The Impact of Public Privacy Concerns on the Acceptance of AI in Social Good Projects

Xinyi Li [1], Yinuo Song [2, *] and Zhenxiang Zhu [3]

[1] Faculty of Humanities and Social Sciences, University of Nottingham Ningbo China, Ningbo, Zhejiang, China

[2] Faculty of Arts, Design and Architecture, University of New South Wales, Sydney, Australia

[3] Data Science & AI, HongKong Metropolitan University, HongKong, China

* Corresponding Author Email: songyinuoaus@gmail.com

Abstract. This study mainly explores the relationship between the public's privacy concerns and the acceptance of artificial intelligence technology in public welfare projects driven by artificial intelligence. According to the privacy calculus model (PCM) and the technology acceptance model (TAM), the study shows that the public's privacy concerns will indirectly affect the perceived usefulness of the technology by affecting the public's perceived risks, and ultimately affect the public's acceptance of artificial intelligence technology in public welfare projects. For example, in public welfare projects such as medical care, education, and environmental protection driven by artificial intelligence, concerns about privacy leakage often reduce public trust and acceptance, affecting the advancement of projects and the development of artificial intelligence technology. On the contrary, effective privacy protection measures and open and transparent information disclosure behaviors can alleviate these concerns and increase the public's willingness to accept. The results of the study provide a theoretical framework for understanding how the public's privacy concerns in social welfare projects affect technology acceptance, and provide a basis for technology developers and policymakers to better improve technology and policies. Finally, the study proposes a strategy to balance technology development and privacy protection and reduce perceived risks while enhancing perceived usefulness.

Keywords: Public Privacy, Social Good Projects, privacy calculus model, technology acceptance model, artificial intelligence.

1. Introduction

In recent years, with the development of artificial intelligence technology, the application of AI in society has become more and more popular. The advancement of technologies such as big data, cloud computing, natural language processing (NLP), and deep learning has given AI great advantages in improving efficiency, optimizing resource allocation, and promoting innovation. It has also shown broad applications in social welfare project prospects. For example, the application of Google's "AI for social good" project in the diagnosis of diabetic retinopathy has significantly improved the efficiency of disease screening, which is a major progress in AI's promotion of social welfare [1].

However, despite these benefits, the expansion of AI has also raised concerns about privacy and security. Since AI systems often collect sensitive data such as users' locations, contacts, calendars, and activity histories, the possibility of privacy leakage has become a major obstacle to the public's acceptance of AI technology in public welfare projects. According to the report "Trust in Artificial Intelligence: A Global Study", 61% of respondents are skeptical about AI and 73% are concerned about privacy issues, especially in applications such as recommendation systems and public safety. Privacy issues are significantly affecting the public's acceptance of technology [2].

In the academic field, although the number of studies on artificial intelligence has increased dramatically, research on the challenges of understanding and applying it at the individual level is still limited. Most studies focus on macro-level research in the business and public administration sectors, with fewer studies on public welfare projects and the individual level [3]. Existing research has confirmed that privacy issues are the main obstacle to public acceptance of technology [4].

Artificial intelligence has great potential to improve human happiness and promote social welfare and is also a major direction of technological progress. Therefore, research on the application of artificial intelligence technology in public welfare projects is very important [5-7].

This study aims to explore the relationship between the public's privacy concerns and the acceptance of artificial intelligence technology in public welfare projects. By integrating PCM and TAM theories, this study aims to provide valuable insights for the future development and policymaking of artificial intelligence, ensuring the responsible and effective use of artificial intelligence technology in social welfare projects.

2. Analysis of the impact of privacy concerns

This section mainly analyzes how the public's privacy concerns in social welfare projects affect the acceptance of AI technology based on PCM and TAM theories.

