

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

The background features a dynamic, abstract pattern of small dots in various shades of blue and cyan. These dots are arranged in a way that creates a sense of movement and depth, resembling a wave or a digital signal. The pattern is denser on the right side and fades out towards the left. The overall color palette is a gradient from light cyan to a deeper blue.

Thank you

This material is provided by the international law firm Freshfields Bruckhaus Deringer LLP (a limited liability partnership organised under the laws of England and Wales authorised and regulated by the Solicitors Regulation Authority (SRA no. 484861)) and associated entities and undertakings carrying on business under, or including, the name Freshfields Bruckhaus Deringer in a number of jurisdictions, together referred to in the material as 'Freshfields'. For further regulatory information please refer to www.freshfields.com/support/legal-notice.

Freshfields Bruckhaus Deringer has offices in Austria, Bahrain, Belgium, China, England, France, Germany, Hong Kong, Italy, Japan, the Netherlands, Singapore, Spain, the United Arab Emirates, the United States and Vietnam.

This material is for general information only and is not intended to provide legal advice.

© Freshfields Bruckhaus Deringer LLP 2022