POLITECNICO DI TORINO
Repository ISTITUZIONALE

Empowering Users: End User Development for Mobile Applications Privacy Management

Original
Empowering Users: End User Development for Mobile Applications Privacy Management / Saenz Moreno, J.P., De Russis, L.. - STAMPA. - (2024), pp. 1-6. (International Workshop on Trusted Computing and Artificial Intelligence applied to Cybersecurity Paris (FRA) 26-29 June, 2024) [10.1109/ISCC61673.2024.10733613].

Availability:
This version is available at: 11583/2990422 since: 2024-11-01T13:21:02Z

Publisher:
IEEE

Published
DOI:10.1109/ISCC61673.2024.10733613

Terms of use:

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright
IEEE postprint/Author's Accepted Manuscript

©2024 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collecting works, for resale or lists, or reuse of any copyrighted component of this work in other works.

(Article begins on next page)

27 November 2026

Empowering Users: End User Development for Mobile Applications Privacy Management

Juan Pablo Sáenz
Dip. di Automatica e Informatica
Politecnico di Torino
Turin, Italy
juan.saenz@polito.it

Luigi De Russis
Dip. di Automatica e Informatica
Politecnico di Torino
Turin, Italy
luigi.derussis@polito.it

***Abstract*—Smartphones have become integral to everyday life, and despite the many advantages they bring, they also raise privacy and security concerns, particularly regarding non-transparent, unauthorized, or malicious data collection risks. While users are aware of these issues, the means the smartphone's operating system provides to manage the applications' permissions and protect personal data often prove challenging or overwhelming for non-technical users. In this context, this article introduces Privacy Manager, a mobile application designed for Android devices that relies on an End-User Development (EUD) approach to offer personalized data protection and privacy security measures to bridge the gap for regular users. The application facilitates effective management of permissions granted to installed applications through user-friendly interfaces and customizable settings, enhancing user awareness and control over their data. A validation study was carried out with 8 participants over a week. The study involved an initial questionnaire followed by a week-long period of real-world application usage. It concluded with a final questionnaire with an assessment using the System Usability Scale (SUS).**

***Index Terms*—end-user development, privacy, mobile applications, android, permissions**

I. Introduction

Smartphones have become integral to everyday life, offering convenience, connectivity, and access to vast information. However, they can present potential privacy and security issues in their daily use. For instance, one of the most common concerns relates to the collection of data by the application developers to resell it, to display targeted advertising, or to access the device's location in a manner that is not transparent to the user [1]. Indeed, users are increasingly concerned about how mobile applications treat personal information, referring to concerns related to location tracking, large amounts of required permissions, and authorized selling data [2].

Several studies have analyzed the perception and trust of end-users regarding the privacy and security of personal data when using their smartphones. The results obtained demonstrate how the majority of users lack trust in the applications they install on their devices and in the means provided by the smartphone's operating system to manage their permissions and protect personal data [3]–[5]. In Android, for instance, the user has to agree to a set of permissions during installation. If the user understands the technical details, he could judge whether permissions are correct and be aware of possible privacy concerns they might encounter while using the application. However, this does not apply to non-expert users, who are at regular risk of getting their privacy and security compromised [6], [7]. Accordingly, the effectiveness of this permission system has been questioned, mainly due to users' inattention and misunderstanding of the system's prompts [8], given that privacy settings are not easy to configure [9].

The challenges users encounter in understanding and efficiently managing their data when using mobile applications stem partly from the lack of user-centered privacy designs and control features that could empower them to assert more control over their data (Bemmann, 2023; Mohsen, 2024). In this sense, while End-User Development (EUD) techniques have demonstrated their effectiveness in various contexts, such as mobile environments [10], smart homes [11], and the Internet of Things (IoT) [12], less attention has been paid to security and privacy aspects in smartphone usage.

Motivated by exploring the extent to which an EUD approach can empower users to protect their privacy and gain better insight into the permissions granted to smartphone applications, in this article, we present **Privacy Manager**. Privacy Manager is an Android application designed to serve two primary objectives: firstly, to provide a user-friendly mechanism for effectively managing the privacy and security of personal data, mainly aimed at less experienced users, and secondly, to enable the customization of data management based on parameters that are most relevant to each user. A validation study involving 8 participants was conducted over the span of a week. Throughout this duration, participants interacted with the application in real-life scenarios, subsequently assessing its usability.

The remainder of this paper is structured as follows: Section II provides context for our research, focusing on two key themes: EUD and privacy concerns in mobile environments. Section III details the design considerations and implementation of the Privacy Manager application. In Section IV, we outline our methodology, participants, and results from the validation process, along with general remarks on the findings. Finally, Section V summarizes our conclusions and points out future research directions.

