Debunking The Mysticism Around AI And Data Privacy

Privacy + Security Forum

May 11, 2023

Cynthia Cole
Sheila Jambekar
Polina Zvyagina

Privacy+ Security Forum

Cynthia Cole

Partner
Baker McKenzie
cynthia.cole@bakermckenzie.com

Cynthia Cole is an Intellectual Property Partner in Baker McKenzie's Palo Alto office, as well as a former CEO and General Counsel. Before joining the Firm, Cynthia was Deputy Department Chair of the Corporate Section in the California offices of Baker Botts where she built the technology transactions and data privacy practice. An intellectual property transactions attorney, Cynthia also has expertise in digital transformation, data privacy, and cybersecurity strategy.

Sheila Jambekar

Chief Privacy Officer
Plaid
sjambekar@plaid.com

Sheila is the Chief Privacy Officer at Plaid, a technology company helping power the next generation of financial services. At Plaid, Sheila oversees the privacy and data ethics program, including development of the organization's Trustworthy ML/AI program. Previously Sheila was Vice President, Deputy General Counsel and Data Protection Officer at Twilio Inc.

Polina Zvyagina

Privacy and Data Policy Manager
Meta
polinaz@meta.com

Polina is a Privacy Lawyer and has worked at Apple, Uber, and Airbnb.

At Meta, Polina specializes in the responsible building of AI. She's building scalable solutions in AI Explainability, AI Governance and Generative AI.

Agenda

1	What is AI?
2	Global Legal and Regulatory Frameworks
3	Practice Tips
4	AI & Internal Governance
5	Takeaways

Is your company using generative AI?

A. Yes
B. No
C. We've banned or restricted the use of ChatGPT and similar tools for work purposes

Privacy+ Security Forum

1. What is AI?

Privacy+ Security Forum

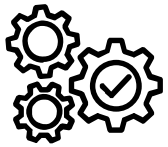
Defining AI

Privacy+ Security Forum

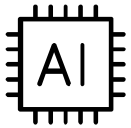
- **Artificial Intelligence (AI)** is “the computerized ability to perform tasks commonly associated with human intelligence, including reasoning, discovering patterns and meaning, generalizing knowledge across spheres of application, and learning from experience” (Source: FPF)
- **Machine Learning** is a branch of AI concerned with AI models that “learn” from the success or accuracy of their outputs, and can adapt their programming over time, with minimal human intervention
- An **AI system** is a group of machine learning models, AI and non-AI technologies that work together to accomplish specific tasks, e.g., such as ranking posts in a feed
- An **AI model** is what is used to perform tasks moving forward, with new data, once the AI has already been trained
- A **foundation model** is a large AI model that can be adapted to a wide variety of tasks and applications
- **Generative AI** is a category of AI that can independently create novel content, such as text, images, audio

What is Generative AI?

Deep Learning is a type of AI that learns to make predictions based on existing data – predicts an outcome and generates insights



Generative AI is a type of AI that is capable of creating new data – it does this by predicting content



Neither reasons, but Generative AI is getting very good at persuading you that it does

AI in Use Today

Tools:

- Computer vision
- Natural language processing (e.g. translation, content understanding)
- Speech recognition
- Content clustering/similarity detection
- Classifiers (e.g. hate speech detection, nudity detection)
- Multimodal understanding (image + text)
- Large Language & Diffusion Models

Uses:

- Content and ads ranking
- Predicting interests
- Product tag suggestions
- Policy enforcement (e.g. detecting images of banned items, copyright violation)
- Video subtitles
- Accessibility tools
- Assistant
- Avatar generation
- Manipulated media detection

What are "Algorithms"

Privacy+ Security Forum

Algorithms:
series of ordered steps

- Algorithms = mathematical formulas

Steps

- Each step is defined (that's what we call an "input")
- Each input is "worth" a certain amount, or "weighted"
- Aiming towards a goal (that's the "output")

Like a recipe

- Flour, salt, sugar, yeast, water, oil = inputs
- Amounts of each = weightings
- Certain steps go first, others follow (activate the yeast, add flour, allow to rise, punch down, rise again, bake)
- Output (goal) = bread

Simple algorithm:
2 (4 + 1) = y

- Goal: "To solve for y"
- Inputs: 2, 4, 1
- Steps: "First, add 4 + 1", "Next, multiply by 2"

Algorithmic Inputs, Weightings and Output

Privacy+ Security Forum

Output: a first step

Formulating the desired goal: what do we want the AI tool to DO?

