Securing the Unknown:
Contours and Choices in AI Security

Privacy+Security Forum

Kate Charlet, Head of Global Privacy and Security Policy, Google

Brock Dahl, Partner, Freshfields

Patrick Kyhos, Director, Operational & Incident Response, ONCD, The White House

Matthew O'Shaughnessy, Visiting Fellow, Carnegie Endowment for International Peace

Spring Academy 2023

Freshfields Bruckhaus Deringer

Agenda

- Setting the Context – What does AI Mean?
- Exploring the Opportunity and Risk Landscape
- Security Exposure – Deep Dive
- Managing Security Risk through Governance and Controls
- Questions

Setting the Context

- What does AI Mean?
- Generative AI
- Automation
- Algorithms

Exploring the Opportunity and Risk Landscape

- Opportunities
- Risks
- Various Interests
  - Private sector considerations
  - Government and public interest
- Contours and Conflicts

Security Exposure

Technical Risks

- Algorithms and Peering Inside the Machine
- Malicious Software Injections
- Inversion Attacks
- Data / Algorithm Poisoning

Security Exposure

Human Risks

- Well-Intentioned Developers
- Misguided Explorers
- Observers
- Talkers

Managing Security Risk

- Establishing Sound Governance and Controls
- Role of Public Policy
- Contours and Conflicts

Questions

Thank you