OPEN ACCESS Freely available online

IJBSI International Journal of Business Studies and Innovation

ISSN 2737-5331
Volume 4, Issue 4
https://ijbsi.iikii.com.sg/
International Journal of Business Studies and Innovation

Technical Paper

Philosophical Review of Privacy and Identity in Modern Technology and Marketing

Jitae Kim [1] and Jongmin Kim[2,*]

[1] Korea International School; Seongnam 13453, South Korea; kjitae324@gmail.com;
[2] Department of Civil Engineering, University of Seoul; Seoul 02504, Korea;
*** Correspondence:** jk303482@naver.com

Received: Sep 10, 2024; **Revised:** Oct 10, 2024; **Accepted:** Oct 13, 2024; **Published:** Oct 30, 2024

Abstract: Technological advancements necessitate the philosophical understanding of privacy and identity more than ever. The intricate relationships between privacy, identity, and technologies must be considered vital to raise user interests by enhancing privacy protection. Recent technologies such as AI, blockchain, and augmented/virtual reality have opportunities and challenges in protecting user privacy and identity. In philosophy, privacy is thought to reflect an individual's control of personal information and personal identity. Privacy makes people selectively disclose information with a multifaceted concept. Philosophical perspectives on identity are individualistic. The aspects of identity are shared with others and decided on the concept of privacy as identity is defined by what is shared by a person. In the technology era, digital privacy and digital identity have emerged for protecting personal information, online behavior, and interactions. As artificial intelligence algorithms are widely used, the protection of digital privacy and identity is critical. Thus, technologies need to be developed to improve the interests, autonomy, and rights of users by considering the philosophical concepts of privacy and identity. The user perception and preference for Apple's products are apparent evidence of the importance of privacy and identity policy, which considerably affects the market position of its products. To improve digital privacy and identity, multifaceted strategies are required. Strong authentication methods need to be developed, and educating users and businesses is demanded. Ethical practices, self-sovereign identity, and the application of regulations must be integrated by combining technology, education, and ethical considerations for better protection of digital privacy and identity and the increase in the marketing performance of technologies and related products.

Keywords: Privacy, Identity, Digital Privacy, Digital Identity, Philosophical Concept, Technology, Marketing

1. Introduction

The philosophical dimensions of privacy and identity have been paid much attention by philosophers. Recently, modern technology is developing at an astonishing rate, and the use of big data is a major driving force behind such a development. In developing and utilizing such technologies represented by artificial intelligence (AI) and ubiquitous mobile technologies, the definition, justification, and interconnection of privacy and identity with their values must be considered due to a growing concern about information leakage and misinformation. Privacy and identity have been defined in diverse ways (Westin, 1968; Gavison, 2011; Lucas, 1997; Hongladarom, 2016; Michelfelder, 2010). In the era of technology development, the concepts of digital privacy and identity have been introduced, and their ethical challenges in technology have been debated in the digital realm (Walker, 2024: Burton, 2022; Christopher, 2021).

In accepting digital privacy and identity, user perception plays a critical role. Users usually express security concerns when installing apps and worry about hacking personal and private information. In addition, it was found that users also have security concerns regarding games and communication apps rather than financial apps such as mobile banking (Yasmeen, 2020). Such user perception and users' concerns about privacy and identity in modern technology are represented best in choosing products and services in the market. The best example is found in Apple's products. Though Apple's annual revenue has fluctuated due to the dynamic business landscape of the related market, Apple secured a market share of 20.1% in 2023 with a sales revenue of USD 383.3 billion, which was the highest in history. Their market share increased by 3.7% compared to 2022, while one of their competitors Samsung showed a market share of 19.4%, experiencing a decline of 13.6%. Such success of Apple is attributed to various marketing factors but its policy for privacy protection must not be ignored (Amadeo, 2024).

A survey result in the USA showed that 65% of iPhone and iPad users favored Apple's new privacy measures (Statistica, 2021). Apple's privacy policy is mentioned in the new feature announcement, emphasizing the protection, transparency in use, and

control of users' information and describing how they collect, use, and share personal data (Markithome, 2024). Apple emphasizes rigorous inspection of apps on its App Store to prevent malware-riddled apps and integrated designs in Apple devices to mitigate security vulnerabilities. Its iOS source code is limited to exposure and imposes stricter limits on third-party access to user data. Apple's "walled garden" approach provides a secured private ecosystem, which is preferred by consumers (Leith, 2021; Daniel and Feng, 2021). Apple's marketing strategy seems to pursue product differentiation by introducing innovations, scarcity, and exclusivity related to privacy and identity (Pereira, 2024), and as a result, Apple has succeeded in securing customer loyalty (Muhammad and Viktoria, 2023).

