2024 International Conference on Intelligent and Innovative Computing Applications (ICONIC)
7th-9th November 2024, Pearle Beach Resort & Spa, Flic en Flac, Mauritius
https://doi.org/10.59200/ICONIC.2024.014

A Systematic Literature Review of Usable Privacy Controls for Mobile Applications

Phumezo Ntlatywa
Sol Plaatje University
Kimberly, South Africa
phumezo.ntlatywa@spu.ac.za, s210243759@mandela.ac.za

Darelle van Greunen
Nelson Mandela University
Gqeberha, South Africa
darelle.vangreunen@mandela.ac.za

Abstract
With the increasing use of mobile devices and the collection of personal data through mobile applications, protecting user privacy has become a critical concern. However, many privacy controls in mobile applications are difficult to use, leading users to either ignore them or disable them altogether. During the review of the selected articles, key overarching categories emerged, including usability and user experience, privacy control features, and user education and support. However, significant gaps persist in translating design principles into practical implementations, understanding the comprehensive user experience with different privacy control designs, considering the influence of contextual factors, addressing the implications of emerging technologies, and exploring the longitudinal aspects of user-privacy interactions. This review highlights the need for a framework that bridges these gaps to enhance user privacy and control in mobile applications. The findings of this review provide insights for researchers and practitioners to develop effective and user-centric privacy controls for mobile applications, ensuring a balance between usable privacy and protection.

Keywords: Usable privacy, mobile applications, privacy controls, systematic literature review

1. Introduction

Our daily lives have become increasingly reliant on mobile applications, which give us access to a variety of features and conveniences. However, as these applications collect and process vast amounts of personal data, concerns regarding user privacy have emerged (Aggarwal et al., 2024; Badiya et al., 2024; Toch et al., 2018). Mobile applications provide privacy controls for users to restrict or give access to their personal data. Privacy controls are provided for users to have control over their experience beyond opting out of the application entirely (Habib et al., 2019). Some of the reported issues with privacy controls include the fact that users do not change default privacy controls (Horne, 2021); users will accept an option if it is pre-selected by default (Anaraky & Knijnenburg, 2021); and privacy controls are frequently missing or hard to find (Feng et al., 2021). Default controls are frequently permissive in nature and allow privacy-invasive practices like excessive data collection (Elahi & Wang, 2018). Additionally, little is known about default features on mobile devices or how users perceive them in terms of privacy, if users are even aware of these features, or the privacy implications of leaving them in place (Ramokapane et al., 2019).
In addition, users who change their default settings find some privacy controls to be confusing and unusable (Karunakaran et al., 2018; Ramokapane et al., 2019). Also, the options are frequently inadequate making it difficult for them to convey their genuine privacy preferences (Colnago et al., 2020).

Lack of usable privacy controls also contributes to a variety of privacy-related attitudes, such as privacy fatigue and privacy helplessness (Cho, 2021). Privacy fatigue is caused by the increasing difficulty in managing one's online personal data leading to an individual feeling a loss of control and making an individual weary of having to think

about online privacy (Choi et al., 2018). Privacy helplessness is the belief that something bad will happen and that nothing can be done to alter it; and it can be a major obstacle that prevents users from responding appropriately to privacy threats (Cho, 2021). Designers are supposed to take a leading role in advancing usable privacy, by designing systems that are usable. However, many designers have limited knowledge about design choices and best practices for privacy policies and privacy controls (Li et al., 2021).

There is a need for more research in the usable privacy domain to bring clarity on the best design choices and best practices when designing usable privacy controls. This is clear from the variety of privacy controls available across mobile applications and is evident from the different privacy controls of different mobile applications found in the marketplace. In the marketplace there are different types of mobile applications used for different purposes including lifestyle, social media, utility, entertainment, productivity, news, education, travel, food, finance, shopping etc. (Kushnir, 2021).

Usable privacy refers to the degree to which a product or service protects the privacy of users in an effective, efficient, and satisfactory manner while considering the unique characteristics of the users, goals, tasks, resources, and the technical, physical, social, cultural, and organizational environments in which the product or service is used (Johansen & Fischer-Hübner, 2020). This definition shows that usable privacy involves various factors that are important and unlike usability that measures how simple user interfaces are to use (Nielsen, 2012). This paper adopts this definition to define usable privacy controls.

