



ANNELIES MOENS
Privacy expert

“My role is to protect one of the most valuable and vulnerable resources in the world – information about people.”



A journey to a career that didn't exist when I was at school

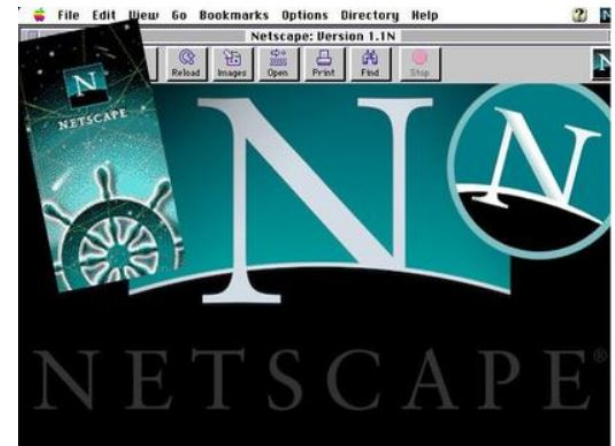
**It Takes a Spark STEM conference,
The Southport School, Gold Coast
16 June 2023**





My journey

The careers you will have in 10 - 15 years' from now don't exist today.



Making privacy core business



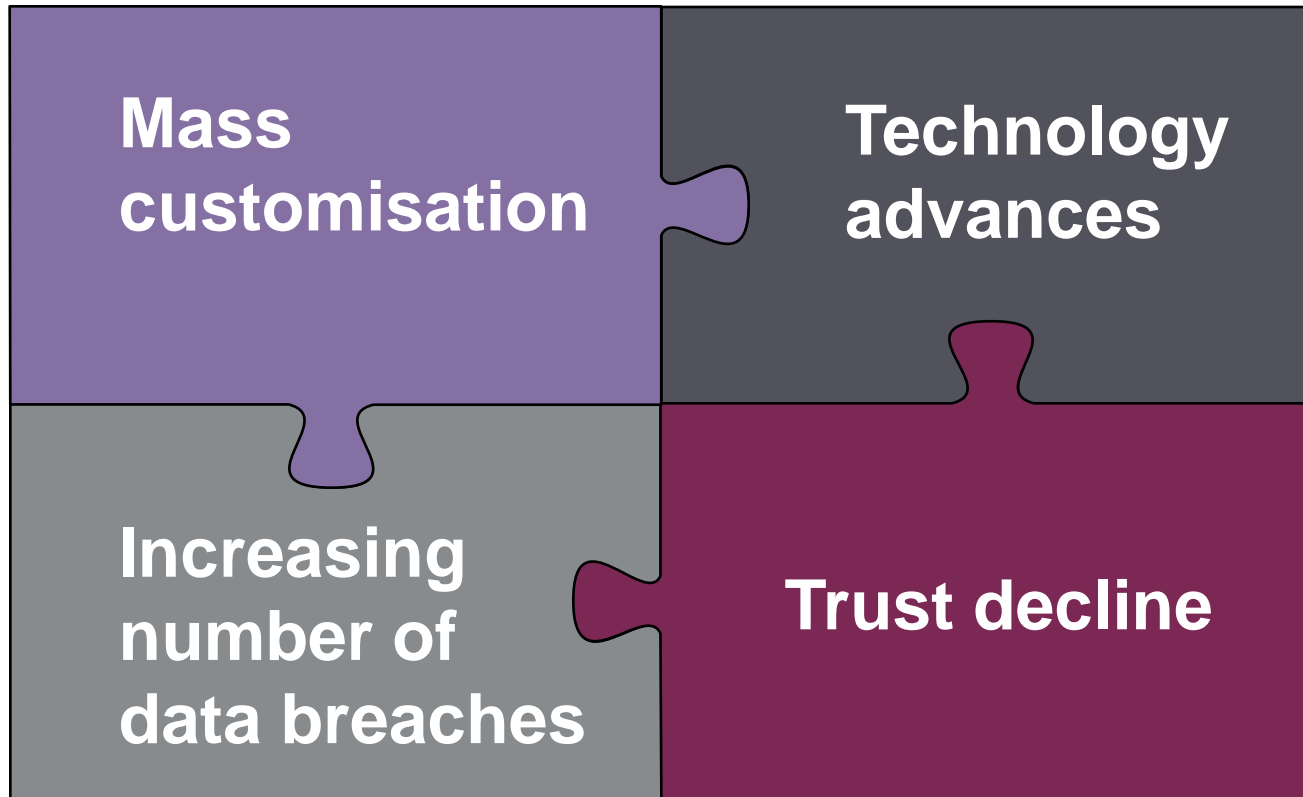
My journey

The careers you will have in 10 - 15 years' from now don't exist today.



Making privacy core business

Why is privacy such a hot topic?



Making privacy core business



Generative AI



Bard Experiment FAQ Sign in

Bard can give you some ideas to surprise your movie-loving friend on their birthday

Meet Bard: your creative and helpful collaborator, here to supercharge your imagination, boost your productivity, and bring your ideas to life.

Bard is an experiment and may give inaccurate or inappropriate responses. You can help make Bard better by leaving feedback.

[Sign in](#)

Search the web  

Introducing the new Bing

Ask real questions. Get complete answers.

[Learn more](#)



Making privacy core business



