

osano





AI & Data Privacy: Minimizing Risk and Maximizing Opportunity

Tuesday, 30 April

11:00-12:00 PST

14:00-15:00 EST

20:00-21:00 CET



Presented by



Scott Hertel

Chief Technology Officer

Osano



Rachael Ormiston

Head of Privacy

Osano

CIPP/E, CIPP/US, CIPM, FIP



Jodi Daniels

CEO & Privacy Consultant

Red Clover Advisors

CIPP/US

Agenda

- What Is AI?
- How AI Introduces Risk and Supports Innovation
- AI Risk Management
- Operationalizing AI
- Innovating with AI
- Q&A

Poll

What Keeps You Up At Night When It Comes to AI?

01

Navigating AI's regulatory compliance requirements

02

Being left behind as competitors adopt AI more quickly and effectively

03

Mitigating the privacy, IP, and cyber risks of AI

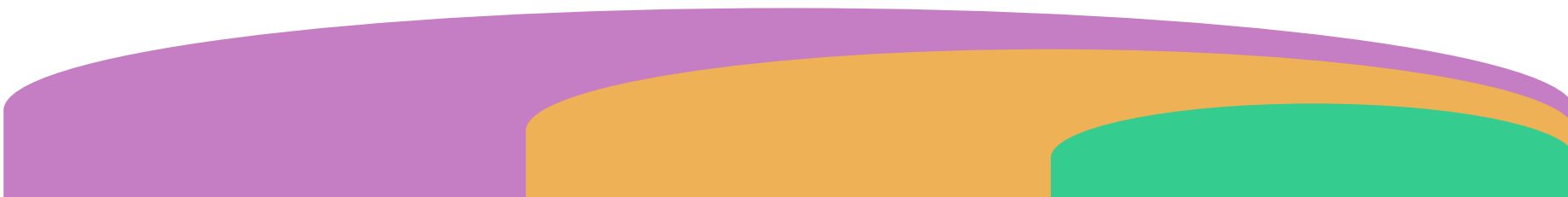
04

Learning how to effectively use AI in my role

05

Learning how to effectively appease our new machine overlords

AI Overview



	AI (1950s)	Machine Learning (1980s)	Gen AI (2020s)
What it is	Performs “human intelligence” tasks	Makes predictions or decisions based on given data.	Generates new data samples that resemble a set of training data.
How you’re already using it	<ul style="list-style-type: none">Automated workflows	<ul style="list-style-type: none">Segmenting customersForecasting sales	<ul style="list-style-type: none">Create text such as formsEmail assistance (let me help you write...)
How your customers are already using it	<ul style="list-style-type: none">Customer support and online chat	<ul style="list-style-type: none">Personalized product recommendations	<ul style="list-style-type: none">Summarizing or translating your content

Why This Matters

Hallucinations

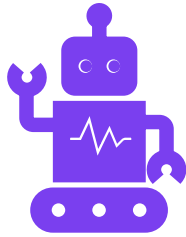
Discriminatory
Automated
Decision-Making

Personal Data
Breaches

Sensitive Data
Sharing

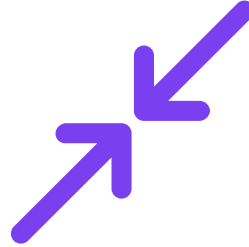
But It Isn't All Bad

AI has potential to unlock an estimated \$17–\$25 trillion in economic value



Automate

Improve CX and free up your time



Enhance

Augment human work







Accelerate






Move faster

Why Compliant AI

Risks Associated With Reckless AI Usage

-  • **Noncompliance**
 - Processing of data must comply with privacy laws as well as AI laws
-  • **Biased/Inaccurate Training Data**
 - Can lead to discrimination and unfair decisions
-  • **Lack of Disclosure and Choice**
 - Violating privacy laws' and AI laws' transparency, accountability, and privacy rights requirements
-  • **Unsecure systems**
 - Lack of security could threaten the AI models, datasets, and ultimate outcomes

Benefits of Compliant AI

-  • **Compliance**
-  • **Cleaner Training Data**
-  • **User Choice and Control**
-  • **Stronger Overall Risk Posture**
-  • **Empowered Technology Without Replacing Humans**

How Do We Govern AI?

