- What is the use of the Technology? What are its limitations?
  - If deployed, will it harm people's health, safety, fundamental rights, or environment?
  - If deployed, could it reflect bias against any consumer population?
  - If deployed, could it cause potential fraud against consumers?
  - If deployed, are there any security risks of protected consumer data?
  - Is the technology free or enterprise based?
  - If free, does the technology utilize any dark patterns or surveillance capitalism elements?
  - Does the technology have a contract with confidentiality protections?
  - Does the technology have any self coding elements to it?
  - Will the technology be deployed in a way that is transparent to the consumer?

- Internal or External Use
  - Is the technology consumer facing?
  - Will the technology be used for "back end" work or employee based?
  - What level of human oversight is involved in the technology?
  - Are there any ethical considerations with its use?

- Attorney usage may have additional ethical considerations including:
  - Rule 1.1 Competence
  - Rule 1.6 Preservation of client confidentiality
  - Rule 3.3 Candor to tribunal
  - Rule 1.4 Communication of use to clients
  - Rule 1.3 Diligence - Misunderstanding technology is not a defense for misusing technology

- What Type of Technology is Used?
  - Generative AI
    - Open Sourced v. Third Party Public v. Internal Enterprise
    - Outputs: Ability for Hallucinations v. Limited Outputs or "I don't know"
    - Internal Use v. Consumer Facing
  - RPA/Automation
    - Rules based Bot v. AI Based Bot
    - Attended Bot v. Unattended Bot
    - Ability to Self Code
  - Conversational AI
    - Use: Inbound v. Outbound
    - Phone Calls v. Webchat
    - Outbound Regulations
      - TCPA
      - FCC Rule on Announcement of AI
      - State Consent for Call Recordings
    - Source of Outputs
      - Rules Based Scripts v. AI Based Black Box Algorithms
      - Hallucinations v. "I don't know"
    - Functionality of Output
      - Ability to Solve Complex Problems?
      - Ability to access Human during call?
      - Ability to Verify Correct Consumer & Account
    - Any other technical limitations or security risks?
  - Machine Learning/Data Collection
    - Data Input:
      - What type of Data is being Used?
      - What data is being used for input?
      - PHI/PII or other protected data?
      - Proprietary or Confidential Information?
      - Public or Synthetic Data?

        - Does Data Fall Outside Existing Legal Protections?
            - Location Data
            - Biometric Data
            - Behavioral Data
            - Neuro Data
        - Is Data Reliable or Accurate?

    - Data Output:
        - PHI/PII?
        - Proprietary or Confidential Information?
        - Is output public or private?
        - Is the data reliable?
        - Is the data accurate?

- **ROI Analysis**
    - What are the benefits? What problem are you trying to solve?
        - Staffing
        - Efficiencies
        - Consumer Preference
    - What are the costs?
    - Are there any benefits to the consumer?
    - Are there any benefits to employee efficiency?
    - Are there any benefits to accuracy of consumer experience?

- **Compliance Assessment**
    - Is this technology compliant with all current state and federal laws?
    - Is the technology compliant with CFPB & FTC guidance on uses?
    - Are there any other areas of law that should be considered like, GLBA, the FTC Safeguards Rule, HIPPA, or any state laws?
    - Are there potential that this technology could be regulated in the future? If so, how?
    - Does the technology incorporate any legal but surveillance capitalism elements?
    - Does the technology incorporate any dark patterns?
    - Is the technology transparent and able to be explained?

