Research

With the advent of the AI Big Data era, AI is making our lives easier, but at the same time AI is also invading our private information: phone numbers, email addresses, home addresses and even more private personal data. So I often wonder whether AI poses unpredictable management and new risks to humans.

Process

Stage one

I started by compiling a few keyword fragments about the topic and researched these phrases to come up with keywords that would be a better fit for the topic.

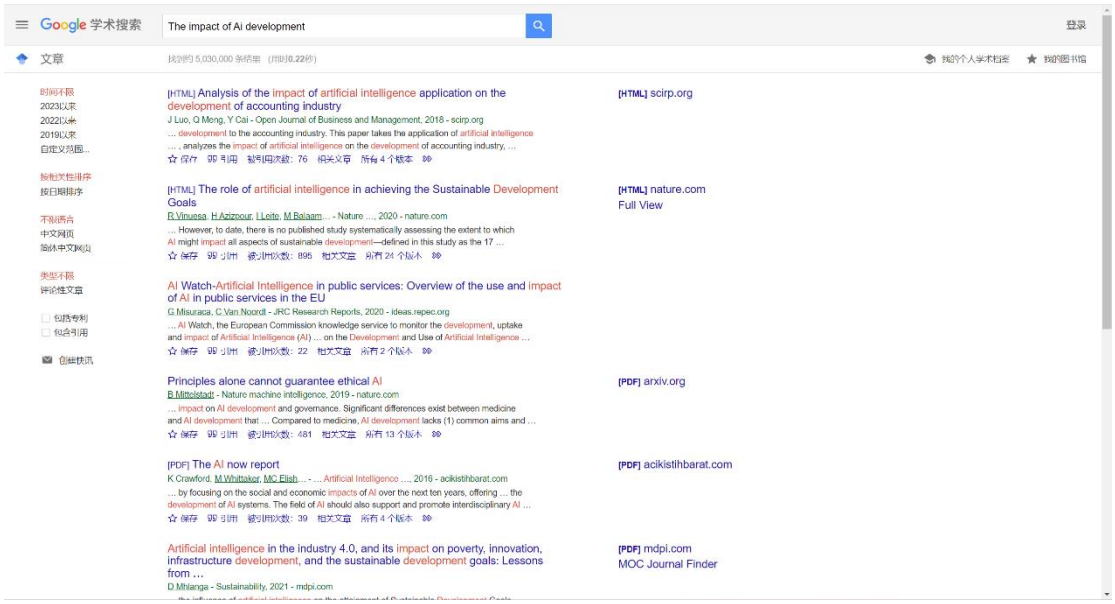
More effective keywords	More invalid keywords
The impact of Ai development	The history of artificial intelligence, the future of artificial intelligence, the impact of artificial intelligence
Surveillance of personal privacy	The need for privacy, information theft and how to protect personal privacy in the age of big data
Artificial intelligence privacy	Positive and negative impacts of artificial intelligence

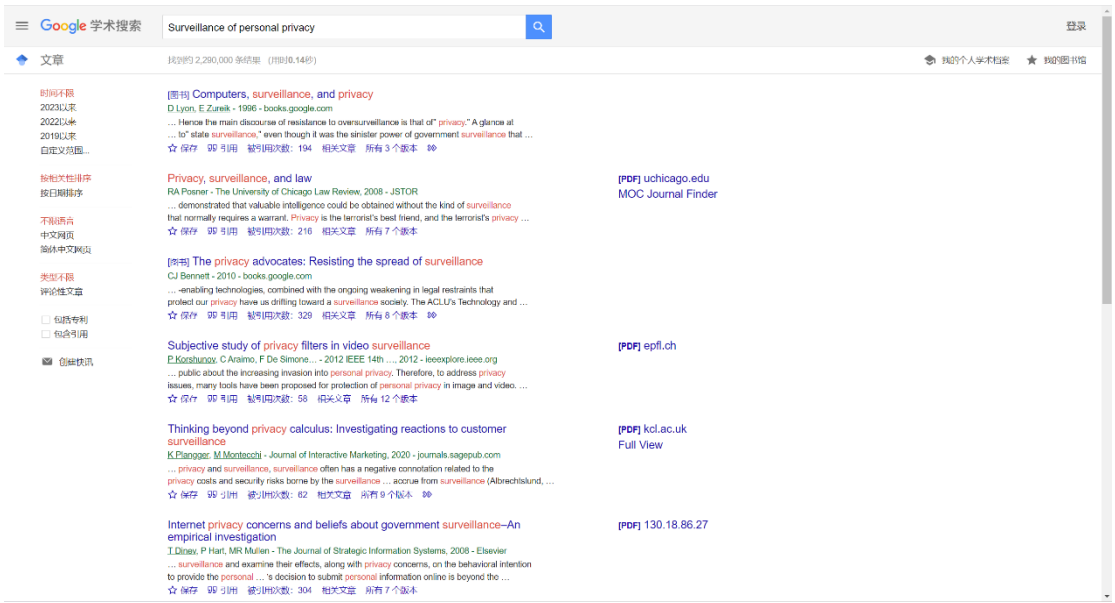
Stage two

I have therefore identified two initial keywords for the direction of this research: "The impact of Ai development" and "Surveillance of personal privacy". The objective of the research was to systematically analyse and collate the literature on the Internet. The objective of the research is to systematically compile Privacy Issues in Artificial Intelligence through research and collation of literature on the internet.