2.1. Public privacy concerns and AI technology acceptance from the perspectives of PCM and TAM theories

The PCM theory was proposed by Dinev and Hart. It refers to the fact that when users decide whether to disclose personal information, they will calculate to weigh the potential risks and benefits [8]. This theory provides a framework for understanding people's decision-making in the process of technology acceptance and information disclosure. Among them, perceived risk refers to the subjective assessment of potential losses when using a service or product, reflecting a combination of uncertainty and the severity of consequences [9]. In contrast, perceived benefits refer to the positive utilities that users believe the technology may bring, such as functional, economic, or social advantages [10]. In the PCM framework, privacy concerns are considered to be the core antecedent affecting perceived risk. High privacy concerns amplify users' perceived risks, thereby reducing their willingness to disclose information and technology acceptance [8,10].

This trade-off between perceived benefits and risks also exists in the context of AI being applied to social welfare projects. In recent years, due to the lack of transparency in technology development and frequent data abuse incidents, the public's awareness of privacy rights has continued to increase, and privacy issues have become a key factor affecting technology acceptance [11]. In public welfare projects, in the medical field, although AI technology has improved the accuracy and efficiency of diagnosis, the sensitivity of personal health data has led some members of the public to adopt a cautious attitude [12]. In the field of education, AI can improve learning outcomes and resource equity through personalized teaching plans, but due to data bias and surveillance culture, it has caused concerns among parents and students [13]. In terms of environmental protection, AI can effectively monitor environmental data and optimize resource allocation. However, users' personal location or behavior data may be leaked, which hurts their willingness to accept [14]. Therefore, in the context of AI being applied to social welfare projects, the public's degree of concern about privacy will significantly affect its acceptance. Individuals with lower privacy concerns may be more inclined to prioritize functional or social benefits, while individuals with higher privacy concerns may reduce their willingness to adopt such technologies due to their concern about potential privacy risks, affecting the development of the technology.

TAM is one of the basic theories for understanding user behavior and technology adoption. It was proposed by Fred Davis based on the Theory of Reasoned Action (TRA) and the Theory of Planned Behavior (TPB) in psychology to predict and explain users' acceptance of technology. TAM shows that external variables indirectly affect the actual acceptance and use of technology by affecting users' perceived usefulness (PU) and perceived ease of use (PEOU). PU refers to "the subjective probability that a potential user will improve his or her work performance in an organizational environment by using a specific application system" [15]. PEOU refers to the degree to which users find technology easy to learn and use. In other words, PU and PEOU are two key variables that affect users' behavioral intentions, and they can directly predict users' actual usage behavior [16].

As the model develops, TAM incorporates more variables that affect perceived usefulness, such as perceived risk and privacy concerns. For example, Pavlou integrated trust and perceived risk into TAM in his research, pointing out that perceived risk is a key factor affecting technology acceptance [17]. In addition, the study by Schomakers et al. applies variables (e.g., privacy concerns, perceived risk, and perceived benefits) from the PCM to the TAM model, which further complements the explanatory power of TAM from a privacy perspective [10]. These changes enrich the TAM theory and increase the persuasiveness of the model on modern technology acceptance behavior.

In this study, the model can be shown to indicate that an increase in the public's perceived risk of an AI public good project will weaken the perceived usefulness of the AI technology, thereby reducing the technology acceptance of the project. For example, in the medical field, although AI technology can improve diagnostic efficiency and accuracy, if the public's concerns about privacy leakage are high, they will be skeptical about the actual usefulness of the technology, thus reducing their willingness to accept the technology. Similarly, in the education sector, while AI can personalize education programs and improve resource allocation, parents and students may perceive its utility as less than expected due to concerns about misuse or improper storage of student data, which can undermine its perceived usefulness. In the environmental domain, while AI technologies for optimizing resources and monitoring the environment have significant social benefits, potential risks to personal data (e.g., leakage of location information) may reduce the public's trust in the technology, which in turn affects its adoption intentions.

