Privacy Tech Talk on Artificial Intelligence and Machine Learning

January 29, 2020

Agenda for Data Privacy Day 2020 @ GSA!

- Welcome, Richard Speidel; GSA Chief Privacy Officer
- Krista Kinnard; Director of AI for the TTS Centers of Excellence
- Recent CTO Tech Talk on AI/ML; some GSA considerations and tools
- Resources and Contact Information

TECHNOLOGY TRANSFORMATION SERVICES

GSA

Artificial Intelligence

Agenda

- Community of Practice
- Center of Excellence

What we will do

- Create, collect, curate and share best practices, success stories, use cases, programs, and policy
  - Range of topics including: data readiness, AI tools and techniques, privacy, security, ethics, workforce development
- Identify and share perspectives on workforce development, including programs, platforms and strategies for how to get there.
- Host speaker sessions, workshops, trainings and other knowledge sharing events on a range of issue areas.

Areas of Focus

Events and Speakers	Highlighting speakers from the community to share success and challenges in applying AI — can include structured activities to help agencies work through challenges and opportunities.
Practice Areas	User-driven, active community engagement on specific AI topics, e.g. Ethics, AI tools & techniques, privacy, security, including specific challenges to solve for.
Use Case Sharing	Aggregation and sharing of use cases to build awareness and engagement within the community.
Content	Aggregating, curating, and creating materials to be shared in the community.
External Engagement	Engaging beyond government to academia, industry and other consortia to foster continuous learning.

Our Community - Interest and Opportunity

Sample Practice Areas

- **AI Tools & Techniques**
  (machine learning, NLP, deep learning...)
- **Data Governance**
  (AI-readiness, security, privacy)
- **AI Ethics** (Transparency, Accountability, Explainability, Fairness, Privacy)
- **AI Business Analysis and Acquisition**
  (ROI and cost/benefit analysis, vendors)

Use Case Areas We're Seeing

- **Customer experience:** Chatbots for improved customer interaction and request processing.
- **Human Resources:** Tools for generating job descriptions and filtering applicants.
- **Advanced Cybersecurity:** Cloud, connection, and application anomaly and threat detection
- **Business Processes:** Classifying resource requests, predictive analytics for future workload/demand and financial risk, grant application, fraud prevention

IT MODERNIZATION Centers of Excellence

GSA

Centers of Excellence

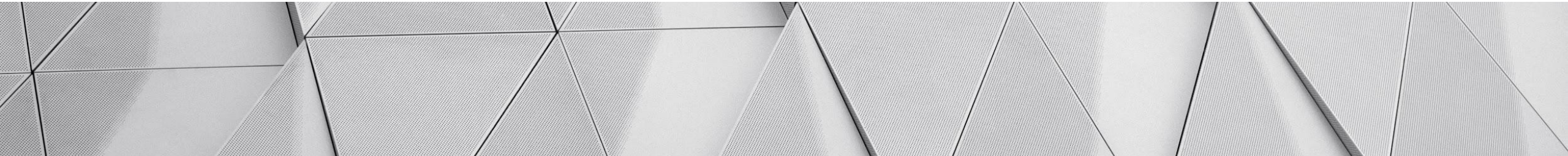
Accelerating IT Modernization

Overview: What we do

Accelerate **IT modernization** across government to improve the **public experience** and increase operational efficiency.

To accomplish this, we partner with industry subject matter experts to solve agencies problems in the following functional areas:

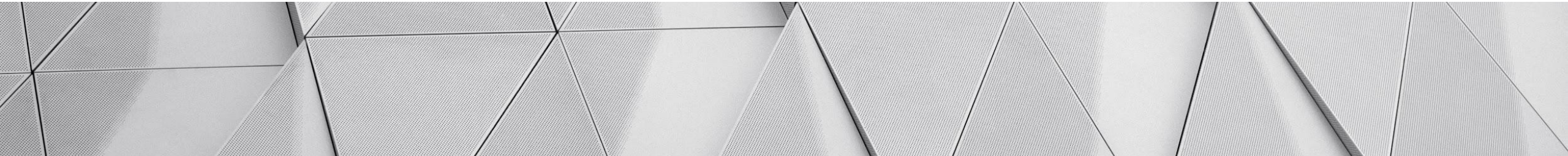
Cloud Adoption | Contact Center | Customer Experience | Data Analytics | Artificial Intelligence



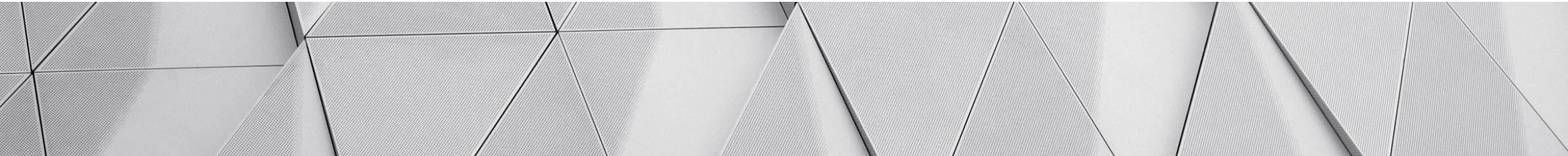
Overview: How We Work

People First:
We use human centered design to identify and validate the needs and priorities of key stakeholders

Rapid Prototyping & Implementation:
Deliver prioritized recommendations to address pain points, through prototyping and enterprise implementations



Overview: Current Engagements



How to engage

AI COP:
digital.gov/communities/artificial-intelligence/

AI CoE:
https://coe.gsa.gov/

Recent CTO Tech Talk on AI/ML at GSA

Artificial Intelligence and Machine Learning Tech Talk

GSA is in the early phases of deploying machine learning to provide business value.

