CEP Magazine - July 2023

Jennie Clarke (jennie.clarke@globalrelay.net) is Head of Content at Global Relay in London, United Kingdom.

Generative AI: Risks, responsibilities, and regulation

By Jennie Clarke

Bill Gates recently announced that the age of artificial intelligence (AI) has begun, noting that recent developments in generative AI—such as OpenAI's ChatGPT and Google's Bard—are "the most important advance in technology since the graphical user interface."[1] Similarly, a report by Goldman Sachs predicted that 300 million jobs could be changed or replaced by advancements in generative AI, though most roles will be "complemented rather than substituted."[2]

Over the past five years, the use cases of AI have become more apparent, with many compliance teams now employing AI-driven tools to assist with run-of-the-mill tasks, including regulatory change management or surveillance. However, while AI is becoming mainstream, new advances in generative AI are taking automated capabilities to a new level, posing various challenges as they evolve.

The risks of generative AI

On February 27, 2023, Retail Banker International reported that the likes of JP Morgan, Citigroup, and Deutsche Bank had banned staff from using ChatGPT.[3] This didn't appear to be the result of any particular incident or misuse, but because the technology posed an unknown risk.

On March 22, thousands of tech experts, including Elon Musk and Steve Wozniak, signed an open letter that asked all AI labs to pause the training of AI more powerful than GPT-4 for at least six months.[4] This raises several concerns, due partly to the letter being signed by significant innovators in the industry, but particularly because it warns that generative AI systems with human-competitive intelligence can pose profound risks to society and humanity. The letter also suggests we're at a breaking point and must act urgently, and adds that governments should step in and institute a moratorium if we can't enact a pause quickly enough.

Anecdotally, during a series of roundtables hosted by Global Relay, several compliance officers at United Kingdom-based hedge funds and broker–dealers commented that they also had banned the use of generative AI on the basis that all new technology must undergo a rigorous verification process within risk and IT teams. ChatGPT, though revolutionary, is no exception to the onboarding controls that financial institutions have in place.

It is likely that, having undergone scrutiny from within risk and IT, generative AI will continue to be banned from use by employees because of the many unknowns it poses. OpenAI's own FAQs note that certain OpenAI employees (as well as third-party contractors) can access the information or queries posted by users for review. Financial services hold vast quantities of consumer and employee data; if a single employee were to plug this

data into ChatGPT, there could be a far-reaching data exposure and regulatory breach.

Some compliance technology vendors have recently announced they are trialing use cases in which ChatGPT is plugged into their technology via an application programming interface to conduct tasks such as translation. ChatGPT's translation capabilities, after all, far outweigh most AI-generated translation tools. No doubt, the functionality would be enhanced. But the concern here is security. Are your existing data protection policies and contracts developed enough to cater to the constantly evolving technology of generative AI? How can you show customers and regulators that you can successfully manage data transfer and deletion requests if using this tool? Data security is a minefield, one that OpenAI will look to clarify as a priority.

Beyond data, many see residual risks ranging from ethical concerns to concerns around the vast number of potential use cases. Some institutions are worried that their quantitative analysts could use ChatGPT to build their predictive models, which is a risk given that ChatGPT's training data was cut off in 2021, which could lead to inaccurate results. Others are worried that, in order to keep up with the pace of innovation of generative AI, they will need to invest vast sums of money to either build similar technology or buy licenses that allow them to integrate the tool.

This document is only available to members. Please log in or become a member.

Become a Member Login