Laws & Regulations

- EU:
 - AI Act
 - AI Liability Directive
- U.S.:
 - Executive Order on Trustworthy AI
 - NYC Local Law 144 AI Hiring law
 - Utah AI Law
 - Connecticut AI Act
 - Colorado Insurance AI rules
 - State Privacy laws on AI/ADM
- Canada: AI and Data Act
- Brazil: AI Bill 2338/202
- China:
 - Algorithmic Recommendation Law
 - Generative AI Services Law
 - Deep Synthesis Law
- Peru: Law 31814
- South Korea: AI Act
- Mexico: Federal AI Regulation
- Chile: Draft AI Bill
- International:
 - UN AI Resolution
 - G7 Agreement
 - Bletchley Declaration

Frameworks & Principles

- NIST: NIST AI Risk Management Framework
- White House: Blueprint for an AI Bill of Rights
- OECD:
 - OECD AI Principles
 - OECD AI Risk Classification Framework
- Council of Europe: Framework Convention on AI, Human Rights, and Rule of Law
- AI Verify Foundation:
 - Singapore AI Verify Framework
 - Singapore Generative AI Governance Framework
- UNESCO: AI Ethics Recommendation
- G7 Hiroshima Process AI Guiding Principles

Technical Standards

- ISO
 - 42001 AI Management System
 - 23894 AI Guidance on Risk Management
- CEN-CENELEC: EU AI Act Standards
- IEEE
 - P2863 Organizational Governance of AI
 - P7003 Algorithmic Bias Considerations



