IG and Artificial Intelligence

Andrew Ysasi, MS, CRM, IGP, CIGO, FIP, CIPM, CISM, PMP

Vice President, Advocacy for VRC

April 2024
Who is Andrew Ysasi?

- VRC Vice President, Advocacy since 2018
- ICRM Chairman 2023, Parts 1-6 Mentor, past Part 6 Grader, past Regent, and ICRM Mentor of the Year in 2020
- San Jose State University Masters of Archives and Records Administration (MARA) Instructor since 2018
- IG GURU Founder: Information Governance News in 2018
- Writer for Information Governance: Concepts, Strategies and Best Practices & ARMA's Information Governance Body of Knowledge (IGBOK)
- Certificate Data Analytics the Wharton School of the University of Pennsylvania
- Certificate Data Privacy Strategy from Cornell
- Masters in Administration from Central Michigan University and BS in Information Technology
AI Overview
AI Defined

AI is a highly interdisciplinary field broadly based on computer science, data science, natural sciences, humanities, mathematics, social sciences and others. Terms such as “intelligent”, “intelligence”, “understanding”, “knowledge”, “learning”, “decisions”, “skills”, etc. are used throughout the ISO Standard.

Research of AI includes aspects such as aspects including:
- learning, recognition and prediction
- inference, knowledge and language
- discovery, search and creation

AI Defined

A number of interesting features that are shared by some or all AI systems:

**Interactive** — inputs to AI systems are generated by sensors, or through interactions with humans, with outputs which can result in stimulating an actuator or providing responses to humans or machines. An example can be object recognition as a result of an AI system being presented with an image of an object.

**Contextual** — some AI systems can draw on multiple sources of information, including both structured and unstructured digital information, as well as sensory inputs.

**Oversight** — AI systems can operate with various degrees of human oversight and control, depending on the application. An example is a self-driving vehicle with varying levels of automation.

**Adaptive** — some AI systems are engineered to utilize dynamic data in real time and retrain to update their operation based on new data.

Machine Learning

Machine learning is a type of artificial intelligence (AI) that allows computers to learn without being explicitly programmed. It's like teaching a child new things, but instead of using words and examples, we use data. The computer takes in large amounts of data, analyzes it for patterns, and then uses those patterns to make predictions or decisions on new data.

Here's a simple analogy: imagine you're trying to teach a computer to identify a cat in a picture. You would show the computer a bunch of pictures of cats and pictures of other things, and the computer would try to find the patterns that make up a cat. Once it thinks it understands what a cat looks like, you can show it a new picture and ask it if it's a cat or not.

Source: Google Bard on 1/4/2024
Machine Learning

There are many different types of machine learning, but they can all be grouped into three main categories:

**Supervised learning:** This is where the computer is given labeled data, meaning that each piece of data has a pre-defined label (e.g., "cat" or "not cat"). The computer then learns from this labeled data to make predictions on new, unlabeled data.

**Unsupervised learning:** This is where the computer is given unlabeled data, and it has to figure out the patterns on its own. This is often used for things like clustering data points into groups or dimensionality reduction.

**Reinforcement learning:** This is where the computer learns by trial and error. It's given a task and a reward system, and it has to figure out how to achieve the task by trying different things and seeing what gets it the most reward.

Source: Google Bard on 1/4/2024
Machine Learning

Machine learning is used in a wide variety of applications, including:

**Image and speech recognition:** Facial recognition software, self-driving cars, and voice assistants all use machine learning to make sense of the world around them.

**Recommendation systems:** The recommendations you see on Netflix, Amazon, and other websites are powered by machine learning algorithms that learn from your past behavior.

**Fraud detection:** Credit card companies and banks use machine learning to detect fraudulent activity in real time.

**Medical diagnosis:** Machine learning is being used to develop new tools for diagnosing diseases, such as cancer and heart disease.

Machine learning is a powerful tool that is transforming the world around us. It's still a young field, but it has the potential to solve some of the world's most challenging problems.
AI at Work
AI and Chat

Chat GPT (Generative Pre-trained Transformer) by OpenAI

Google Chatbot Bard (named after Bard of Avon the storyteller from Shakespeare)

Source: englishlittomato.blogspot.com
What are concerns with Chat GPT? (Asked on 1/4/2024 at 9:35am EDT)

1. **Bias and Fairness**: Language models can inadvertently learn and reproduce biases present in the training data. This can result in biased or unfair responses, perpetuating stereotypes and reinforcing societal prejudices.