The recent introduction of the Protection of Personal Information Act (POPIA), the General Data Protection Regulation (GDPR) and other similar laws and acts further complicates the job of designers, specifically because these laws refer to high level concepts (Feng et al., 2021). For example, when POPIA speaks of safeguards in Condition 7 (19.1), it specifies that "a responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organizational measures" (POPI, 2013). However, this does not give the developer enough guidance.

This paper presents the findings of a systematic literature review (SLR) that was conducted by using predefined keywords to search the Scopus database for research studies on usable privacy controls for mobile applications. Particularly, this review aimed to examine the following main research question: ***"What are the current practices for designing usable privacy controls for mobile applications?"***

This paper is organized into eight sections. Section 1 serves as an introduction, while Section 2 briefly states the goal of the review, and Section 3 discusses the methodology used throughout the review process. Section 4 contains a discussion based on the information gathered during the review process, Section 5 highlights the gaps in literature that this review has identified, Section 6 discusses future work. Section 7 discusses the limitations of the study and Section 8 concludes the review.

2. Goal of the review

A systematic literature review is a rigorous and structured approach to gather and analyze information from various sources to answer a specific research question (Kitchenham & Charters, 2007). In this case, the goal was to examine the current practices in designing usable privacy controls for mobile applications. The process involved defining the research questions, conducting the search, screening, and selecting relevant studies, analyzing, and synthesizing the findings, and presenting the results. The topic of designing usable privacy controls for mobile applications is important, given the increasing use of mobile devices and the growing concerns over data privacy. The systematic literature review helped to identify the current practices in this area and provided insights into what works and what does not work.

3. Methodology

The methodology used in conducting the review used Kitchenham's technique for completing SLRs, which involves defining research questions, determining data sources and search process, specifying inclusion and exclusion criteria, obtaining search results, and discussing the findings to answer the research questions (Kitchenham & Charters, 2007). Kitchenham's technique lists seven critical steps when conducting an SLR:

1. **Plan the review:** In this step, you need to define the research questions, identify the scope of the review, and specify the inclusion and exclusion criteria for selecting studies.
2. **Conduct the search:** This step involves identifying relevant studies by searching electronic databases and other sources.
3. **Select studies:** In this step, you need to screen the search results based on the inclusion and exclusion criteria defined in the planning step.
4. **Assess study quality:** This step involves assessing the quality of the selected studies.
5. **Extract data:** In this step, you need to extract relevant data from the selected studies.
6. **Synthesize results:** This step involves analyzing and synthesizing the data extracted from the selected studies.
7. **Report the review:** In this step, you need to report the results of the review concisely.

These seven steps are combined as follows in this review:

1. **Planning** (plan review)
2. **Execution** (conduct the search, select studies, assess study quality, and extract data)
3. **Reporting** (synthesize results and report the review)

3.1 Planning

The SLR sought to answer the following sub-questions:

4. **RQ1:** What are the various ways that are used in designing usable privacy controls for mobile applications?
5. **RQ2:** What are the key factors that influence the design of usable privacy controls in mobile applications?
6. **RQ3:** What are the current trends and emerging practices in the design of usable privacy controls for mobile applications?
7. **RQ4:** What are the key challenges in designing usable privacy controls for mobile applications, and how can they be addressed?

This review's inclusion criteria centered on studies that addressed the design of usable privacy controls specifically for mobile applications. Only studies that were published in peer-reviewed journals or conference proceedings and written in the English language were considered eligible for inclusion in this review.

3.2 Execution

A search was conducted using the Scopus database, a large abstract and citation database of peer-reviewed articles that provides access to over seventy-six million records from over 24,000 journals across various disciplines. The search aimed to identify journal articles and conference papers published between 2013 and 2023 that discussed the topic of usable privacy in mobile applications. The first search term was *"Usable privacy" AND "Mobile Applications"* and yielded only six articles.

The initial search using the first search term yielded an insufficient number of papers to address the research questions, and so a second search was performed. The second search term, *"Usable Privacy,"* was used with a period to 2023, which resulted in 166 papers. However, to further narrow down the search results, the period was reduced to 2018-2023. This reduced the number of papers to 121, which was still a large enough sample size to proceed with the review. After reducing the period, additional parameters were added to the search, including the inclusion of conference papers, articles, and the English language. This refinement process resulted in a final set of 101 articles that met the inclusion criteria for the systematic literature review.