Inputs

- No golden tablet
- No master set of accepted principles
- Can be: chosen by humans
- Chosen by the software (pattern recognition)
- Importance of WHO decides
  - How decisions are made
  - Is there a validation process

Design an algorithm directed at achieving that goal

Weightings of inputs

- No golden tablet with all the "correct" measurements
- Who decides: machine or human? adjustments?

2. Global Legal and Regulatory Frameworks

Privacy+ Security Forum

Patchwork of Laws

- New law
- Updates to existing law
- Use case specific laws
  (e.g., self-driving cars, employment)
- Industry regulation
  (e.g., FS, healthcare, public sector)
- Guidance from regulators
- Data and AI-adjacent laws

Legal and regulatory frameworks on AI

Privacy+ Security Forum

UK

- Data Ethics Framework - 2018
- Guidance on use of AI in the Public Sector, updated October 2019
- ICO Regulatory Sandbox 2019
- Guidance understanding artificial intelligence ethics and safety 2019
- National AI Strategy and Standards Hub 2021/2022
- AI Regulation Policy Paper 2021

EU

- General Data Protection Regulation 2016 (provisions on automated decision making)
- High-Level Expert Group on Trustworthy AI 2018
- HLG Recommendations on Trustworthy AI 2019
- Draft EU Regulation on AI 2021
- Review of Product Liability Framework 2021
- Regulation on Machinery Products 2021
- Digital Services Act 2022
- Digital Markets Act 2022

Canada

- Directive on use of Automated Decision-Making by Federal Government in effect April 2020
- Artificial Intelligence and Data Act (AIDA) June 2022

China

- Principles on Governing the New Generation of AI: Developing Responsible AI 2019
- Regulation on Promoting the Development of Artificial Intelligence Industry (Shanghai, Shenzen) 2022
- Regulation of Algorithmic Recommendation Systems – 2022
- CAC draft Administrative Measures for Generative Artificial Intelligence Services 2023

Norway

- DPA Sandbox on AI - 2020

France

- CNIL creates AI department -Jan 2023

Egypt

- National AI Strategy framework 2019

Japan

- Social Principles of Human-centric AI, 2019
- AI Governance Guidelines 2022

United States

- Bot Disclosure Law 2018
- Commercial Facial Recognition Privacy Act of 2019
- Executive Order on Promoting the Use of Trustworthy AI in the Federal Government 2020
- OMB Guidance on Regulation of AI in Private Sector- 2020
- The National AI Initiative Act 2021
- NY automated employment decision tools law 2021
- Blueprint for an AI Bill of Rights
- Algorithmic Accountability Act of 2022
- Draft NIST AI Risk Management Framework 2022
- Federal Trade Commission issues warning

Italy

- Guarante decision banning ChatGPT/OpenAI (since reversed)

India

- Exploring AI Principles 2021

Singapore

- Model AI Governance Framework 2019 (Updated 2020) + Implementation Self-Assessment Guide
- Trusted Data Sharing Guidance 2019
- A Guide to Job Re-Design in the Age of AI 2020
- MAS Framework for Responsible AI + Veritas Consortium Phase 1 – 2020; Phase 2 - 2021

OECD

- Principles on Artificial Intelligence

Australia

- AI Ethics Framework 2019
- Automated Decision Making and AI Regulation Consultation 2022