II. Background and Related Works

According to the definition proposed by Lieberman *et al.* [13], EUD can be described as a set of methods, techniques, and tools that enable computer system users, acting as non-professional software developers, to create, modify, or extend a software artifact. The dissemination of this paradigm is driven by its empowerment of users without specific technical backgrounds to create and customize artifacts according to their needs [14]. EUD is used in different areas, like IoT and smart homes. In these domains, the aim has been to empower end-users to transition from passive consumers to active producers, shaping the behaviors of their smart environments. However, regarding mobile environments, the use of End-User Development has been less common. A study by Barricelli *et al.* [15] found that it represents only a small fraction (6%) of all EUD applications. Moreover, according to Tetteroo *et al.* [16], who reviewed research methods in EUD, most research on understanding and evaluating EUD tools has been conducted in lab settings, rather than in the field or through qualitative interviews and surveys. In this regard, our approach aims, on the one hand, to integrate EUD into mobile applications in the relatively unexplored context of privacy, and on the other hand, to validate this approach through an in the wild study.

Meanwhile, privacy of information can be defined as the right of individuals, groups, or institutions to autonomously determine when, how, and to what extent the information concerning them is communicated to others [17]. In network-connected mobile devices, this definition can extend to the users' ability to control access to their personal data [3], [18]. With the widespread adoption of smartphones and the continuous growth of the mobile application market, user data collection by service-providing companies has increased significantly. Therefore, it becomes crucial in such a context to implement measures that enable users to protect their data adequately. There is a real risk that users may lack the means to understand the nature of the collected data [19], while companies often hinder the spread of user-friendly and intuitive control mechanisms to gather more user information.

In such a context, addressing the security issues associated with mobile applications is crucial. With the vast application market, cybercriminals could lure users into installing malicious applications, leading to potential threats such as malware, ransomware, identity theft, and data breaches, particularly affecting less experienced users [6], [20]. Indeed, to address security and privacy risks, Android introduced the permissions mechanism. Applications use permissions to request access to specific device functionalities. Before Android 5.1 (Android Lollipop[1], 2014), users were informed about all permissions they had requested before installing the app. They could either accept all conditions or refuse, thus preventing installation. From version 6.0 (Android Marshmallow[2], 2015), permissions were introduced at runtime, allowing applications to request access to specific functionalities during runtime, avoiding the previous 'all or nothing' model. Since Android 10[3] (2019), this model has expanded to give users greater transparency regarding which applications have which permissions. Users can now grant permissions always, only during use, or deny them.

Android updates have proven effective, with users finding the runtime permission model more intuitive. However, there is still a critical issue regarding users' understanding of permission alerts. Additionally, some users suffer from 'warning fatigue,' overlooking permissions due to alerts that do not convey real risks [21], [22]. Consequently, at a general level, user trust in privacy measures remains inadequate. For instance, according to Zhou *et al.* [4], three out of four users feel they lack sufficient control over their device data. Many are unaware of specific settings or assume certain privacy settings are already active, like ad profiling blocking. Additionally, navigating device settings is challenging for some, leading to the belief that manufacturers intentionally make it difficult to maximize data collection profits [1].

Consequently, users recognize some of the risks associated with granting specific permissions. However, they encounter challenges in effectively utilizing the tools provided by their smartphones for self-defense. In this context, it becomes crucial to provide users with practical tools that can guide them adequately in protecting their data and addressing their difficulties and expectations. Privacy Manager aims to offer a user-friendly solution that enables non-technical users to consciously and effectively personalize the privacy permissions they grant to mobile applications on their phones.

III. Design and implementation

The underlying design principle that we envisioned for the application was to empower the user to create **security rules** based on a set of parameters. In this regard, we drew inspiration from 'If This Then That' (IFTTT[4]), which is a widely diffused EUD web platform that enables users to create chains of simple conditional statements, known as applets or rules, which automate tasks based on changes in other web services or devices [23]. Users define triggers ('if this') and actions ('then that') to specify what should occur when certain conditions are met, enabling seamless automation across various online services and devices.

In the Privacy Manager application, whose main screenshots are presented in Figure 1, we defined these rules to encompass four key parameters: permissions, applications, conditions, and behavior (Figure 1a). Below, we will elaborate on each parameter and illustrate how they are set within the application.

