Online Social Networks (OSNs)

Sattikar and Kulkarni (2012) discussed the role of AI techniques based on neural networks, genetic algorithms, expert systems, and fuzzy logic in solving security and privacy issues of social networking. They mention how AI can help reduce subjectivity in security assessments. The authors introduced some of the various AI techniques like ML, data mining, and pattern recognition that can be used to solve problems such as identity theft detection, and privacy concerns on social networks. Hirschprung and Alkoby (2022) proposed a new framework called Online Information-Sharing Assistance (OISA) to help users better navigate the trade-offs between benefits and the costs of privacy risks when sharing information online. OISA models information sharing as a game using concepts from game theory. It represents all relevant factors like benefits, costs, privacy losses in sharing different types of information. It develops AI agents that use heuristic search algorithms to maximize a user's "bottom line utility" in the information sharing environment. An empirical study which simulated Facebook showed that OISA AI agents achieved significantly higher utility scores than human participants, proving that AI can help with this challenging task. The authors claim that OISA is an important initial step towards bridging the gaps between theory and reality in information sharing and developing intelligent assistants. Wang et al. (2021) investigated the dynamics between consumer privacy and AI-driven e-commerce. In their work the authors utilize evolutionary game theory to model the interactions between consumers and e-commerce platforms, focusing on the privacy concerns arising from AI technology in online shopping. The study explores the balance between personalized services and privacy, suggesting strategies for both consumers and platforms to maximize benefits while safeguarding privacy. It emphasizes the importance of effective regulation and trust-building in this evolving landscape.

Majeed and Hwang (2023) investigated the relations of AI and information privacy. They primarily focus on the dual role of AI as both a protector and a threat to privacy in the context of data sharing. The authors emphasize the underestimated threats posed by AI-generated synthetic data to information privacy, particularly in undermining existing anonymization methods. With experiments using real-life datasets, the authors demonstrate how AI can compromise individual privacy, stressing the need for more robust privacy mechanisms in the era of advanced AI technologies. They focus on the ongoing discourse on balancing AI's benefits against the potential risks to privacy in data publishing scenarios. Wang et al. (2022) provided a comprehensive overview of the metaverse, including its architecture, characteristics, enabling technologies, and applications. They discuss security and privacy challenges in the metaverse, such as threats to authentication, access control, data management, and privacy. Their survey highlights current and potential countermeasures for these challenges, emphasizing the need for scalable, resilient, and interoperable solutions. Their work serves as a foundation for understanding the metaverse's complexities and guiding future research to build secure and privacy-preserving metaverse systems. Subramanian (2017) explored the legal, security, privacy, ethical, and policy considerations surrounding the use of social robots, which are becoming increasingly prevalent in society. He discusses various legal cases and judgments related to robots, highlights the challenges of ensuring security and privacy in the development and use of social robots, and delves into ethical issues such as emotional attachment to robots and the potential for manipulation. The paper emphasizes the need for comprehensive research and policymaking to address these emerging challenges as social robots become more integrated into daily life. Cheng and Jian (2020) explored the influence of AI-driven chatbots on user satisfaction, perceived privacy risks, loyalty, and continued usage intentions across various brands in the U.S. The study found that utilitarian, hedonic, technological, and social gratifications from chatbot interactions positively affect user satisfaction. Specifically, users appreciated the efficient information and entertainment provided by chatbots, which enhanced their overall brand satisfaction. The perceived privacy risks associated with chatbot interactions negatively impact user satisfaction. Users concerned about how their data might be used or shared tend to be less satisfied with the chatbot services. The study provides a comprehensive analysis of how AI-driven chatbots can affect various aspects of user experience and offers practical insights for improving chatbot implementations in customer service contexts.

References

Cheng, Y., & Jiang, H. (2020). How do AI-driven chatbots impact user experience? Examining gratifications, perceived privacy risk, satisfaction, loyalty, and continued use. *Journal of Broadcasting & Electronic Media, 64*(4), 592--614. doi:https://doi.org/10.1080/08838151.2020.1834296

Hirschprung, R. S., & Alkoby, S. (2022). A game theory approach for assisting humans in online information-sharing. *Information, 13*(4), 183. doi:https://doi.org/10.3390/info13040183

Majeed, A., & Hwang, S. O. (2023). When AI meets information privacy: The adversarial role of AI in data sharing scenario. *IEEE Access*. doi:https://doi.org/10.1109/ACCESS.2023.3297646

Sattikar, A., & Kulkarni, R. (2012). A role of artificial intelligence techniques in security and privacy issues of social networking. *International Journal of Computer Science Engineering & Technology, 2*(1), 792--806. Retrieved from https://ijcset.net/docs/Volumes/volume2issue1/ijcset2012020107.pdf

Subramanian, R. (2017). Emergent AI, social robots and the law: Security, privacy and policy issues. *Journal of International, Technology and Information Management, 26*(3). Retrieved from https://ssrn.com/abstract=3279236

Wang, S., Chen, Z., Xiao, Y., & Lin, C. (2021). Consumer privacy protection with the growth of AI-empowered online shopping based on the evolutionary game model. *Frontiers in public health, 9*, 705777. doi:https://doi.org/10.3389/fpubh.2021.705777

Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2022). A survey on metaverse: Fundamentals, security, and privacy. *IEEE Communications Surveys & Tutorials*, 319--352. doi:https://doi.org/10.1109/COMST.2022.3202047