2. **Ethical Use**: There is a concern about the ethical use of language models for malicious purposes, such as generating harmful content, misinformation, or engaging in deceptive activities.

3. **Lack of Accountability**: The decentralized and open nature of the internet makes it challenging to trace the origin of content generated by language models. This lack of accountability raises concerns about the potential misuse of the technology.

4. **Security Risks**: Language models can be vulnerable to adversarial attacks, where intentional manipulations of input can lead to unexpected or incorrect outputs. This poses a risk in scenarios where the model’s responses are crucial, such as in chatbots handling sensitive information.

5. **Privacy**: As language models are trained on vast amounts of data, there are concerns about the potential disclosure of sensitive information during interactions. Striking a balance between providing useful responses and preserving user privacy is an ongoing challenge.

6. **Dependence on Training Data**: The quality and diversity of the training data significantly influence the performance of language models. If the training data is incomplete or biased, the model may not generalize well to diverse user inputs.

7. **Unintended Consequences**: Language models might generate content that, while technically accurate, could have unintended consequences or mislead users. This poses challenges in ensuring that the output aligns with user expectations and is not misinterpreted.

8. **Resource Intensity**: Training and running large language models require significant computational resources and energy consumption. This raises concerns about the environmental impact and sustainability of deploying such models at scale.

9. **Explainability**: The inner workings of complex language models are not always transparent or easily explainable. This lack of interpretability can be a barrier to understanding how decisions are made, which is a concern, especially in critical applications where transparency is crucial.
What are concerns with Google Bard? (Asked on 1/4/2024 at 9:36am EDT)

Google Bard, like any large language model, comes with both potential benefits and drawbacks. While it can be a powerful tool for creativity, information access, and automation, there are also several concerns worth considering:

**Misuse and malicious intent:** Malicious actors could potentially use Bard to create harmful content, like spam, phishing emails, or propaganda. Bard's ability to mimic human language could make such content appear more authentic and deceive users.

**Overreliance and automation:** While Bard can be helpful for completing tasks and generating creative content, overreliance on such tools could lead to a decrease in critical thinking, research skills, and problem-solving abilities. Additionally, automating certain tasks with AI could raise concerns about job displacement and ethical implications.

**Privacy and data collection:** Bard's training requires substantial data, which raises questions about user privacy and how the data is collected and used. It's important to ensure transparency and ethical practices in data handling.

**Transparency and explainability:** Bard's decision-making process can be complex and opaque, making it difficult to understand how it arrives at certain outputs. This lack of transparency raises concerns about accountability and potential manipulation.

**Accessibility and equity:** Access to AI tools like Bard may not be equally distributed, potentially exacerbating existing inequalities and biases. It's important to consider accessibility and design AI in a way that benefits all users.
QuillBot AI – Paraphrasing Tool

Summarized Chat GPT and Google Bard responses in QuillBot (on 1/4/2024 at 9:53am EDT)

Short
Language models, like Bard, can be used to generate harmful content, perpetuate stereotypes, and generate misinformation. However, they also pose ethical and security risks, as they can be vulnerable to adversarial attacks. The quality and diversity of training data also affect their performance. The lack of transparency and explainability in these models raises concerns about potential misuse, overreliance, and ethical implications. Additionally, the lack of accessibility and equity in AI design can exacerbate existing biases.

Semi-Short
Language models, such as Bard, can be used to generate harmful content, misinformation, and deceptive activities. However, there are concerns about their ethical use, lack of accountability, security risks, privacy, and dependence on training data. The quality and diversity of training data significantly influence the model's performance, and unintended consequences can arise. The environmental impact and sustainability of deploying large language models at scale are also concerns. The complexity of the model's decision-making process raises questions about accountability and potential manipulation. Overreliance on AI tools like Bard can lead to a decrease in critical thinking and problem-solving abilities. Privacy and data collection are also concerns, as Bard's training requires substantial data, raising questions about user privacy and ethical practices. Access to AI tools like Bard may not be equally distributed, potentially exacerbating existing inequalities and biases.
I understand that you might have some concerns about using Microsoft Copilot. It’s natural to be curious and cautious when trying out new technologies. Let me address some common concerns:

1. Privacy and Data Security:
   - Microsoft Copilot processes the text you provide during the conversation, but it does not store any personal data or retain information from previous interactions.
   - Your privacy is important, and Microsoft takes data security seriously. Copilot adheres to strict privacy policies and guidelines.