Apple's successful marketing strategy emphasizing privacy and identity is a representing example of how privacy and identity are understood and valued by the consumers or users of recently developed technology. Therefore, it is essential to investigate how privacy and identity are introduced in technology and related marketing activities, especially amid the emergence of unprecedented AI technologies. Thus, in this study, we explored the fundamental concept and its development of privacy and identity from the ancient philosophical view to its implication in modern technology, especially mobile technology and its marketing activities. The results of the exploration provide the basis for understanding the user perception of new technologies or products based on the inherent concept of privacy and the identity of users. Therefore, in this article, we discussed the philosophical view of privacy and identity, its applications in modern technology, and suggestions for how to cope with privacy and identity in developing and marketing technologies and products in each section.

2. Philosophical Concept of Privacy and Identity

2.1. Nature of Privacy and Identity

Privacy is viewed as an individual's control of how information about themselves is communicated to others or a measure of control over personal information or sensory access. Privacy is related to access to personal information, and intimacies of personal identity. Several philosophers regard a state or condition of limited access to a certain aspect of one's life as privacy (Hongladarom, 2016). However, privacy may be misused for the deceit and hypocrisy of a person to defend wrongdoing and not to be examined for it. Thus, the right to privacy, sometimes, is related to moral cowardice or avoiding stating one's position. Privacy makes people selectively disclose information and feel inferior due to ignorance about others' inner lives, which promotes individualistic values over socially oriented ones (Westin, 1970: Gavison, 1980; Smith et al., 2011). Privacy is a multifaceted concept from ethical, cultural, and societal perspectives. Thus, it is important to understand the philosophical concept of privacy to delve into the fundamental aspect of human existence (Hongladarom, 2016; Michelfelder, 2010).

Ancient philosophical perspectives on identity are more individualistic or relational than those of modern ones. For example, Stoicism emphasized self-mastery and inner virtue as essential components of identity, while Plato regarded identity as the idea of an ideal and unchanging self beyond the material world based on the theory of Forms. Aristotle considered identity as one's unique essence and purpose. Plato and Aristotle had a dualistic view and considered the body as a vessel for the soul, the true self. They believed that the soul's desires and beliefs shaped personal identity. In the 'Republic'. Plato reimagined education within an ideal city-state (polis), emphasizing social identity and communal influence on individual development (Christopher, 2012). In philosophy, identity is regarded as a marker distinguishing one object from another. It is not only an individual uniqueness but relational and contextual. Such ancient ideas still refer to understanding selfhood and existence (Phillip, 2014; Christopher, 2012).

As privacy is related to access to one's personal information, the aspects of identity shared with others or kept private are decided in the concept of privacy. Sometimes, privacy can be defined by how and what to reveal or conceal identity. For example, identity can be defined by what is shared by a person. Kayas et al. (2023) examined how privacy boundaries are set in academics and their influence on identity. They claimed the dialectical privacy boundaries based on preferences, social meanings, trust levels, and workplace norms. The negotiated boundaries provide an intimate territory where identity is formed through complex social interactions. Thus, privacy and identity impact the self-image, reputation, and social interactions of an individual and are intertwined as identity influences privacy boundaries while privacy can determine identity.

2.2. Digital Privacy and Identity

In the technology era, digital privacy and digital identity have emerged as essential concepts to understand and apply. Researchers have put efforts into safeguarding digital privacy by protecting digital identity such as personal information in digital environments. Examples of such efforts are found in an approach for IEEE to lead in digital privacy (Christopher, 2021), privacy-preserving techniques for smart home data collection and analysis (IEEE Digital Privacy, 2024), and user privacy in training machine learning models (Mikhail and Keith, 2007).

