M+E JOURNAL

A SECURE

AI WORLD?

How AI is being used both by and against the industry

SECURITY SOLUTIONS
Where and how AI is being used to attack and protect M&E

SMART CONTENT
Massive amounts of data now required new tools, including AI

23.02

CHARTING LEGAL, SECURITY AND PRIVACY WATERS: AI'S ROLE IN CONTENT CREATION AND LOCALIZATION

Achieving a balance between automation and safeguarding sensitive information is crucial

ABSTRACT: The adoption of AI in content creation and localization operations poses significant legal, security and data privacy risks. Concerns center around copyright infringement, mishandling of personal data, and vulnerabilities to cyber threats. Achieving a balance between automation and safeguarding sensitive information is crucial for ethical and legal compliance in AI-driven processes.

By Nicole Quilfen, COO, Mediartis, and Stephanie Iyayi, SVP, Legal, Privacy, Convergent Risks

The media and entertainment industry is witnessing a revolution with the integration of artificial intelligence in content creation and localization. AI-powered algorithms can now generate written content, translate languages, and even voice-act in multiple languages. The appeal lies in speed, consistency, and cost-efficiency, but the transition is not without its share of challenges.

The adoption of AI in content creation and localization operations poses significant legal, security and data privacy risks. Concerns center around copyright infringement, mishandling of person-

THE ADOPTION OF AI IN CONTENT creation and localization offers transformative benefits but carries a profound responsibility to address legal, security, and data privacy risks. Concerns surrounding copyright infringement, data mishandling, and vulnerabilities to cyber threats demand meticulous attention.

al data, and vulnerabilities to cyber threats. Achieving a balance between automation and safeguarding sensitive information is crucial for ethical and legal compliance in AI-driven processes.

REGULATORY LANDSCAPE

AI has given governments and policy makers a lot to grapple with. Several high-level questions are now being debated:

- *What interests should AI regulations protect?*
- *Should existing regulatory structures be adapted or new ones put in place?*
- *How should regulatory burdens be kept proportionate?*
- *What role should central government play?*

The EU is taking a leading role in the development of AI-specific regulations with a proposal for harmonized rules on artificial intelligence and amending certain Union legislative acts (the "AI Act"). The AI Act proposes broad-brush rules designed to ensure AI systems are sufficiently safe and robust before they enter the EU market. This includes banning certain prohibited AI practices outright and defining a new category of high-risk AI systems to which granular responsibilities, obligations and duties apply.

In contrast to developments in Europe, the UK has decided against creating a single regulatory function to govern AI, stating that AI is a general-purpose technology having applications in many industry sectors. Instead, the UK issued a white paper setting out principles to support existing regulators, such as the Information Commissioner's Office (ICO, the UK's privacy regulator) and the Financial Conduct Authority (FCA), to develop a bespoke approach for AI development and use within their sectors.

The regulatory framework for AI in the United States involves multiple federal and state agencies, and there isn't a single comprehensive law dedicated solely to AI regulation. Instead, AI is subject to a patchwork of existing laws and regulations that may apply depending on the specific use and impact of the technology.

LEGAL CONSIDERATIONS

Perhaps the most prominent legal concern in AI-driven content creation is copyright infringement. AI algorithms trained on vast databases may inadvertently generate content that closely resembles copyrighted material. This poses a risk to both creators and organizations that utilize AI-generated content. To mitigate this risk, organizations should implement robust copyright checks and educate their AI models on intellectual property rights, emphasizing the importance of original content creation.

AI systems also encounter complexities in navigating licensing agreements and fair use policies. While AI can assist in content creation, it must operate within the

Continued on page 4

***Nicole Quilfen** is the chief operating officer of Mediartis. She comes from a business development background specializing in international strategy, personal data protection, and accompanying media and entertainment professionals with their operational privacy strategies. nicole@mediartis.com @Mediartis_*

***Stephanie Iyayi** is the senior vice president of legal and privacy for Convergent Risks. She comes from a legal background specializing in privacy and data protection and advises clients on all areas of UK, EU, and international data protection law, from general privacy compliance to risk management issues, including compliance implementation, privacy impact assessments, data breach incidents, cross-border data transfers, employee monitoring and data subject access requests. info@convergentrisks.com @ConvergentRisks*

MEDIARTIS *Continued from page 3*

bounds of licensing agreements, which may restrict the extent to which content can be modified or distributed. Organizations must conduct thorough reviews of licensing agreements, ensuring that AI-generated content complies with the terms and conditions set forth.