Brazil

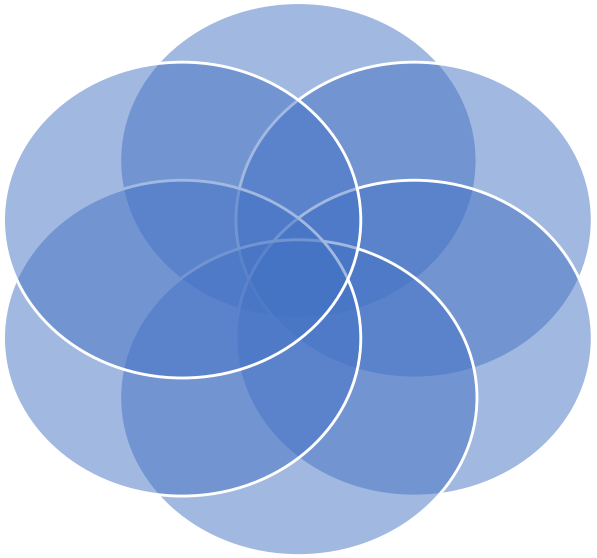
- Senate Committee Publishes AI Report and Draft AI Law Dec 2022

Non-exhaustive list. More information
https://oecd.ai/en/dashboards/overview

Key Themes

Transparency & Explainability

Fairness & Bias



Accountability Mechanisms

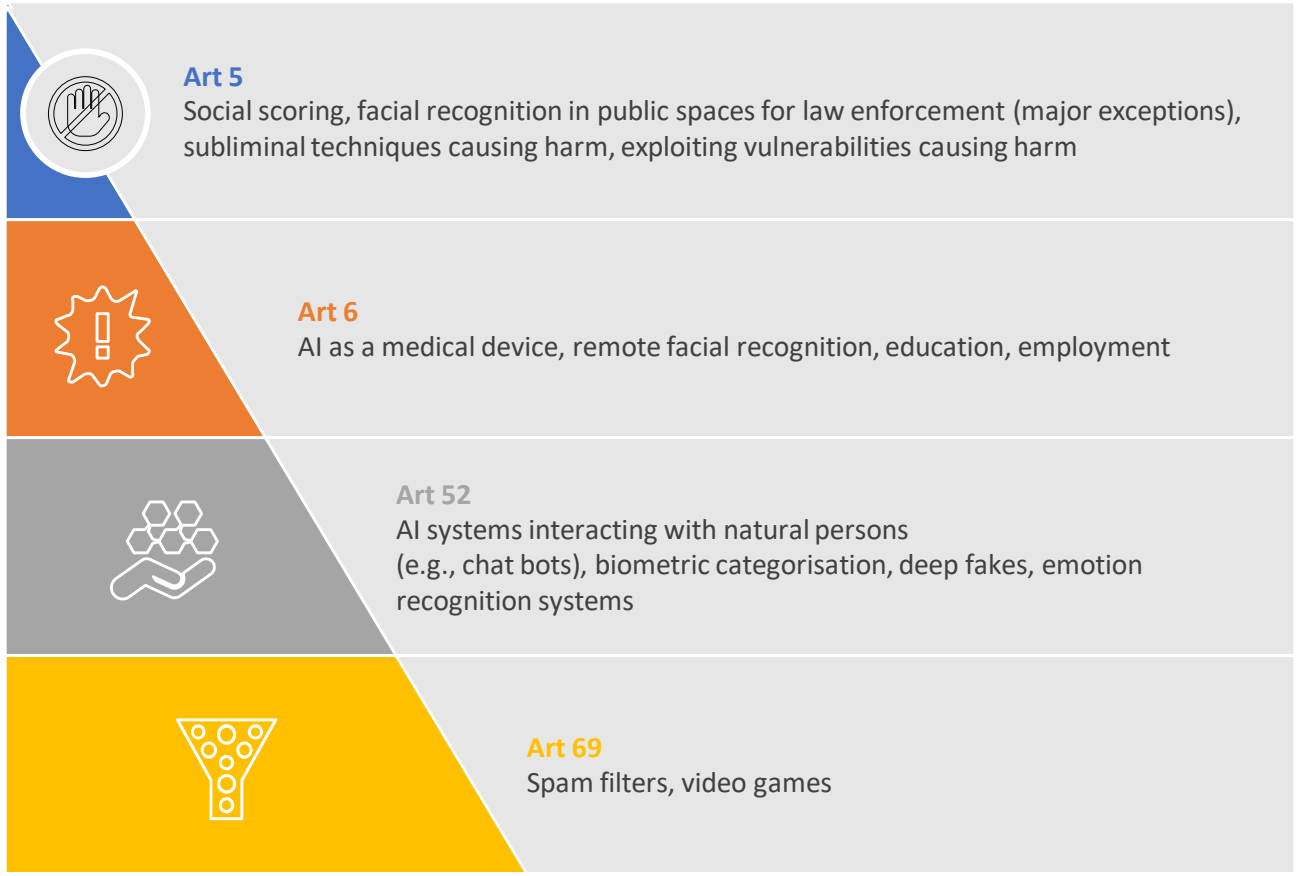
Risk Management

Restrictions of Specific Uses

Model Documentation

Myth: EU AI Act enables you to categorize AI systems according to level of risk

Reality: Risk assessment is more nuanced



Excluded from scope: AI systems for sole purpose of scientific research and development

Generative AI: new proposals adopts a multi-tiered risk approach to General Purpose AI and Foundation Models

Who manages AI risk issues in your organization?

A. Legal/Compliance
B. IT
C. HR