Digital identity represents an individual's identity in the digital realm. It includes personal information, online behavior, and interactions. Digital identity comprises biographical data such as name, date of birth, and contact details, biometric data such as fingerprints and facial recognition, online behavior on digital platforms, social media, and online services. For collecting and using digital identity data, the informed consent of users (or information providers) is crucial and the users must be notified how their information is used. In using digital identity, its ownership and service providers' needs must be declared. Otherwise, it must be difficult to protect personal data from unauthorized access or misuse. Therefore, security measures are necessary to prevent information theft or breaches. Nowadays, digital identity is created upon an individual's birth and maintained with continuous updates until the individual's death. Thus, it is vital to maintain the integrity of an individual's digital identity. However, AI engines can pose risks to digital identity, especially when manipulated without consent. In business, the licensing, purchasing, or transferring of digital identities can create economic opportunities and influence social dynamics. Therefore, legal and technical means to protect digital identity are required, which demands the collaborative efforts of experts, regulators, and users. It is also important to balance innovation and ethics in using digital identities (Sollberger, 2013; Camp, 2004).

3. Identity and Privacy in Technology

Mobile technology has become an integral part of our daily lives. From smartphones to wearable devices, users are connected to streamline tasks and communicate with each other. With the convenience that mobile technology allows for, digital identity and privacy are shaping the digital experiences of users. Digital identity has individual attributes including inherent attributes, assigned attributes derived from external sources or interactions, and verifiable attributes based on evidence or credentials (Sedlmeir et al, 2021). In the interconnected digital environment, privacy extends beyond physical boundaries so sensitive information must be protected to prevent the illegal use of personal data. There have been many incidents related to data breaches, identity theft, and large-scale fraud (Hannah, 2024). Therefore, in using mobile technology, mobile devices must serve as trusted ones for identity verification using biometrics such as fingerprints, facial recognition, and iris patterns and provide digital wallets to store payment credentials (Alcatraz AI, 2024). Yet, many users of mobile technology lack digital credentials. For them to participate in the digital economy, secure identities are demanded. Thus, the World Economic Forum emphasizes the development of robust digital identity systems to benefit stakeholders and protect against cyber risks. In mobile technology, identity and privacy are paramount as they are essential in digital transactions (Bergfeld et al., 2011).

Mobile devices including smartphones and tablets store personal information for communication and various services. Thus, users are concerned about privacy protection when purchasing mobile devices, emphasizing informed consumer choices. Since the first release of the original Apple iPhone in 2007, the modern smartphone transformed the global digital landscape. Apps, data collection, and connectivity have been improved rapidly and considerably with privacy controls lagging. As a result, users become vulnerable to data exploitation. Several apps contain hidden software development kits (SDKs) that collect user information, such as location and app usage data. Users are unaware of the related data breaches. Ad-tech companies and data brokers also operate to track user's data flow or prevent sharing. In this case, privacy settings are difficult to find as the operating system lacks privacy-protecting configurations (Klosowski, 2022). Thus, security software is needed to scan for malware, viruses, and privacy risks. However, it is not easy for most users to minimize exposure and find apps that protect user privacy. Therefore, when purchasing mobile devices, users prefer to be informed to prioritize privacy (Mendes et al. 2022).

Concern about privacy and identity protection is rooted in ancient philosophical ideas. The ancient Greeks thought that privacy emerged from the tension between various realms. Privacy was regarded as a privative trait that indicated a state of being deprived of relationships with others. For example, the household represented the private, while the political realm embodied the public in Greek philosophy. This dichotomy presented the need for boundaries of personal identity and privacy. In the marketing of mobile technology, customer data are essential, which triggers privacy concerns among consumers. Such concerns are inherent in humans. Therefore, consumers want to prevent data breaches and have privacy control. As consumers are worried about the data behaviors of the service providers or the device manufacturers, their privacy concerns influence their decisions on their purchase. However, many consumers lack understanding about the specifications of the device or service that they want to purchase. In addition, stricter regulations increase the costs which burden consumers eventually (Komamura, 2019)

As consumers are increasingly aware of the risks associated with data collection and sharing, their preference for Apple products and iOS has become strengthened. As stated in Section 1, the sales of Apple have been increasing with an increase in global market share. By understanding important considerations and improvements, new technologies and products can be aligned with consumer preferences for robust privacy protection. Thus, understanding the origins of privacy controls in iOS helps to address how to satisfy consumer demand for privacy protection effectively (Klosowski, 2022). When comparing the privacy policies and security structures of Android and iOS, significant differences are found. Android is an open-source platform and allows manufacturers to modify the operating system with flexibility but also has potential vulnerabilities. Android devices comprise

multiple layers including the Google operation system, manufacturer embedments, and customized apps of carriers. However, these delay security updates and increase opportunities for attacks. This multi-layered structure makes Android more prone to malware and third-party data access than iOS. The large number of apps available in the Play Store also increases the risk of malware infiltration. While iOS offers more robust privacy and security measures due to its centralized control and stringent app vetting, Android, despite its flexibility, faces challenges with app security and delayed updates (Piatos, 2024).