Therefore, the TAM model combined with privacy-related variables not only explains the key influencing factors in the process of technology acceptance but also provides a systematic analytical framework for the study of privacy risk and technology adoption in AI public benefit projects. Through this model, it is possible to further understand how to increase perceived usefulness while reducing perceived risk to enhance public acceptance of AI public benefit projects.

2.2. Exploring the relationship between public privacy concerns and technology acceptance in AI social good projects based on the integration of PCM and TAM

The above analysis reveals that the PCM and the TAM share common ground in studying users' technology acceptance decisions. The intersection lies in the role of privacy concerns, which indirectly influence PU through perceived risk. This pathway reflects the theoretical integration of the two models. In this study, this relationship is manifested as follows: when the public expresses concern about privacy breaches in AI social good projects, they weigh the risks against the benefits. If perceived risks outweigh anticipated benefits or individuals are unwilling to accept privacy risks for technological benefits, their perception of the technology's usefulness diminishes, thereby reducing their willingness to accept the technology.

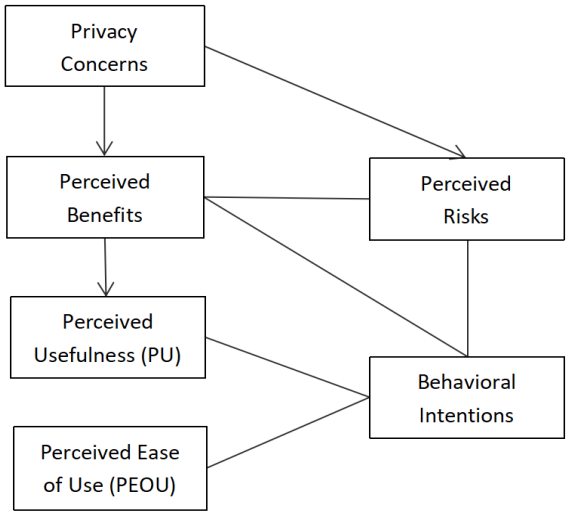

Fig. 1. Privacy Concerns and Technology Acceptance Path Model.

As illustrated in Fig. 1, the summarized influence pathway in this study is: Privacy Concerns → Perceived Risk → Perceived Usefulness → Behavioural Intention → Technology Acceptance. In this pathway, users with higher privacy concerns exhibit greater sensitivity to the collection and misuse of their information, intensifying their perception of potential threats posed by the technology [17,18]. The increase in perceived risk significantly reduces users' expectations of technological benefits. When risks are deemed to exceed functional or economic benefits, evaluations of the technology's usefulness decline [9]. Since perceived usefulness is a core driver of behavioral intention, negative perceptions directly suppress the intention to adopt the technology, ultimately lowering actual technology acceptance [15].

In conclusion, the integration of PCM and TAM provides a critical theoretical framework for understanding how the public weighs privacy concerns in AI social good projects. It also offers an analytical foundation for further exploring how privacy concerns affect technology acceptance.

3. The specific impact of privacy concerns

3.1. Differentiated impacts of privacy concerns across AI fields

Privacy concerns have different impacts (both positive and negative) in different domains, but the transmission mechanisms are very similar.

For example, in healthcare, generative AI can revolutionize the healthcare field in several ways: the ability of AI to identify conditions, patterns, abnormalities, and risks (e.g., the aforementioned Google AI identifying diabetic retinopathy); and delivering dramatic improvements from administration to clinical decision support, which in turn improves patient outcomes, reduces costs, and accelerates medical discovery [19]. However, these systems that rely on large amounts of data also present new security and privacy risks, especially as it relates to the privacy of information in protected health information (PHI) and healthcare information systems (HIS). According to Akamai's report, the healthcare industry faces unique challenges in terms of cybersecurity, and the value of the information it holds is higher than that of other industries, which makes the healthcare industry one of the primary targets for data breaches, and the magnitude of the problem remains particularly acute across industries [20]. The impact mechanism is specifically that privacy concerns elevate perceived risk and lead to lower patient trust in AI technology. Until regulations and regulatory systems are improved, the importance users place on privacy concerns will also be a major obstacle preventing the application and development of AI in healthcare.