2. Bias and Fairness:
   - Copilot’s responses are generated based on patterns in the training data it was exposed to. While efforts have been made to reduce bias, it’s essential to remember that no AI system is entirely free from bias.
   - If you encounter any problematic responses, please provide feedback so that improvements can be made.

3. Accuracy and Reliability:
   - Copilot aims to provide helpful and accurate information, but it’s essential to verify critical details independently.
   - If you have specific requirements, consider cross-referencing Copilot’s responses with other reliable sources.

4. Ethical Use:
   - Copilot should be used ethically and responsibly. Avoid generating harmful, offensive, or misleading content.
   - Remember that Copilot is a tool, and the responsibility for the content ultimately lies with the user.

5. Learning and Adaptation:
   - Copilot learns from user interactions and continuously improves over time.
   - If you encounter any issues or have suggestions, feel free to share them.

In summary, while Copilot is a powerful tool, it’s essential to use it thoughtfully and critically. If you have specific concerns or questions, feel free to ask, and I’ll do my best to address them! 😊
Night Café AI Image Creator

AI Image Creator can create new images using keywords or modify existing images.
Night Café AI Image Creator

AI Images Created Two Years Ago

“Cigar and Whiskey”
“Hacker”
“Records Management Person”
Night Café AI Image Creator

AI Images Created January 2024

“Cigar and Whiskey”

“Hacker”

“Records Management Person”
Figure 2 — A visual demonstration of how the processes relate to each stage

Source: ISO 8183:2022 – AI Data lifecycle framework
AI Objectives and Planning

The organization shall establish AI objectives at relevant functions and levels.

The AI objectives shall:

a) be consistent with the AI policy
b) be measurable (if practicable);
c) take into account applicable requirements;
d) be monitored;
e) be communicated;
f) be updated as appropriate;
g) be available as documented information.

Source: ISO 42001:2023 – AI Management system
Set a plan

What should you do?
1. Explore AI standards for guidance
2. Ask how AI is used throughout your organization
3. AI Policy Development
4. Ensure legal is aware of AI Intellectual Property concerns
5. Thoroughly understand how data is used and stored in AI systems (i.e., security, privacy, quality, etc.)
6. Incorporate AI matters into compliance training
7. Advocate for RIM concepts in AI
8. AI is a tool
9. Microsoft Co-Pilot Governance planning
10. Know how is the cyber security team using AI
RESOURCES
Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

• Artificial intelligence (AI) holds extraordinary potential for both promise and peril. Responsible AI use has the potential to help solve urgent challenges while making our world more prosperous, productive, innovative, and secure. (1.0)

• At the same time, irresponsible use could exacerbate societal harms such as fraud, discrimination, bias, and disinformation; displace and disempower workers; stifle competition; and pose risks to national security. (1.0)

• AI reflects the principles of the people who build it, the people who use it, and the data upon which it is built. (1.0)

• developing a companion resource to the AI Risk Management Framework, NIST AI 100-1, for generative AI. (4.1.i.A)

• any ongoing or planned activities related to training, developing, or producing dual-use foundation models, including the physical and cybersecurity protections taken to assure the integrity of that training process against sophisticated threats. (4.2.i.A)

• To help train the Federal workforce on AI issues, the head of each agency shall implement — or increase the availability and use of — AI training and familiarization programs for employees, managers, and leadership in technology as well as relevant policy, managerial, procurement, regulatory, ethical, governance, and legal fields. (10.2.g)

• Such training programs should, for example, empower Federal employees, managers, and leaders to develop and maintain an operating knowledge of emerging AI technologies to assess opportunities to use these technologies to enhance the delivery of services to the public, and to mitigate risks associated with these technologies. (10.2.g)

NIST Internal Report
NIST IR 8477 ipd

Mapping Relationships Between Documentary Standards, Regulations, Frameworks, and Guidelines
Developing Cybersecurity and Privacy Concept Mappings

Initial Public Draft

Karen Searefood
Muriqiaj Souppaya
Michael Fagan

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8477.ipd

NIST Drafts Major Update to Its Widely Used Cybersecurity Framework

NIST has revised the framework to help benefit all sectors, not just critical infrastructure.

August 08, 2023

The world’s leading cybersecurity guidance is getting its first complete makeover since its release nearly a decade ago.

After considering more than a year’s worth of community feedback, the National Institute of Standards and Technology (NIST) has released a draft version of the Cybersecurity Framework (CSF) 2.0, a new version of a tool first released in 2014 to help organizations understand, reduce and communicate about cybersecurity risk. The draft update, which NIST has released for public comment, reflects changes in the cybersecurity landscape and makes it easier to read the CSF rules.

