Watch Out!
Governance is in AI Waters
Do You Have Your Lifejacket?

Kimberly “KJ” Haywood

NOMAD CYBER CONCEPTS

Executive Summary

Why the Criticality for AI Literacy?

As Artificial Intelligence (AI) continues to transform industries globally, it's more important than ever for businesses to understand and manage its impact. The rapid pace of AI development has created a significant gap between technological advancements and the regulations designed to govern them. With over 20 years of experience in cybersecurity, governance, risk, and compliance, I've come to realize that AI literacy is critical for businesses striving to stay secure, ethical, and compliant.

AI is more than just a technology; it's reshaping industries, workflows, and entire economies. Businesses looking to remain competitive must invest in AI literacy across their organizations. This enables them to navigate the complexities of AI while leveraging its immense potential.

From my experience, organizations should focus on four key areas of AI literacy:

- **Mitigating Risk**: Understanding AI's limitations and vulnerabilities is essential to reduce exposure to threats.
- **Adaptability**: Staying agile with evolving regulations and standards is crucial to leading in compliance and innovation.
- **Fostering Responsible Innovation**: AI literacy ensures ethical use, reducing negative impacts while maximizing benefits.
- **Maintaining a Competitive Edge**: AI-literate businesses will lead in their sectors by strategically leveraging AI for growth.

At Nomad Cyber Concepts, we specialize in guiding businesses through these challenges, helping them leverage AI's potential while staying secure and compliant.

Watch Out! Governance Circling in AI

In August 2023, my exploration into AI Governance was published, featuring a notable subsection titled "Governance Circling in AI's LLM Waters." As serendipity would have it, within only five months, "Circling" rapidly evolved into a Tidal Wave.

The original article advocated for a holistic strategy to incorporate security and governance frameworks, highlighting a multi-faceted approach that included Secure Software Development Life Cycle (SDLC) adaptations, ethical and privacy considerations, and compliance with technical standards such as NIST AI RMF 1.0 and OWASP.

Over the past 18 months, we have all observed explosive growth in this area, with global legislators racing like the DC Comic character "The Flash's" alter-ego, against what seemingly is an unprecedented pace of Artificial Intelligence (AI) advancements; all to establish regulatory guardrails. This urgency only emphasizes the vital need for an "AI Governance Life Jacket" to navigate these tumultuous waters.

A Small Step Back in Time...

Let’s take a small step back, and bring you up to speed on the pace of things occurring let's start with UX (User Experience).

Let’s take a step back to review the current pace of developments, starting with UserExperience (UX). According to Sujan Sarkar’s analysis in “AI Industry Analysis: 50 Most Visited AI Tools and Their 24B+ Traffic Behavior,” AI tools received a total of 24 billion visits between September 2022 and August 2023. Of the 3,000 AI tools analyzed, ChatGPT accounted for 60% of the overall traffic. Notably, ChatGPT, Character AI, and Google Bard saw net increases in traffic by 1.8 billion, 463.4 million, and 69 million visits, respectively. During this 12-month period, the AI industry averaged 2 billion visits per month.

The study also revealed that the United States contributed 5.5 billion visits, representing 22.62% of the total traffic, while European countries collectively accounted for 3.9 billion visits.

This data further reinforces the urgency for global legislators to rapidly establish regulatory frameworks. As technology practitioners and corporate stakeholders, we must commit to governance oversight, recognizing that AI and ML advancements are unlikely to slow down.

This necessity stems, in part, from growing concerns about AI’s potential societal impacts, including its influence on political elections, medical devices, and automotive production. Ethical concerns, algorithmic bias, privacy issues, and the governance of autonomous decision-making processes also drive the call for swift legislative action.

Regulatory Initiatives

Simultaneously, as AI tool usage skyrocketed from January to August 2023, we witnessed a parallel increase in regulatory initiatives, such as the Executive Order on AI in the U.S. and the adoption of the EU. With the U.S. and Europe at the forefront, global legislators have accelerated efforts to address challenges related to ethical usage, algorithmic bias, privacy, and control over autonomous decision-making.

This period only underscores the significant strides made towards reinforcing governance oversight, highlighting the necessity for your AI Governance Life Jacket.

Importance of the Life Jacket

AI advancements have emerged as one of the leading meta-forces of this century. However, the rapid push for new laws to regulate AI and ML technologies raises valid concerns. Human imperfection underscores the necessity of comprehensive security measures, doesn’t it?

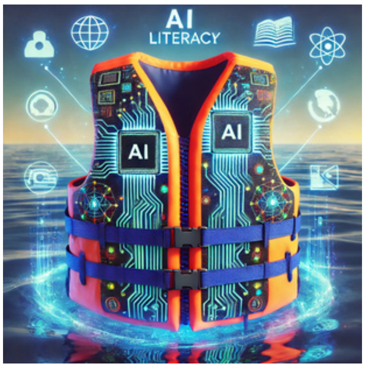
Historically, hastily implemented regulations have rarely served society’s long-term interests, often acting as temporary fixes. There is also skepticism about whether regulators fully grasp the complexities of AI and ML design and development.

Importance of the Life Jacket

The involvement of various stakeholders in the regulatory process—such as technology educators, social scientists, cognitive psychologists, and cybersecurity experts—is crucial. However, there's a looming concern about their ability to effectively comprehend the complexity of AI and ML systems and apply new laws and guidelines at the current accelerated pace, which may result in fragmented or inadequate regulatory frameworks that fail to address the complexities and risks inherent in these technologies.