In education, AI in education offers many opportunities to improve the educational process, from personalized curricula to the automation of assessment and administrative tasks. However, as Dzhorobaeva et al point out in their study, overuse of AI can also have serious negative consequences: insufficiently protected student data may be compromised, affecting student privacy; AI algorithms may exacerbate or reproduce social biases, especially on gender, race, or socio-economic background; and participants in the educational process (e.g., teachers, students) may lack understanding of the AI process, leading to misunderstanding or reliance on its results [21]. The specific mechanism of impact is also that privacy concerns elevate the perceived risk, thus weakening parents' and students' trust in educational AI systems. Therefore, it is crucial to increase the transparency of AI applications in education, such as the type of data collected, how it is processed, and how conclusions are drawn, but the increase in transparency is challenged due to intellectual property protection and the complexity of AI algorithms [22].

In the field of environmental protection, AI and big data technologies can help to collect complex, heterogeneous, high-resolution environmental data and process them through AI models to estimate and predict climate change, and environmental quality (e.g., air quality), to generate personalized alerts and recommendations to improve individual health and well-being and to facilitate relevant decision-making [23]. However, in environmental protection, much of the data is collected and shared by multiple entities (e.g., governments, businesses, and research organizations). If the sharing and use of these data are not sufficiently transparent or regulated, it may lead to data misuse or

unauthorized use, such as for commercial purposes or political manipulation [24]. According to the Citizen Ecological environmental behavior survey report, the public is more concerned about environmental benefits, with nearly 80% of respondents actively disseminating or participating in environmental information exchange. However, the public's priority for privacy concerns in environmental protection scenarios is relatively low compared to other areas, with only 14.8% of respondents having been involved in reporting environmental problems, suggesting that privacy concerns have had a very limited impact on the public's acceptance of technology in the environmental protection arena [25].

However, another study shows that privacy concerns reverse the public's willingness to accept technology when privacy policies are transparent, and protections are in place [26]. In 2020, Apple released changes regarding privacy labeling and introduced an Application Tracking Transparency (ATT) policy [27]. According to Statista, the strong correlation between iPhone sales in 2020 and the introduction of privacy-protecting features in 2020 is enhanced, with about 81% of Apple users stating that one of the reasons they chose an Apple product was the company's commitment to privacy, especially after Apple publicly promised that its products would not sell users' data and introduced related privacy-protecting features [28].

In summary, privacy concerns can have different impacts in different domains. For example, in the medical field, privacy concerns significantly reduce public trust in AI technology, especially in the case of health data leakage; in the education field, in addition to data leakage, privacy concerns lead to more serious social problems, such as exacerbation of social prejudices such as gender, race, and economic background; and in the field of environmental protection, privacy concerns are less common and the public is more concerned about the environmental benefits of the technology. On the contrary, the impact of privacy concerns on various domains is not necessarily negative; the example of iPhone sales proves that in information security, privacy concerns enhance users' preference and use of a certain product when the privacy policy is sound. In sum, although the structure of the impact of privacy concerns on different domains is different, there is a consistency in the transmission mechanism: by affecting the perceived risk (elevated or lowered) and thus changing users' acceptance of AI.

3.2. Differential impact of privacy concerns at the individual level

Research shows differences in acceptance of AI privacy concerns among different age groups. Younger people are typically open to new technologies, including AI, but their privacy concerns are on the rise [29]. According to the Pew Research Centre, about 70% of young people (18-29 years old) are willing to use AI technologies (e.g., smart assistants) in certain situations, and respondents over 55 years old have significantly higher concerns than young people about AI surveillance and data collection, especially about inappropriate use or leakage of important information such as personal health data and financial data [30].