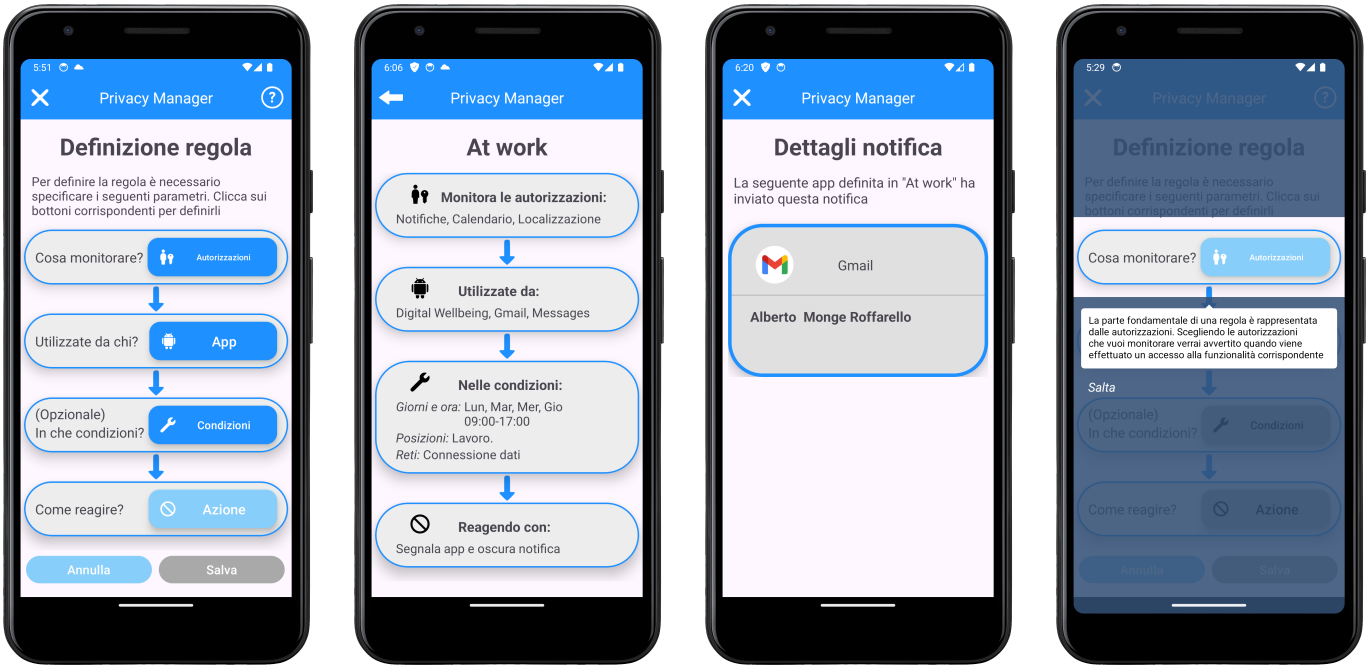
- **Permissions**: Given the issues stemming from Android's permission model and its gaps, the decision was made

[1] "Android Lollipop | Android Developers", https://developer.android.com/about/versions/lollipop, (accessed May 10, 2024).

[2] "Android 6.0 Marshmallow | Android Developers", https://developer.android.com/about/versions/marshmallow, (accessed May 10, 2024).

[3] "Android 10 | Platform | Android Developers", https://developer.android.com/about/versions/10, (accessed May 10, 2024).

[4] "IFTTT - Automate business & home", https://ifttt.com, (accessed May 10, 2024).



(a) (b) (c) (d)

Fig. 1. Screenshots of the Privacy Manager mobile application. In (**a**), users can create the security rule by defining all the essential parameters. Each button corresponds to a specific parameter, allowing users to specify permissions, applications, and conditions. Later, in (**b**), after the user saves the rule and assigns it a name ('At work'), a summary displaying all the rule's parameters is presented. In (**c**), the user is notified when an application performs an action (such as receiving a push notification) that has been intercepted by any of the security rules defined by the user. Finally, in (**d**), the tutorial explains in detail the various sections of the respective screen and how users can effectively utilize the application.

to base the definition of security rules precisely on permissions.

Similarly, since not all permissions provided by Android are equally critical or risky for users, it would be pointless for users to define safeguarding measures based on functionalities that do not compromise their security. For this reason, following the work proposed by Liu *et al.* [24], it was decided to consider only those permissions deemed risky for users' security and privacy.

Although the set of permissions managed by Android is broader, due to the limitations imposed by the operating system, only a restricted subset of these permissions can be monitored without root permissions. Therefore, those permissions included in the Privacy Manager were location, calendar, and camera, detailed in Table I.

TABLE I
PERMISSIONS INCLUDED IN THE APPLICATION

Permission	Description	Potential Risk
Location	Geographic location of the device	Location-based attacks or malware; location-based advertising
Calendar	Activities recorded on the users calendar	Disclosure of users schedule information
Camera	Capture of images	Access to camera functionality without user awareness

Alongside these permissions, however, it has also been decided to consider the **notifications** sent by the device's applications. Indeed, although not strictly risky for the user's security, they could compromise their privacy under certain conditions. For this reason, we have also decided to include them in the list of permissions that can be monitored, also considering the flexibility provided through the customizable conditions set by the user during the rule definition phase.

