Ethical AI and Privacy Series: Article 1, The Primer

Artificial intelligence (AI) is rapidly transforming the way we live and work. From virtual assistants to self-driving cars, AI-driven solutions are becoming increasingly integrated into our daily lives. Recent developments in generative AI technologies, which can produce text, images, audio, and video, have contributed to the use of AI in enterprise settings. However, with this new type of technology comes with concerns about privacy and data protection.

This article is the first in a series of three developed to provide the privacy community with a baseline understanding of AI and machine learning. The next article digs deeper into the legal implications presented by AI and machine learning, and the third helps you to implement an Ethical AI Governance framework.

The proliferation of privacy and data protection laws governing artificial intelligence continue to expand.

- EU (European Union) AI (Artificial Intelligence) Act
- US (United States) State privacy laws with AI as a key aspect of the law
- China AI Laws, including Generative AI Regulation (Provisions on Management of Generative Artificial Intelligence Services)
- NY (New York) City AEDT (Automated Employment Decision Tools) Law

Each of these laws specify that companies must use AI tools and capabilities to protect consumer data rights while applying ethical uses of the underlying data. Before you can implement an AI Governance program it is necessary to understand some of the basics about artificial intelligence. Common types of AI include rule-based systems, machine learning systems, deep learning systems and generative AI.

RULE BASED SYSTEMS

Rule-based systems are the simplest form of AI. They operate based on a set of predefined rules and are limited in their ability to learn and adapt. One example of a rule-based system is an automated attendant, or virtual receptionist. Rule-based systems can respond to frequent questions and direct callers to the proper extensions by recognizing common phrases or language. Such a system is unable to respond to questions outside of the provided ruleset.