4. Implication of Identity and Privacy in Marketing Technology

Since the first release of the iPhone in 2007, controversies on the privacy of apps have continued from unauthorized data access to opaque data-sharing practices. To prevent such unexpected operations, Apple rigorously inspects every app on the Apple store to reduce the risk caused by malware. Though fewer apps are available than Android, this ensures a safer use of apps. Apple integrates and controls hardware and software to reduce the chances of exploitation and minimize security vulnerabilities. iOS provides software-based protection. Apple's "walled garden" approach limits third-party access to user data, too. iOS also updates patch vulnerabilities swiftly and regularly. By managing devices strictly, fewer security issues occur than in Android. Robust biometric authentication (Face ID and Touch ID) and strict app permission controls are also strong measures of iOS for privacy protection. Android also uses such methods but may lack consistency due to fragmentation as it focuses on flexibility. iOS's closed ecosystem, stringent app review process, and regular updates contribute to its superior privacy protection. Android, while improving, faces challenges due to its open nature and diverse device landscape (Leith, 2021).

The privacy protection policy of Apple seems to raise consumer recognition and perception of its products. Apple has announced new privacy and security features, including updates to Safari browsing, communication safety, and lockdown mode. These efforts show that Apple cares for a fundamental human right and builds strong security in every product and its features. In 2015, Apple introduced default encryption on the iPhone 6S to protect user data from Apple and government authorities. This sparked debates about privacy and public responsibilities, emphasizing Apple's commitment to user privacy. By describing how to collect, use, and share personal data, Apple assures users about data and privacy protection in its products, emphasizing transparency and user control, Apple has influenced consumer perception and trust (Harvard Business Review, 2024; Daniel and Feng, 2021). By empowering consumers, fostering transparency, and adhering to ethical data practices, Apple constructs a mobile ecosystem to better protect privacy and provide technology without compromising the fundamental rights of users.

In comparison, Android devices market security and privacy for their brand positioning under Google's leadership. Android emphasizes the protection of user identity and privacy corresponding to growing consumer concerns about data security. Android is integrating advanced privacy settings to enable users to monitor how the data is shared and used. Google is marketing these features such as Privacy Dashboard to show app permissions in real-time and allow users to revoke permissions easily. Google Play Protect is also marketed as it scans billions of apps. Google highlights this as a key differentiator, claiming that Play Protect safeguards against malicious apps. Google uses AI for threat detection for privacy protection without compromising user data to ensure that personal data is not leaked out of the device for more privacy. Android is marketed for transparency, user control, and state-of-the-art security technologies to relieve the privacy concerns of users (Falcon, 2023).

AI technologies also significantly impact privacy and identity, especially raising concerns about data security, surveillance, and ethical use of personal information. The growing use of AI in marketing has introduced new challenges for data privacy. AI-driven marketing systems use vast amounts of personal data to offer personalized experiences with prominent risks. Companies are using AI to analyze user behavior, analyze online activity, and collect biometric data which can lead to misuse or privacy violations. AI systems learn from the data including sensitive information without transparency. Technologies such as homomorphic encryption and federated learning are explored to secure AI systems to preserve user privacy. In these methods, encrypted data is used without exposing individual datasets. However, the lack of transparency in data usage is still a significant issue. The future of AI in marketing and devices needs a collaborative approach where privacy is integrated into AI systems. In an "opt-in" model, users must explicitly agree to data collection. As AI becomes more integrated into daily life, these privacy challenges will grow without ethical data use (van Rijmenam, 2023).

5. Conclusions

With rapid technological advancements, privacy, and identity become more important than ever in digital lives. The rapidly evolving technology necessitates the understanding of philosophical principles. There are intricate relationships between privacy, identity, and technologies, all of which are vital to secure and enhance user interests and privacy protection. Privacy and identity are at the forefront of societal discourse. In recent technologies such as AI, blockchain, and augmented/virtual reality, opportunities

and challenges are found in how to protect user privacy and maintain identity. The related concepts are essential for user-centric innovations, as more concerns are arising regarding the use of such technologies.

