AI Governance, Data Protection, and Compliance: Strategies for Governance and Risk Management

May 9, 2024

relyanceai

Introduction

This panel session explores the intricate balance between AI innovation, data privacy, and regulatory compliance. It covers strategies for governance and risk management in AI-driven environments, focusing on safeguarding sensitive information and mitigating risks. The session aims to empower participants to guide their organizations in responsibly harnessing AI, ensuring data privacy, and meeting regulatory requirements.

Panelists

Introduction

Leila Golchehreh
Co-Founder &
Chief Strategy Officer

Driving strategy at Relyance AI with a focus on AI governance.

Jacqueline Cooney
Partner

Specializing in data privacy and security at Arnall Golden Gregory.

Charlotte Jones
Senior Director, Head of Privacy & Product Legal

Leading product privacy and regulatory legal efforts at Five9.

Lena Ghamrawi
Senior Privacy Counsel & DPO

Ensuring privacy compliance at Quora and advising on data protection.

This panel brings together industry leaders with diverse expertise in AI governance, data protection, and compliance.

Meet Charlotte Jones, Jacqueline Cooney, Leila Golchehreh, and Lena Ghamrawi.

relyanceai

Agenda

Introduction

Panelists' Introduction

Building an AI Governance Program In-House

Assessing Data Training For In-House Counsel

Using AI Governance to Support Privacy Programs

AI Governance in Agreements

Consumer vs. Enterprise AI Considerations

Balancing AI Innovation with Compliance & Collaborative Strategies

Impact Assessments for AI Deployments

Managing Vendor Risks in AI

Ethical Dilemmas in AI

Conclusion

relyanceai

Meeting the Moment: Building an AI Governance Program In-House

- Start by understanding AI use within your own product and company. Identify areas of AI application (e.g., employee use, HR functions).
- Gain comprehensive knowledge of all vendors involved. Determine who is developing AI products and assess existing vendors with new AI offerings requiring vetting.
- Evaluate changes in data usage. Determine if companies allow vendors to use their data for product improvement and recognize heightened standards for data usage transparency and risk mitigation.
- Establish an AI governance program.
    - Verify vendors' compliance with data usage regulations and ensure transparency in data handling practices.
    - Implement safeguards to mitigate potential risks and adverse outcomes.
    - Tailor the AI governance program to address specific risks and establish protocols for risk management and incident response.

When Training on Data is Acceptable

Reviewing the training data: Identify the data itself and the source. Ensure it is compatible with pertinent laws, regulations, and company policies regarding data privacy and security.

Verifying accuracy: Confirm that the training data is current and its processing accurately reflects prevailing legal and regulatory requirements.

Assessing comprehensiveness: Determine if training on data adequately addresses various scenarios and potential risks associated with data handling.

Monitoring compliance & policy implementation: Implement mechanisms to track data training and ensure ongoing adherence to data policies and procedures, especially in the areas of IP, data protection, and when evaluating the terms of service and other

Evaluating effectiveness: Is the data going to be effective when building the model? Will it serve its intended purpose?

Using AI Governance to Support Privacy Programs

Strategic Importance of AI Governance

- Highlight the critical importance of AI governance in mitigating ethical and legal risks associated with AI technologies.
- Emphasize the need for robust data privacy measures within AI systems to maintain trust with customers and regulatory compliance.
- Position AI governance as a strategic imperative to enhance data protection frameworks, aligning with evolving privacy regulations.

Budget Justification

- Demonstrate the potential consequences of inadequate AI governance, such as data breaches or misuse, which could incur significant financial and reputational damage.
- Present AI governance as an opportunity to strengthen organizational resilience and competitiveness by fostering responsible AI innovation.
- Propose leveraging AI governance initiatives as a justification for securing additional privacy budget, enabling comprehensive safeguards and proactive risk management.

AI Governance in Agreements

Key Considerations

- Clearly define roles and responsibilities regarding AI development, deployment, and data management.
- Incorporate data protection provisions outlining data ownership, usage rights, and confidentiality measures.
- Address liability, indemnification, and compliance with regulations, including provisions for audits and certifications.

Ensuring Compliance with Regulations

- Require adherence to relevant legal and industry standards, and include provisions for audits and compliance certifications.
- Specify obligations for AI development, deployment, and data management in alignment with data protection regulations.
- Establish protocols for disclosing AI algorithms, data sources, and decision-making processes to ensure transparency and accountability.

How do AI considerations shift as they relate to consumers v. enterprise organizations?

- Focus on user experience and user expectations
- Increase transparency. Add disclosures beyond Privacy Policy
- Follow data purpose principle. Don’t use existing data to train without affording user rights
- Contractually limit third party vendor’s ability to train on user data
- B2B customers - More probing and proof required, long evaluation/RFP processes where they ask about your AI governance processes
- B2C users - One-sided relationship we set policies and proclaim them, offering a notice period and an opportunity to no longer use the service

Strategies

Balancing AI Innovation with Compliance

Continuous Adaptation

- Embrace continuous adaptation: Recognize achieving full compliance is ongoing due to evolving regulations; prioritize regular assessment and adjustment of strategies. Prioritize implementing technology to assist. Forms + surveys are no longer effective.

Regulatory Integration

- Integrate regulatory considerations into development: Design AI initiatives with regulatory requirements in mind from the outset to minimize rework; document processes and decisions within standard development frameworks.

