Farella
Braun + Martel

AI and Privacy: What Every Company Needs To Do Today

Sushila Chanana, Ben Buchwalter, Sunny Seon Kang, Amanda Katzenstein

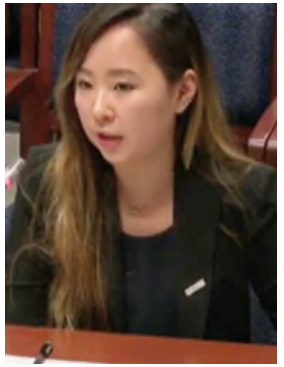
May 22, 2024

This presentation is provided for informational purposes and does not constitute legal advice

Panelists

Sushila Chanana
Partner
Farella Braun + Martel

Ben Buchwalter
Special Counsel
Farella Braun + Martel



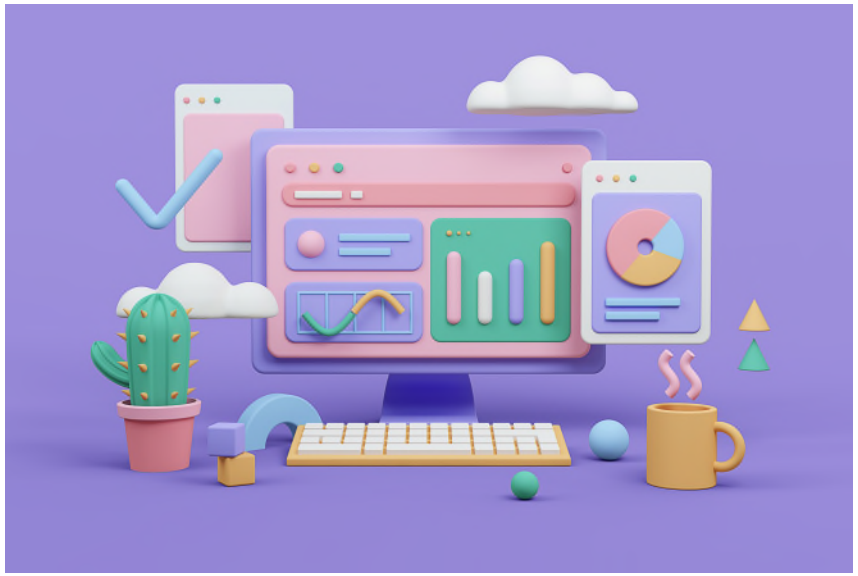
Sunny Seon Kang
Global Privacy Counsel, AI & Data
Visa

Amanda Katzenstein
Corporate Counsel, Product
Salesforce

Farella
Braun + Martel

Agenda

- AI Governance and Privacy Laws
- NIST AI Risk Management Framework
- Management of AI-Related Risks
- AI in Employment Decisions



Farella Braun + Martel

Basics of AI Governance

- What Is AI Governance?
  - Policies and best practices
    - Transparency
    - Fairness, avoid unfair bias while maximizing the intended benefits.
    - Privacy and data protection
    - Accountability and oversight
  - AI Supplier Risk Management

Farella Braun + Martel

Impacted Industries (Examples)

- **Healthcare**: to diagnose diseases, predict patient outcomes, and develop personalized treatment plans.
- **Medical Devices**: to assist with medical care.
- **Finance**: to detect fraud, automate customer service, and provide personalized investment advice.
- **Retail**: to optimize pricing, forecast demand, and personalize marketing campaigns.
- **Manufacturing**: to optimize production, reduce downtime, and improve quality control.
- **Transportation**: to determine the best routes, reduce fuel consumption, and improve safety.
- **Education:** to support school instruction and access to technology

Farella Braun + Martel

Existing & Proposed Privacy Frameworks

Existing

- CCPA
- EU AI Act
- GDPR, Art. 22
- FTC
- Biometrics laws

Proposed

- CCPA amendments
- APRA
- Other states

Farella
Braun + Martel

NIST AI Risk Management Framework

- Guidelines for AI governance
- AI Risks
  - Harm to people
  - Harm to organization
  - Harm to ecosystem
- “GMMM” Guideposts
  - Govern
  - Map
  - Measure
  - Manage

Farella Braun + Martel

FTC on AI

On January 25, 2024, the FTC Office of Technology hosted a virtual tech summit to discuss key developments in the field of AI

- The FTC noted that the summit was scheduled due to the rise in the development and deployment of AI technologies and the potential risks and harms posed by the information asymmetry enforced by dominant AI suppliers
- Specifically, the FTC noted the role AI may play in facilitating fraud and scams, and the risk that companies may use the rapid popularity of AI to leverage anticompetitive tactics to impair competition
- After the summit, the FTC released a blog post stating that companies using AI should proceed with caution when updating terms of service or privacy policies