Helping Clients Unlock Their Compliance and Technology Initiatives
Heath Morgan, Partner - hmorgan@mgl.law

Sample Risk Assessment Use Case: ChatGPT

Categorize the type of Technology	Public Facing LLM
What is the use of the Technology? What are its limitations?	Uses: First Draft generation of Compliance Policies & Procedures & Training Materials including questions & presentations Limitations: Hallucinates, is wrong, and not best used for research
If deployed, will it harm people's health, safety, fundamental rights, or environment?	Depends on prompts & output.
If deployed, could it reflect bias against any consumer population?	Depends on prompts & output.
If deployed, could it cause potential fraud against consumers?	Depends on prompts & output. Disclosure of consumer information in prompts could be third party disclosure that results in potential fraud.
If deployed, are there any security risks of protected consumer data?	Depends on prompts & output. Disclosure of consumer information in prompts could be third party disclosure that results in potential fraud.
Is the technology free or enterprise based?	Free.
If free, does the technology utilize any dark patterns or surveillance capitalism elements?	Yes, ChatGPT just launched a web crawler bot that will follow users to other sites to mine data. This could be detrimental to consumers if the sites followed contain consumer information. i.e. client portals, vendor collection software systems. Additional safeguards have been implemented in the Company AI policy to 1) prohibit use of web browser after use of ChatGPT and 2) to only use ChatGPT on safer web browser engines like Duck Duck Go.
Does the technology have a contract with confidentiality protections?	No.
Does the technology have any self coding elements to it?	Not at this time. ChatGPT 3.5 and ChatGPT 4 do not.
Will the technology be deployed in a way that is transparent to the consumer?	No, but prompts will not be used for consumer facing tasks.
Internal or External Use	Internal Only
Is the technology consumer facing?	Potentially, but company AI policy will prohibit prompts from being used for consumer facing tasks.
Will the technology be used for internal "back end" work or employee based?	Yes.
What level of human oversight is involved in the technology?	Employees are responsible for initial prompts with a log that records and stores prompts.

Are there any ethical considerations with its use?	Potentially. The Company AI policy prohibits the use of ChatGPT for unauthorized prompts, especially those that may have ethical concerns. Additionally, there may be additional ethical considerations for attorneys using ChatGPT
What Type of Technology is Used?	Public Facing Generative AI, capable of hallucinations and wrong output
What type of Data is being Used?	The Company's AI policy prevents the use of any PHI, PII, and Confidential and Proprietary Information
What data is output?	Public information, which should not include PHI, PII, proprietary or confidential information
Is the data reliable?	The data output comes from black box algorithms and is not reliable as a final product. It can be used as first draft generation only.
Is the data accurate?	No, and it should not be used for research or search based outputs.
What are the costs?	Free or $20 a month for GPT 4; GPT Teams cost more
Are there any benefits to the consumer?	Yes the Company use of ChatGPT to improve efficiencies, compliance, and training will benefit the consumer.
Is this technology compliant with all current state and federal laws?	Depends on prompts & output. The Company AI policy outlines the usage that will be compliant with all state and federal laws.
Is the technology compliant with CFPB & FTC guidance on uses?	There is no current guidance with ChatGPT usage from the CFPB or FTC. The uses outlined in the Company AI policy will be compliant with any guidance.
Are there any other areas of law that should be considered like, GLBA, the FTC Safeguards Rule, HIPPA, or any state laws?	Yes, that is why the Company AI policy prohibits the usage of PHI and PII in prompts. Additionally, because no contract exists between the Company and ChatGPT, there is no vendor oversight of ChatGPT which should be factored into the FTC Safeguards risk assessment.
Are there potential that this technology could be regulated in the future? If so, how?	Yes. The CFPB could require transparency with all inputs and outputs of ChatGPT. This is why the Company AI policy requires employees to log and record their use of all prompts and outputs to ensure compliance with the AI policy.
Does the technology incorporate any legal but surveillance capitalism elements?	Yes. Chat GPT has launched a web crawler bot to monitor internet usage after using ChatGPT. The Company AI policy has been updated to include safeguards from this development including having all sites within its control, internal sites, vendor sites, to block the GPT bot's access to their sites.
Does the technology incorporate any dark patterns?	None known at this time, but it is still unknown how ChatGPT generates the output and all of the sources it uses.
Is the technology transparent and able to be explained?	The Company AI policy outlines authorized usage in a transparent way that can be explained to potential regulators.