Use cases are currently only limited by your imagination

TECHNOLOGY EXECUTIVE COUNCIL

How ChatGPT is changing the job hiring process, from the HR department to coders

PUBLISHED SAT, APR 8 2023-10:00 AM EDT | UPDATED MON, APR 17 2023-1:23 AM EDT



Kevin Travers
@KEVOBT

SHARE [f](#) [t](#) [in](#) [✉](#)

HEALTH TECH

University of Kansas Health System taps Abridge to roll out AI-based medical transcription for thousands of docs

By Anastassia Gliadkovskaya • Mar 3, 2023 12:03pm

Physician Satisfaction

Workforce

EHR

Artificial Intelligence

A&O announces exclusive launch partnership with Harvey

NEWS 15 February 2023 2 min read

Related people



David Wakeling
Partner, Head of MG
London

Press contacts

For media enquiries relating to this topic, please contact:

Allen & Overy (A&O), the leading international law firm, has broken new ground by integrating Harvey, the innovative artificial intelligence platform built on a version of Open AI's latest models enhanced for legal work, into its global practice. Harvey will empower more than 3,500 of A&O's lawyers across 43 offices operating in multiple languages with the ability to generate and access legal content with unmatched efficiency, quality and intelligence.



Making privacy core business

Unintended consequences?