D. C suite level (CISO, COO)
E. It's a team effort
F. No one

Privacy+ Security Forum

3. Practice Tips

Privacy+ Security Forum

What functional, legal and compliance areas need to account for AI?

Privacy+ Security Forum

EXAMPLES

- Product and Procurement
- Privacy Compliance & Cybersecurity
- M&A
- R&D and IP management
- HR

Product and Procurement

- How can you incorporate AI questions into existing procurement process?
- What are the key questions you should ask when contracting for AI platforms?
- What questions should you be asking when building an AI platform?
- Special terms in vendor contracts and licenses?

Privacy & Cybersecurity

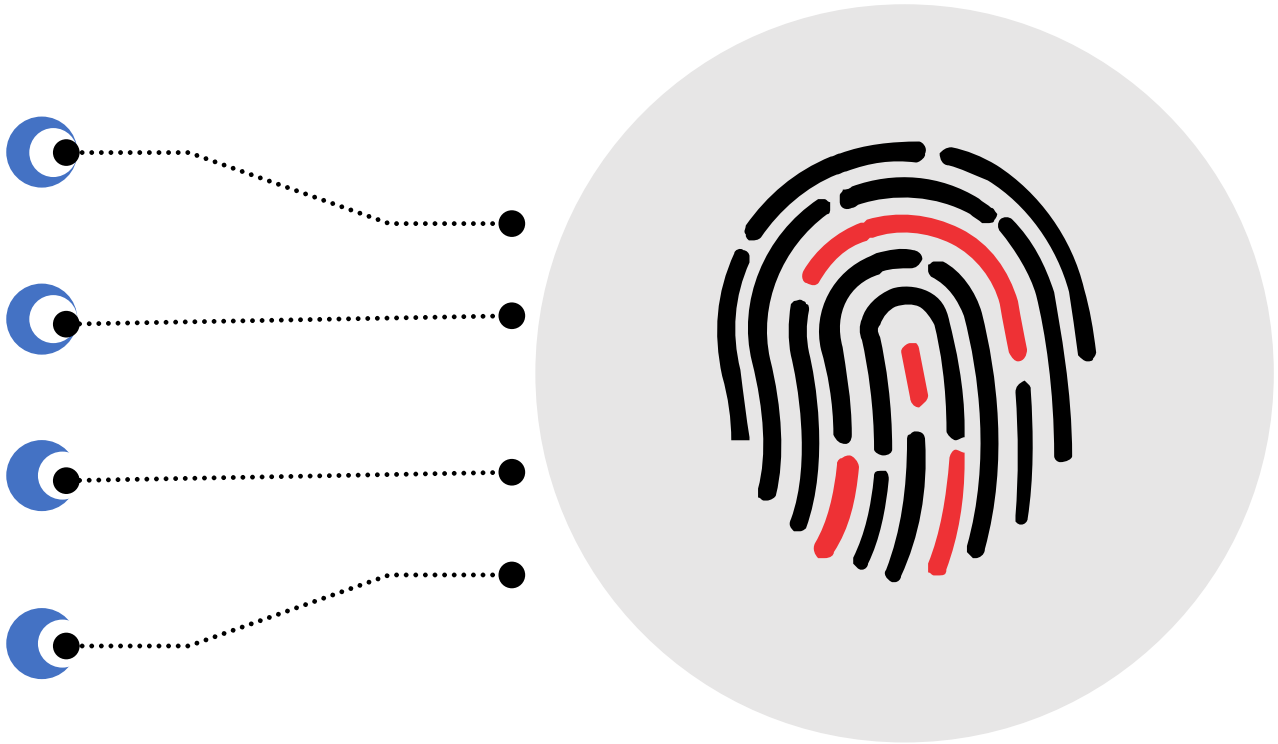
Privacy+ Security Forum

How important is it to understand how AI was trained? Where did the data sets come from?

