Making privacy core business

Privacy by Design in AI

12 August 2021

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

Privacy by Design in AI

Artificial Intelligence (AI) that relies on personal information needs to be assessed from a privacy perspective. Below are three Privacy by Design considerations for AI-enabled technologies based on recent work Privcore has undertaken.

1) Ensure the objectives and benefits to all stakeholders are worth the privacy risks

"Privacy Impact Assessments can help assess the overall proportionality of a policy or project, that is whether the use of personal information strikes an appropriate balance between the project objectives and the resulting privacy impacts" as outlined in the NSW Government's AI User Guide.

Consider the objectives sought from the technology deploying AI from all stakeholder perspectives, particularly those the AI is most likely to affect. Are the benefits to them worth the increased privacy risks and is there enough financial support to minimise the risks to an acceptable level?

2) Determine what personal information can be used to train the AI

Machine learning AI needs data to learn. Where the subject matter are people, it is likely to need personal information. However, a general privacy principle is that personal information collected for one purpose cannot be used for another secondary purpose, unless certain conditions are satisfied.

A recent case in South Korea on AI and privacy demonstrates this point. The South Korean Personal Information Protection Commission held that ScatterLab was in breach of the Personal Information Protection Act when it used its customers' personal information to train its chatbot. Customers did not expect their personal information to be used for that purpose. ScatterLab could not rely on a "service development" clause, rather it needed explicit consent from its customers for it to be able to use their personal information to train the AI.

3) Ensure transparency - No black boxes

Where the reasoning and decision making of an AI is not known to those that rely and use the AI, the AI is considered to be a "black box". Non-transparent algorithms can have massive negative consequences on people impacted by the AI and is particularly problematic in government settings where users often have no choice but to submit to the AI the government agency uses. The Australian Human Rights Commission has recently reflected on this in its Human Rights and Technology Final Report. For examples of the destructive nature of black box algorithms, read "Weapons of Math Destruction" by Cathy O'Neil.

About Privcore

Privcore's team with 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, 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.