



PRIVACYENGINE

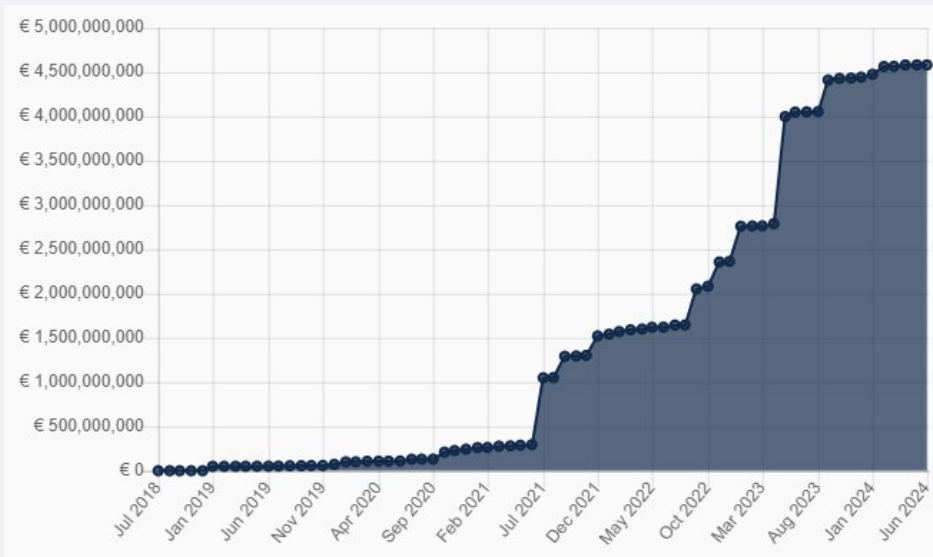
Dr. John Ghent
Co-Founder and CEO

From - “Privacy is Dead” To - “Privacy is Paramount”

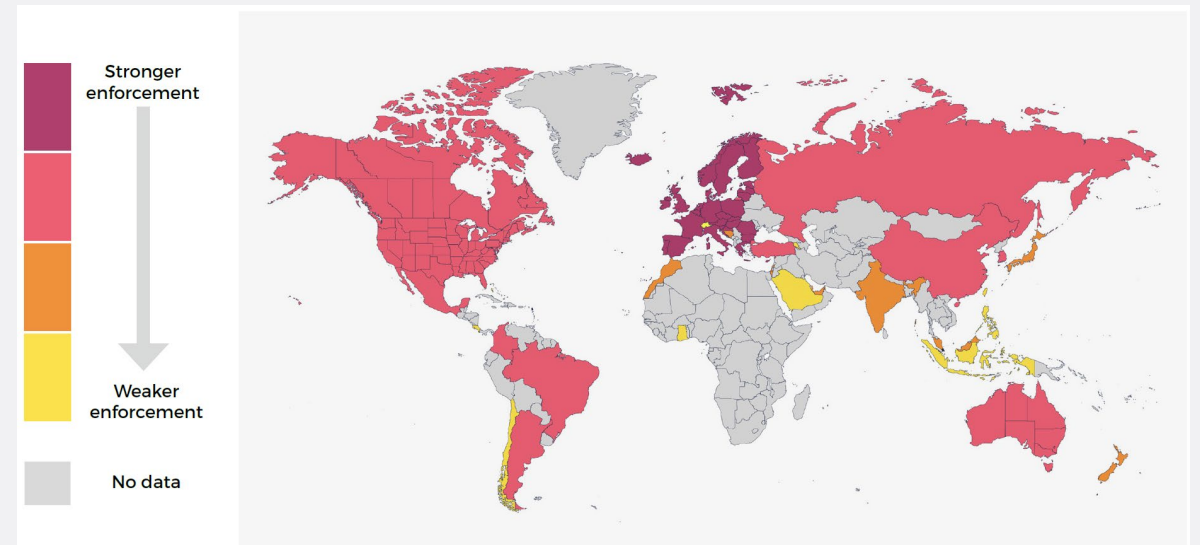
The Implications of the AI Revolution

Growing Enforcement & Growing Global Importance

GDPR Fines



Active Regulators



At the cusp of a surge in demand for privacy software for SMEs due to increased breaches, fines and DSARs, 51% of UK SMEs had breach in 2022

It's **NOT** all about fines – for B2B companies in the SMEspace, you now need to demonstrate compliance to win business