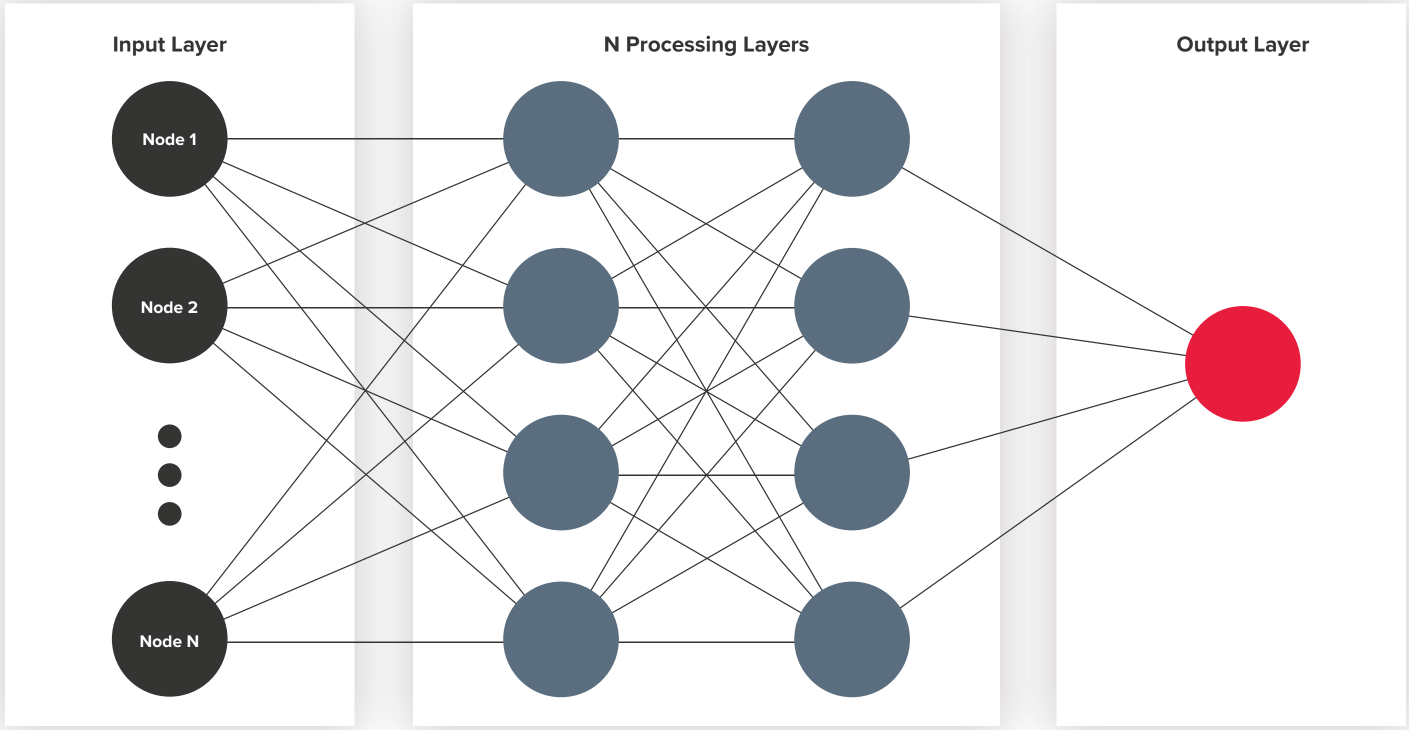
MACHINE LEARNING SYSTEMS

Machine Learning (ML) systems, on the other hand, learn from large volumes of data and adapt over time through the introduction of new data. ML systems use algorithms to identify patterns in data and make predictions based on those patterns. One common application of ML is email spam filtering. In addition to learning from an initial set of known examples, spam programs continue to learn based on user behavior. Therefore, the original data set grows over time as users select to block spam messages.

DEEP LEARNING SYSTEMS

Deep learning systems are a subset of Machine Learning systems that use layered algorithmic 'thinking' to mimic how the human brain thinks. Rather than merely recognizing and repeating patterns, deep learning systems utilize multiple layers of processing to learn and perform increasingly complex tasks with minimal human intervention. This is accomplished through a technique called neural networks, which consist of three or more layers of nodes that allow the system to become smarter over time. Neural networks attempt to simulate the human brain as it learns from substantial amounts of data.