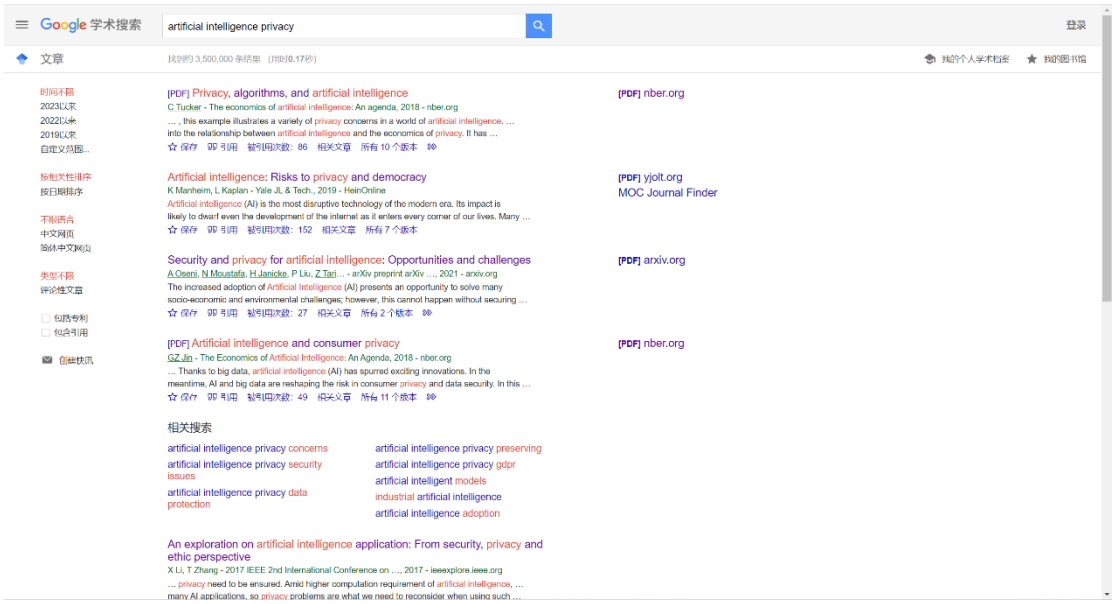
Initially, I chose to search for the keywords 'product design' and 'user requirement' on the Google book platform. This is because I am usually more used to using Google directly to search for what I want and it is easy to use.

Searching for the keywords 'The impact of Ai development' and 'Surveillance of personal privacy' gave me several million results. There is no doubt that there are so many results that it is difficult to find literature that is directly relevant to what I am searching for.





I got the same millions of search results, but on closer inspection I found that the search results were not only related to the keywords in the title, but also in the description of the profile, which showed that these documents were indeed the answers I was looking for.

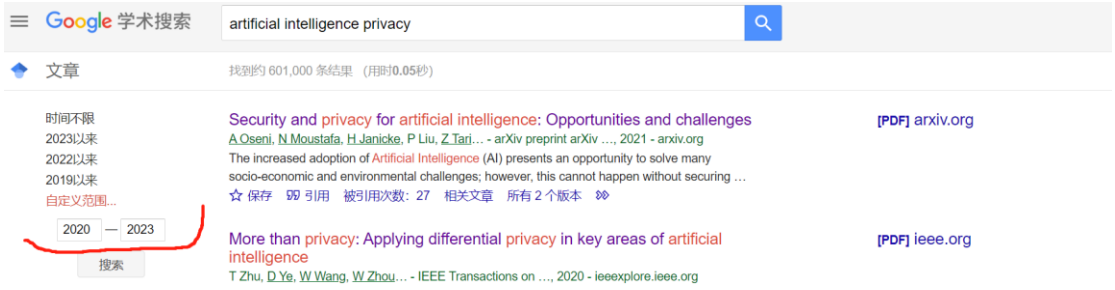


At the same time, I got different results for each platform using this keyword search.

Catalogue of the University of Arts London library	Artificial intelligence privacy	7
Google scholar	Artificial intelligence privacy	3,600,000
Google book	Artificial intelligence privacy	Not shown

Stage three

I then narrowed my search for articles to between 2020-2023 and the results were obvious, the search was narrowed down to 60,000 results. Although it may seem like a lot of results, these were the most recent articles on my keywords and saved me a great deal of time compared to before. I decided to start by looking at these articles from the first page and if this did not contain the answer I was looking for, I would then consider adding restrictions to narrow it down further.



For the first page of literature, I began a quick skim from title to synopsis, from which I found three pieces of literature that were useful to me.

Oseni A, Moustafa N, Janicke H, et al. Security and privacy for artificial intelligence: Opportunities and challenges[J]. arXiv preprint arXiv:2102.04661, 2021.

Curzon J, Kosa T A, Akalu R, et al. Privacy and artificial intelligence[J]. IEEE Transactions on Artificial Intelligence, 2021, 2(2): 96-108.

Murdoch B. Privacy and artificial intelligence: challenges for protecting health information in a new era[J]. BMC Medical Ethics, 2021, 22(1): 1-5.

This first paper describes the main challenges and future research directions in the area of security and privacy for artificial intelligence technologies. Adaptive defences are developed to evaluate in order to protect AI applications. Finally, the main challenges and future research directions for AI technologies in the area of security and privacy are described.

The second literature surveys and provides various scenarios for the use of AI, highlighting the potential risks to privacy and providing various mitigation strategies.

The third literature provides a healthcare perspective to enhance the systematic oversight of big data health research. Appropriate protections are put in place to maintain privacy and patient agency. Private custodians of data may be subject to competing objectives and should be structured to encourage this to ensure that data is protected and discourage other uses.