Making privacy core business

The first cars didn't have brakes, neither does generative AI

26 June 2023

Privcore Pty Ltd

ACN: 167 388 178

ABN: 46 167 388 178

Email: operations@privcore.com

Website: www.privcore.com

Address: Level 14, 5 Martin Place, Sydney NSW 2000, Australia

The first cars didn't have breaks, neither does generative AI

Annelies Moens, Managing Director Privcore recently presented on a panel discussing 'ChatGPT and Generative AI for business and cyber - embrace or displace?' at AISA's security conference in Sydney, 20 June 2023. This summary covers some of the topics Annelies presented.

Key privacy risks of generative AI

Much like the first cars of the 18th century, generative AI has limited controls. When cars were first invented they had no brakes. It wasn't until accidents occurred that the idea for brakes surfaced. Today, we would not be able to drive fast if we did not have brakes in vehicles.

The same with generative AI; we can't have beneficial innovation for society without effective controls in place. There is no point developing or deploying such models if the risks outweigh the benefits to society. For the benefits to exceed the risks, the brakes (controls) need to be included in their design, development and deployment.

The last few months has seen a proliferation of reports, regulatory interventions globally and risks crystallising with the release to the mass public of generative AI with limited controls.

Generative AI uses natural language learning capabilities to provide text, code, images and music in ways that humans can readily understand. In particular, human-like conversations and interaction can occur with chatbots like ChatGPT.

When these tools use personal information, then privacy laws globally become relevant to their application. Privacy by design has generally not been a consideration in their release, forcing some data protection regulators initially to ban generative AI or issue warnings in their countries. Privacy regulators globally continue to investigate, reacting to wide spread risks that are crystallising.

Below are some key privacy risks that need to be considered from an input, output and governance perspective.

Input

- Data used for training – consider what data is used for training generative AI – people may not expect certain data to be used in training sets. For example, scraping sensitive data, such as facial images from the Internet without consent, is in breach of the Australian Privacy Act as the AAT recently affirmed in its review of the Information and Privacy Commissioner's determination relating to Clearview AI
- Using massive amounts of personal information in training may violate data minimisation principles
- Not being transparent about how algorithms work and whether prompt data from users is fed into continuous learning of the AI is problematic
- Low quality data that has bias and thus generates bias may impact accuracy requirements under privacy law

Output

- Misinformation, disinformation and hallucinations are common outputs of generative AI creating harms that go well beyond privacy risks
- Knowing where your data comes from can be particularly important and is currently required for direct marketing activities
- Cybersecurity risks can arise through the creation of malware and identification of cybersecurity weaknesses

Governance

Who is responsible when things go wrong will become more and more topical. Where will accountabilities lie between developers and deployers of generative AI and other stakeholders?

Proposed changes to the Australian Privacy Act if enacted will also further impact generative AI

In particular, attention should be given to the following proposed changes to the Australian Privacy Act when developing and deploying generative AI as outlined in the Attorney-General's Discussion Paper:

- Passing the fair and reasonable test, particularly in the context of training generative AI models (see proposal 12. 1)
- Conducting privacy impact assessments (PIAs) for high risk activities (extending mandatory PIAs imposed on government to the private sector)(proposal 13.1)
- Transparency in privacy policies about the use of automated decision making and algorithmic transparency required for targeting and profiling (proposal 19)
- Being able to explain where organisations obtained peoples' personal information and dealing with new rights (proposal 18)
- More litigation through a direct right of action where the Privacy Act may have been breached (proposal 26)

Addressing generative AI risks

Many risks can be identified through conducting algorithmic and privacy impact assessments. Privcore conducts these assessments and is listed as a supplier on the National Artificial Intelligence Centre's AI Discoverability Platform Directory.

For further information on other proposed changes to the Australian Privacy Act, read Privcore's article in the May 2023 edition of the Australian Institute of Company Directors magazine.

About Privcore

Privcore's team with over 40 years' combined experience helps business and government make privacy core business, so they can deliver services with the trust and confidence of customers and citizens. Privcore conducts privacy impact assessments, algorithmic impact assessments, privacy health checks or audits, data breach prevention and recovery, privacy by design, builds privacy programs, provides advice, policies and conducts research into privacy and cybersecurity.

Annelies Moens, CIPP/E, CIPT, FIP, FAICD, CMgr FIML, a Superstar of STEM in 2021-2022 and a privacy professional practising since 2001 founded Privcore. She has led and conducted hundreds of privacy consulting deliverables globally. She is a former President of the International Association of Privacy Professionals which she co-founded in Australia and New Zealand in 2008. She has been instrumental in shaping and building the privacy profession in Australia and New Zealand and influencing privacy developments in APEC. She also has extensive privacy regulatory experience and resolved hundreds of privacy complaints whilst working at the Australian privacy regulator.

"My role is to protect one of the most valuable and vulnerable resources in the world - information about people."
ANNELIES MOENS
Privacy expert
Science & Technology AUSTRALIA
SUPERSTARS OF STEM