How can compliance steps be built in to existing process?

What can be done to mitigate data privacy risks associated with AI platforms?

Are AI systems secure? What are the unique vulnerabilities?



M&A and Corporate Transactions

- What is the current deal environment? What are the key drivers in deals involving AI?
- How should you approach diligence in deals involving AI assets?
- In light of the emerging regulatory and legal framework, how can parties allocate AI-related risks and liabilities?

What are the most significant AI-related opportunities?

A. New customer facing products and services
B. Coding/engineering/IP generation
C. Streamlining existing workstreams

Privacy+ Security Forum

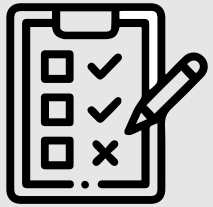
4. AI & Internal Governance

Privacy+ Security Forum

AI Internal Governance: Top Issues

Privacy+ Security Forum

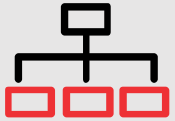
Getting people in your organization to care and engage



The role of industry standards/frameworks (e.g., NIST)

What are the key red flags?

How does AI governance vary by organization size and industry?

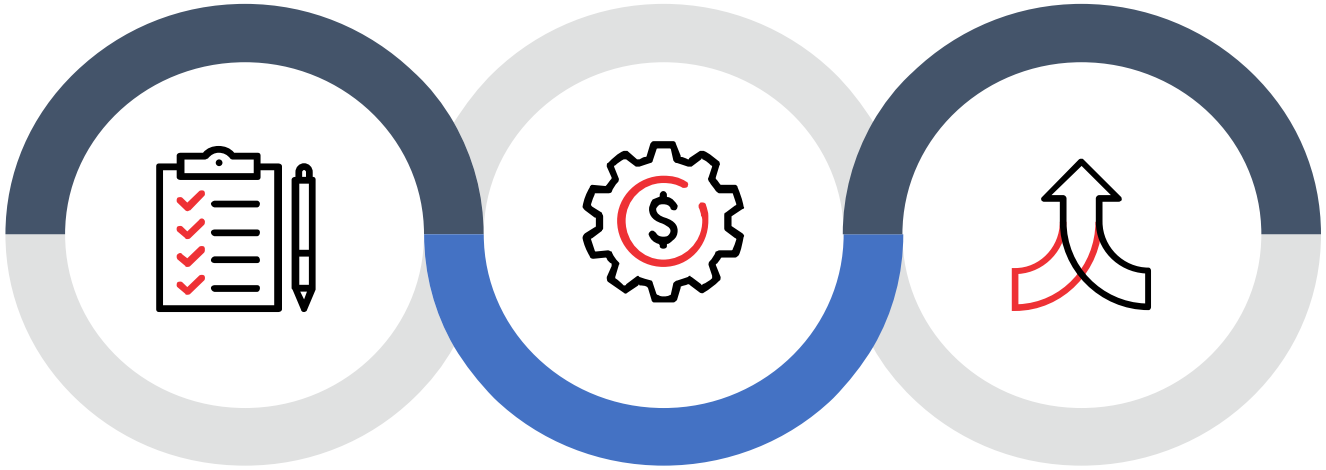


Which functions need to be involved?

5. Takeaways

Privacy+ Security Forum

Takeaways



Incorporating AI issues into
Product & Procurement Process

Questions

Privacy+ Security Forum

Debunking The Mysticism Around AI And Data Privacy

Privacy + Security Forum

May 11, 2023

Cynthia Cole
Sheila Jambekar
Polina Zvyagina

Privacy+ Security Forum