NRF® Center

for Digital Risk & Innovation

NRF Principles for the Use of AI in the Retail Sector

November 2023

Agenda

- Introductions
- Retail AI Context
- Overview of AI Principles
- ✓ Next Steps
- Discussion

Retail AI Context

Business

- Retail sector is active user of AI products and services
- Dozens of AI use cases for retailers of all sizes
- Retailers are developing generative AI capabilities

Stakeholder

- Increased policymaker attention to AI issues
- Consumer understanding of AI use in retail is uncertain and evolving
- Important for retail sector to engage in public dialogue on AI

NRF Principles for the Use of AI in the Retail Sector

- **Four Categories:**
  - Governance and Risk Management
  - Customer Engagement and Trust
  - Workforce Applications and Use
  - Business Partner Accountability

1. Governance and Risk Management

Retailers should develop strong internal governance of AI tools and capabilities as a foundational basis for managing risks and ensuring that AI delivers expected benefits.

Retailers should develop company-wide **governance practices** for the use of AI, involving not only the company's direct AI or data science teams but also stakeholders in legal, compliance, marketing, communications and other business roles.

Company-wide governance teams should have responsibilities for risk management, oversight and security of AI capabilities **throughout the lifecycle**, from testing to deployment to post-deployment monitoring.

Retailers should develop practices to maintain **internal awareness** of AI tools in deployment, the current and planned use cases for these tools, and the data sets used to support them.

Retailers should be proactive in assessing and reporting **emergent AI-related risks**, especially those from external adversarial activities by cyber criminals and fraudsters.

2. Customer Engagement and Trust

Retailers should be transparent about their uses of AI that have a legal or similarly significant effect on a customer, establish safeguards to prevent unlawful discrimination against protected classes of individuals, and align their governance of consumer-facing AI applications with existing internal privacy, cybersecurity and other data governance policies.

Retailers should remain focused on **customer trust** with respect to their use of AI tools and capabilities, ensuring that these tools support the customer experience and do not inadvertently harm or undermine their trust.

For AI tools that use customers’ personal data, retailers should be **transparent** about how they are using these tools to support the customer experience where their use of AI could have a legal or similarly significant effect on a customer. They should strive to ensure that their **uses of AI are explainable**, with appropriate exceptions from disclosing AI capabilities that protect the company and its customers against malicious activity.

When using AI-enabled technology to serve customers, retailers should carry out internal oversight, develop safeguards and engage with their AI developers and other third parties to prevent **automated outcomes that unlawfully discriminate** against protected classes of individuals.

Retailers should develop additional internal controls, including human oversight and engagement, for **AI capabilities that facilitate monitoring in stores** for purposes of security, fraud prevention and asset protection.

3. Workforce Applications and Use

Retailers should engage in ongoing oversight and review of AI applications that may directly impact employees or that can be used by the workforce to support business needs.

Retailers should develop and deploy AI applications that affect **hiring and promotions for employees** with clear guidelines and in a manner consistent with all applicable laws and regulations.

Retailers should engage in ongoing oversight and review of AI-enabled capabilities that monitor or assess **employee performance** to ensure compliance with existing laws and regulations.

Retailers should consider providing guidelines to their employees about the use of **publicly available generative AI tools** within the company, including appropriate warnings about inadvertently exposing trade secrets and other non-public company information.

4. Business Partner Accountability

Retailers should establish clear guidelines and expectations for business partners that are providing AI tools, data sets and services.

Retailers should consider integrating AI governance into their existing **third-party risk management** activities and contracts to establish expectations for vendors and service providers with respect to their own AI governance.

Retailers should strongly encourage **technology service providers** to be transparent to them about their own AI governance, including with respect to the applications, data sets and algorithms they are using in support of retail AI use cases.

Using the AI Principles

- High-level reference framework – not a checklist
- Starting point for work on specific issues and use cases
- Engagement with policymakers and external stakeholders

Future Initiatives

Work on specific AI use cases

Map retail sector use of AI against NIST AI Risk Management Framework

Evolve principles based on changes in retail use of AI and technology and policy developments

How to Engage

- NRF Center for Digital Risk & Innovation
- NRF AI Working Group
- Discussions within NRF Councils and Committees
- Policy Advocacy

NRF Center for Digital Risk & Innovation

https://nrf.com/cdri

cdri@nrf.com