Sovereign Knowledge Risk from Foundation AI Models

Foundational AI models pose a very high risk to the protection of Australian intellectual property and corporate knowledge. Legislation is required to discourage the unscrupulous use of commercial data for potentially anticompetitive commercial behaviour.

Discussion

The Australian Government has taken the first steps to protect data sovereignty by ensuring that certain data is hosted within Australian data centres. However, with a rapidly emerging technology framework, new challenges have emerged, and these protections are no longer enough.

Getty Images recently sued Stable Diffusion for including 12 million of its images in its foundational model[1], and popular internet site Stack Overflow[2] joined Reddit and Twitter for charging technology giants to use their content. The legal framework around AI and intellectual property is not clear.

What is clear though, is that knowledge now has value, and technology giants will increasingly require new sources of knowledge to feed their models. While there is an argument that publicly available knowledge published on the internet, such as Wikipedia, represents a public good, the same cannot be said of knowledge belonging to individuals and organisations.

The emergence of these foundational models now poses a significant threat to intellectual property rights if technology giants start to train **proprietary models using their customer's data**. While privacy policies offer some basic assurance, such policies vary from company to company and can be changed overnight. The enormous cost of moving customer data between applications makes it impossible for customers to respond if the privacy policy is updated in an unfavourable way.

There is a strong incentive for such companies to use customer knowledge in this way because they can obtain an unfair advantage over their competitors, who do not have access to their customer knowledge. This industry has been plagued with accusations of anticompetitive practices[3].

If a business holds its digital knowledge in a cloud solution, it is technically possible that an AI model could steal this knowledge through harvesting the data hosted on the platform. It would be impossible for any business to know that this has occurred. The software provider could then generate insights about its customers to help cement its dominant market position.

Some technology companies, such as IBM[4], have highlighted this issue and have established their own governance frameworks to reassure customers of data sovereignty. However, other companies have a history of aggressive commercial and anti-competitive practices, and we ought to treat their assurances with caution.

---

1 https://www.theverge.com/2023/2/6/23587393/ai-art-copyright-lawsuit-getty-images-stable-diffusion
2 https://www.wired.com/story/stack-overflow-will-charge-ai-giants-for-training-data/
3 https://www.cnbc.com/2023/06/21/google-accuses-microsoft-of-anticompetitive-practices-in-azure-cloud.html
4 https://www.ibm.com/blog/trustworthy-ai-foundations/

Examples

To illustrate the risk, let's examine the two largest software vendors in the enterprise software market: Microsoft and SAP. Both have the ability and the incentive to harvest knowledge from customers for commercial gain. While there is no suggestion this has, or will occur, there is an obvious commercial incentive to use data in this way, and legislative protection is needed to safeguard Australian intellectual property.

Microsoft hosts millions of government and commercial documents on its cloud services such as SharePoint. It also controls commercial sites such as LinkedIn and GitHub and therefore has unique access to an enormous pool of knowledge about its customers, employees, and business processes.

Similarly, SAP is the market leader in enterprise software, particularly in large multinationals. This software typically covers multiple business functions, such as accounting, human resources, procurement, production, and sales. It also has access to an enormous pool of knowledge about its customers and entire industry sectors.

Even if all identifying information was removed in accordance with privacy laws, a proprietary model trained over these enormous knowledge bases could be incredibly useful to these companies for their internal commercial purposes.

Technology companies using customer knowledge in this way creates an unfair competitive advantage and exposes its customers intellectual property, such as designs, processes, key personnel and "how-how", to the world.

Recommendations

Governments should also put in place protections to ensure that Australian intellectual property and commercial knowledge is not automatically included in such models. Government should examine whether harvesting customer knowledge for the purpose of training foundation models creates an unfair competitive advantage.

The unauthorised inclusion of commercial knowledge in such models is irreversible and must not be left to voluntary codes of conduct to prevent.

Although the Australian Government cannot control the actions of overseas technology giants, it can take steps to ensure that Australians maintain the right to keep their data outside of these foundational models through existing data sovereignty provisions.

Dr Errol Brandt
Knowledge Orchestrator Pty Ltd