Artificial Intelligence, Real Risk:
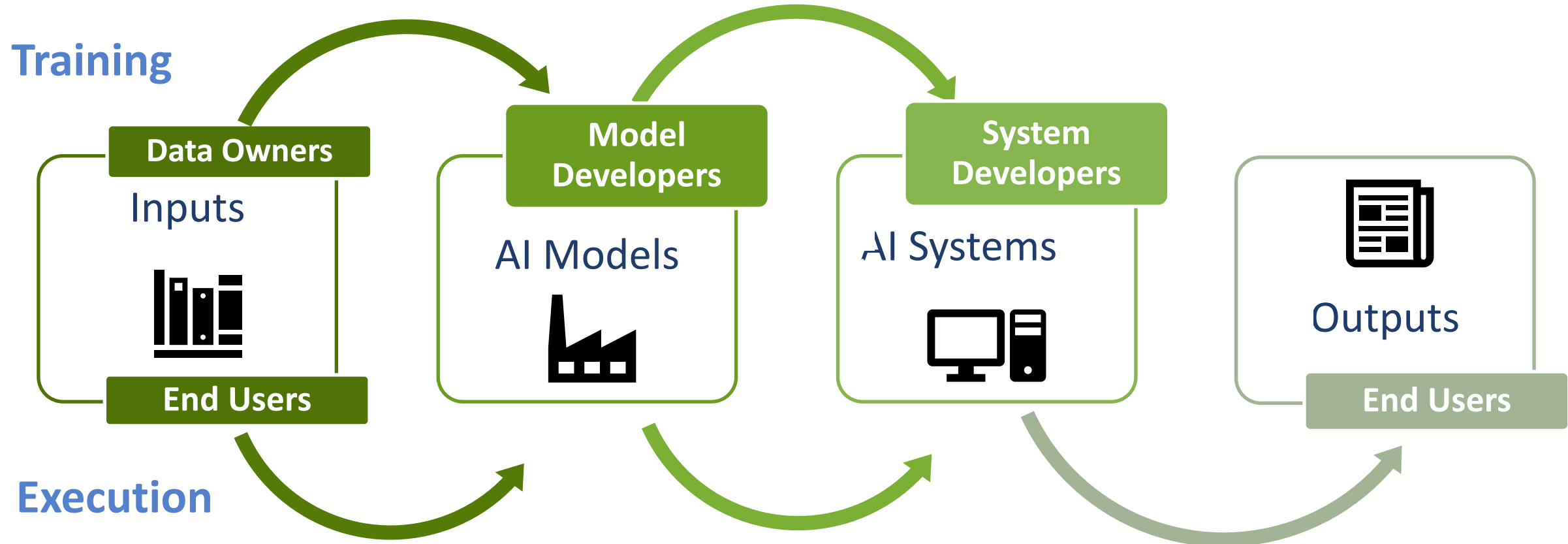
Don't Let the Robots Take Down Your School

October 2, 2025

AI Process at a Glance

Training

Execution

Data Owners

Inputs

End Users

Model Developers

AI Models

System Developers

AI Systems

Outputs

End Users

DuaneMorris®

AI Uses in Education

- Creating curriculum, lesson plans, tests, etc.
- Improving outcomes
  - Personalized learning platforms
  - Intelligent Tutoring
  - AI based gamification
  - Analyzing student data
- Increasing inclusiveness (e.g. speech recognition software)
- Marketing content (e.g. SEO optimized copy, images, marketing copy)
- Customer support (e.g. chatbots)
- AI meeting assistants
- Artificial Voice Calling

Regulatory and Legal Environment

- AI laws in the U.S. – States
  - ➢ No comprehensive Federal law on AI.
    - ▪ Increasing Federal regulatory agency enforcement actions and guidance.
      - » Prohibiting discriminatory, deceptive and unfair business activity.
    - ▪ NIST voluntary risk framework.
  - ➢ State law is predominantly issue driven, seeking to regulate discriminatory uses of AI and protect consumers' data relating to:
    - ▪ Discrimination and bias
    - ▪ Election deep fakes
  - ➢ Privacy laws address automated decision making and data minimization

Applicable California AI Laws

18 New Laws Effective Jan 1, 2025

AB 2905 requires telemarketing calls that use AI-generated or significantly modified synthetic marketing to disclose that use. (Pub. Util. Code, § 2874.)

