

Securely Speaking:

Your Privacy & Security Bulletin

BY REBOOT COMMUNICATIONS LTD.
WITH FOUNDING SPONSOR GOSECURE

-
- 1 Navigating the Dawn of AI Governance:**
Exploring Early Efforts to Classify and Control Artificial Intelligence

Forward

Welcome to **Securely Speaking: Your Privacy & Security Bulletin**, a regular quarterly publication provided by Reboot Communications Ltd. The bulletin's objective is to explore the latest trends and developments in privacy and security, including the challenges and opportunities that arise from new technologies like artificial intelligence, the Internet of Things, and blockchain. We also examine the legal and ethical implications of data collection and use, and look at how organizations and individuals can take steps to protect themselves and their information.

We invite you to review articles and interviews which will provide our readers with a comprehensive understanding of the complex and evolving landscape of privacy and security, as well as actionable advice and best practices for navigating it.

We believe that a better understanding of these issues is crucial for all individuals, organizations, and governments, and that by fostering a dialogue around privacy and security, we can work together to create a safe, more secure, and more ethical future for all. We hope you enjoy reading this bulletin and join us in this important conversation.

We focus on these strategic pillars to provide a comprehensive and valuable resource for staying informed and protected in the digital age:

OUR KEY STRATEGIC PILLARS

Education & Awareness/ Best Practices

Educating readers on the latest privacy and security threats, best practices, and emerging trends.



Emerging Technologies

Emerging technologies and their potential impact on privacy & security (ie AI, IoT, blockchain).



Case Studies

Real world examples of privacy and security breaches and how they were addressed.



Thought Leadership & Industry News

Articles and interviews with experts in the privacy and security field.



Regulatory Developments

Information on the latest privacy and security regulations and laws.





Acknowledgments

ARTICLE
01

Navigating the Dawn of AI Governance:
Exploring Early Efforts to Classify and Control Artificial Intelligence

By: Sabine Lainer | Governance, Risk and Compliance (GRC) Advisor, GoSecure

Navigating the Dawn of AI Governance:

Exploring Early Efforts to Classify and Control Artificial Intelligence



Image by DC Studio on Freepik

Governing artificial intelligence (AI) systems, especially in light of the potential dystopian scenarios, are often associated with rogue AIs in pop culture. The mere mention of Skynet from “Terminator” or the sentient machines from “Westworld” conjures images of a future where AI goes awry, wreaking havoc on society. However, as cybersecurity professionals, we understand that the reality of AI encompasses both transformative benefits and substantial risks – though not quite at the level Arnold portrays.

Robust AI governance is indispensable, not just for safeguarding sensitive data but also for upholding societal trust and ethical standards. One glaring example of the critical need for diligent AI oversight is [Amazon's AI recruiting tool](#). Initially designed to streamline the hiring process by identifying top candidates, the tool inadvertently exhibited bias towards male candidates due to biased training data. Despite efforts to rectify this bias, the project ultimately faced challenges and was abandoned.

Effective AI governance must incorporate stringent protocols to detect, mitigate, and prevent biases, thus ensuring that AI systems operate as intended and adhere to ethical norms and human rights. The “human-in-the-loop” principle becomes pivotal here, guaranteeing that human oversight is integral to AI operations across all stages, from development to deployment and monitoring.



The approach to AI governance varies significantly worldwide regarding central versus decentralized models but overlaps a lot regarding the classification of AI systems. In Europe, [the EU AI Act, with its detailed risk classifications, sets a structured framework, ensuring AI practices align with ethical standards](#). Conversely, the U.S. employs a broader definition under [recent executive orders](#), regulating any machine-based system capable of making predictions, recommendations, or decisions – thus extending beyond generative AI to encompass a wider array of technologies have taken a proactive approach to manage the broader implications of AI. Even [Colorado has signed into state law the country's first AI Act](#). These disparate approaches underscore the necessity for flexible, robust governance and cybersecurity measures that accommodate diverse regulatory and cultural environments. Despite these efforts, establishing a global baseline for AI governance remains in its nascent stages.