Privacy transcends confidentiality in recent technologies. As technology encroaches into private spaces, privacy must be protected as a human right. Thus, technologies must be developed to align with this ethical imperative and balance between innovation and privacy protection in the digital environment. Identity in recent mobile technology is not confined to virtual personas and the extension of the physical self. Therefore, to protect privacy and identity in the digital realm, privacy-enhancing technologies (PETs) for access control, differential privacy, and tunnel encryption must be integrated into technologies and devices to minimize data collection (Quach et al. 2022; Lin and Marc, 2022). As AI algorithms are used widely in diverse applications, the protection of privacy and identity becomes especially critical. Technologies must be developed to prioritize the interests, autonomy, and rights of users by considering philosophical insights into privacy and identity. The user perception and preference for Apple's products have led to its dominating global market share. This implies that users of technologies will be concerned more about privacy and identity policy, which considerably affects the outcome in the market. Being different from Apple, Android and AI technologies cause vulnerabilities in data security and privacy but corresponding measures and technologies are being developed to compete and/or be used more widely.

To improve digital privacy and identity, multifaceted strategies are required. Other than the PETs mentioned above, strong authentication methods need to be developed, and educating users and businesses is demanded to raise awareness about privacy risks and best practices. It is also necessary to consider ethical practices while monetizing user data (Quach et al., 2022). Self-sovereign identity such as Blockchain can be used as a solution or the key to privacy and identity protection (MIT Initiative on the Digital Economy, 2016). Regulations such as the General Data Protection Regulation and the California Privacy Rights Act must be formulated and enforced for strict compliance. It is also necessary to use a holistic approach by combining technology, education, and ethical considerations for better protection of digital privacy and identity.

Author Contributions: Conceptualization, Jitae Kim and Jongmin Kim; investigation, Jitae Kim and Jongmin Kim; writing—original draft preparation, Jongmin Kim; writing—review and editing, Jitae Kim and Jongmin Kim.

Funding: This research did not receive external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Alcatraz AI. (2004). Facial Biometrics vs. Iris Biometrics: Which is Better? Available online: https://alcatraz.ai/blog/facial-biometrics-vs-iris-biometrics-which-is-better (accessed on July 15, 2024)
2. Amadeo, Ron. (2024). Apple Hits "All-Time High" Smartphone Market Share, Takes #1 Spot for 2023. Available online: https://arstechnica.com/gadgets/2024/01/apple-hits-all-time-high-smartphone-market-share-takes-1-spot-for-2023/ (accessed on July 15, 2024)
3. Bergfeld, Marc-M. & Spitz, S. (2011). Privacy and Identity Management on Mobile Devices: Emerging Technologies and Future Directions for Innovation. (Fischer-Hübner, Simon, Duquenoy, Penny, Hansen, Marit, Leenes, Ronald, & Zhang Ed.) In *Privacy and Identity Management for Life*. Berlin/Heidelberg, Germany: Springer. https://doi.org/10.1007/978-3-642-20317-6_22.
4. Burton, Joe. (2022). Digital Identity: Where We Began, Where We Are And Where We Are Going. Available online: https://www.forbes.com/sites/forbestechcouncil/2022/03/24/digital-identity-where-we-began-where-we-are-and-where-we-are-going/. (accessed on July 15, 2024)
5. Camp, L. Jean. (2004). Digital identity. *IEEE Technology and Society Magazine*, *23*, 34–41. https://doi.org/10.1109/MTAS.2004.1337889.
6. Christopher, Gill. (2012). Ancient Concepts of Personal Identity. (Graziosi, Barbara, Vasunia, Phiroze, and Boys-Stones, George Ed.) In *The Oxford Handbook of Hellenic Studies.* Oxford, UK: Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199286140.013.0023.
7. Christopher, Gorog, (2021). A Synergistic Approach to Digital Privacy. Available online: https://doi.org/10.48550/arXiv.2103.14783. (accessed on July 15, 2024)
8. Gavison, Ruth. (2011). Privacy: Legal Aspects. Available online: https://www.researchgate.net/publication/228154411_Privacy_Legal_Aspects. (accessed on July 15, 2024)
9. Falcon, Ronnie. (2023). I/O 2023: What's new in Android Security and Privacy. Available online: https://security.googleblog.com/2023/05/io-2023-android-security-and-privacy.html. (accessed on July 15, 2024)

