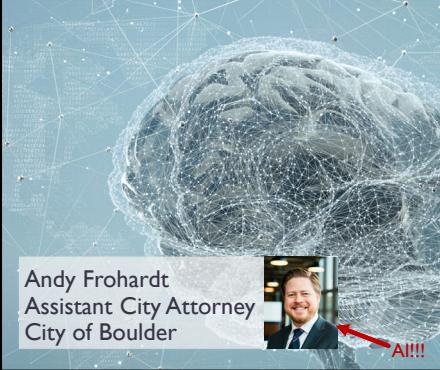




Cybersecurity,
Data Privacy, &
Artificial
Intelligence For
Muni Attorneys

Andy Frohardt
Assistant City Attorney
City of Boulder

AI!!!

1

BEFORE WE GET
STARTED

- Principal goal – raise baseline awareness of AI and its security, privacy, and other issues
- Collective expertise is critical! Please speak up!



2

WHAT IS AI?

3

AI DEFINED

15 USC 9401(3)

"Artificial Intelligence" means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to— (A) perceive real and virtual environments; (B) abstract such perceptions into models through analysis in an automated manner; and (C) use model inference to formulate options for information or action.

6-I-1701, C.R.S.

"Artificial Intelligence System" any machine-based system that, for any explicit or implicit objective, infers from the inputs the system receives how to generate outputs, including content, decisions, predictions, or recommendations, that can influence physical or virtual environments.

4

Generative AI vs.
Agentic AI vs. AI Agents



Generative AI

Generative AI generates new content such as text, images, and music based on training data



Agentic AI

Agentic AI performs tasks autonomously and can pursue goals by interacting with its environment



AI Agents

AI agents combine generative and agentic capabilities to accomplish complex objectives

Pratibha Kumari Jr., Chief Digital Officer, DataThick (via LinkedIn)

5

AI USAGE

Market Leaders in AI Tools and Platforms

AI Tool	Market Share (2025)	Primary Use Cases	Key Features
ChatGPT (OpenAI)	59.7%	Writing, analysis, coding	Conversational AI, multimodal capabilities
Microsoft Copilot	14.4%	Office integration, productivity	Microsoft 365 integration, enterprise features
Google Gemini	13.5%	Research, content creation	Google Workspace integration, search capabilities
Perplexity	6.2%	Research, fact-checking	Real-time search, citation features
Claude AI	3.2%	Long-form content, analysis	Large context window, safety focus

6

2

AI – WHY IT MATTERS

7

IN THE WORKPLACE

What shares of workers are most exposed to AI in their jobs?

% of U.S. workers employed in jobs that are the most exposed to AI in 2022

All workers	19%
Men	17
Women	21
White	20
Black	15
Hispanic	13
Asian	24
Amer. Indian or Pacific Islander	16
Other	18
Less than HS	3
HS grad	12
Some college	19
Bachelor's+	27

Note: Occupations are ranked by the relative importance of work activities with high exposure to AI. Those in the top 25% are the

8

Digital Education Council Global AI Student Survey 2024 | Section 1. AI Usage

86% of students already use AI in their studies

Percentage of students using AI in their studies

Question: How often do you use AI tools?

86%

of students claim to use AI in their studies

54%

of students use AI at least on a weekly basis

Frequency of students using AI in their studies

Question: How often do you use AI tools?