Example Artificial Neural Network



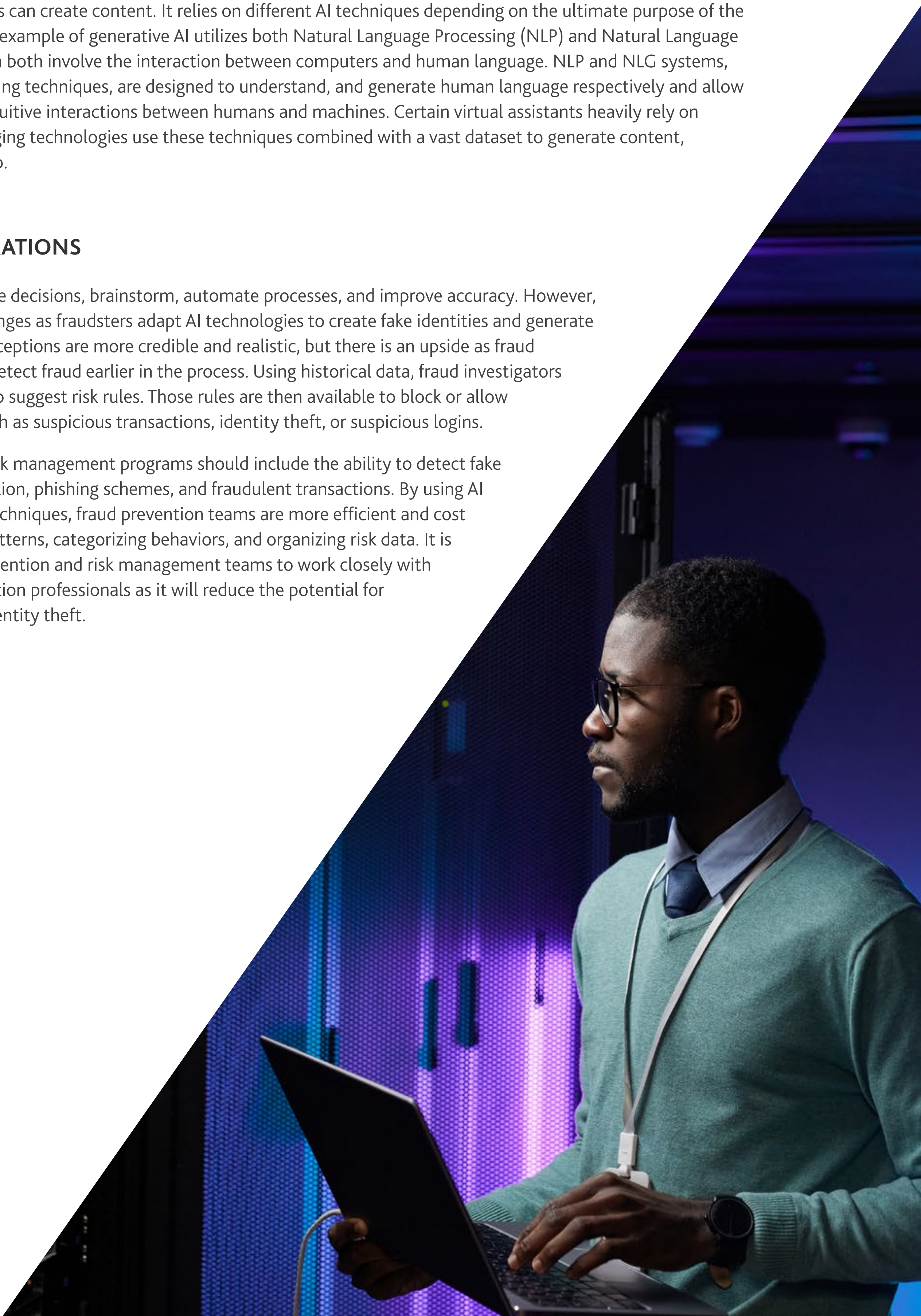
GENERATIVE AI

With Generative AI users can create content. It relies on different AI techniques depending on the ultimate purpose of the algorithm. One popular example of generative AI utilizes both Natural Language Processing (NLP) and Natural Language Generation (NLG) which both involve the interaction between computers and human language. NLP and NLG systems, often rely on deep learning techniques, are designed to understand, and generate human language respectively and allow for more natural and intuitive interactions between humans and machines. Certain virtual assistants heavily rely on these techniques. Emerging technologies use these techniques combined with a vast dataset to generate content, images, audio, and video.

FRAUD CONSIDERATIONS

AI is a great tool to make decisions, brainstorm, automate processes, and improve accuracy. However, they also present challenges as fraudsters adapt AI technologies to create fake identities and generate fake documents. The deceptions are more credible and realistic, but there is an upside as fraud investigators use AI to detect fraud earlier in the process. Using historical data, fraud investigators can train that data set to suggest risk rules. Those rules are then available to block or allow certain user actions, such as suspicious transactions, identity theft, or suspicious logins.

Fraud prevention and risk management programs should include the ability to detect fake identities, false information, phishing schemes, and fraudulent transactions. By using AI and machine learning techniques, fraud prevention teams are more efficient and cost effective in analyzing patterns, categorizing behaviors, and organizing risk data. It is important for fraud prevention and risk management teams to work closely with privacy and data protection professionals as it will reduce the potential for privacy breaches and identity theft.



PRIVACY CONSIDERATIONS

AI has transformed the way we live and work. Industries like healthcare, transportation, and retail is reliant on AI solutions. Privacy professionals need to understand the use of AI to enable companies to respect individual privacy rights. Similar to our fraud considerations, privacy teams must consider several factors that could impact consumers' individual privacy rights.

- Misuse of Personal Information: AI technology relies on learning from and recognizing patterns in substantial amounts of data, including personal information. It is crucial to ensure that individuals provide their consent for a company to use their personal data for those purposes. Additionally, there is a risk of fraudsters misusing personal information for identity theft or spreading misinformation. Collaboration between privacy, fraud prevention, and risk management teams could help to mitigate the misuse of personal information.
- Biased Algorithms: The use of algorithms to help with decision-making processes continues to grow. They are dependent on teaching machines to reflect human biases in which the algorithm then delivers systematically biased results because of erroneous assumptions of the machine learning process. Privacy professionals should advocate for diverse and representative datasets, the ability to structure data to allow for different opinions or outcomes, and diverse machine learning teams that ask diverse questions, to minimize biases and discrimination.
- Privacy Breaches: With the increasing reliance on AI and the collection of growing amounts of personal information, there is a continued threat of data breaches. Privacy professionals must work with security and technology professionals to protect personal information and establish robust technical and physical safeguards to prevent data leaks, misuse of information, and unauthorized access.
- Surveillance and Monitoring: Facial Recognition Technologies (FRT) are plagued with privacy concerns – a lack of consent, transparency, and the potential for abuse are just a few. Privacy professionals should implement enterprise standards that require DPIAs (Data Protection Impact Assessments) and the implementation of Data Protection by Design and by Default practices prior to introducing FRTs to the workforce to manage legal and ethical boundaries.

AI and machine learning offer amazing opportunities to streamline and automate processes, brainstorm, and improve decision making capabilities. However, privacy professionals must play an active role in developing ethical standards, monitoring, and reducing risk, and protecting the privacy of consumers, users, and employees. BDO's Ethical AI Governance model allows an organization to prioritize privacy, data management and protection, and system functionality. Stay tuned for our next article, which explores the ethical frontiers of AI and charts a course for a more secure and responsible future.

Have questions or want to learn more? **Contact us!**

Our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes and value for our people, our clients and our communities. BDO is proud to be an ESOP company, reflecting a culture that puts people first. BDO professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C., a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. For more information, please visit: www.bdo.com.