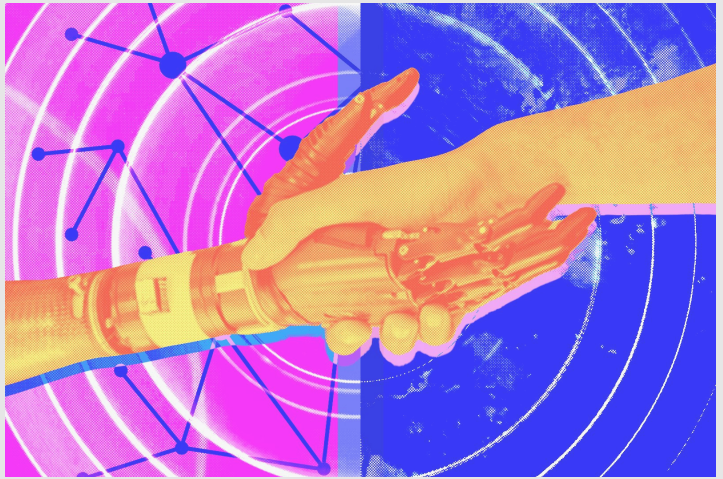
User Experience Enhancement

- Enhance user experience through transparency and choice: Prioritize user-centric design by providing transparent information and empowering users with meaningful choices, fostering trust and engagement.

Collaborative AI Governance Programs & Strategies

Internal Collaboration

- Educate executives and relevant teams on AI governance principles and requirements.
- Align on priorities and risk appetite to ensure strategic alignment and decision-making cohesion.
- Create internal guidelines with concrete examples for clear direction on AI governance implementation.
- Provide clear instructions to engineers, assuming no legal knowledge, to facilitate compliance with AI governance standards.
- Implement technology to help assist with the program.



Impact Assessments for AI Deployments

Objectives and Scope

Define the goals and scope of the impact assessment, evaluating ethical, legal, and societal implications of AI deployments.

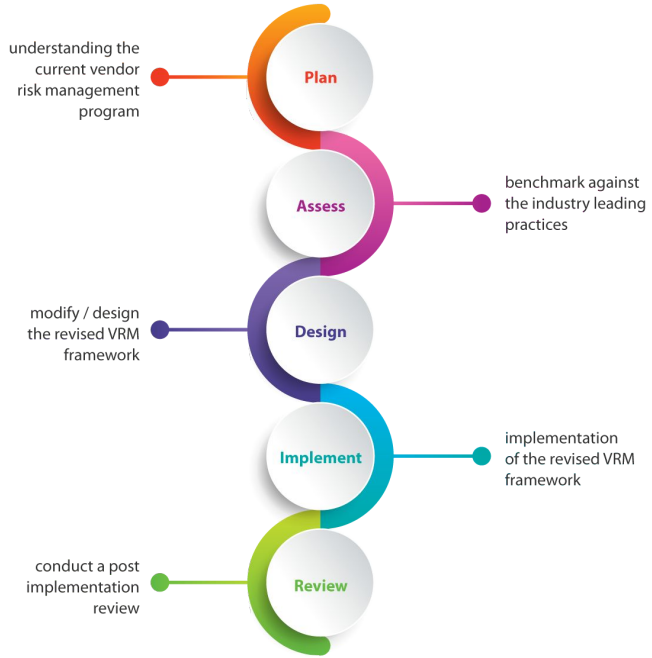
Risk and Benefit Analysis

Conduct a thorough analysis of risks and benefits associated with AI deployments, addressing bias, fairness, privacy, accountability, and transparency. Implement technology to assist on a continuous basis.

Transparency and Accountability

Foster transparency in AI decision-making processes, promote accountability for outcomes, and establish mechanisms for continuous monitoring of ethical, legal, and societal implications, including by implementing tooling.

Managing Vendor Risks in AI



Vendor Risk Management

- Develop vendor review process; integrate product, security, privacy, and legal teams
- Conduct safety testing; determine risk areas and level; add additional safety measures
- Contractually and technically limit what vendor can do with your users' data.
- Track what the vendor is doing using technology which continuously monitors vendor activities.
- Address liability and indemnification: Allocate responsibility for AI-related risks, including potential harm or regulatory violations, and outline procedures for resolving disputes and providing indemnification.
- Facilitate collaboration and communication: Foster open dialogue between parties to address emerging AI governance challenges and adapt contractual arrangements accordingly.

relyanceai

Ethical Dilemmas in AI

Addressing Ethical Dilemmas

- Conduct quality control and safety testing to understand limitations of AI models.
- Get involved in the vendor vetting process and internal product development to address ethical risks. Use AI technology to accurately assess vendor data processing).
- Set expectations with end users and enforce usage guidelines to ensure responsible AI deployment.

Aligning Objectives and Consequences

- Ensure AI objectives align with ethical standards and mitigate unintended consequences.
- Promote transparency in AI development and decision-making processes to highlight potential issues.
- Implement ethical guidelines and standards throughout the AI lifecycle to foster trust and mitigate risks.

More Information

EU AI Act

OECD Principles on AI Governance

ISO Standards on AI Governance

NIST Framework

relyanceai

Conclusion

The panel explored the complex interplay between AI innovation, data privacy, and regulatory compliance. Key themes included the need for comprehensive AI governance and the importance of aligning AI initiatives with privacy principles and regulatory requirements. The panel concluded by underscoring the critical importance of effective AI governance and compliance by way of continuous monitoring of an organization's technology stack.

Thank you.

relyanceai

Panelists

Connect with us!

Leila Golchehreh
Co-Founder &
Chief Strategy Officer

leila@relyance.ai

Jacqueline Cooney
Partner

Jacqueline.Cooney@agg.com

Charlotte Jones
Senior Director, Head of Privacy
& Product Legal

charlotte.jones@five9.com

Lena Ghamrawi
Senior Privacy Counsel &
DPO

lghamrawi@quora.com

relyanceai