MEDIA CONTACT
Chad Boutin
charles.boutin@nist.gov
(301) 975-4251

ORGANIZATIONS
Information Technology Laboratory
Applied Cybersecurity Division
Applied Cybersecurity - HQ

RELATED LINKS
Draft Cybersecurity Framework 2.0
Leadership & Personal Development

- **Built to Last**
  - Successful Habits of Visionary Companies
  - Jim Collins and Jerry I. Porras

- **Traction**
  - Get a Grip on Your Business
  - Gino Wickman

- **Impact Players**
  - How to Take the Lead, Play Bigger, and Multiply Your Impact
  - Liz Wiseman

- **Multipliers**
  - How the Best Leaders Make Everyone Smarter
  - Liz Wiseman

- **The Innovation Code**
  - The Creative Power of Converging Disciplines
  - Jeff DeGraff

- **Future Proofing You**
  - Jay Samit

- **Scaling Up**
  - How a Few Companies Make It...and Why the Rest Don’t
  - Verne Harnish

- **Rules**
  - Leaderships Respectful Policies Directives
  - Lewis Eisen

- **Tomorrow’s Jobs Today**
  - Wisdom and Career Advice from Thought Leaders in AI, Big Data, Blockchain, the Internet of Things, Privacy, and More
  - Rafael Moscatel and Abby Moscatel

- **Algorithms to Live By**
  - The Computer Science of Human Decisions
  - Brian Christian and Tom Griffiths
IG Presentations Available

IGIM v2.0 and IG ISO 24143_2022
We will be taking a deeper look into ARMA’s Information Governance Implementation Model (IGIM) v.2.0, which is a valuable tool to connect the various stakeholders of IG inside any organization.

IG Career Planning
Information governance is still a young profession. So, where does one go to get an education? What does a resume look like for information governance? What are earning possibilities?

IG Education and Leadership
How do you prepare one’s staff for IG? What about your educational needs? This presentation will explore academic programs and certification opportunities for IG professionals. Further, a sample of resources will be reviewed, along with an introduction to other IG/RIM and leadership resources that can be used to improve and evolve an IG program and career.

IG and Cybersecurity
Organizations face myriad security concerns; sometimes, understanding these concerns can be overwhelming. IG professionals must understand security threats to their organizations and the information they are charged to protect.

IG and Artificial Intelligence
Artificial intelligence (AI) tools have garnered much interest over the past few years. Organizations such as Harvard talk about AI’s future, ZDNet says business success and growth involve AI, and The White House has issued an executive order in 2023 on the use of AI. AI is no longer an emerging technology, and we must be prepared to address AI as IG/RIM professionals.
Leadership or Keynote Presentations

The Phoenix
Overcoming a toxic workplace that propelled a new career

Addiction to Excellence
How a disruptive event derailed an addiction and created a passion

Accidental IG and Treasure
How quietly implementing IG improved a business and contributed to unfound treasure
The James Webb telescope had 344 ‘single point failures’ before launch. Then, success.

The Pillars of Creation

James Webb Telescope
Currently 1 Millions miles from Earth

Deep Space
In 1981, the original VRC site was in Memphis, TN – a custom-built vault protecting personal assets. VRC was formally founded in 1988. Forty years later, we have become a premier leader in records and information management.

Our Company

- 3rd Largest and Fastest Growing RIM Company in US
- 130+ VRC Facilities Nationwide
- Proven 40+ Year Track Record
- Only provider using RFID tracking in every process
- Highest Customer Satisfaction Rating in Industry
National Footprint

Servicing organizations coast-to-coast

130+
VRC Facilities

2000+
Employees

NATIONAL COVERAGE FROM

200+
Markets
Our Commitment to Compliance

Holding ourselves to rigorous standards for governance and compliance

SSAE-18/ SOC 2
TYPE II Auditing
Annual third-party audit report for every facility

NAID AAA Certified
For information destruction

HIPAA Compliant
Certified HIPAA Security Specialists

HITRUST Compliant
Demonstrates our commitment to healthcare data

PCI Compliant
Facilities
STAY CONNECTED

Email: aysasi@vrcnetwork.com
LinkedIn: https://www.linkedin.com/in/andrewysasi/
VRC LinkedIn: https://www.linkedin.com/company/vital-records-control-llc/