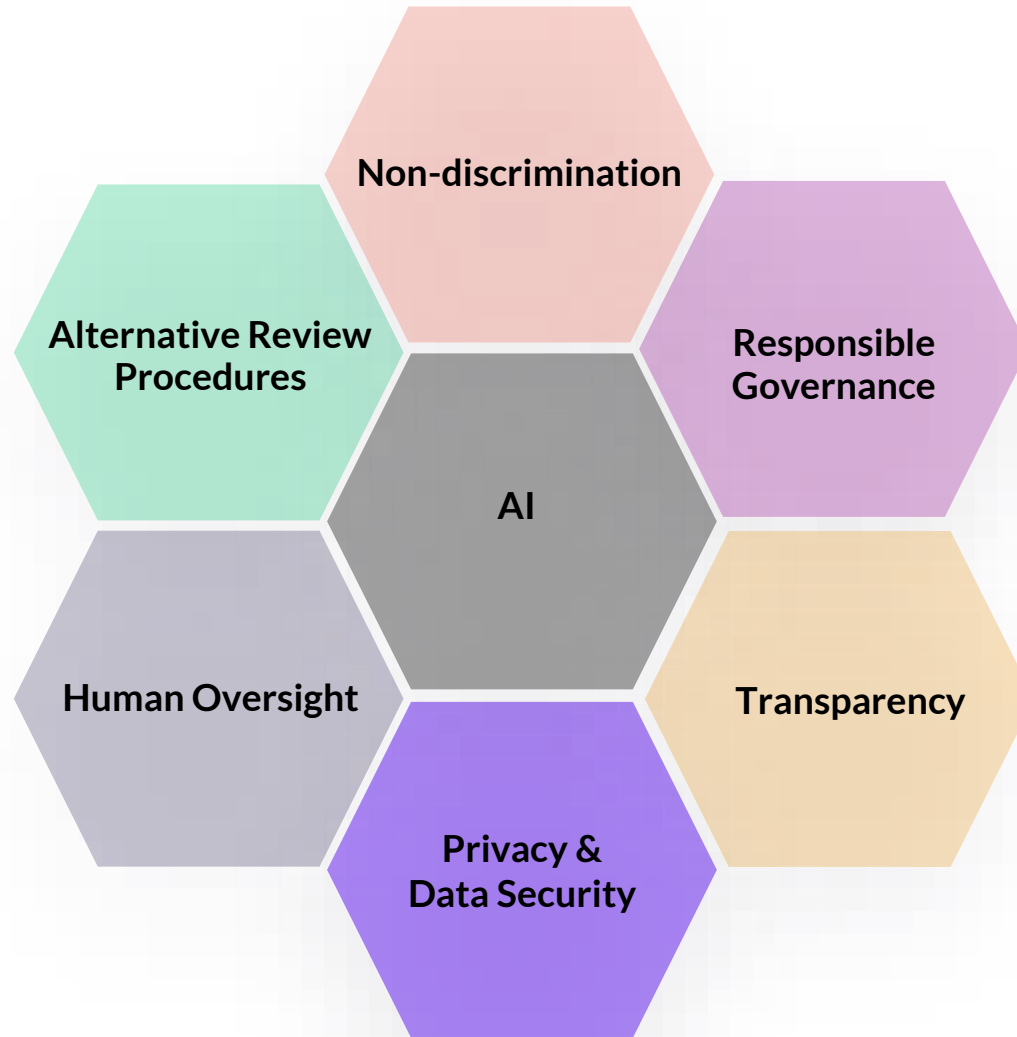
Understand Your Privacy Risks

Confidentiality	<ul style="list-style-type: none"> • Sensitive data, PI exposed in outputs • Sensitive data, PI accidentally introduced into model
Consent/Ethical Permissions	<ul style="list-style-type: none"> • Lack of consent and notice when scraping for training data • Varying legal definitions of publicly available information and acceptable bases of processing
Retention	<ul style="list-style-type: none"> • Privacy rights requests • Deleting data in the model w/out damaging model
Sharing	<ul style="list-style-type: none"> • Preventing data leaks • Ensuring data protection w/ AI service providers
Transparency & Explainability	<ul style="list-style-type: none"> • Unexplainable/unjustifiable outcomes • Unreliable outcomes
Contractual	<ul style="list-style-type: none"> • Knowing who is a controller vs processor
Fairness & Accuracy	<ul style="list-style-type: none"> • Hallucinations • Bias • Denial of rights

Practical Tips for AI Data Privacy Management

Follow Best Practices from AI Frameworks

- UNESCO's Recommendation on the Ethics of AI
- The OECD AI Principles
- The Ethics Guidelines for Trustworthy AI



Practical Tips for AI Data Privacy Management

Follow IT Risk Management Guidelines

1. Prepare

Identify risk mgmt. roles, establish an overall risk strategy, assess risk and risk tolerance.

2. Categorize

Determine adverse impact of the loss of confidentiality, integrity, and availability of the AI system and related information.

3. Select

Select baseline controls to apply, tailor them to the specific system, document controls.

4. Implement

Implement selected privacy and security controls.

5. Assess

Select team of assessors, develop an assessment plan, assess and report on findings, take remediation actions as necessary.

6. Authorize

Require senior official to determine whether controls are sufficient and privacy and security risk are acceptable.

7. Monitor

Continuously monitor and assess the system and controls.

NIST Special Publication 800-37
Revision 2

Risk Management Framework for Information Systems and Organizations

A System Life Cycle Approach for Security and Privacy

This publication contains comprehensive updates to the *Risk Management Framework*. The updates include an alignment with the constructs in the NIST Cybersecurity Framework; the integration of privacy risk management processes; an alignment with system life cycle security engineering processes; and the incorporation of supply chain risk management processes. Organizations can use the frameworks and processes in a complementary manner within the RMF to effectively manage security and privacy risks to organizational operations and assets, individuals, other organizations, and the Nation. Revision 2 includes a set of organization-wide RMF tasks that are designed to prepare information system owners to conduct system-level risk management activities. The intent is to increase the effectiveness, efficiency, and cost-effectiveness of the RMF by establishing a closer connection to the organization's missions and business functions and improving the communications among senior leaders, managers, and operational personnel.