54%

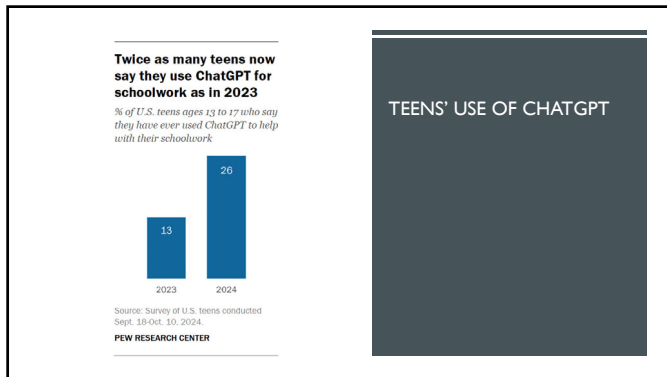
use daily or weekly

24%

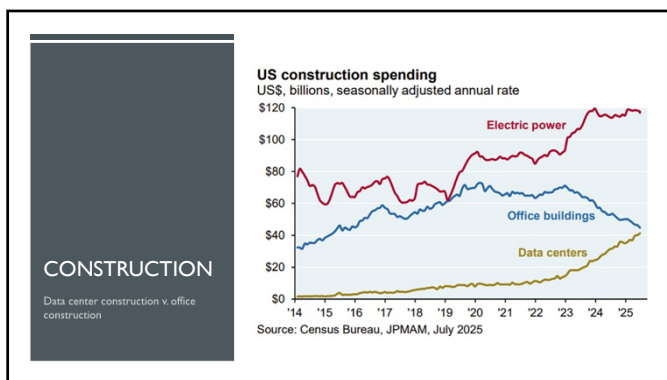
use AI daily

Source: Digital Education Council Global AI Student Survey, 2024

9



10



11

IS AI THE REAL DEAL?

- OpenAI CEO Sam Altman → \$100 million signing bonuses to AI engineers.

