Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: Elise Quevedo

AI, Privacy, and the Looming Security Crisis: Who's Protecting Our Data?

Last week, I mentioned our technological strides in my article about DeepSeek's R1 large language model (LLM). However, as we embrace these advancements, a pressing concern looms: what do these new LLMs and AI technologies mean for our privacy and security?

We must ask the question, what about our data? Who will regulate what information is taken? We can all agree that AI's allure is undeniable. Yet beneath this shiny exterior lies a potential minefield for our personal information.

It can feel like a magician's trick sometimes: look over here so you don't see what I'm doing over there. LLMs ingest vast amounts of data to function effectively, but this data often includes sensitive personal information, which is what raises significant privacy concerns.

Government Concerns Rising

South Korea's industry ministry has temporarily banned access to DeepSeek due to security concerns and has advised agencies to exercise caution when using AI services such as DeepSeek and ChatGPT.

In the United States, they are working to ban federal employees from using DeepSeek on government devices, citing national security risks. As we continue integrating AI into our daily lives, we must be careful about the data these platforms access and how it's used. It's not just about the data we knowingly provide but the information taken without our consent.

> OpenAI has been the centre of controversy over how its models process user data

This issue extends beyond government use. Individuals and businesses must contend with the risks of data leakage, unauthorised data mining, and AI models learning from user interactions in potentially harmful ways.

OpenAI, for example, has been the centre of controversy over how its models process user data. ChatGPT's interactions with users have also raised alarms, particularly in cases where proprietary business information or confidential conversations have been inadvertently exposed to the model's training system.

Have you heard of the European Union's AI Act?

The AI Act regulates (or at least tries to regulate) AI technologies and ensures they adhere to specific standards. It categorises AI applications into three risk levels: unacceptable, high-risk, and low-risk.

Applications that are deemed inappropriate, such as government-run social scoring, are banned entirely. High-risk applications face strict legal requirements, while low-risk applications are subject to minimal regulations.

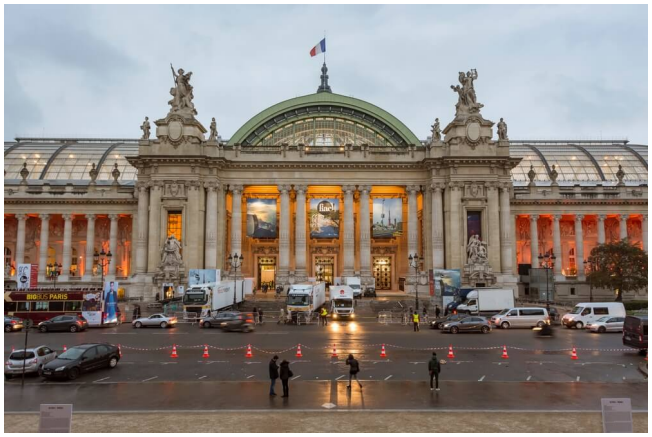
> The regulatory landscape must now adapt swiftly to address emerging threats

Although this regulatory framework is a step in the right direction, it is not without challenges. The regulatory landscape must now adapt swiftly to address emerging threats.

Companies using AI for hiring, financial decisions, and law enforcement, for example, must meet stricter transparency and auditing requirements under the AI Act.

Global Efforts to Regulate AI

Next week, France is hosting the "AI Action Summit" to address issues like labour disruption and environmental impact, reflecting a global shift in AI discourse toward tangible impacts.



Next week, France is hosting the "AI Action Summit" to address issues like labour disruption and environmental impact - Grand Palais, Paris

China has introduced strict guidelines on generative AI models, requiring AI developers to register their models and ensure compliance with state regulations before releasing them to the public.

The United States remains divided on how to regulate AI. While states like California are in charge of consumer protection laws related to AI-powered decisions, there is no comprehensive federal AI regulation akin to the EU's AI Act yet. I am sure this will change in the near future.

The Risks of Lower-Cost AI Platforms

Lower-cost platforms might offer very attractive pricing and accessibility, but at what cost? Some budget AI services may lack the necessary investment in data security infrastructure, making them more susceptible to breaches, unauthorised data collection, or even adversarial manipulation.

For example, there have been reports of AI models unintentionally leaking sensitive training data, such as personal messages, passwords, and internal corporate communications.

Last year, researchers found that some open-source LLMs accidentally revealed fragments of their training data when prompted in specific ways.

> A lower price point shouldn't come at the expense of our privacy

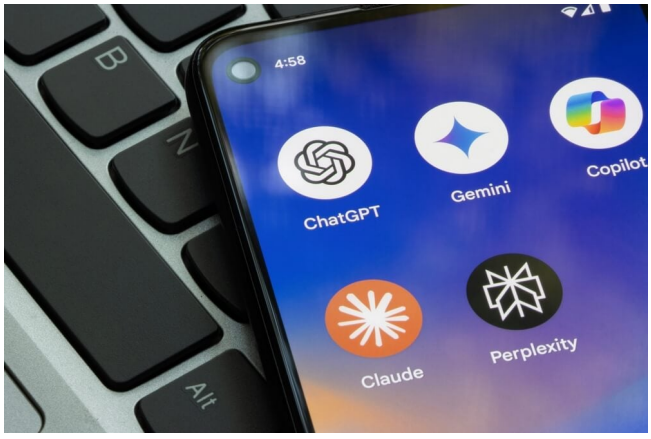
If such vulnerabilities exist in widely used models, the question is, what does this mean for smaller and new, less scrutinised AI services? Of course, it's tempting to opt for more affordable AI solutions, especially for small businesses or individual users.

However, we must consider whether these lower-cost platforms compromise on quality, particularly concerning data security. A lower price point shouldn't come at the expense of our privacy.

How do we navigate these challenges?

We are back to a keyword I often use: awareness. As individuals, we are all digital users, and we must educate ourselves about the data practices of the platforms we use even when tech is not your business.

From a business point of view, there is a need to advocate for and develop AI systems that put user privacy and data security first. Including implementing robust encryption methods, ensuring transparency in data usage, and regularly auditing systems for vulnerabilities.



AI developers should take the lead in self-regulation, embedding ethical guidelines into their development process before new legislations arrive

I will never get tired of saying that collaboration is key. In this case, a collaborative approach can bridge the gap between the rapid technological advancements we are experiencing and the slower pace of regulatory frameworks.

AI developers should also take the lead in self-regulation, embedding ethical guidelines into their development process before new legislations arrive.

Another solution is to leverage privacy-enhancing technologies (PETs) within AI systems. Pets can help mitigate some of the risks associated with data collection by minimising the amount of sensitive information stored in centralised databases.

AI, Privacy, and The Future

More AI companies need to explore and implement solutions that build trust with us, the users, and adaptable regulations that evolve alongside new AI technologies.

The advancements in LLMs and AI technologies are exciting; however, we must remain vigilant about our privacy and security. As we integrate these technologies into our lives, let's do so with a commitment to safeguarding our data and upholding users' trust worldwide.

The question isn't just about what AI can do but what it should do and how we ensure it serves humanity responsibly.