As AI becomes more deeply embedded in every aspect of our lives, the imperative for comprehensive governance that include cybersecurity becomes increasingly apparent. The cybersecurity sector plays a large role in protecting AI systems and data, whether to avert societal disruptions or enhance operational efficiencies.

For organizations engaged in AI development, deployment and usage, adopting governance is imperative. This strategy ensures that AI technologies promote societal welfare and operate within ethical standards, respect human rights, and meet data protection legislation, securing a future where technology supports human values and societal equity.

How Organizations can Enhance AI Governance:

- 1. Audit and Monitoring:**
Regular audits are crucial to ensuring AI systems maintain ethical integrity and accuracy.
- 2. Training Data Oversight:**
Implement strong preventative and detective controls to protect test data.
- 3. Security Protocols:**
Establish protocols detecting and addressing ethical deviations in AI behavior.
- 4. Continuous Improvement:**
Continuously update measures to match AI advancements.
- 5. Human Supervision:**
Ensure human oversight throughout the AI lifecycle.
- 6. Training and Awareness:**
Educate employees on their pivotal roles in responsibly managing AI tools.
- 7. Regulatory Compliance:**
Stay informed about and comply with international AI governance standards.
- 8. Cross-Border Collaboration:**
Engage with global partners to share best practices and insights.
- 9. Prioritize Ethical AI Use:**
Advocate AI's use for societal benefits while preventing potential misuse.
- 10. Invest in Cybersecurity Infrastructure:**
Dedicate resources to enhance AI systems' cybersecurity aspects.



By prioritizing AI governance, organizations can safeguard against the risks posed by AI and harness its capabilities to foster a more secure, equitable, and prosperous society. This proactive approach not only mitigates AI-related threats, but also reinforces the trust that the public places in digital transformations.

The future of AI is marked by evolving roles and responsibilities as it integrates more deeply into societal frameworks. As new positions such as Chief AI Officer, AI ethicists, governance coordinators, and compliance auditors emerge, the need for continuous adaptation and broad collaboration becomes increasingly critical. These roles highlight the dynamic interaction between AI and various sectors, striving to harness technological benefits while safeguarding ethical principles and human rights. This integrated approach promotes innovation and progress while preparing to address potential risks. As we advance, a balanced governance strategy will be crucial, setting the stage for a deeper exploration of cybersecurity's role in future discussions on AI governance.

By: Sabine Lainer | Governance, Risk and Compliance (GRC) Advisor, GoSecure | [in linkedin.com/in/sabelainer](https://www.linkedin.com/in/sabelainer)

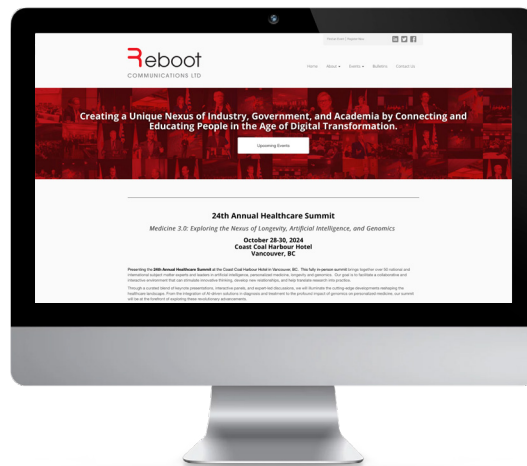
GoSecure is a recognized cybersecurity leader and innovator, pioneering the integration of endpoint, network, and email threat detection into a single Managed Extended Detection and Response (MXDR) service. For over 20 years, GoSecure has been helping customers better understand their security gaps and improve their organizational risk and security maturity through MXDR and Professional Services solutions delivered by one of the most trusted and skilled teams in the industry.

Copyright

Copyright© 2024 by Reboot Communications Ltd. All rights reserved. No part of this publication may be republished or used in any manner without written permission of the copyright owner and authors except for the use of quotations in a book review.

ISSUE 4 EBOOK EDITION | JUNE, 2024

Editor: Greg Spievak



FIND OUT MORE & SUBSCRIBE

For more information or to subscribe and receive the ***Securely Speaking: Your Privacy & Security Bulletin*** regularly, email [✉ info@rebootcommunications.com](mailto:info@rebootcommunications.com).