The next step was to screen the search results based on the inclusion criteria that were established in the planning stage of the SLR. The initial screening was conducted based on the titles, abstracts, and keywords of the articles to quickly identify and exclude any irrelevant or clearly unsuitable studies. During this process, it was discovered that one article was a duplicate, resulting in a reduction of the total number of articles from 101 to 100. After the initial screening, twenty-six articles met the inclusion criteria and were selected for further analysis.

After the initial screening, the remaining articles were subjected to a second screening based on their full texts. This step was necessary to ensure that only studies meeting the inclusion criteria were considered for the review. Several articles were excluded due to reasons such as not addressing the topic of privacy controls but focusing on privacy policies or surveying user concerns, focusing on compliance instead of usable privacy controls, or describing the design of privacy-preserving applications. After the second screening, eleven articles were found to be eligible for the review.

The chosen articles were analyzed and yielded a total of thirty-nine concepts, which were

classified into three overarching categories. These categories encompassed the themes of usability and user experience as shown in Table 1, privacy control features as shown in Table 2, and user education and support as shown in Table 3. The examination of these concepts shed light on the diverse aspects influencing the design and implementation of privacy controls for mobile applications.

3.3 Reporting

The following section gives the results of the SLR; Tables I - III give the lists of the themes and concepts that emerged from the review.

3.3.1 Usability and user experience: The reviewed literature consistently emphasized the importance of making privacy controls accessible and user-friendly. It was found that ensuring accessibility will allow users of all abilities to effectively engage with the privacy controls. Clear or clarity emerged as another essential aspect, where the presentation of privacy controls should be straightforward and easily understandable to users. Simplicity, without overwhelming users with complex options, was identified as a key factor in promoting user satisfaction and acceptance of privacy controls.

Additionally, providing meaningful options that align with users' needs and preferences was highlighted as a critical aspect of usable privacy controls. Designing appropriate default controls was also emphasized to guide users towards privacy-enhancing controls while allowing customization options for advanced users. The literature also stressed the importance of error prevention, responsive interfaces, and providing help and guidance to users to enhance their understanding of privacy controls and ensure a positive user experience.

Incorporating media diversity in the presentation of privacy controls emerged as an important theme within the usable and user experience domain. The literature emphasized the use of various media types, including text and speech, to cater to different user preferences and accessibility requirements. Providing alternative modes of interaction, such as checkboxes, drag and drop, or swiping, was also highlighted to enhance user engagement and control customization.

Table 1: Usability and user experience

Themes	Author/s
Accessibility	(Albesher & Alhussain, 2021; Pattakou et al., 2018)
Clear	(Albesher & Alhussain, 2021; Kävrestad et al., 2022)
Simplicity	(Albesher & Alhussain, 2021; Kävrestad et al., 2022; Pattakou et al., 2018)
Meaningful	(Albesher & Alhussain, 2021; Pattakou et al., 2018)
Appropriate defaults	(Albesher & Alhussain, 2021; Jacobs & McDaniel, 2022)
Adaptability	(Pattakou et al., 2018)
Aesthetic	(Pattakou et al., 2018)
Control customization	(Pattakou et al., 2018)
Error prevention	(Pattakou et al., 2018)
Help	(Pattakou et al., 2018)
Learnability	(Pattakou et al., 2018)
Memorability	(Pattakou et al., 2018)
Predictability	(Pattakou et al., 2018)
Reliability	(Pattakou et al., 2018)
Responsiveness	(Pattakou et al., 2018)
Valuableness	(Pattakou et al., 2018)
Varying designs	(Jacobs & McDaniel, 2022; Kävrestad et al., 2022; Lindegren et al., 2019)
Mental models	(Jacobs & McDaniel, 2022)
Limit cognitive load	(Kävrestad et al., 2022)
Media diversity (text, speech)	(Kävrestad et al., 2022)

Furthermore, the concept of limiting cognitive load should play a significant role in designing usable privacy controls. By reducing complexity and streamlining the decision-making process, privacy controls can be made more user-friendly and effective. This involves organizing the controls in a logical and intuitive manner, adhering to consistent design patterns, and employing mental models that align with users' existing knowledge and expectations. The reviewed literature stressed the importance of minimizing cognitive load to prevent decision fatigue and support users in making informed choices regarding their privacy preferences.

