How can the compliance officer be intelligent about AI?

Deborah Lynne Adleman
US & Americas Data Protection Leader
Ernst & Young LLP
deborah.adleman@ey.com

Disclaimer

► The views expressed by the presenters are not necessarily those of Ernst & Young LLP or other members of the global EY organization.
► These slides are for educational purposes only and are not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.
Today's topics

1. AI: the lingo and the landscape
2. AI: risks — visible and invisible
3. AI: an intelligent road map for the compliance officer

---

AI: the lingo and the landscape

1. AI is confusing, even to experts.
2. AI is a form of automation.
3. AI can be a capability or consumed as a service or feature.
4. AI is not IT; IT is more applied than implemented.
Every challenge in the world, and in business in particular, is an opportunity for AI.

- 73% of CEOs are already adopting or planning to adopt intelligent automation or machine learning in the near term (two years).
- 85% of AI projects through 2020 will deliver erroneous outcomes due to bias in data, algorithms or development teams.
AI: risks — visible and invisible

IT performance is defined and measured mostly by observable vectors.

- Access: “I can’t get into the system; could the server be offline?”
- Loading speed: “This image is taking too long; is something wrong?”
- Bug: “I am getting an error message; we may need to roll out a patch.”

AI systems perform human-like cognitive functions — they see, listen, engage, learn, navigate, etc. — so they fail differently.

- Sometimes they fail in observable, if not tragic ways: a self-navigating vacuum falls down the stairs, or an autonomous vehicle slams into people, killing them.
- But sometimes, the AI ‘fails’ in unobservable ways due to operational shifts.
- While a traditional IT dashboard may be green — the AI system is on-line, accessible, taking inputs and generating outputs, enabling a larger system that supports key business processes — it may be quietly failing to operate in a trustworthy, reliable way.
- There won’t always be a “crash” to indicate AI failure.

European Commission issues ethics guidelines for trustworthy AI, April 2019

AI brings a balancing act between regulation and innovation

- General Data Protection Regulation
  - GDPR includes rules related to profiling and automated decision-making.
- Country-level regulations
  - GDPR includes rules related to profiling and automated decision-making.
AI: risks — visible and invisible

Using AI to see like humans

Researchers demonstrated using a few-pixels attack that deep neural networks can be fooled by modifying a well-placed pixel. Imperceptible to the human eye, these changes significantly altered the output produced by the AI models.

Using AI to think like humans

AI algorithms used by US courts to profile a defendant’s risk of committing more crimes have raised concerns about inherent bias toward minorities. There has been a call for greater transparency in AI models used by public institutions.

Chatbots designed to read, interpret and adapt to written language have demonstrated bigoted and racist behavior when performance parameters were too narrowly focused on grammatical correctness and not “political” correctness.

How can the compliance officer be intelligent about AI?

AI: risks — visible and invisible

01 How will employees or citizens respond?
02 How will they influence employees’ day-to-day activities?
03 How do you consider all legal, ethical and social ramifications are not overlooked before implementing AI within your organization?

How can communication programs win employee approval?

How can ethics and legal issues be dealt with at the start of any project?

How can job consequences be evaluated?
The AI's outcomes are aligned with stakeholder expectations and perform at a desired level of precision and consistency.

When interacting with an AI, an end user is given appropriate notification and an opportunity to select their level of interaction.

Inherent biases arising from the development team composition, data and training methods are identified and addressed through the AI design.

The data used by the AI system components and the algorithm itself is secured from unauthorized access, corruption and/or adversarial attack.

The AI's training methods and decision criteria can be understood, are documented and are readily available for human operator challenge and validation.

**Ethics**
- Does this AI comply with ethical and social norms, including your own corporate values?

**Social responsibility**
- Does this AI have larger social implications that could negatively affect society or human well-being?

**Accountability**
- Is there clarity on how this AI operates, its inputs and the decisions it's supporting?

**Reliability**
- Can we rely upon this AI to make decisions that affect people and our business?
AI: an intelligent road map for the compliance officer

The six domains outlined below play a critical role in successful implementation of an AI program.

Policy
Alignment to process, risk and control framework, user access management, disaster recovery/resilience plan

Governance
Strategy, standards, program risk, vendor risk, monitoring, oversight

Technology
Cyber threat detection, incident response, threat intelligence, data privacy, code flows, authentication, post-deployment review

Process
Process control logs, repository of business rules and algorithms, exception scenarios and decision-making, documenting process/standard operating procedures

Change management
Stakeholder engagement across teams (IT, risk, business), institutionalization of an effective communication protocol, driving focus toward value-creating activities

Controls
Audit trails, early-warning signs, controls to monitor performance, prevent sensitive data, assurance on effectiveness of controls

Traditional risk and control categories apply to AI technology, but each brings its own unique risk considerations.

Intelligent automation advisory board
A multidisciplinary advisory board providing independent advice and guidance on ethical considerations in intelligent automation development
  • Advisors should be drawn from ethics, law, philosophy, technology, privacy, regulations and science. The advisory board should report to and/or be governed by the Board of Directors.

AI ethical design standards
Intelligent automation design policies and standards for the development of AI, including updates to the code of conduct and creation of intelligent automation design principles
  • The intelligent automation design standards should define and govern the governance and accountability mechanisms to safeguard users, follow social norms and comply with laws and regulations.

AI inventory and impact assessment
An inventory of all RPA and AI agents, including key details of the agents, that is generated using software discovery tools
  • Each agent in the inventory should be subject to an impact assessment to assess the risks involved in its development and use.

Validation tools
Validation tools and techniques to confirm the agents are performing as intended and are producing accurate, fair and unbiased outcomes
  • For AI, these tools can also be used to monitor changes to the algorithm’s decision framework.

Awareness training
Educating executives and intelligent automation developers on the potential legal and ethical considerations for the development of RPA and AI, and their responsibility to safeguard impacted users’ rights, freedoms and interests

Independent audits
Undergoing independent RPA as well as AI audits by a third party against your intelligent automation and technology policies and standards, and international standards, to enhance users’ trust in your environment
  • An independent audit would evaluate the sufficiency and effectiveness of the governance model and controls across the RPA and AI life cycle, from problem identification to model training and operation.
AI Discussion

Deborah Lynne Adleman
US and Americas Data Protection Leader
Ernst & Young LLP
deborah.adleman@ey.com