Costs of Generative AI

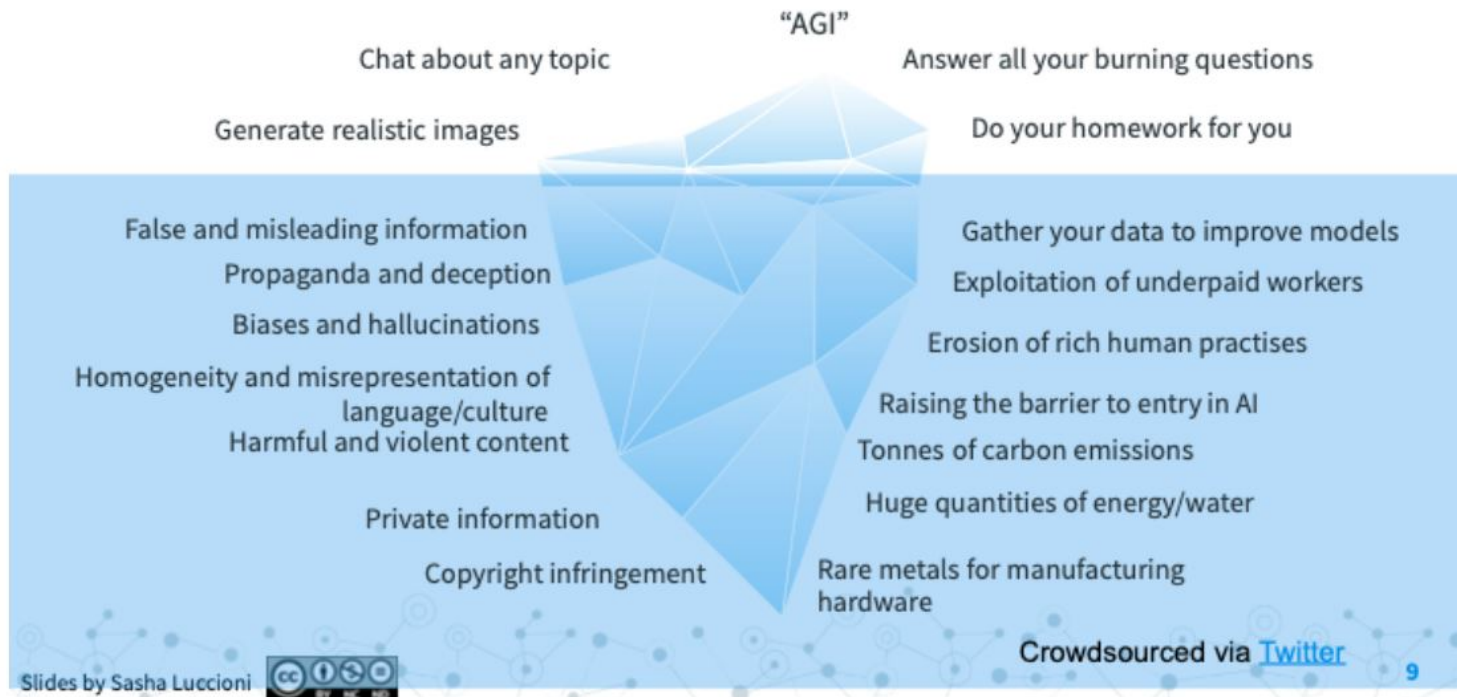


Figure 1: Credit: Sasha Luccioni

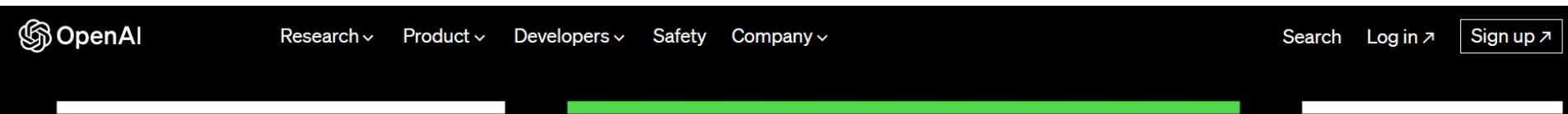


Making privacy core business



What does OpenAI say?

Open AI Limitations: “GPT-4 still has many known limitations that we are working to address, such as social biases, hallucinations, and adversarial prompts. We encourage and facilitate transparency, user education, and wider AI literacy as society adopts these models. We also aim to expand the avenues of input people have in shaping our models.”



We spent 6 months making GPT-4 safer and more aligned. GPT-4 is 82% less likely to respond to requests for disallowed content and 40% more likely to produce factual responses than GPT-3.5 on our internal evaluations.

Making privacy core business



Input, output, governance

So, critical thinking skills are essential when deploying and using generative AI.