3.3.2 Privacy Control Features: The literature review revealed several essential concepts related to privacy control features in mobile applications. Consent emerged as a critical aspect, with emphasis placed on the apparency, explicitness, and the ability for users to easily revoke their consent. The visibility of privacy controls was highlighted as a key factor, ensuring that users can readily locate and access the necessary controls to manage their privacy preferences. Transparency was another key concept, underscoring the

importance of providing clear and understandable information about the data practices and privacy implications of mobile applications.

Table 2: Privacy control features

Themes	Author/s
Consent apparency	(Albesher & Alhussain, 2021; Johansen & Fischer-Hübner, 2020; Toch et al., 2018)
Available	(Albesher & Alhussain, 2021; Pattakou et al., 2018)
Transparency	(Albesher & Alhussain, 2021; Johansen & Fischer-Hübner, 2020; Pattakou et al., 2018; Pins et al., 2022)
Data (access to own, portability)	(Albesher & Alhussain, 2021; Johansen & Fischer-Hübner, 2020)
Awareness	(Albesher & Alhussain, 2021)
Warnings / audio feedback (-/+)	(Gopavaram et al., 2020; Jacobs & McDaniel, 2022)
Timing (launch, use, after)	(Gopavaram et al., 2020)
Correction	(Pins et al., 2022)
Deletion/eraser	(Johansen & Fischer-Hübner, 2020; Pins et al., 2022)
Traffic lights/severity scale	(Johansen & Fischer-Hübner, 2020; Yankson et al., 2021)
Data minimization	(Johansen & Fischer-Hübner, 2020)
Purpose limitation	(Johansen & Fischer-Hübner, 2020)
Provenance data	(Gupta et al., 2021)

The reviewed articles also emphasized the need for enabling users to access their own data and easily transfer it across platforms, promoting data portability and empowering users with control over their personal information. Awareness of security measures was also emphasized, with privacy controls designed to educate and inform users about potential risks and security threats associated with their data.

The literature also highlighted several user-focused design aspects for privacy controls. It was found that appropriate warnings and audio feedback can enhance the user experience by providing timely and contextually relevant information regarding privacy choices and potential consequences. Consideration of timing, such as the presentation of privacy controls during app launches, during app use, and after certain actions, was identified as crucial to ensure users can make informed decisions at relevant points in their interactions.

3.3.3 User Education and Support:

The reviewed literature emphasized the importance of error prevention measures to minimize user mistakes and enhance the overall user experience. Providing helpful resources and guidance within the application interface, such as contextual help or tooltips, can assist users in understanding the implications of privacy controls and making informed decisions. Learnability was another key concept, highlighting the need for privacy controls that are intuitive and easy to grasp, even for users who are not technologically savvy.

Table 3: User education & support

User Education & Support	Author/s
Error prevention	(Pattakou et al., 2018)
Help	(Pattakou et al., 2018)
Learnability	(Pattakou et al., 2018)
Memorability	(Pattakou et al., 2018)
Understand trade-offs	(Jacobs & McDaniel, 2022)
Warnings / audio feedback (-/+)	(Gopavaram et al., 2020; Jacobs & McDaniel, 2022)
Timing (launch, use, after)	(Gopavaram et al., 2020)
Correction	(Pins et al., 2022)
Deletion/eraser	(Johansen & Fischer-Hübner, 2020; Pins et al., 2022)

Incorporating memorability into the design of privacy controls helps users remember their previous choices and preferences, ensuring consistency and reducing decision-making efforts. Furthermore, understanding trade-offs was identified as essential for users to comprehend the implications and consequences of their privacy choices, empowering them to make well-informed decisions. The literature also emphasized the importance of providing warnings or audio feedback to alert users to potential privacy risks and enhance their awareness of security measures.

In addition to user education, ensuring accessibility of privacy controls for all users was a recurring theme in the reviewed literature. Designing controls that are accessible to individuals with disabilities, including visual impairments or motor limitations, is crucial for inclusive user experiences. The use of alternative media types, such as text and speech, can improve accessibility and cater to users with diverse needs and preferences. Moreover, media diversity was identified to enhance user engagement and

customization of privacy controls. By providing a variety of interface designs and interaction options, such as checkboxes, drag and drop, or swiping, mobile applications can accommodate different user preferences and increase the sense of control over privacy controls. Incorporating media diversity not only enhances usability but also contributes to a more inclusive and user-centric design approach.