Acceptance of AI influenced by privacy concerns also varies across educational backgrounds, with the Pew Research Centre study showing that higher education groups (bachelor's degree and above) typically have higher rates of AI privacy concerns. Specifically, in the U.S., 71% of highly educated people say they are concerned that AI will invade their privacy or misuse their data, compared to 45% of lower-educated people. Compared to the low-education group, the high-education group is typically more cognisant of privacy risks and also tends to be concerned about the transparency of the technology and the controllability of the data.

In summary, the differentiation of privacy concerns is also reflected in the context of age and education, while young people's openness to new technologies and increased concern for privacy protection further reflect the public's core demands for technology transparency and data security. This diverse demand provides an important reference for the future development of AI technology and the optimization of privacy policies.

4. Discussion and recommendations

When analyzing how the public's privacy concerns affect the acceptance of AI technology in public interest projects, we need to consider multiple perspectives. It is important to pay attention to the public's increasing demand for privacy protection and ensure that technology developers' efforts in transparency and security are balanced with the actual needs of public interest projects.

4.1. Enhancing public awareness and trust in privacy protection

Privacy issues are one of the core obstacles to the public's acceptance of AI technology. Research shows that when the public faces the risk of privacy leakage, they may be more inclined to refuse to use AI technologies involving personal data, even if these technologies can significantly improve the efficiency or effectiveness of welfare projects [31]. Therefore, recognizing the public's demand for privacy protection and enhancing their trust in technology are necessary conditions for technological development and are also key to achieving the goals of public welfare projects.

First, governments, non-profit organizations, and technology developers need to work together to continuously improve ethical standards laws, and regulations regarding AI technology and enhance the importance of privacy protection [32]. For example, Google has detailed its ethical standards and commitment to transparency in the use of AI technology in public interest projects in its 'AI Principles' white paper, an open and transparent approach that not only helps to enhance public trust in the technology but also enables the public to understand the ethical considerations and safety and security behind the technology, thus easing their concerns [33]. Besides, public interest projects themselves need to find a balance between privacy protection and technology applications. For example, when designing public interest services, priority can be given to the use of anonymization or differential privacy technologies, which can ensure the validity of the data while minimizing the infringement of personal privacy.

As some scholars have pointed out, the public will be more willing to participate and share personal information when they realize that AI technologies are not only safe and secure but also can improve the effectiveness of public interest projects. But all this presupposes that the promise of privacy protection must be really credible and rigorously implemented in practice [34].

4.2. Strengthening privacy protection measures for AI technology

The application of AI technology in public welfare projects needs to strictly follow the principle of privacy protection. Developers should not only adopt advanced encryption technology, differential privacy, federated learning, and other technical means but also establish comprehensive data access and use rights management mechanisms. For example, differential privacy technology can effectively protect personal information while safeguarding the overall efficacy of data; federated learning allows model training without sharing the original data, thus finding a balance between data privacy and technology development [35].

In addition, AI technology developers and public interest organizations should develop clear standards and industry norms for the practice of privacy-preserving technologies. By introducing independent third-party organizations to evaluate and certify the privacy protection measures of AI technology, public trust in the technology can be further enhanced. Meanwhile, the establishment of a data leakage response mechanism, including risk warning, incident notification, and emergency response plan, can also effectively reduce the negative impact of possible privacy leakage [36].

By strengthening the privacy protection measures of AI technology, the public's concern about privacy leakage can be significantly reduced, thus enhancing their acceptance of AI technology. This will not only help promote the widespread application of AI technologies in public welfare projects but also contribute to the overall well-being of society.

4.3. Balancing public good needs and individual privacy interests

When applying AI technology in public welfare projects, it is necessary to carefully weigh the relationship between public welfare needs and individual privacy rights. When designing technology, the public's privacy needs should be fully considered to ensure that the use of the technology complies with legal and ethical standards. At the same time, it is necessary to establish an effective public feedback mechanism and actively listen to the public's requirements, which will not only enhance public trust but also support the sustainable development of public welfare projects.