From a privacy perspective, I see three key categories of risks relating to:

- Data inputs into generative AI
- Data outputs from generative AI
- Governance





Input risks

- Data used to train generative AI - scraped from the Internet
- Uses massive amounts of data
- Lack of transparency
- User prompt data used to further train generative AI?
- Data quality





Output risks

- Garbage in – garbage out?
- Misinformation – disinformation?
- Sources?
- Is it factual, fake, plausible but not real?
- Incorporates and promulgates biases?
- People tend to believe machines over people





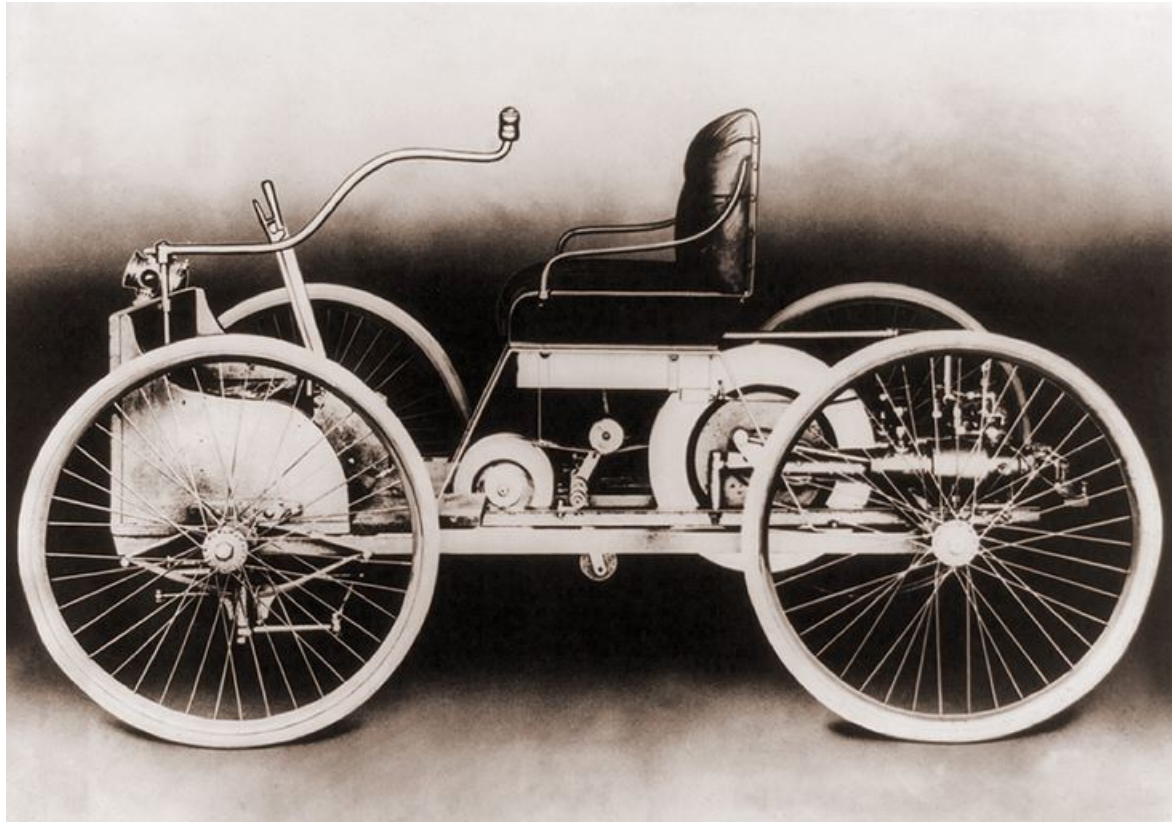
Governance risks

- Who is responsible if something bad happens?
- How do we allocate responsibility?
- How do we stop the proliferation of bad use cases?
- How do people get a say about what happens to their data?





Limited controls in generative AI – much like the original cars



Making privacy core business



Take aways

- Use safe environments to conduct testing – not the mass population
- Build in security and privacy by design (build the brakes!)
- Respect laws

- Don't believe everything you see or hear – apply your critical thinking skills
- Be open to the career that doesn't yet exist today



- [The AI Dilemma](#), presentation created by the Center for Humane Technology
- [Women in Security magazine – my career journey](#)
- [Parliamentary Inquiry to probe AI use in schools and higher education](#) - a framework to guide schools in harnessing AI tools to support teaching and learning is being drafted

Disclaimer: Generative AI was not used in this presentation as far as Privcore is aware.





Source:
<https://shorturl.at/nuFO9>