Matt Deitke
AI Researcher at MSL

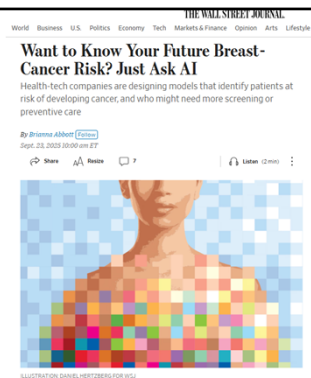
12

AI USE CASES

13

HEALTHCARE

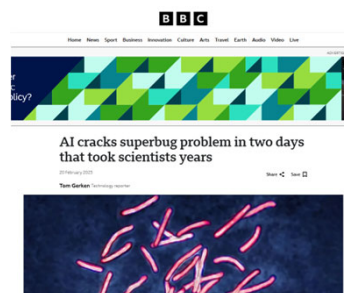
- Clarity



14

HEALTHCARE

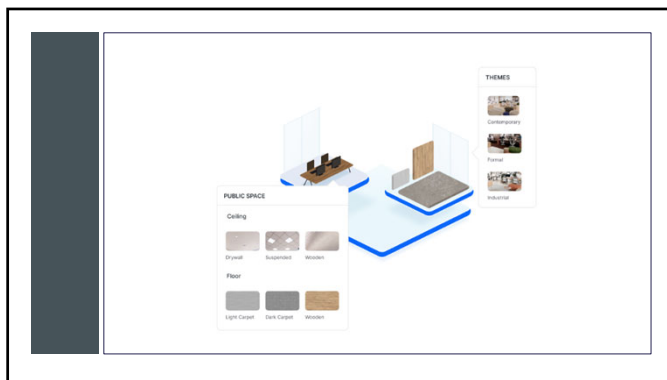
- Research



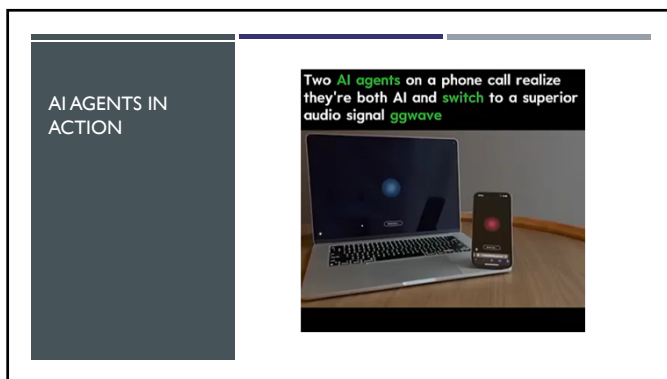
15



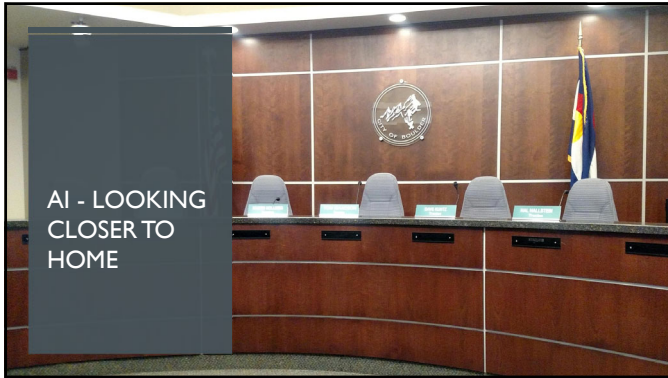
16



17



18



19

MUNICIPAL USES

- Axon - Prepared

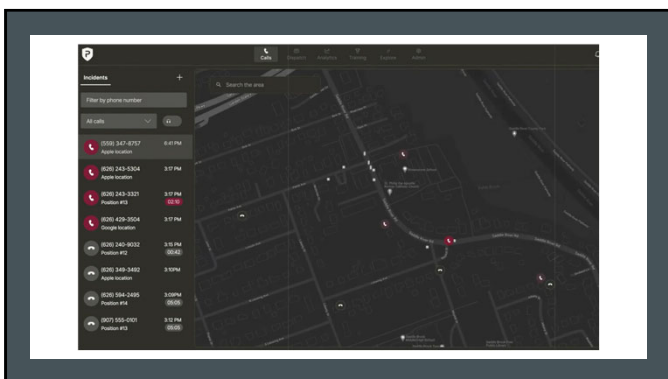
GOVTECH.DIG

Axon Says It Will Buy 911 AI Call Center Tech Firm Prepared

The deal reflects the growing use of artificial intelligence in the public safety space, and combines a hardware supplier with a young firm focused on artificial intelligence. Prepared has raised more than \$130 million.

September 23, 2023 • News Staff

20



21

MUNICIPAL USES

- Sewage Blockages

AI trial cuts sewage pollution, water firm says

7 days ago

KIN England South West environment and water correspondent



AI is being used to help identify changes in water levels in the network that could indicate if a blockage is developing or if

22

MUNICIPAL USES

- HR (Agentic AI)

IBM watsonx Agents

IBM used **IBM AskHR**, an AI agent, to streamline its employee experiences and free up HR professionals to focus on higher-value tasks.

40%
reduction in HR budget*

94%
of employee inquiries resolved with AskHR*

Over
55 point
improvement of HR Net Promotor Score (NPS)*

23



24

EXAMPLE – CONTRACT LANGUAGE

Prompt

You are an attorney for a municipality that is contracting for land surveyor services. Draft contract language that will hold a surveyor accountable for their survey services to a municipality. Incorporate any industry standards or professional requirements for surveyors, whether nationally or in the State of Colorado.

Draft Contract Language – Professional Surveying Services (Colorado Municipality)

1. Standard of Care
Surveyor represents and warrants that all services performed under this Agreement shall:

- (a) conform to the standards of practice of professional land surveying as defined by the *Colorado Revised Statutes Title 12, Article 120 (Professional Land Surveyors Act)*, and the rules promulgated by the Colorado State Board of Licensure for Architects, Professional Engineers, and Professional Land Surveyors;
- (b) comply with the *Colorado Minimum Standards for Land Surveying* (8 CCR 1505-8); and
- (c) meet or exceed the degree of skill and care ordinarily exercised by professional land surveyors practicing under similar circumstances in the State of Colorado.

2. Professional Responsibility and Licensure
Surveyor shall perform all services under the responsible charge of a Colorado-licensed Professional Land Surveyor ("PLS") whose license is current and in good standing. Surveyor shall maintain such licensure, and all necessary registrations, certifications, and permits, throughout the term of this Agreement.

3. Deliverables and Accuracy Requirements
Surveyor shall deliver survey maps, plats, legal descriptions, and associated documents that:

- (a) are complete, accurate, and suitable for the Municipality's intended use;
- (b) clearly identify the basis of bearings, datum, monuments, and control points in accordance with Colorado statutory and regulatory requirements;
- (c) comply with all applicable state and local recording requirements; and
- (d) be sealed, signed, and dated by the responsible PLS as required by Colorado law.