Moreover, AI's involvement in content creation can raise concerns about meeting contractual obligations. For example, if a company uses AI to produce content for a client, they must ensure that the content aligns with the agreed-upon terms and quality standards. It is crucial to establish clear contracts that outline the scope of AI involvement, quality expectations, and mechanisms for dispute resolution.

SECURITY RISKS

AI systems can exacerbate security risks and create new ones. AI models, particularly those used for content generation, may be vulnerable to cyberattacks, including adversarial attacks that manipulate the AI's output. To protect against such threats, organizations should regularly update AI models, implement robust security measures, and conduct penetration testing to identify vulnerabilities.

In addition, AI relies on vast datasets, which can contain sensitive information. Mishandling or inadequate protection of these datasets can lead to data breaches, resulting in significant legal and financial consequences. Organizations should prioritize encryption, access controls, and data protection protocols while adhering to data privacy regulations.

AI AND DATA PROTECTION

UK and EU GDPR laws have disrupted the way organizations around the world are required to protect personal data. The processes through which businesses collect, process, store and share personal data have irreversibly changed, and as more of these organizations use AI technologies as a part of their business processes, data protection laws are being extended to accommodate these new and emerging technologies.

The UK's ICO has identified AI as a priority area and advises organizations to take a risk-based approach when developing and deploying AI. Specifically, the ICO recommends that organizations assess whether they need to use AI for the context it will deploy it in - AI is generally considered a high-risk technology and there may be a more privacy-preserving and effective alternative.

Where an organization does develop and/or deploy AI, it needs to assess the risks and implement appropriate technical and organizational measures to sufficiently mitigate them. It is impossible to realistically remove every risk (and data protection law does not require organizations to do so) however, certain measures should be taken to ensure accountability:

- *Take time and dedicate resources to ensure the quality of the data inputted into the AI system – preparing the data to train an AI system will result in better outputs.*

- *Conduct a data protection impact assessment (DPIA) to help identify and minimize the risk of non-compliance with applicable data protection legislation that the use of AI poses, as well as preventing harm to individuals.*

- *Be clear, open, and honest with people within a privacy notice about how and why you use their personal data and consider what explanation is needed in the context that you will deploy your AI system in.*

- *Obtain user consent for data collection and specific processing purposes where required. Users have the right to know how their data is being used and to have the option to opt out.*

- *Obtain documentation from any supplier that demonstrates a data protection by design approach.*

- *When using AI for decision-making, decide whether to use it to support a human decision-maker, or whether it will make solely automated decisions — under the GDPR, individuals have the right not to be subject to solely automated decisions with legal or similarly significant effects.*

- *Ensure that informed consent of use is obtained for personal data that is collected and used for AI training. When sensitive personal data, such as voice, is being used, obtain explicit opt-in consent of use, and make sure data subject consent is updated on a regular basis.*

- *Securely store personal data used for training AI. If it's not adequately protected, it can become vulnerable to data breaches, leading to unauthorized access and exposure of private information.*

- *Determine who owns the personal data used for training AI. Ownership can be a complex legal and ethical issue. Individuals may expect that their data is being used solely for their benefit and using it for AI training purposes without their consent can raise questions about data ownership and control.*

RISK VS. REWARD

The adoption of AI in content creation and localization offers transformative benefits but carries a profound responsibility to address legal, security, and data privacy risks. Concerns surrounding copyright infringement, data mishandling, and vulnerabilities to cyber threats demand meticulous attention. Achieving the ethical and legal compliance required for training AI and in AI-driven processes necessitates a comprehensive strategy that safeguards information while harnessing the power of automation responsibly. As technology continues to advance, organizations must remain vigilant in protecting both their interests and the privacy rights of their users and clients. ⊞