The risks of oversharing with generative AI

Picture this: you're scrolling through social media and you come across a video of a celebrity doing something outrageous. It looks real, but something about it seems off. It's only when you read the caption that you realize it's a deepfake, created using generative AI. From deepfake videos to ChatGPT-generated responses, it's becoming increasingly difficult to tell the difference between human-made and AI-generated content.

But with this growing reliance on generative AI comes a new concern: the oversharing of personal data. As we become more comfortable with AI, we might be unknowingly giving away sensitive information that can be used for purposes we never intended. We're in danger of opening a Pandora's box of privacy breaches, where our personal information is being used in ways we can't even imagine.

The consequences of oversharing personal data can be dire, with risks ranging from data breaches to the creation of malicious content. While the potential benefits of generative AI are endless, we need to be mindful of the potential risks that come with it. In this article, we'll delve deep into the privacy breaches and potential risks associated with oversharing personal data with generative AI, and ways to mitigate the risks and protect yourself and your data.

Walking on a double-edged sword with generative AI

Generative AI is a technology that uses algorithms to create new and original content by learning from a dataset. The AI algorithm can generate new content that is similar to the original data, but not identical. It's like a chef who learns the recipe and ingredients of a dish and then uses their creativity to make new variations of it.

But with great power comes great responsibility, and generative AI is no exception. The technology requires large amounts of data to work effectively, which can lead to privacy concerns. The more data you feed into the algorithm, the more accurate and personalized the content it generates becomes. However, this also means that personal data is being used, which can be a cause for concern.

One of the major privacy concerns with generative AI is the risk of oversharing personal

and confidential information. This happens when individuals or companies feed large amounts of personal data into the algorithm, which can include sensitive information such as medical records, financial information, and personal contacts. If this data falls into the wrong hands, it could be used for malicious purposes, such as identity theft, cyberattacks, and social engineering scams.

For example, generative AI models could be trained on personal data such as email addresses, names, and social media profiles to create highly convincing phishing emails. These emails could then be used to trick people into providing sensitive information such as passwords or credit card details. The volume of malware scams has visibly grown since the dawn of chatbot technology, and the technology's quick adoption in applications raises concerns about data collection, privacy, and the prevalence of plagiarism and misinformation.

Others are noticing the problem with ChatGPT, a famous generative AI application, being promoted so quickly and forcefully as well. Leaders in technology and AI have also raised the alerts about this. In 2021, researchers from Stanford University and the University of Washington demonstrated that it is possible to use GPT-3, another variant of ChatGPT, to extract personal information such as names, phone numbers, and email addresses from text.

> A study by Home Security Heroes shows that a new AI password cracker can decipher 71% of common passwords in less than a day.

Exploring ways to defend confidentiality

Generative AI can offer many benefits, but we cannot turn a blind eye to the chance of personal information leaking from training data, making it difficult to secure it. A relational database can limit access to a particular table with personal information, but an AI can be queried in dozens of different ways. Attackers will quickly learn how to ask the right questions to obtain sensitive data. Teaching an AI to protect private data is something we don't yet understand.

To protect yourself and your data from generative AI, it is important to be aware of what data you're sharing and use strong and unique passwords to protect your data. Limit

access to devices, keep software up to date, and use privacy-preserving tools like VPNs and browser extensions to protect data. Additionally (and importantly), read the privacy policy carefully to understand what data is being collected, how it's being used, and who it's being shared with.

Regulators around the world are increasingly taking steps to protect users' data from generative AI. Mentioning AI in global legislative proceedings have increased 6.5 times since 2016, from 1 in 2016 to 37 in 2022. Here are some of the steps initiated by them:

1. **Data Protection Laws**: Governments are enacting or strengthening data protection laws to ensure that companies are held accountable for the data they collect from users.
2. **Algorithmic Accountability**: Regulators are also pushing for greater algorithmic accountability, which means holding companies accountable for the algorithms they use and ensuring that they are transparent and fair.
3. **Privacy-by-Design**: Another approach being taken by regulators is to encourage companies to adopt a "privacy-by-design" approach, which means designing products and services with privacy in mind from the outset.
4. **Ethical AI Guidelines**: Many organizations, including the European Union, have developed ethical AI guidelines to help companies navigate the complex ethical issues surrounding AI, and ensure that AI is developed and used in an ethical and responsible manner.
5. **Regulatory Bodies**: Governments are also creating regulatory bodies specifically dedicated to overseeing AI, such as the European Commission's High-Level Expert Group on AI, which provides advice and recommendations on AI-related policy and regulatory issues.

Overall, the aim of these measures is to ensure that companies using generative AI are held accountable for the data they collect and use, and that users' privacy rights are protected. The rush to integrate this technology can result in data breaches, inaccuracies, and abuse, demonstrating the need for caution and responsible management.

The Future of Life Institute has released an open letter requesting that AI laboratories and businesses cease the development of OpenAI systems after ChatGPT-4. Reputable individuals including Steve Wozniak, the co-founder of Apple, and Elon Musk, the co-founder of OpenAI, have agreed that progress should be halted to make sure that people

can profit from and enjoy existing systems.

As this article draws to an end, one burning question keeps me up–what will happen when we humans become so dependent on generative AI that we can no longer produce new material for training models?

About ManageEngine

ManageEngine crafts comprehensive IT management software with a focus on making your job easier. Our 120+ award-winning products and free tools cover everything your IT needs. From network and device management to security and service desk software, we're bringing IT together for an integrated, overarching approach to optimize your IT.

For more information, visit **manageengine.com**

ManageEngine Insights is the thought-leadership and knowledge sharing platform of ManageEngine. As the go-to destination for tech enthusiasts, we offer tailored content specifically crafted to keep you in the know about the ever-evolving world of technology.

LinkedIn | **Twitter** | **Facebook** | **Instagram**