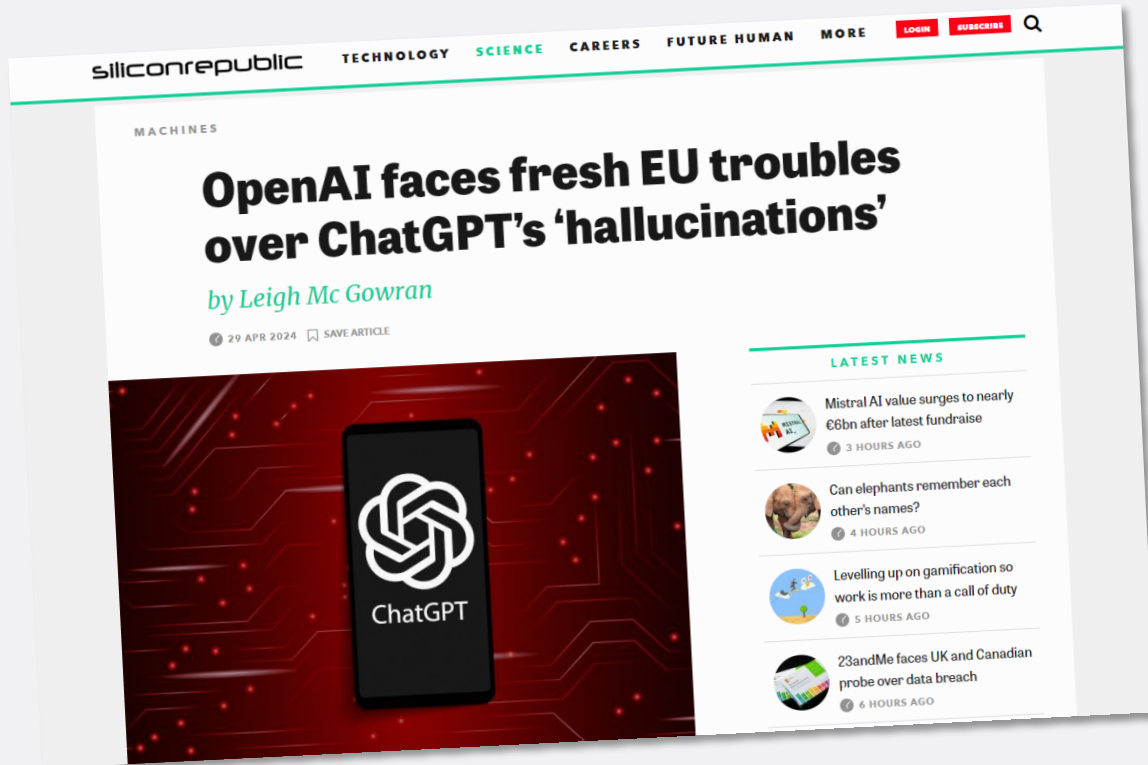


EU AI Act

- Risk based approach
- Prohibited AI: Social Credit Scoring, Purposefully Manipulative techniques, Untargeted scraping of facial images.
- High Risk
 - Critical infrastructures (e.g. transport),
 - Safety components of products (e.g. AI application in robot-assisted surgery);
 - Employment, workers
 - Law enforcement
 - Administration of justice
 - ALL BIOMETRIC IDENTIFICATION
- Obligations
 - Adequate risk assessment and mitigation systems;
 - High quality of the datasets feeding the system to minimise risks and discriminatory outcomes;
 - Logging of activity to ensure traceability of results;
 - Clear and adequate information to the user;
 - Appropriate human oversight measures to minimise risk;
 - High level of robustness, security and accuracy.
- Fines
 - Up to 7% of global turnover – designed to work hand in hand with the GDPR.



A Sample Case. OpenAI & NOYB



NOYB Argument –

“ChatGPT keeps hallucinating - and not even OpenAI can stop it.” - noyb.eu

Complaint filed – NOYB is now asking the Austrian data protection authority (DSB) to investigate OpenAI's data processing, and the measures taken to ensure the accuracy of personal data processed in the context of the company's large language models. (LLMs)



So, what is an LLM?

Do I need to understand how it works?

Came from a google research paper called “Attention is all you need” – published in Advances in Neural Information Processing Systems 30 (NIPS 2017) - Ashish Vaswani et al...

It basically created the transformer architecture – i.e. GPT, **Generative Pre- Trained Transformer**.

The transformer relies primarily on **word embeddings** (which give the meaning of each word) and **the attention mechanism** (which gives structure of the text).

In short, it's a technology and ALL technology can be implemented compliantly or non-compliantly.



How you use technology determines if it is compliant or not – GDPR still applies

GDPR	LLM considerations (examples)
Acquire Fairly	Is Fair Notice provided.
Specific Purpose	Is there a human oversight.
Data Minimization	Choose an LLM that doesn't store prompts.
Quality/ Accuracy	Prevent hallucinations from being possible. Choose use case carefully. Is there transparency.
Retention/Storage Limitation	Do I have a retention policy, is it implemented.
Secure (Integrity and Confidentiality)	Prevent access to the LLM of confidential information.
Accountable	Design privacy in from the start, did you complete a DPIA. Is testing and monitoring sufficient.



Practical & Technical Approaches

Privacy by Design – DPIAs always needed – GDPR principles still apply

Technical Approaches for AI implementation.

Methods for **reducing** the need for a **training set**

- **General Adversarial Networks (GAN)** – Generating Synthetic Data

Methods for **protecting privacy** without reducing the data set.

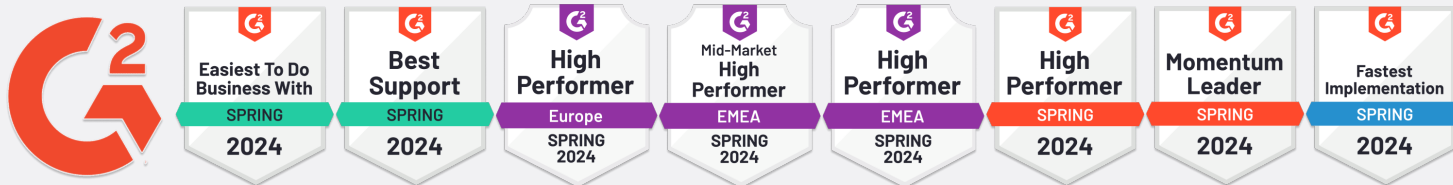
- **Differential Privacy**
- **Homomorphic Encryption**

Methods for **solving the blackbox effect**

- **Explainable AI (XAI)**
- **LIME** – Locally Interpretable Model Agnostic Explanations.



Q&A



PRIVACYENGINE



www.privacyengine.io



PRIVACYENGINE

Thank You!