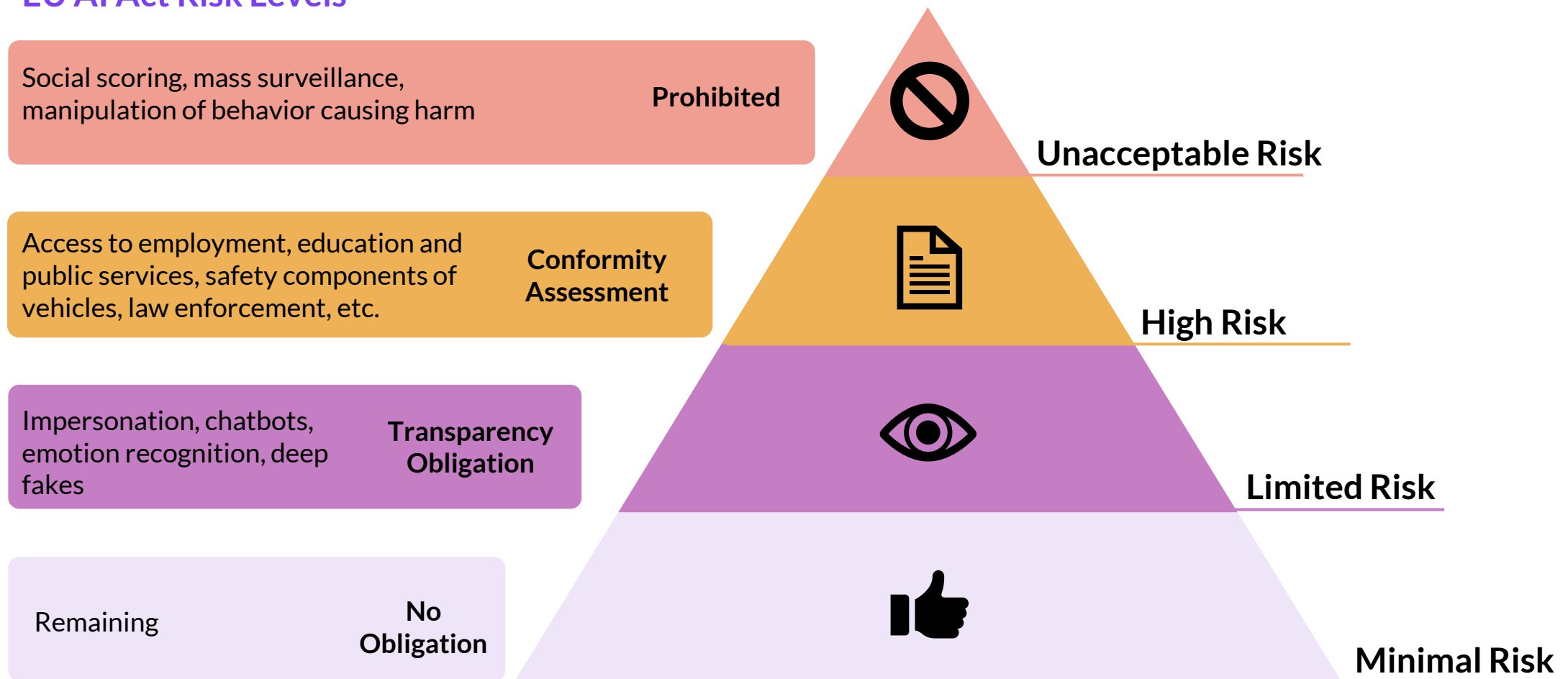
JOINT TASK FORCE

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-37r2>

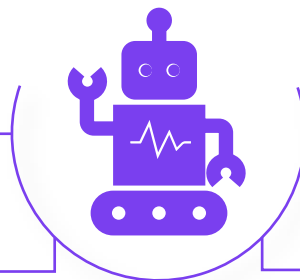
NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Risk Assessments

EU AI Act Risk Levels



Operationalizing Privacy-Aware AI



Establish a Legal Basis for Data Processing

- Personal data used in an AI model must be in compliance with privacy laws
- Review what personal data is OK prior to use
- Delete data no longer needed in the model.

Conduct PIAs & Other Assessments

- Review AI initiatives before launching
- Leverage existing PIA processes
- Review vendors & security measures

Develop an AI Policy

- Create a company AI policy on what type of data is and isn't OK to be used.
- Train employees using department examples
- Socialize the policy with departments
- Roles and responsibilities
- Disclosures

Be Aware of Automated Decision-Making, Profiling Requirements

- Evaluate the input and decision models
- If appropriate, engage in third party testing
- Align automated decision types to applicable privacy laws

How Do Developers... Develop?