It's essential to remember that this journey toward establishing AI governance, ethical standards, and safety regulations is very much in its infancy. Having an "AI Governance Life Jacket" is not only prudent but a strategic necessity. Leveraging expertise in security and compliance can help mitigate risks such as fines, penalties, or loss of contracts due to non-compliance. Being well-prepared for the challenges ahead is essential to navigating the complexities of AI and ML deployment while ensuring safety, fairness, and accountability.

AI Literacy Stitched into the Life Jacket



It is more critical than ever to recognize that a foundational understanding of AI and ML is becoming increasingly essential.

AI literacy is stitched into the fabric of the AI Governance Life Jacket, woven with three core elements: trust, security, and usage. These elements are intricately tied to the overarching goal of optimizing operations, improving workflows, and enabling more informed decision-making.

AI Literacy Stitched into the Life Jacket

Given the complexity of the field, it is widely acknowledged that AI presents a steep learning curve for many. If this is true, it follows that security professionals also face challenges in identifying key areas for protection, including privacy, data security, and ethical practices. This raises the question: how can organizations address the widespread lack of understanding regarding AI and ML across various departments?

A comprehensive understanding of AI requires distinguishing between Artificial Intelligence, Machine Learning models, Artificial Super Intelligence (ASI), Artificial General Intelligence (AGI), and the unique risks associated with each. Without a clear grasp of these fundamental concepts, navigating the complexities of drafting or assessing contracts, policies, and compliance requirements becomes a daunting task. A good starting point is familiarizing oneself with the specific terminology and frameworks involved.

To illustrate this, in an article entitled: "Teaching Artificial Intelligence Literacy: AI is for Everyone," written by Andrea Azzo, she interviews prominent leaders from elite institutions. One particularly enlightening interview was with Ken Holstein, an associate professor at Carnegie Mellon University's (CMU) Human-Computer Interaction Institute and director of the Co-Augmentation, Learning, and AI (CoALA) Lab at Northwestern University.

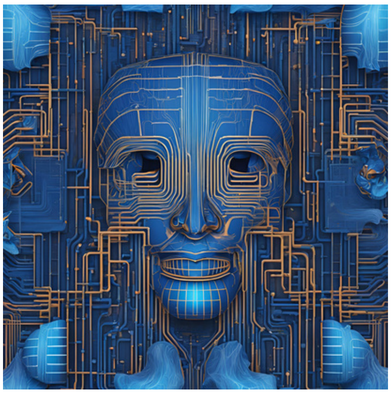
Holstein's insights into adult understanding of AI concepts, alongside Azzo's article, underscore the collaborative efforts of researchers to enhance AI literacy. CMU's CoALA Lab conducted workplace studies on interactions with AI-augmented tools. Holstein remarked during the interview, "... his group's research has found there is often little to no training aimed at helping workers learn how to use AI tools effectively and responsibly. Additionally, AI-based tools are often not designed to solve the right problems."

AI Literacy Stitched into the Life Jacket

Holstein continued, "These misunderstandings bring dangers, such as the risk of overreliance on AI recommendations." This misunderstanding often stems from poor AI literacy, which may indeed be prevalent in some cases. Nonetheless, the larger issue lies in ensuring that AI designs address the correct problems. Machine Learning models are just as capable of detecting bias in data as they are of being used for discriminatory practices.

Technology practitioners and other stakeholders should strongly consider developing an AI literacy initiative, focusing on educating and empowering all areas of the organization about the fundamentals and implications of AI technologies.

Final Thoughts



The "AI Governance Life Jacket" metaphor was intended to emphasize the necessity for strong governance and enhanced AI literacy amidst the rapid evolution of AI technologies. It advocates for trust, security, and responsible usage as key to managing AI's intricacies. Organizations can uphold ethical standards, compliance, and operational integrity by adopting strategic AI governance practices and fostering AI literacy.

This strategy equips businesses to navigate AI's challenges effectively and leverage its benefits responsibly.

Kimberly “KJ” Haywood, Principal CEO
Nomad Cyber Concepts
(4) Kimberly KJ Haywood | LinkedIn

Motto: “I live believing I can make a difference; I consider myself a Bridge Builder and Catalyst for Change”.

With over 25 years of experience across finance, technology, healthcare, and government sectors, Ms. Haywood has established and led management and security practices throughout her career, including her own firms; Knowledge Management & Associates, Inc., and now, Nomad Cyber Concepts, LLC.

Her expertise in Cybersecurity, Governance, Risk, and Compliance has driven successful collaborations with top organizations like USAA, Google, Bank of America, and Wells Fargo.

She currently serves on the Board of AI Connex as the Global Chief Governance and Education Advisor and is an Adjunct Professor of Cybersecurity at Collin College in Frisco, TX. Additionally, she contributed to the IAPP’s (a global privacy and governance organization) Artificial Intelligence Governance Professional (AIGP) Practice Exam. She has published articles on AI and is currently co-authoring a white paper on an AI Governance Framework. Her expertise in cybersecurity and governance has earned her recognition on international platforms.

To learn more about her advisory services, articles, or other resources, please visit her website at www.nomadcyberconcepts.com