Finally, balancing public interest and privacy requires strengthening interdisciplinary collaboration. Governments, technology companies, academic institutions, and nonprofit organizations can work together to develop industry standards and policy frameworks to provide clear guidelines for the application of technology. Such collaboration can not only reduce the arbitrariness of data use but also provide a legal basis for privacy disputes, thereby enhancing public trust.

5. Conclusion

The public's privacy concerns play a key role in influencing the acceptance of artificial intelligence technology in public welfare projects. This study uses PCM and TAM as theoretical frameworks to sort out the impact relationship between privacy concerns and technology acceptance. By exploring the application of artificial intelligence in public welfare fields such as medical care, education, and environmental protection, this study found that although increased privacy concerns often lead to reduced public trust and adoption, effective privacy protection measures can effectively avoid these risks and improve the public's acceptance of these technologies. Therefore, when designing these technologies, technology developers should fully consider the public's privacy rights, provide adequate protection, and enhance public trust by increasing transparency and data usage statements. Only in this way can artificial intelligence technology better serve public welfare and promote social progress while protecting public privacy.

Authors Contribution

All the authors contributed equally, and their names were listed in alphabetical order.

References

[1] M. O. Khan, Towards Efficient and Responsible AI: Developing Resource-Efficient and Fair Deep Learning Models, Ph. D. thesis, New York University, Tandon School of Engineering (2024)

[2] N. Gillespie, S. Lockey, C. Curtis, J. Pool, A. Akbari, Trust in artificial intelligence: A global study. The University of Queensland and KPMG Australia, 10 (2023)

[3] J. Radhakrishnan, M. Chattopadhyay, Determinants and barriers of artificial intelligence adoption–A literature review. In Re-imagining Diffusion and Adoption of Information Technology and Systems: A Continuing Conversation: IFIP WG 8.6 International Conference on Transfer and Diffusion of IT, TDIT 2020, Tiruchirappalli, India, December 18-19, Proceedings, Part I. Springer International Publishing 89-99 (2020).

[4] S. A. Vannoy, P. Palvia, The social influence model of technology adoption. Communi. ACM, 53, 149-153 (2010)

[5] M. Nayak, J. Tiyadi, Social Welfare, and Artificial Intelligence's Role: A Comprehensive Summary of the Study. AI in the Social and Business World: A Comprehensive Approach, 32-66 (2024)

[6] U. Lindqvist, P. G. Neumann, The future of the Internet of Things. Communi. of the ACM, 60, 26-30 (2017)

[7] E. Attié, L. Meyer-Waarden, the acceptance and usage of smart connected objects according to adoption stages: an enhanced technology acceptance model integrating the diffusion of innovation, uses and gratification and privacy calculus theories. Technol. Forecast. Soc. Change. 176, 121485 (2022)

[8] T. Dinev, P. Hart, An extended privacy calculus model for e-commerce transactions. Inf. Syst. Res. **17**, 61-80. (2006)

[9] M. S. Featherman, P.A. Pavlou, Predicting e-services adoption: a perceived risk facets perspective. Int. J. Hum. Comput. Stud. **59**, 451-474 (2003)

[10] E. M. Schomakers, C. Lidynia, M. Ziefle, the role of privacy in the acceptance of smart technologies: Applying the privacy calculus to technology acceptance. Int. J. Hum. Comput. Stud. **38**, 1276-1289 (2022)

[11] P. Carey, Data protection: a practical guide to UK and EU law. Oxford University Press, Inc. (2018)

[12] M. Y. Shaheen, Applications of Artificial Intelligence (AI) in healthcare: A review. Sci. Open Preprints. (2021)

[13] W. Holmes, I. Tuomi, State of the art and practice in AI in education. Eur. J. Educ. **57**, 542-570 (2022)

[14] Y. Himeur, B. Rimal, A. Tiwary, A. Amira, Using artificial intelligence and data fusion for environmental monitoring: A review and future perspectives. Inf. Fusion **86**, 44-75 (2022)