SB 942 starting January 1, 2026, AI developers will need to make free and accessible tools to detect whether specified content was generated by generative AI systems and offer visible markings on AI-generated content. (Bus. & Prof. Code, § 22757 et seq.)

Civil Rights Department Regs October 1, 2025 - prohibit employers from using ADS or selection criteria that discriminate against applicants or employees and requires preservation of ADS data

Other California Laws Applicable to AI Technology

- CA Constitutional Right to Privacy
- California Consumer Privacy Act (CCPA)
- California Invasion of Privacy Act (CIPA)
- California's Unruh Civil Rights Act
- California Fair Employment and Housing Act (FEHA)
- Unfair Competition Act (Bus. & Prof. Code, § 17000)
- False Advertising Law (Bus. & Prof. Code, § 17500)

Summary of Legal Risks

FERPA

How is AI Using Student Data?

- Need to control use of data

- Use limited to educational purpose

- Consent to use student data for model training

- Is it really deidentified?

California Consumer Privacy Act (CCPA)

- Mandatory Disclosures

- Managing Rights Requests

- Contractual Requirements

- High Risk Disclosures and Profiling – Risk Assessments

- Automated Decision Making

Automated Decision Making

- The process by which a decision is made without any human involvement
- Privacy Laws – transparency and right to opt out if used for
  - Admission or acceptance into academic or vocational programs;
  - Educational credentials (e.g., a degree, diploma, or certificate);
  - Suspension and expulsion
  - Hiring;
  - Allocation or assignment of work for employees;
  - Salary, incentive compensation such as a bonus, or another benefit
  - Promotion
  - Demotion, suspension, and termination from employment
- Bias risk

California Invasion of Privacy Act (CIPA)

- Unlawful wiretapping and recording
- California – 2 party consent
- Transcriptions and meeting assistants
- Class Action Trends
  - Pixels and web tracking technology
  - Chat bots
  - Session replay technology

Misrepresentation

- Hallucinations
- Inaccurate or dated material from training data limitations
- Biased training data
- Unsubstantiated claims
  - Salary, earnings, job demand, employment opportunities, qualifications, placement rates, etc.
  - Extent or nature of accreditation or approval

TCPA

- AI = artificial message

- Express written consent

- Transparency and opt-out requirements:

  - Identifying the company initiating the call or text at the beginning of the message

  - Providing a telephone number or address for the company

  - Including an automated, interactive opt-out mechanism (such as a key-press or voice command for calls, or a reply option for texts) that allows the recipient to easily opt out and add their number to the company's do-not-call list

Intellectual Property

- Loss of IP Protection

- Diligence Risks

- Infringing Output

Examples in Higher Education

What Our Clients Are Using

- Admissions
  - Balto
  - RingCentral
  - Meera
  - HALDA
- Education
  - NotebookLM by Google
  - Turnitin
  - Quilgo
  - Elsevier's AI tutor
- Misc.
  - CoPilot
  - ChatGPT
  - Airtable (simple software development) : It's perfect for developing simple software within a team and moving away from Excel spreadsheets.
  - Ramp: (expense tracking and reimbursement)

Chatbots

- Misinformation / Misrepresentation
- CIPA Litigation
- FERPA and unauthorized use of data by vendor
- States where admissions reps must be licensed
  - Admissions reps required to provide certain data

Transcription and Meeting Assistants

- Automated
- Discussion of personal data
- Inaccuracies
- Discoverability
- Privilege
- FERPA
- Consent and CIPA