- Data Minimization
- AI by Design
- Map for Traceability
- Risk Assessments

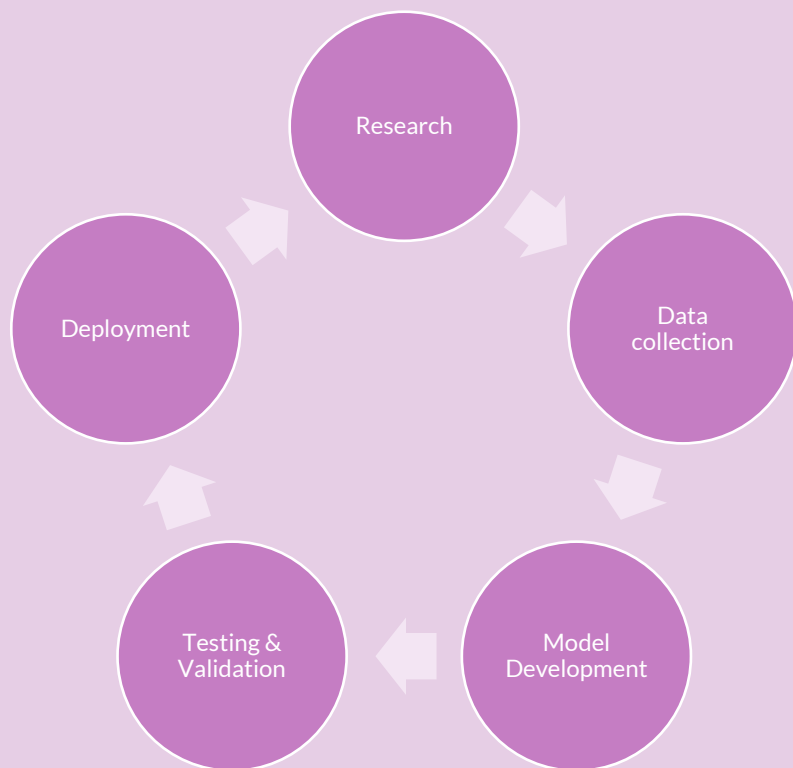
Before you've got the data

Once you've got the data

- Secure the Data
- Red Team
- Scoring for Fix Prioritization
- Education
- Audit