25

EXAMPLE – CONTRACT LANGUAGE

Prompt

You are an attorney for a municipality that is leasing an autonomous lawn mower. The lessor's autonomous lawn mower is found at the following website: [WEBSITE URL]. Analyze the website and create contract language that binds the lessor to the various promises it makes on its website.

B. Contract Clauses (drop-in language)

2. Safety Feature Warranty and Operational Safeguards
3. Training, Onboarding & Documentation — Success System

(a) Lessor shall provide, at Lessor's expense, the full Success System as described on the Manufacturer Website, which includes pre-delivery planning and implementation guidance, personalized onboarding with in-field training and operator certification, ready-made communication tools for staff and the public, and ready-made signage for worksites and vehicles. Training must be provided by qualified personnel and shall result in written certification that Lessee's named operators have completed the training and are competent to operate and supervise the Equipment. RC 1505-8

Purpose/note: locks in on-site training and certification promises. RC 1505-8

Purpose/note: binds the lessor to the numeric/functional specs and claims displayed on the site. RC 1505-8

26

EXAMPLE – SUMMARIZE RESEARCH REPORT

Prompt

Summarize this research report in 1,500 words or less.

Microsoft Research Report.pdf PDF

Below is a concise summary of the Microsoft Research report "Working with AI: Measuring the Applicability of Generative AI to Occupations" in under 1,500 words.

Purpose and Scope
This study investigates how generative AI—specifically Microsoft's Bing Copilot—affects different kinds of work. Rather than predicting theoretical impacts, the authors analyze **real-world usage data**: 200,000 anonymized U.S. conversations with Copilot over nine months in 2024. By mapping these conversations to the U.S. Department of Labor's O*NET database of work activities, the team measures where AI is already assisting or performing tasks and calculates an **AI applicability score** for every U.S. occupation.

Key Concepts

- **User Goal vs. AI Action:**
 - *User goal* is the task the human wants to accomplish.
 - *AI action* is the task the AI actually performs.
 - These differ often—for example, a user may want to "research a topic" while the AI "provides information."
- **Work Activities (IWAs):** O*NET defines 332 "Intermediate Work Activities" (IWAs) that describe tasks shared across occupations.
- **AI Applicability Score:** Combines (1) how often an IWA appears in conversations, (2) how successfully Copilot completes the task, and (3) the scope of Copilot's contribution. This weighted score estimates each occupation's potential exposure to generative AI.

Data and Methods
Data: Public

27

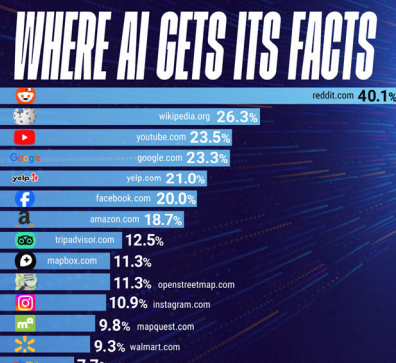
AI DANGERS

28

ACCURACY CONCERNS

- Source reliability?
- Hallucinations/confabulations?
- Current?

VisualCapitalist.com, Marcus Lu



29



"Use of AI without careful oversight of counsel would seriously undermine this court's ability to deliver justice," he said.

The guidelines state use of AI must not "directly mislead another participant in the litigation process as to the nature of any work understood or the content produced by that program".

30

Draft Contract Language – Professional Surveying Services (Colorado Municipality)

1. Standard of Care

Surveyor represents and warrants that all services performed under this Agreement shall:

- (a) conform to the standards of practice of professional land surveying as defined by the Colorado Revised Statutes Title 12, Article 120 (Professional Land Surveyors Act) and the rules promulgated by the Colorado State Board of Licensure for Architects, Professional Engineers, and Professional Land Surveyors;
- (b) comply with the Colorado Minimum Standards for Land Surveying (8 CCR 1505-8) and
- (c) meet or exceed the degree of skill and care ordinarily exercised by professional land surveyors practicing under similar circumstances in the State of Colorado.

