

Generative AI: Government Use & Records Implications

Ginger Armbruster | Chief Privacy Officer & Division Director

Sarah Carrier | Privacy & Responsible AI Program Manager



Agenda

- AI & Use Cases
- Thinking About the Issues
- Unique Challenges for Government
- Recent Guidance
- Practical Approaches to Generative AI Records



• Gen AI Legal Issues at a Glance

- Records issues
- Labor and HR
- Privacy
- Contract law
- Bias and discrimination
- Legal personhood issues
- Compliance risk
- Products liability
- Accuracy and reliability
- Intellectual property
- Security
- Copyright
- Vendors – 3rd party mgmt
- Data integrity
- 1st Amendment issues
- Procurement
- Unfair and deceptive acts
- Fraud

Credited with thanks to Kathryn Ruckle, Chief Privacy Officer, WaTech

NASCIO 2024 ANNUAL



What is AI?

AI

When machines simulate human intelligence processes or behavioral patterns

Generative AI

A class of AI systems capable of generating content such as text, images, video, or audio based on a large set of input/training data

Leverages Deep Learning techniques inspired by our brain's neural networks (LLMs)



AI Uses

- **Traffic management:** Classification and automation
- **Public Safety:** Evaluate non-emergency response calls and recommend dispatch resources
- **Customer Service:** Improve chatbot intent identification; summarize conversations; answer customer questions; direct customers to resources, soften tone or professionalize text
- **Personal Assistant:** Manage schedules; summarize emails; compose emails (and chains), replies and summaries; draft common documents; translation services
- **Software programming:** Write code from prose; convert code from one programming language to another; correct erroneous code; explain code
- **Risk Mitigation:** analysis and better visualization of data; pattern recognition, potential risks
- **Sustainability:** “Precision agriculture”; grid management; optimizing building design & controls



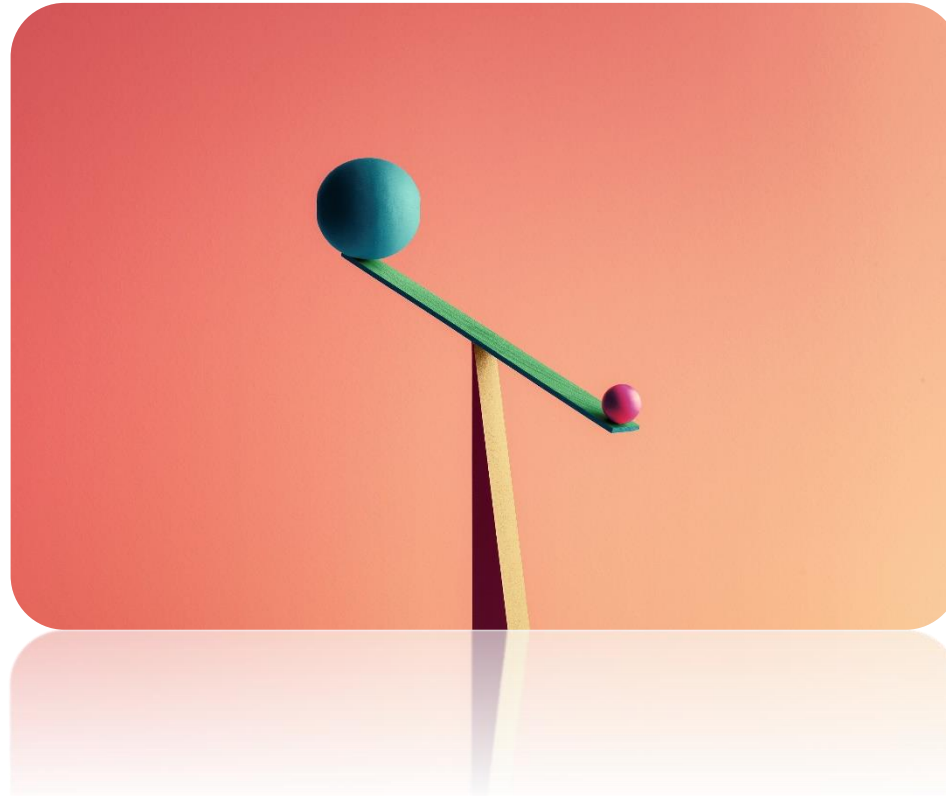
Potential



Efficiency &
Utility



Innovation



Ethics



Compliance



Privacy & Security

Why does it Matter?

U.S. NEWS

NYC's AI chatbot was caught telling businesses to break the law. The city isn't taking it down



Workforce impacts



Policy decisions impact constituents



PDR Complexity & AI Hype

What Are Some of the Issues?

- Legal | Regulatory

- Copyright/IP
- Records Retention & Production

- Security | Privacy | Data

- New unanticipated risks
- Lack of insight into training data, data flows & processing activities (including 3rd parties)
- Data access & permissions gaps

- Policy | Governance

- Policy Gaps
- Ethics & Bias
- Strong Governance Required



Lack of Insight



- ❓ Who owns the data?
- ❓ What types of data/records are being created/generated?
- ❓ Where is the data stored & how long it is stored/retained there?
- ❓ Can the data be destroyed, by whom, & who determines destruction cadence?
- ❓ Who all 'uses', accesses, or processes the data along the way?
- ❓ What are those third-party systems doing with the data, and where in the data flow are they doing it?
- ❓ How is data made accessible? Does the system integrate with existing search tooling? How might we retrieve records or data?

Recent WA Guidance

Are prompts and outputs
from Gen. AI use a record?

YES!

.....

But aren't they transitory
records?

Maybe!

Recent WA Guidance

Content	What is the interaction about?
Function	Why did it take place and for what purpose?

Practical approaches to addressing issues

- Develop robust policy – Broad topics & specific guidance
- Incorporate Generative AI records considerations into training
- Integrate records retention & production requirements into existing technology use and procurement pipelines
- Establish contract terms
- Use tools that are searchable & exportable
 - Focus on how integrations can be leveraged to help
 - Provide tools to help people do what you're asking of them



City of Seattle Generative AI Policy

Policy Highlights

- Human in the loop (HITL) must be involved prior to use of outputs in official City capacity
- Attribution requirements
- No City data or records to be used for training or tuning outside of City control
- RSJI resources/RET completed prior to use
- Records must be retrievable (technically and/or by contract) for PDR purposes

AI Principles

- Innovation & Sustainability
- Transparency & Accountability
- Validity & Reliability
- Bias, Harm Reduction & Fairness
- Privacy Enhancing
- Explainability & Interpretability
- Security & Resiliency

Questions

Q & A