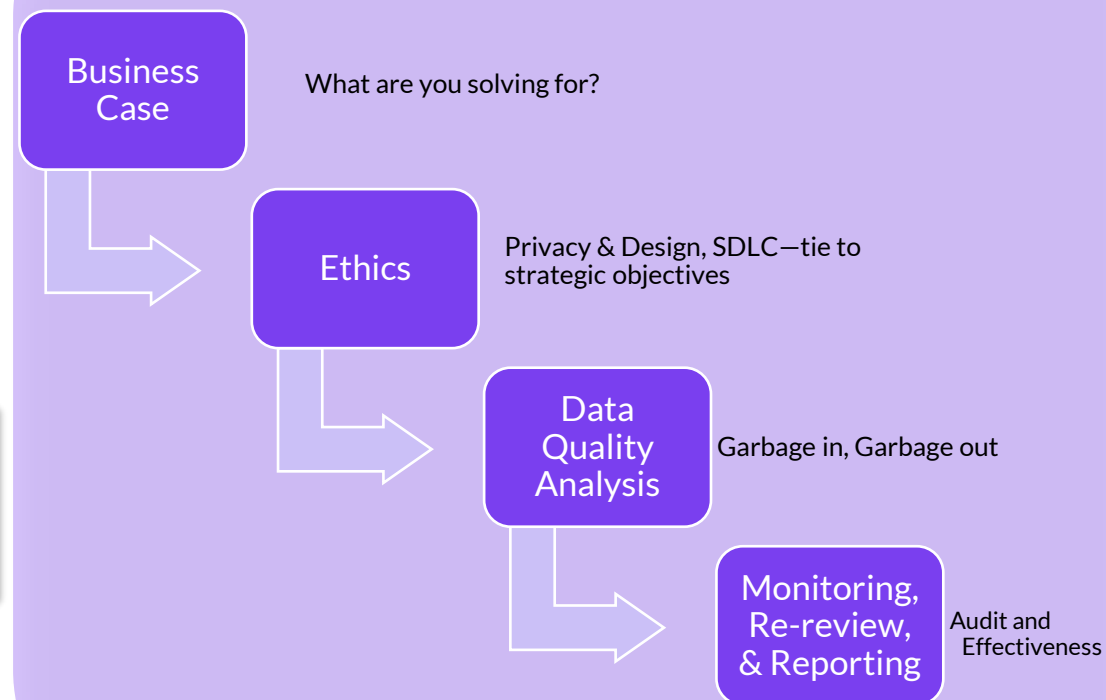
AI Development Lifecycle

Design & Deployment Workflow



Know
Your
Data

AI Ethics & Compliance Workflow



AI Audits

- Garbage in, Garbage Out
- Bias
- Inaccuracy of Data
- Incomplete Data
- Association Bias

01

Code Audits

02

Scraping Audits

03

API Audits

04

Sock puppet audits

05

User surveys

06

Crowd-sourced audits

Techniques for Data Privacy & Protection

The Right to Be Forgotten & DSARs

- Deleting data isn't easy with current solutions.¹
- “Machine-unlearning” techniques are being explored, like SISA (Sharded, Isolated, Sliced, and Aggregated training).²

Protecting PI & Securing Trust

- Privacy-enhancing technologies like differential privacy can allow AI to use datasets without exposing PI contained within.³
- Content filtering techniques sit between the AI and end user, filtering out PI before it reaches the user or is ingested by the model.⁴

These are emerging techniques—building a homegrown AI model that incorporates them may be a challenge.

1. Right to be Forgotten in the Era of Large Language Models: Implications, Challenges, and Solutions
(Zhang et al., 2023)

2. Machine Unlearning (Chandrasekaran et al., 2020)

3. More Than Privacy: Applying Differential Privacy in Key Areas of Artificial Intelligence (Zhu et al., 2022)

4. Contesting algorithms: Restoring the public interest in content filtering by artificial intelligence (Elkin-Koren, 2020)

Checklist

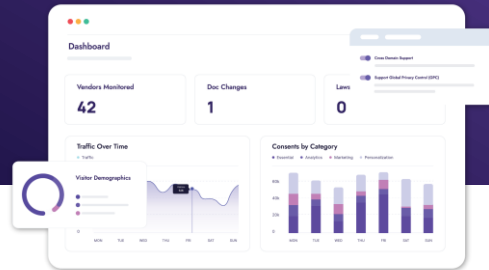
Questions to ask

- What data are you processing?
- What's your role?
- What's your legal bias?
- How are you using the data?
- Are automated decisions being made?
- Who are you sharing it with?
- How will you manage your risks?

What to do

- Verify results with other sources;
- Use human judgment about the AI's conclusions; and
- Disclose any use to others
- Perform risk assessments
- Map data
- Review your consents and permissions

Stay In Touch and Learn More!



[Schedule a Demo](#)



[Check out the Osano Blog](#)



[Contact Red Clover Advisors](#)



Q&A

Ask your most pressing AI & data privacy questions.



Thank You!

A collection of decorative geometric shapes in the bottom-left corner, including a large pink-to-orange gradient arc, a white hexagon outline, and several smaller orange, purple, and pink circles and polygons.

osano

Web Conference Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

Click here: **IAPP TO ADD SURVEY LINK HERE**

Thank you in advance!

For more information: www.iapp.org

Attention IAPP Certified Privacy Professionals:

This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your CIPP/US, CIPP/E, CIPP/A, CIPP/C, CIPT or CIPM credential worth 1.0 credit hour. IAPP-certified professionals who are the named participant of the registration will automatically receive credit. If another certified professional has participated in the program but is not the named participant then the individual may submit for credit by submitting the continuing education application form here: [submit for CPE credits](#).

Continuing Legal Education Credits:

The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body's rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of programming.

For questions on this or other
IAPP Web Conferences or recordings
or to obtain a copy of the slide presentation please
contact:

livewebconteam@iapp.org