10. Hammack, L. Phillip. (2014). Theoretical Foundations of Identity. (McLean, C. Kate C. and Syed, Moin Ed.) In *The Oxford Handbook of Identity Development, Oxford Library of Psychology*. Oxford, UK: Oxford University. https://doi.org/10.1093/oxfordhb/9780199936564.013.027.
11. Hannah, Sutor. (2024). Safeguarding Identity and Privacy: Fundamental Human Rights in the Digital Age. Available online: https://idpro.org/safeguarding-identity-and-privacy-fundamental-human-rights-in-the-digital-age/.(accessed on July 15, 2024)
12. Harvard Business Review. (2024). Apple's Dilemma: Balancing Privacy and Safety Responsibilities. Available online: https://hbr.org/podcast/2024/02/apples-dilemma-balancing-privacy-and-safety-responsibilities. (accessed on July 15, 2024)
13. Hongladarom, Soraj. (2015). Philosophical Foundations of Privacy. (Hongladarom, Soraj) In *A Buddhist Theory of Privacy*. Singapore: SpringerBriefs in Philosophy. https://doi.org/10.1007/978-981-10-0317-2_2.
14. IEEE Digital Privacy. (2024). Understanding Privacy in the Digital. Available online: https://digitalprivacy.ieee.org/publications/topics/understanding-privacy-in-the-digital-age. (accessed on July 15, 2024)
15. Kayas, Oliver G., Matikonis Karl, Cranmer, Eleanor E. & Pereira C. Jorge. (2024). Socially Negotiating Privacy Boundaries and Academic Identities, Studies in Higher Education. *Studies in Higher Education 49,* 1241–1252. https://digitalprivacy.ieee.org/publications/topics/understanding-privacy-in-the-digital-age 80/03075079.2023.2262507
16. Klosowski, Thorin. (2022). How Mobile Phones Became a Privacy Battleground—and How to Protect. Available online: https://www.nytimes.com/wirecutter/blog/protect-your-privacy-in-mobile-phones/.(accessed on July 15, 2024)
17. Komamura, Keigo. (2019). Privacy's Past: The Ancient Concept and Its Implications for the Current Law of Privacy. *Washington University Law Review, 96,* 1337–1343. https://openscholarship.wustl.edu/law_lawreview/vol96/iss6/8/.
18. Leith, J. Douglas. (2021). Mobile Handset Privacy: Measuring the Data iOS and Android Send to Apple and Google. (Garcia-Alfaro, J., Li, S., Poovendran, R., Debar, H., and Yung, M. Ed.) In Security and Privacy in Communication Networks. SecureComm 2021. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 399. Berlin, Germany: Springer. https://doi.org/10.1007/978-3-030-90022-9_12.
19. Lin, Jinghuai, & Marc, Latoschik, E. (2022). Digital Body, Identity And Privacy In Social Virtual Reality: A Systematic Review. *Frontiers in Virtual Reality, 3.* https://doi.org/10.3389/frvir.2022.974652.
20. Lucas, D. Introna. (1997). Privacy and The Computer: Why We Need Privacy In The Information Society. *Metaphilosophy, 28,* 259–275. https://www.jstor.org/stable/24439066.
21. Markithome (2024). The Apple Effect: How Apple's Marketing Strategy Continues to Revolutionize the Tech Industry. Available online: https://markitome.com/blog/apples-marketing-strategy-for-the-tech-industry/.(accessed on July 15, 2024)
22. Mendes, Ricarado, Cunha, Mariana, Vilela, João P., Beresford, R. Alastair. (2022). Enhancing User Privacy in Mobile Devices Through Prediction of Privacy Preferences. (Atluri, V., Di Pietro, R., Jensen, C.D., & Meng, W. Ed.) In *Computer Security –ESORICS 2022. Lecture Notes in Computer Science, Vol. 13554*. Berlin/Heidelberg, Germany: Springer. https://doi.org/10.1007/978-3-031-17140-6_8.
23. Michelfelder, P. Diane. (2010). Philosophy, privacy, and pervasive computing. *AI & Society, 25,* 61–70. https://doi.org/10.1007/s00146-009-0233-2.
24. Mikhail J. Atallah, & Frikken Keith B. (2007). Privacy-Preserving Cryptographic Protocols. (Acquisti, Alessandro, Gritzalis, Stefanos Lambrinoudakis, Costos, & di Vimercati, Sabrina di Ed.) In *Digital Privacy: Theory, Technologies, and Practices* 1st ed. New York, NY, USA: Auerbach Publications. https://doi.org/10.1201/9781420052183.
25. MIT Initiative on the Digital Economy. (2016). Digital Identity: The Key to Privacy and Security in the Digital World. Available online: https://ide.mit.edu/insights/digital-identity-the-key-to-privacy-and-security-in-the-digital-world/.(accessed on July 15, 2024)
26. Muhammad, Kahlid, A., & Vida, Viktoria. (2023). Strategic Marketing Plan for APPLE Inc. Available online: https://www.researchgate.net/profile/Muhammad-Anas-Khalid/publication/371902832_Strategic_Marketing_Plan_for_APPLE_Inc/links/649b0cd1b9ed6874a5df0478/Strategic-Marketing-Plan-for-APPLE-Inc.pdf. (accessed on July 15, 2024)
27. Piatos, Taziana. (2024). iOS vs. Android Security: Which One is More Secure? Available online: https://privacysavvy.com/security/mobile/ios-iphone-vs-android-security/.(accessed on September 22, 2024)
28. Pereira, Danie. (2024). Apple Marketing Strategy. Available online: https://businessmodelanalyst.com/apple-marketing-strategy/. (accessed on September 22, 2024)
29. Quach, Sara, Thaichon, Park, Martin, D. Kelly, Weaven Scott, & Palmatier, W. Robert. (2022) Digital Technologies: Tensions in Privacy And Data. *Journal of the Academy of Marketing Science, 50,* 1299–1323. https://doi.org/10.1007/s11747-022-00845-y.
30. Scoccia G. Luca, Autili Marco, Giovanni Stilo, & Inverardi Paola. (2022). An Empirical Study of Privacy Labels On The Apple Ios Mobile App Store. Proceedings of the 9th IEEE/ACM International Conference. 113–124. https://doi.org/10.1145/3524613.3527813.

