Privacy Protection Technology in the Age of A.I.

Zhizong Chen*

School of Economics and Management, Southeast University, China

*Corresponding author e-mail: sx_meizi520@163.com

Abstract. In the era of artificial intelligence, no user has ever disclosed personal privacy data to a certain party. The current AI software can fully integrate the fragment information of a user on different site platforms, and finally complete the portrait of the user. In order to prevent personal privacy leakage under the condition of AI, this paper studies the technology of personal privacy protection from the perspective of social engineering. It is found that by fully splitting the personal account group, i.e. using multiple mobile phone numbers and account binding status, and avoiding the use of the registration free login function, personal information is split into multiple or even more than ten user information by AI. At this time, these information will be discarded by AI due to incomplete information, so as to achieve the effect of protecting personal information.

Keywords: Privacy Protection, Social Engineering, Age of A.I.

1. Introduction
Artificial intelligence is a branch of computer science. It attempts to understand the essence of intelligence and produce a new kind of intelligent machine which can react in the similar way of human intelligence. The research in this field includes robot, language recognition, image recognition, natural language processing and expert system, etc. Since the birth of artificial intelligence, the theory and technology are increasingly mature, and the application field is also expanding. It can be imagined that the technological products brought by artificial intelligence in the future will be the "container" of human intelligence [1]. Artificial intelligence can simulate the information process of human consciousness and thinking. Artificial intelligence is not human intelligence, but it can think like human beings and may surpass human intelligence.

In life, everyone has a secret of personal life that they don't want others to know, and this secret has nothing to do with other people's legitimate interests. In law, this secret is called privacy, such as personal private life, diary, photo album, living habits, communication secret, physical defects, etc. It is one's own right to keep one's secrets secret from others [2]. This right is called the right of privacy. However, in the Internet society, personal privacy has become a kind of commodity. On the dark Internet, personal privacy is marked and sold. So no matter in the legal level or computer technology level, the protection of personal privacy has become urgent.
2. The Invasion of Personal Privacy by AI
Even if a person has never disclosed complete personal information to any network platform or any institution, artificial intelligence still has the ability to fully integrate the personal privacy of each Internet user into commercial data through non-standard data integration mining technology and personal network behavior portrait technology [3]. It mainly includes four stages: information crawler, information integration, feature analysis and user portrait. The personal privacy data integrated by AI may be used for various advertising push, and may be directly sold to lawbreakers for illegal purposes.

![Personal Privacy Fragment Data Mining under the Condition of AI Technology](image)

**Figure 1.** Personal Privacy Fragment Data Mining under the Condition of AI Technology

Information crawler: information crawler technology is to save and filter hypertext data returned to the browser by HTTP or HTTPS through legal URL access or XML access, and get effective information in the data after eliminating the identifying statements in hypertext. The latest version of information crawler can also crawl the data in video, audio and photos, with face recognition and other technologies to achieve a comprehensive data crawling [4]. All technologies used by information crawlers are legal technologies, but their ultimate purpose is not legal. So most websites have built the corresponding function of anti data crawler, but this does not completely eliminate the harm of information crawler.

Information integration: for AI systems that steal personal information, when information crawlers cannot provide them with sufficient data support, for their unilateral interests, they will purchase web service interface, API interface or XML interface from some sites with relatively perfect anti crawler technology to obtain the data they need urgently. The construction of data crawler prevention technology system for each website platform is not to protect the personal privacy of users, but to protect the economic interests of the website [5]. So when these data integrators AI buy response data interfaces from them, they generally sell them.

Feature analysis: through the construction of user identification code, the personal privacy information obtained through information crawler or data integration on different platforms is fully integrated, and the data feature analysis is carried out by using scale method, index method and state space projection method, so as to realize the systematic management of personal privacy data.

User profile: the user data through feature analysis has exposed almost all of the user's privacy, the user's contact information, asset status, etc. have been fully exposed, even the case data, credit data, marriage and family members' relevant data have been exposed. However, after the user portrait, AI will cluster all users in different dimensions according to the characteristics of users, form different user data groups, and develop the use value of user privacy data to the extreme.