4. Discussion

The SLR on usable privacy controls for mobile applications identified several key themes related to usability, privacy control features, and user education and support. The findings highlight the importance of designing privacy controls that are accessible, clear, and not overburdening for users. Ensuring meaningful options, appropriate defaults, and adaptability of privacy controls can enhance user satisfaction and acceptance. Additionally, the literature emphasizes the significance of transparency, data access, and awareness of security measures to empower users in managing their privacy preferences effectively. The concepts of media diversity, limiting cognitive load, and user education emerged as essential aspects, contributing to a user-friendly and inclusive design of privacy controls.

4.1 RQ1: What are the various ways that are used in designing usable privacy controls for mobile applications?

To design usable privacy controls for mobile applications, several strategies and concepts can be employed. First, explicit consent plays a crucial role in ensuring user awareness and control over their data. By incorporating clear and easily understandable consent mechanisms, mobile applications can obtain informed consent from users before accessing or processing their personal information. Additionally, the concept of revocation is essential, allowing users to revoke their consent at any time and providing them with the ability to manage their privacy preferences actively. Furthermore, the design should emphasize data access and portability, allowing users to access their own data stored within the application and enabling them to easily transfer it to other platforms. This empowers users with greater control and fosters a sense of trust and transparency.

Moreover, mobile applications should prioritize accessibility, ensuring that privacy controls are accessible to users with varying abilities and needs. Clarity and simplicity are key, as privacy control interfaces should be intuitive and easily comprehensible, guiding users through the options available to them. Context and meaningful options contribute to user-centric designs, presenting privacy controls in a relevant and contextual manner. Defaults and awareness also play a role, with well-considered default controls that respect user privacy and transparently informing users about the security measures in place. By incorporating these design strategies, mobile applications can enhance the usability of privacy controls, fostering a positive user experience and strengthening user trust in the application's data handling practices.

4.2 RQ2: What are the key factors that influence the design of usable privacy controls in mobile applications?

The design of usable privacy controls in mobile applications is influenced by several key factors. Primarily, user needs play a pivotal role. Designers must understand the diverse range of user requirements and preferences when it comes to privacy. Factors such as accessibility become critical, ensuring that privacy controls are designed to accommodate users with disabilities and different usage contexts. Moreover, factors like clarity and simplicity are essential to cater to users who may have varying levels of technological expertise. By prioritizing user needs, mobile applications can create privacy controls that are intuitive, user-friendly, and aligned with users' expectations.

Legal and regulatory requirements also heavily influence the design of privacy controls. Concepts like data minimization and purpose limitation ensure that privacy controls are designed to collect and process only the necessary user data for the intended purposes. Provenance data, which provides information about the source and history of data, helps ensure compliance with legal and regulatory frameworks. Designing privacy controls that align with these requirements not only helps organizations meet their legal obligations but also instills user confidence and trust in the application's commitment to protecting their privacy. By considering these factors, mobile applications can design privacy controls that strike a balance between user needs, legal compliance, and ethical data handling practices.

4.3 RQ3: What are the current trends and emerging practices in the design of usable privacy controls for mobile applications?

In the design of usable privacy controls for mobile applications, several current trends and emerging practices are shaping the landscape. One of these is adaptive design, which aims to personalize privacy controls based on individual user preferences and context. This approach leverages concepts like adaptability, customization, and varying designs/interfaces to allow users to tailor their privacy controls according to their specific needs and preferences. By offering flexible and personalized privacy controls, mobile applications can enhance user satisfaction and empower individuals to make informed choices about their privacy.

Another emerging practice focuses on enhanced transparency in privacy controls. Concepts such as data access, portability, consent apparency, and explicit consent are being emphasized to provide users with a clearer understanding of how their data is being collected, used, and shared. Mobile applications must strive to present privacy controls in a transparent and easily understandable manner, empowering users to make informed decisions about their data. This trend also encompasses the disclosure of information regarding security measures and the impact of privacy controls on users' data security. By embracing these practices, mobile applications foster trust, transparency, and accountability in their privacy control designs, promoting a positive user experience and mitigating privacy concerns.

4.4 RQ4: What are the key challenges in designing usable privacy controls for mobile applications, and how can they be addressed?