[15] F. D. Davis, Technology acceptance model: TAM. Al-Suqri, MN, Al-Aufi, AS: Information Seeking Behavior and Technology Adoption. **205**, 219 (1989)

[16] N. Marangunić, A. Granić, Technology acceptance model: a literature review from 1986 to 2013. Universal Access Inf. **14**, 81-95. (2015)

[17] P. A. Pavlou, Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. Int. J. Electron. Commer. **7**, 101-134. (2003)

[18] T. Dinev, P. Hart, An extended privacy calculus model for e-commerce transactions. Inf. Syst. Res. **17**, 61-80 (2006)

[19] Y. Chen, P. Esmaeilzadeh, Generative AI in medical practice: In-depth exploration of privacy and security challenges J. Med. Internet Res. 26 (2024)

[20] Akamai. Cyber Attack Healthcare Report 2024. (2024)

[21] M. A. Dzhorobaeva, K. A. Mamadalieva, A. S. Kaliev, Ethical aspects of the use of AI in education: issues of confidentiality, fairness and transparency. (2025)

[22] R. Vilsack, Emerging Innovations in Data Transparency, Governance, and Quality. NSC. (2022)

[23] S. Madan, P. Kumar, S. Rawat, T. Choudhury, Analysis of weather prediction using machine learning & big data. In 2018 International conference on advances in computing and communication engineering (ICACCE) 259-264 (2018)

[24] C. Wang, L. Ma, Third-party monitoring and environmental data manipulation: the case of air quality control in Chinese cities. In Handbook on Climate Change and Environmental Governance in China 345-359 (2024)

[25] Ministry of Ecology and Environment. Citizen ecological environmental behavior survey report. Beijing: Center for Environmental and Economic Policy Research. (2022)

[26] P. Esmaeilzadeh, The impacts of the perceived transparency of privacy policies and trust in providers for building trust in health information exchange: an empirical study. JMIR Med. Inform. **7**, e14050 (2019)

[27] Apple, App privacy details on the App Store. (2020) Retrieved from: https://support.apple.com/zh-cn/102399

[28] Statista, User opinion on Apple's new privacy policies in the United States. Statista. (2023) Retrieved from: https://www.statista.com/statistics/1224850/user-opinion-on-apple-s-new-privacy-policies-us/

[29] Time, what teenagers think about AI. (2024) Retrieved from: https://time.com/7098524/teenagers-ai-risk-lawmakers/

[30] Pew Research Center, U.S. adults under 30 have different foreign policy priorities than older adults. Pew Research Center. (2024) Retrieved from: https://www.pewresearch.org/short-reads/2024/07/19/us-adults-under-30-have-different-foreign-policy-priorities-than-older-adults/

[31] B. C. Stahl, D. Wright, Ethics and Privacy in AI and big data: Implementing responsible research and innovation. IEEE Secur. Priv. **16**, 26-33 (2018)

[32] W. J. Von Eschenbach, Transparency and the black box problem: Why we do not trust AI. Philos. Technol. **34**, 1607-1622 (2021)

[33] Google, AI Principles: Responsible AI for everyone. (n.d.) Retrieved from: https://ai.google/responsibility/principles/

[34] N. Tomašev, J. Cornebise, F. Hutter, S. Mohamed, A. Picciariello, B. Connelly, C. Clopath, AI for social good: unlocking the opportunity for positive impact. Nat. Commun. **11**, 2468 (2020)

[35] A. El Ouadrhiri, A. Abdelhadi, Differential privacy for deep and federated learning: A survey. IEEE **10**, 22359-22380 (2022)

[36] K. Wei, J. Li, M. Ding, C. Ma, H. H. Yang, F. Farokhi, H. V. Poor, Federated learning with differential privacy: Algorithms and performance analysis. IEEE Trans. Inf. Forensics Secur. **15**, 3454-3469 (2020)