ChatGPT

- Free:
  - Not confidential, can shared with others as output (FERPA)
  - Default uses data to train models
- Enterprise:
  - Confidential, not combined or made available to others
  - Not used to train models
- Hallucinations / Inaccurate / Dated (Misrepresentation)
- Loss of IP

Best Practices

Takeaways

Understand relevant regulatory environment and risks of AI

– Privacy and AI laws are rapidly changing

– California is very active in passing new AI legislation

Establish AI committee(s) to:

– consider internal and external use cases

– establish principles for using AI aligned with business values and interests

– identify mature tools with appropriate protections

– vet new technologies

– approve employee requests

– monitor AI uses

Takeaways

Use enterprise version AI

- Prevent use of content for training
- Ownership and confidentiality generally more favorable
- Minimum opt out if using free versions

Check privacy policies and consents

- Is use of AI properly disclosed in privacy policy?
- Is consent needed to process personal information or record?

Human review / intervention is key

- No third party IP or Name, Image, Likeness
- No bias or discrimination in automated decision making

Takeaways

Don't assume the output of AI is current or accurate

– Verify the accuracy of AI Output and its sources

Determine what business tools rely on AI and address the risks

– Personal information or proprietary business information could be used to train the AI model

– Address privacy laws

Consider whether AI is being used by employees and/or service providers and mitigate risks

– Develop an AI policy with appropriate guardrails

– Check terms to understand ownership of output and models

– Document what content is created using AI vs human

– Include AI provisions in service provider contracts

Contractual Issues and Terms of Use

To address unlicensed use of Company data to train an AI model

- Enforce current contractual provisions (whether as website terms of use or in offline agreements)
  - ➤ E.g., license restrictions, obligation to prevent/report unauthorized use
- Revise relevant contracts to include express restrictions and audit rights
  - ➤ E.g., "Except as expressly permitted by this section, no other rights or licenses are granted or implied, including any right to use Company's data for other purposes, such as for training a machine learning or artificial intelligence model, without the express permission of the Company."
- Add disclaimers regarding use and trustworthiness of use of Company data by AI

Contractual Issues and Terms of Use

To address vendor use of AI to provide deliverables or services

- Include questions about the vendor's use of AI during the due diligence process
- Conduct an impact assessment of how any such vendor use of AI will affect the Company
- Include contractual provisions in vendor agreements (new or by amend.) that:
  - ➤ expressly address vendor use of AI (e.g., strict prohibition, limited permitted uses, ad hoc review and consent)
  - ➤ provide for warranties, indemnification, carve-outs from limitations of liability, and other risk-shifting provisions to clearly apportion risk with respect to the use of AI (*see, e.g.,* risk-shifting provisions re data security)
  - ➤ provide for audit rights ("trust, but verify")
  - ➤ contemplate insurance where neither party wants to bear the full risk

Contractual Issues and Terms of Use

Ownership

- Based on training data or input? Based on processing or output?
- License back for use of non-identifiable data, trends, learnings?

Representations/Warranties

- The use of AI will not: degrade standard for performance or service levels; produce inaccurate, biased or non-representative outputs; and take into consideration protected characteristics
- AI outputs will be subject to QA/human review
- Use of AI will comply with all applicable laws (e.g., privacy laws)

Contractual Issues and Terms of Use

Limit on Liability, Indemnity & Insurance

- Consider AI uses in risk-shifting provisions

- Scope and scale of exposure

- Carve-outs and exceptions

- Indemnity obligations for risks best controlled by each party

Ethics and Reputation

- Alignment with safe, responsible, non-biased AI use principles and pledges

Contract Considerations for ADM

- Prohibit use of ADM

- Provide safeguards for use of ADM

  - Human review or intervention

  - Obtaining Consent

  - Options to contest/appeal ADM

  - Limits on processing sensitive category data

- Terms for handling opt out requests

Questions?

Ed Cramp
619.744.2223
EMC@duanemorris.com

Michelle Donovan
619.744.2219
MHDonovan@duanemorris.com

Jessica High
619.744.2214
JHigh@duanemorris.com