Designing usable privacy controls for mobile applications comes with its share of challenges. One key challenge is cognitive load. Privacy controls can sometimes be complex and overwhelming for users, leading to decision fatigue and confusion. To address this challenge, designers can implement concepts such as limit cognitive load and simplicity. By simplifying the user interface, organizing options intuitively, and providing clear explanations, mobile applications can reduce the cognitive burden on users, making privacy controls more manageable and understandable.

Balancing privacy protection with usability is another significant challenge. While robust privacy controls are essential, overly complex, or restrictive controls can hinder the user experience. Designers can tackle this challenge by incorporating concepts like clear, meaningful options, defaults, awareness, and mental models. Offering privacy controls that align with users' expectations and mental models ensures a balance between privacy protection and usability. Additionally, providing informative default controls and raising awareness about the importance of privacy can guide users towards making informed choices without burdening them with excessive decision-making.

Another challenge is user education and awareness. Many users may not fully understand the implications of their privacy controls, or the potential risks involved. To address this challenge, concepts such as awareness, warnings, feedback, and help can be implemented. Mobile applications can provide clear explanations, visual cues, and warnings to inform users about the potential consequences of their privacy choices. Additionally, offering contextual help and resources can empower users to make informed decisions and effectively utilize the available privacy controls. By addressing these challenges, mobile applications can enhance the usability and effectiveness of privacy controls, leading to improved user satisfaction and privacy management.

5. Gaps in Literature

The existing body of research on usable privacy controls for mobile applications, while growing, exhibits several notable gaps. A primary focus on the theoretical underpinnings of privacy control design is evident, with a relative dearth of studies delving into the practical implementation of these principles in real-world mobile applications. This practical implementation gap underscores the need for research that bridges the gap between design concepts and their operationalization in tangible mobile products.

Furthermore, a comprehensive understanding of the user experience in relation to various privacy control designs remains elusive. While the literature touches on usability aspects, a deeper exploration of how different privacy control configurations impact user satisfaction, trust, and overall privacy behaviors is warranted. This user experience evaluation gap necessitates empirical research to inform the development of user-centric privacy controls.

Moreover, the influence of contextual factors on the effectiveness of privacy controls has been inadequately investigated. Limited research exists on how user demographics, cultural nuances, and the specific context of mobile application usage shape user interactions with privacy controls. Addressing this contextual factor gap is crucial for designing privacy controls that resonate with diverse user populations and effectively mitigate privacy risks. The rapid evolution of technology introduces novel privacy challenges that require ongoing research. The implications of emerging technologies such as artificial intelligence, the Internet of Things, and blockchain on privacy control design remain unexplored. Filling these emerging technologies gap is essential for developing privacy controls that are future-proof and capable of addressing the privacy challenges posed by these advancements.

Additionally, most existing studies adopt a cross-sectional research design, offering snapshots of user perceptions and behaviors at specific points in time. A longitudinal perspective is missing, hindering our understanding of how user attitudes and interactions with privacy controls evolve over time. Addressing this longitudinal studies gap is vital for capturing the dynamic nature of user-privacy interactions. Finally, while the literature identifies various privacy control design principles, comparative studies evaluating the relative effectiveness of different design approaches are scarce. This comparative analysis gap limits our ability to identify optimal privacy control designs that balance usability, privacy protection, and user acceptance.

By addressing these identified gaps, future research can significantly advance the field of usable privacy controls for mobile applications, leading to the development of more effective, user-centric, and privacy-protective mobile experiences.

6. Future work

The review has highlighted significant gaps in the existing body of knowledge pertaining to usable privacy controls for mobile applications. While previous research has made valuable contributions to understanding the components of usable privacy controls, a critical void exists in translating these design principles into practical, implementable frameworks for developers and designers. This gap is particularly pronounced when considering the increasing complexity of mobile applications and the rapidly evolving technological landscape. The absence of a comprehensive framework hinders the development of privacy-centric mobile applications that effectively balance user needs, privacy protection, and usability. This ongoing PhD research aims to address this gap by developing a comprehensive framework for designing usable privacy controls for mobile applications. By building upon the identified design principles and incorporating insights from user-centered design methodologies, the proposed framework seeks to provide a practical roadmap for creating privacy controls that are not only usable but also effective in safeguarding user privacy.

This framework will incorporate a systematic approach to evaluating the usability and privacy implications of different design options, thus bridging the gap between theoretical knowledge and practical implementation. By filling this critical void, this research contributes to the advancement of privacy-enhancing technologies and empowers users to exercise greater control over their personal information in the mobile ecosystem.