Farella Braun + Martel

Privacy-Enhancing Technologies and AI

- NIST Differential Privacy Guidance
- Executive Order reference to privacy preserving techniques
- Federal Tech Sprint on Privacy Enhancing Techniques

Administration

(b) Within 365 days of the date of this order, to better enable agencies to use PETs to safeguard Americans' privacy from the potential threats exacerbated by AI, the Secretary of Commerce, acting through the Director of NIST, shall create guidelines for agencies to evaluate the efficacy of differential-privacy-guarantee protections, including for AI. The guidelines shall, at a minimum, describe the significant factors that bear on differential-privacy safeguards and common risks to realizing differential privacy in practice.

(c) To advance research, development, and implementation related to PETs:

(i) Within 120 days of the date of this order, the Director of NSF, in collaboration with the Secretary of Energy, shall fund the creation of a Research Coordination Network (RCN) dedicated to advancing privacy research and, in particular, the development, deployment, and scaling of PETs. The RCN shall serve to enable privacy researchers to share information, coordinate and collaborate in research, and develop standards for the privacy-research community.

Farella Braun + Martel

EU AI Act – Different Rules for Different Risk Levels

- Unacceptable Risk AI systems
  - Ex: social scoring, biometric identification and categorization, behavior manipulation
  - Ban them
- High Risk AI systems: negatively affect health, safety or fundamental rights
  - AI systems used in products covered by the EU's product safety legislation (vehicles, medical devices, toys, etc.)
  - AI systems that will have to be registered in an EU database (critical infrastructure, education, employment, border control management, etc.)
  - Review/access prior to GTM and continuous process during lifecycle
  - Transparency, disclaimers, documentation, human review, model design, de-identify, opt-out, results traceability, prompt testing & red teaming

Farella Braun + Martel

EU AI Act – Different Rules for Different Risk Levels (Cont.)

- Limited Risk and Minimal Risk
  - Limited risk means risk associated with lack of transparency in AI usage
  - Transparency obligations for limited risk
- Accuracy – training, validation, testing, and provision of services
- Bias – model cards, documentation, testing and ethical review
- AI Acceptable Use Policy

Farella Braun + Martel

AI in Employment Decisions – Existing Laws

- Existing employment laws apply
  - Title VII of Civil Rights Act
  - FEHA
- AI use is no defense to discrimination claims
- Existing state laws
  - New York
  - Illinois
  - Colorado
  - *California and Federal laws being considered*

Farella Braun + Martel

Anticipated AI in Employment Laws

CA Consumer Privacy Act

- Automated decision-making technology (ADMT)
- Applies to all consumers, including employees
- Pre-use notices
- Right to opt out
- Requests to access information
- Risk assessments

American Privacy Rights Act (Fed)

- Covered algorithms
- “Consequential decisions”
- Notice Requirements
- Opt out rights
- Small businesses exclusion
- Right to access and delete
- Collaboration with state agencies

Farella Braun + Martel

Best Practices for HR Recruiting Purposes

- Human should make ultimate employment decisions
- Consider disparate impact
- Be conscious of geography (whether NY, IL laws apply)
- Develop AI policies or processes with key stakeholders
- Train HR / Recruiting teams on AI tech to understand impact
- Carefully vet / audit vendors
- Indemnification with vendors (not a panacea)

Farella Braun + Martel

Key Takeaways

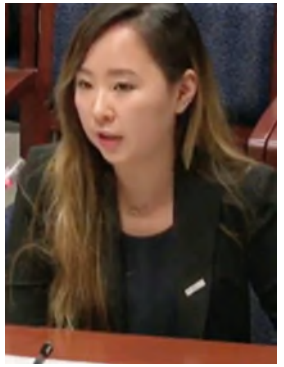
- Consider company's approach to generative AI
- Identify key stakeholders who should provide input to AI processes
- Carefully vet vendors before onboarding and periodically audit their use
- Build AI safeguards for product development and data processing
- Develop policies, procedures, and training related to AI

Farella
Braun + Martel

Questions?

Sushila Chanana
Partner
Farella Braun + Martel
415-954-4472
schanana@fbm.com

Ben Buchwalter
Special Counsel
Farella Braun + Martel
415-954-4791
bbuchwalter@fbm.com



Sunny Seon Kang
Global Privacy Counsel, AI & Data
Visa
seon.sunnykang@alumni.stanford.edu

Amanda Katzenstein
Corporate Counsel, Product
Salesforce
amanda.katzenstein@gmail.com

Farella Braun + Martel