3. Personal Privacy Protection Strategy in the Age of AI
In the age of AI, there is no technical feasibility to protect personal privacy completely in theory, and the personal privacy sorting system driven by artificial intelligence has reached an all pervasive state.
And driven by huge economic benefits, we can't avoid websites sharing personal privacy data. Therefore, we must adopt a certain anti-reconnaissance strategy to fully protect personal privacy.

First, fully isolate the personal network account.

At present, WeChat, Weibo, QQ, etc. have opened the quick login API interface to all websites. As long as you use existing accounts such as WeChat, Weibo, QQ, etc., you can log in to most website platforms without registration. But this behavior is the key to the loss of privacy for most users. If new registration is adopted in all common websites, and there is no logical correlation between the registered user name, avatar and other features, it is difficult for AI to analyze the relationship between these accounts, and its mining of personal privacy will judge each account as an independent owner, and it is difficult to conduct a comprehensive mining and analysis of personal privacy.

Second, use multiple mobile phone numbers and email addresses.

Mobile phone number and email address are the key references for each platform to identify user ID code. If multiple mobile phone numbers and email addresses are used, the system cannot determine whether the owner of the mobile phone number and email address is the same person. But in this case, the cross use of mobile phone number and email address should be avoided, and the mobile phone number and email address should be bound. If the two are used together, it is easy for AI to find the correlation between all mobile phone numbers and all mailboxes, and this protection becomes virtual.

That is, by fully separating the user name, avatar, mobile phone number, mailbox, etc. used by individuals, the personal online information is divided into multiple roles, so that the AI system can identify one person's behavior as the information of multiple individuals, so that everyone's information is incomplete, and invalid information will be formed in the AI system, which will be automatically dropped. In the process of participating in ground activities, for example, the information input of work units, bank card credit card information, mobile phone number information and email information used for information registration such as car purchase and house purchase are separately blocked, and even different mobile phone numbers and personal account information combinations are used in these information, while other mobile phone numbers and personal account information are used in Internet behavior This situation can make the personal information acquired by AI more useless.

Of course, if the personal information has indeed been used by lawbreakers, and it brings trouble to the daily life of individuals, even brings life danger or property loss to individuals, then it is difficult to fully protect the personal privacy by technical means alone, and alarm processing is also an inevitable choice.

4. Summary

Under the current AI technology conditions and the current Internet economic interest driven mode, the protection of personal privacy can only be limited at the technical level. Through the analysis of this paper, the state of personal privacy protection is to divide the logical relationship between accounts reasonably, so that the personal privacy information mined by artificial intelligence is allocated to multiple user portraits, resulting in each portrait being discarded because of incomplete data. This mode can still effectively protect personal privacy under the current AI technology conditions, but it does not exclude whether artificial intelligence technology will be further improved in the near future. But personal privacy awareness is an effective way to ensure personal security.

References

[1] Cheng-Kai Liu, Ching-Yen Tu, Hsing-Ru Lin, Ko-Ting Cheng. Asymmetrical transmission windows for daily privacy protection using cholesteric liquid crystals[J]. Optics and Laser Technology, 2020, 121.

[2] Wei Kong, Jian Shen, Pandi Vijayakumar, Youngju Cho, Victor Chang. A practical group blind signature scheme for privacy protection in smart grid[J]. Journal of Parallel and Distributed Computing, 2020, 136.

[3] Zhaoe Min, Geng Yang, Arun Kumar Sangaiah, Shuangjie Bai, Guoxiu Liu. A privacy
protection-oriented parallel fully homomorphic encryption algorithm in cyber physical systems[J]. EURASIP Journal on Wireless Communications and Networking, 2019, 2019(1).

[4] Dong Jing, Ting Liu. Context-based influence maximization with privacy protection in social networks[J]. EURASIP Journal on Wireless Communications and Networking, 2019, 2019(1).

[5] Chunyong Yin, Biao Zhou, Zhichao Yin, Jin Wang. Local privacy protection classification based on human-centric computing[J]. Human-centric Computing and Information Sciences, 2019, 9(1).