2. Professional Responsibility and Licensure

Surveyor shall perform all services under the responsible charge of a Colorado-licensed Professional Land Surveyor ("PLS") whose license is current and in good standing. Surveyor shall maintain such licensure, and all necessary registrations, certifications, and permits, throughout the term of this Agreement.

3. Deliverables and Accuracy Requirements

Surveyor shall deliver survey maps, plats, legal descriptions, and associated documents that:

- (a) are complete, accurate, and suitable for the Municipality's intended use;
- (b) clearly identify the basis of bearings, datum, monuments, and control points in accordance with Colorado statutory and regulatory requirements;
- (c) comply with all applicable state and local recording requirements; and
- (d) be sealed, signed, and dated by the responsible PLS as required by Colorado law.

31

ALGORITHMIC BIAS



32

COLORADO ARTIFICIAL INTELLIGENCE ACT (CAIA)

SB24-205 (SB25B-004 delayed the effective date to June 30, 2026)

Seeks to avoid algorithmic discrimination by regulating "high-risk" AI.

Algorithmic Discrimination

- "[A]ny condition in which" the use of [AI] "results in an unlawful differential treatment or impact that disfavors an individual or group of individuals on the basis of their actual or perceived age, color, disability, ethnicity, genetic information, limited proficiency in the English language, national origin, race, religion, reproductive health, sex, veteran status, or other classification [protected under the law]."

33

COLORADO ARTIFICIAL INTELLIGENCE ACT (CAIA)

What is "**high-risk AI**"? → AI that is a "substantial factor" in making a "consequential decision." 6-1-170, C.R.S.

- "**Substantial factor**" –
 - A factor generated by an AI system that is used to assist in making, and is **capable of altering the outcome** of, a consequential decision.
- "**Consequential decision**" –
 - Has a material, legal or similarly significant effect;
 - On the provision or denial to any consumer of, or the cost or terms of: (A) Education; (B) Employment; (C) Financial or lending services; (D) Essential government services; (E) Healthcare service; (F) Housing, (G) Insurance, or (H) Legal services.

34

COLORADO ARTIFICIAL INTELLIGENCE ACT (CAIA)

If it is a regulated AI, then →

- **Risk Management Program** "to govern deployment of" high-risk AI with "regular, systematic review and updates."
- **Impact assessments** (annually and within 90 days of each "substantial and intentional modification" to the AI, that includes testing, monitoring, and risk analysis of the system.
- Must **notify consumers** of the use of AI:
 - (1) before the decision is made;
 - (2) via website statement that identifies the high-risk AI and how it is used;
 - (3) give consumer the right to opt-out of having their data processed by the AI; and
 - (4) give consumers who receive an adverse decision a statement about how AI was used and opportunity to appeal/correct their information.

Record-keeping obligations (for everything!)

35

COLORADO ARTIFICIAL INTELLIGENCE ACT (CAIA)

- **Algorithmic discrimination** →
 - Notice to Colorado AG "without unreasonable delay" and in no event later than 90 days after discovery.

36

COLORADO ARTIFICIAL INTELLIGENCE ACT (CAIA)

ENFORCEMENT

6-1-1706, C.R.S.:

- (1) Notwithstanding section 6-1-103, the attorney general has exclusive authority to enforce this part 17.
- (5) **Nothing in this part 17**, including the enforcement authority granted to the attorney general under this section, **preempts or otherwise affects any right, claim, remedy, presumption, or defense available at law or in equity.** A rebuttable presumption or affirmative defense established under this part 17 applies only to an enforcement action brought by the attorney general pursuant to this section and does not apply to any right, claim, remedy, presumption, or defense available at law or in equity.
- (6) This part 17 does not provide the basis for, and is not subject to, a private right of action for violations of this part 17 or any other law.

37

COLORADO ARTIFICIAL INTELLIGENCE ACT (CAIA)

FULL CIRCLE

Novel, often seldom-tested technology

Designed to think on its own

Trained on unknown (and potentially-biased!) data

Managed and controlled by a third party

Reasoning often not apparent

Regular impact assessments

May discover disparate treatment/impact

Notice to Colorado AG

38

CYBERSECURITY

- New cybersecurity risks!
- Connecting systems/crossing boundaries
- Autonomous authority?