31. Sedlmeir, Johannes, Smethurst, Reuilly, Rieger, Alexander, & Fridgen Gilbert. (2021). Digital Identities and Verifiable Credentials. *Business & Information Systems Engineering, 63*, 603–613. https://doi.org/10.1007/s12599-021-00722-y.
32. Smith, H. Jeff, Dinev, Tamara, & Xu, Heng. (2011). Information Privacy Research: An Interdisciplinary Review. Available online: http://dx.doi.org/10.2307/41409970. (accessed on September 22, 2024)
33. Søe, S. Obelitz & Mai, Jens-Erik. (2022). Data Identity: Privacy and the Construction Of Self. *Synthese, 200*, 492. https://doi.org/10.1007/s11229-022-03968-5.
34. Daniel, Sokol, D, & Feng, Zhu. (2021). Harming Competition and Consumers under the Guise of Protecting Privacy: An Analysis of Apple's iOS 14 Policy Updates. *Cornell Law Review Online*, *107*, 2021. https://www.cornelllawreview.org/2022/07/21/harming-competition-and-consumers-under-the-guise-of-protecting-privacy-an-analysis-of-apples-ios-14-policy-updates/.
35. Statistica. (2021). Do you agree with Apple's new privacy policies? Available online: https://www.statista.com/statistics/1224850/user-opinion-on-apple-s-new-privacy-policies-us/. (accessed on July 15, 2024)
36. van Rijmenam, Mark. 2023. Privacy In the Age of AI: Risks, Challenges and Solutions. Available online: https://www.thedigitalspeaker.com/privacy-age-ai-risks-challenges-solutions/.(accessed on July 15, 2024)
37. Walker, Justin. (2024). The history of Digital Identity. Available online: https://www.business-reporter.co.uk/technology/the-history-of-digital-identity. (accessed on July 15, 2024)
38. Westin, F. Alan. (1968). Privacy and Freedom. *Washington University Law Review*, *25*, 166–170. https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr&ref=hackernoon.com.
39. Yasmeen Elsantil. (2020). User Perceptions of the Security of Mobile Applications. *International Journal of E-Services and Mobile Applications. 12*. 18. http://dx.doi.org/10.4018/IJESMA.2020100102.