7. Limitation of the study

This systematic literature review has certain limitations. First, the review relied on a specific set of articles, potentially excluding relevant studies. Second, it used existing research without collecting new data, limiting the depth of understanding. Finally, the small number of studies included might restrict the applicability of the findings. Despite these limitations, this review provides a solid foundation for understanding key concepts in usable privacy controls. It highlights the importance of user-centered design, transparency, and user education for effective privacy management. Future research should address several areas. These include:

- Researching how to apply privacy control design principles in real-world mobile applications.
- Studying how different privacy control designs affect user satisfaction, trust, and privacy behaviors.
- Exploring how factors like demographics and culture influence the use of privacy controls.

- Investigating how emerging technologies impact privacy control design.
- Conducting long-term studies to understand how user attitudes and behaviors change over time.
- Comparing different privacy control designs to determine the most effective approaches.

By addressing these gaps, future research can significantly improve the development of usable and privacy controls for mobile applications.

8. Conclusion

In conclusion, this systematic literature review provides valuable insights into the concepts associated with usable privacy controls for mobile applications. The findings underscore the significance of user experience, privacy control features, and user education in designing effective privacy controls. By implementing accessible, clear, and adaptable controls with meaningful options, mobile applications can enhance user satisfaction and privacy management. Furthermore, transparency, data access, and awareness of security measures play crucial roles in empowering users and building trust in the privacy practices of mobile applications. Incorporating media diversity, limiting cognitive load, and providing user education and support can further improve the usability and effectiveness of privacy controls. By incorporating these elements, developers can create applications that empower users to make informed decisions about their personal information.

7. References

Aggarwal, R., Dhingra, S., & Mittal, S. (2024). What reduces the privacy concerns of the customers towards the use of location-based advertising? An empirical investigation. *Journal of Location Based Services*, *18*(2), 139–161. https://doi.org/10.1080/17489725.2023.2256701

Albesher, A. S., & Alhussain, T. (2021). Evaluating and Comparing the Usability of Privacy in WhatsApp, Twitter, and Snapchat. *International Journal of Advanced Computer Science and Applications*, *12*(8), 251–259. https://doi.org/10.14569/IJACSA.2021.0120829

Anaraky, G. R., & Knijnenburg, B. (2021). A Research Agenda for Studying Young and Older Adults' Privacy Decisions. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.3873573

Badiya, K., Sankuru, R. C., Satya, N. L. V., Sarikonda, S. H. R., Koppineni, R. L., & Aylapogu, P. K. (2024). Security & Privacy Concern of Mobile Cloud Computing. *AIP Conference Proceedings*, *2942*(1). https://doi.org/10.1063/5.0199802/3267810

Cho, H. (2021). Privacy helplessness on social media: its constituents, antecedents and consequences. *Internet Research*. https://doi.org/10.1108/INTR-05-2020-0269

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, *81*, 42–51. https://doi.org/10.1016/j.chb.2017.12.001

Colnago, J., Feng, Y., Palanivel, T., Pearman, S., Ung, M., Acquisti, A., Cranor, L. F., & Sadeh, N. (2020, April 21). Informing the Design of a Personalized Privacy Assistant for the Internet of Things. *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3313831.3376389

Elahi, H., & Wang, G. (2018). A Participatory Privacy Protection Framework for Smart-Phone Application Default Settings. *Communications in Computer and Information Science*, *969*, 168–182. https://doi.org/10.1007/978-981-13-5826-5_13

Feng, Y., Yao, Y., & Sadeh, N. (2021). A design space for privacy choices: Towards meaningful privacy control in the internet of things. *Conference on Human Factors in Computing Systems - Proceedings*, *16*. https://doi.org/10.1145/3411764.3445148

Gopavaram, S. R., Bhide, O., & Camp, L. J. (2020). Can You Hear Me Now? Audio and Visual Interactions That Change App Choices. *Frontiers in Psychology*, *11*. https://doi.org/10.3389/fpsyg.2020.02227

Gupta, S., Camilli, M., & Papaioannou, M. (2021). Provenance Navigator: Towards More Usable Privacy and Data Management Strategies for Smart Apps.