39

PROTECTIONS FOR CONSUMER DATA PRIVACY

24-73-102, C.R.S.

Security Procedures

To prevent personal identifying information from unauthorized access, use, modification, disclosure or destruction, Governmental entities must **implement and maintain reasonable security procedures and practices** that are **appropriate to the nature of the data** and nature and size of the governmental entity.

40

HACKING RISKS

41

DATA PRIVACY

- Will personal information (or other forms of sensitive or protected data) be entered into the model?
- Who has access to data in the model?
 - Does the model train itself using the data entered?

42

PROTECTIONS FOR CONSUMER DATA PRIVACY

24-73-102 and 103, C.R.S.

Requires security of, and prohibits disclosure of, "Personal Information" and "Personally Identifying Information"

43

OTHER DATA PROTECTION LAWS

Law	Data Type
Criminal Justice Information Services (CJIS) Security Policy	Standards for sharing and security of criminal justice information
HIPAA	Covered entities' obligations with respect to "protected health information"
Gramm-Leach-Bliley Act	Protects financial records (potential application to local gov's very narrow; but vendors could be subject to this!)
COPPA (Children's Online Privacy Protection Act of 1998)	Disclosure and protection requirements for personal information of children under 13 (generally not applicable to government entities; but, again, vendors!)

44

Samsung Bans ChatGPT Among Employees After Sensitive Code Leak

By [Shantanu Basu](#), [Fortune Staff](#). [Shantanu Basu](#) is a New Delhi-based Fortune news... [Follow Author](#)

Published May 10, 2023, 11:11am EDT Updated May 10, 2023, 11:11am EDT

[Share](#) [Save](#) [Read in the Google](#)

This article is more than 2 years old.

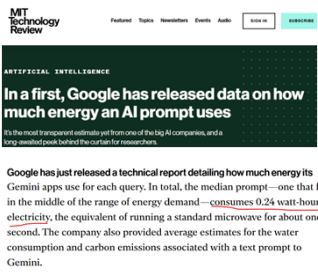
TIPLINE
Samsung Electronics has banned the use of ChatGPT and other AI-powered chatbots by its employees. According to reports, becoming the latest company to crack down on the widespread use of AI services amid concerns about sensitive internal information being leaked on such platforms.



DISCLOSURES

45

ENVIRONMENTAL CONCERNS



46

COPYRIGHT & TERMS OF USE CONCERNS

If AI is producing work product:

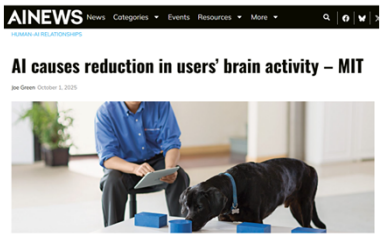
- Who the work product it?
- How can we be sure?
- Are there license restrictions or other terms of use restrictions?

47

TRANSPARENCY & OVERRELIANCE

- For staff and contractors:
 - Do we know if/when they are using AI?
 - If they are, what portion of the work is AI?
- For contractors:
 - How does the contract parse out liability?

Is everyone able to do the work?!

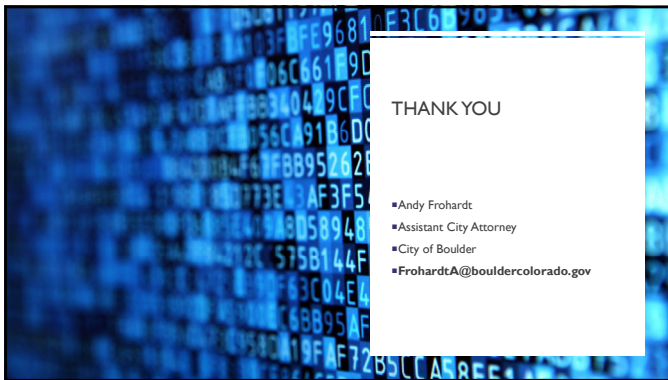


48



SKEPTICISM WARRANTED

49



50