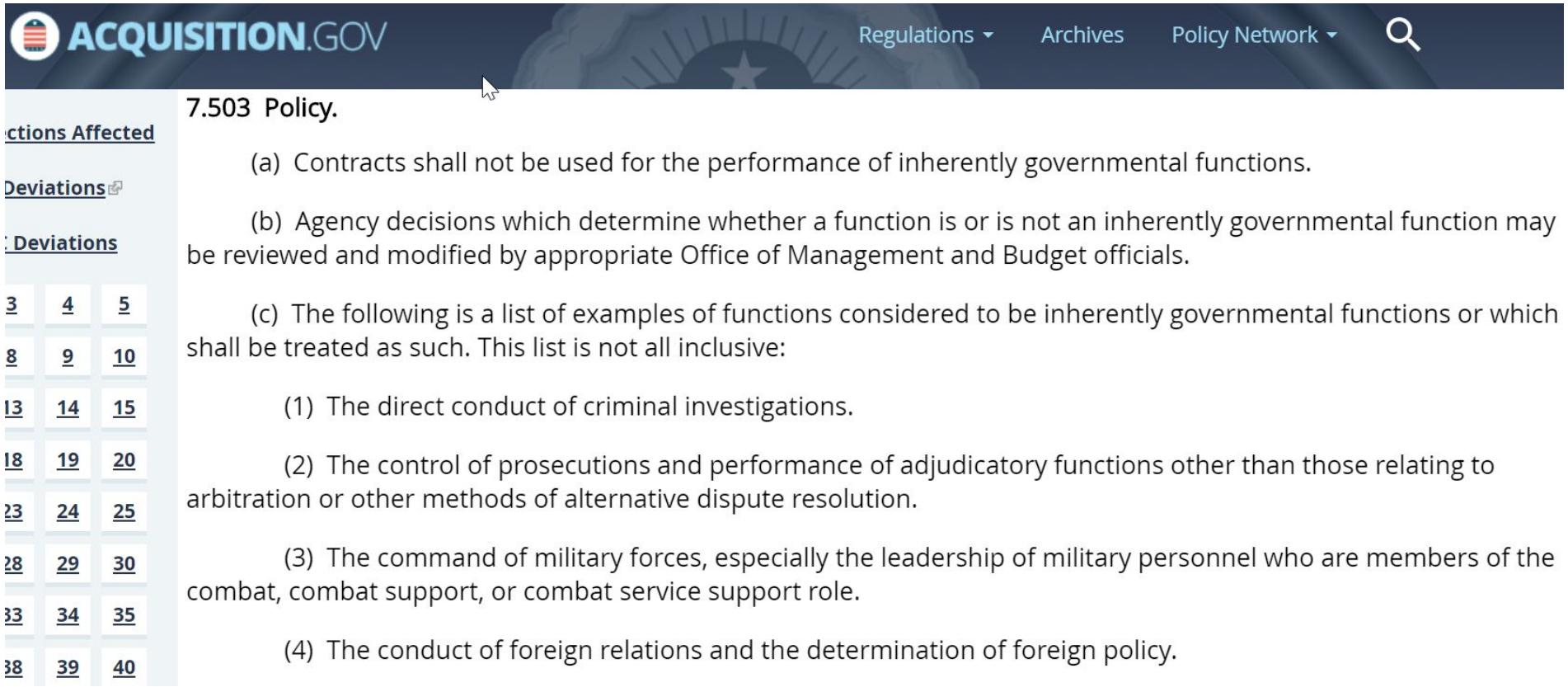
In this tech talk, Ryan Day of the GSA Chief Technology Office discussed some examples of how machine learning is being used in industry and at GSA.

The deck is a terrific resource:

https://drive.google.com/file/d/1309XBGuId7xQHkYVVYTAaJnNLzgUyQME/view

GSA considerations - “Inherently Governmental Functions”

FAR Part 7 contains a list of examples of inherently governmental functions:



Privacy Tools and Strategies for Data Sharing

- **Multi-party computation**: Allows different parties with data to work together to analyze data. Neither data nor private results are shared with other parties, even if other parties collude or act maliciously.

- **Federated learning**: A model which can be used to improve an algorithm without giving personally identifiable information (PII) data directly to the entity that owns the algorithm.

- **Homomorphic Encryption**: Allows one party to have its data analyzed by another party without sharing its data. The encrypted data does NOT reveal any private data without the decryption key from the agency.

Contact Info and Resources

Richard Speidel
richard.speidel@gsa.gov

Krista Kinnard
krista.kinnard@gsa.gov

Data Sheets for Data Sets
https://arxiv.org/abs/1803.09010

Model Cards for Model Reporting
https://arxiv.org/pdf/1810.03993