In Parkin S. & Viganò L. (Eds.), *Socio-Technical Aspects in Security: 11th International Workshop, STAST: Vol. 13176 LNCS* (pp. 24–42). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-031-10183-0_2

Habib, H., Zou, Y., Jannu, A., Sridhar, N., Swoopes, C., Acquisti, A., Cranor, L., Sadeh, N., & Schaub, F. (2019). An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites. *Fifteenth USENIX Conference on Usable Privacy and Security*, 387–406.

Horne, C. L. (2021). Dark Patterns and Privacy Harms: Accountability and Agency in an Age of Disappearing Privacy Chelsea L. Horne American University. *Global Internet Governance Academic Network (GigaNet) Annual Symposium*, 1–11.

Jacobs, D., & McDaniel, T. (2022). A Survey of User Experience in Usable Security and Privacy Research. In Moallem A. (Ed.), *Lect. Notes Comput. Sci.: Vol. 13333 LNCS* (pp. 154–172). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-031-05563-8_11

Johansen, J., & Fischer-Hübner, S. (2020). Making GDPR usable: A model to support usability evaluations of privacy. In Friedewald M., Önen M., Lievens E., Krenn S., & Fricker S. (Eds.), *IFIP Advances in Information and Communication Technology: Vol. 576 LNCS* (pp. 275–291). Springer. https://doi.org/10.1007/978-3-030-42504-3_18

Karunakaran, S., Kurt, T., Bursztein, E., & Comanescu, O. (2018). Data Breaches: User Comprehension, Expectations, and Concerns with Handling Exposed Data. *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, 217–234.

Kävrestad, J., Hagberg, A., Roos, R., Rambusch, J., & Nohlberg, M. (2022). Usable Privacy and Security from the Perspective of Cognitive Abilities. *IFIP Advances in Information and Communication Technology, 644 IFIP*, 105–121. https://doi.org/10.1007/978-3-030-99100-5_9

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing Systematic Literature Reviews in Software Engineering* (Vol. 2).

Kushnir, A. (2021, January 23). *Categories & Types of Mobile Applications*. Bamboo Agile. https://bambooagile.eu/insights/main-categories-and-types-of-mobile-apps/

Li, T., Neundorfer, E., Agarwal, Y., & Hong, J. (2021). Honeysuckle. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *5*(3). https://doi.org/10.1145/3478097

Lindegren, D., Karegar, F., Kane, B., & Pettersson, J. S. (2019). An evaluation of three designs to engage users when providing their consent on smartphones. *Behaviour & Information Technology*, *40*(4), 398–414. https://doi.org/10.1080/0144929X.2019.1697898

Nielsen, J. (2012, January 3). *Usability 101: Introduction to Usability*. World Leaders in Research-Based User Experience. https://www.nngroup.com/articles/usability-101-introduction-to-usability/

Pattakou, A., Mavroeidi, A., Diamantopoulou, V., Kalloniatis, C., & Gritzalis, S. (2018). Towards the Design of Usable Privacy by Design Methodologies. *2018 IEEE 5th International Workshop on Evolving Security & Privacy Requirements Engineering (ESPRE)*, 1–8. https://doi.org/10.1109/ESPRE.2018.00007

Pins, D., Jakobi, T., Stevens, G., Alizadeh, F., & Krüger, J. (2022). Finding, getting and understanding: the user journey for the GDPR'S right to access. *Behaviour & Information Technology*, *41*(10), 2160–2186. https://doi.org/10.1080/0144929X.2022.2074894

Protection of Personal Information Act 2013, Government Gazette 1 (2013).

Ramokapane, K. M., Mazeli, A. C., & Rashid, A. (2019). Skip, Skip, Skip, Accept!!!: A Study on the Usability of Smartphone Manufacturer Provided Default Features and User Privacy. *Proceedings on Privacy Enhancing Technologies*, *2019*(2), 209–227. https://doi.org/10.2478/popets-2019-0027

Toch, E., Rager, N., Florentin, T., Linenberg, D.,

Sellman, D., & Shomron, N. (2018). Augmented-Genomics: Protecting Privacy for Clinical Genomics with Inferential Interfaces. *Proceedings of the 23rd International Conference on Intelligent User Interfaces Companion*, 1–2. https://doi.org/10.1145/3180308.3180326

Yankson, B., de Lima Salgado, A., & Fortes, R. P. M. (2021). Recommendations to enhance usability and privacy of smart toys. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2020-Janua*, 1868–1877.