- **Applications**: Refers to the specific applications installed on the phone for which the previously defined permissions will be monitored. In the Privacy Manager applications, users are presented only with applications with access to previously included permissions.
- **Conditions**: Users also have the option to define a series of conditions that the system must meet during the monitoring. These conditions are optional, meaning users can save a rule without specifying them. Table II lists the customizable conditions and explains how they trigger monitoring activation accordingly.
- **Behaviors**: Finally, once the previous parameters have been defined, the user must select the action the system should take in case a security rule intercepts an action triggered by a monitored application. The selectable actions are reporting or stopping, and if the user has also selected notification permission, the actions of hiding and blocking the notification will be available (Table III) .

TABLE II
USER-CUSTOMIZABLE CONDITIONS

Condition	Description	Monitoring Activation
Day and Time	Days of the week and corresponding time	During the specified days and time
Locations	Geographic location specified by the entered address	When the user is physically present in one of the specified locations
Network	Name of one (or more) Wi-Fi networks, or the device's data connection	When the device is connected to the specified network
Bluetooth	Bluetooth devices stored on the device	When one (or more) of the selected devices are connected to the smartphone
Battery	Device's battery charge percentage	When the device's charge level is lower than the specified one

Once the security rule is created and activated (Figure 1b), the monitoring phase begins. This phase occurs in the background and tracks the behavior of the applications the user selects. If the system detects that an application action has been intercepted by a security rule, it will notify the user through a notification. By clicking on the notification, a screen will be displayed (Figure 1c) to the user showing the application action was intercepted by the security rule and the name of the rule itself.

TABLE III
BEHAVIORS MANAGED BY PRIVACY MANAGER

Behavior	Description
Hide	The notification sent by the application is not displayed. Instead, the system informs the user of a new notification without specifying its content
Block	The notification sent by the application is not displayed. Instead, the system notifies the user that an application has sent a notification that has been blocked, without providing any information about the content

Additionally, since the application is aimed at non-expert users, as seen in Figure 1d, it was decided to include a set of tutorials to present the system's functions and various sections. The tutorials are automatically displayed if the user opens the application for the first time, ensuring proper guidance and instruction. They can also be accessed later by pressing a specific button on each screen.

Technically speaking, the Privacy Manager application was developed on the Android platform using the native Kotlin language. The infrastructure used for the system registration process and for saving usage statistics in the cloud is represented by Firebase. In the case of Privacy Manager, the components utilized are Firebase Authentication and Firestore. The former facilitated the system registration phase by integrating the process through users' Google accounts. On the other hand, the latter enabled the cloud storage of data and statistics generated by users during system usage.

IV. VALIDATION

Once the application implementation was concluded, we conducted an in-the-wild validation, in which users utilized the Privacy Manager under real-world conditions, reflecting their daily routines and habits without direct control over their actions.

A. Methodology and participants

The validation design was 'within-subjects' [25], granting each participant access to all functionalities offered by the application. The validation spanned one week and included: (i) an **initial questionnaire** to gauge user perceptions regarding device usage and privacy protection; (ii) **one week of application usage**; and (iii) a **final questionnaire**, comprising a System Usability Scale (SUS) [26] assessment to measure application usability and a series of questions prompting users to share their impressions and to inquire more specifically about any unclear or malfunctioning aspects of the application.

Participants in this validation phase were individuals from our circle recruited via private messages. Initially, 10 participants were contacted. Of these, 8 completed all phases of the validation. Therefore, only the data from these 8 participants were for result analysis. Among the 8 participants, five self-identified as women, and three self-identified as men. Their ages range from 20 to 30 years, with an average age of approximately 24.

B. Results

The **initial questionnaire**, apart from gathering demographic data, comprised three questions for participants to rate using a 5-point Likert scale:

Q1: How satisfied are you with the privacy and security protections provided by the applications you use?
Q2: How easy do you find the way your smartphone allows you to manage your privacy and security?
Q3: How interested would you be in having greater control over how your smartphone and the applications you use manage your privacy and security?

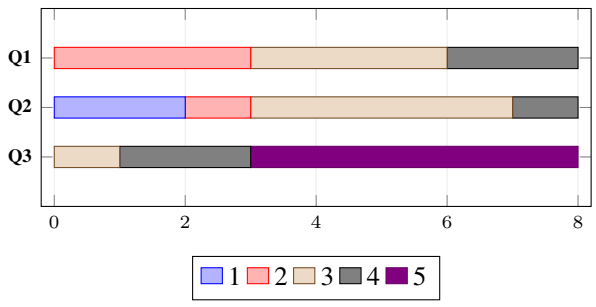


Fig. 2. Participants' perceptions regarding the use of their device and the protection of their privacy using a Likert scale ranging from '*Not at all*' (1) to '*Very much so*' (5).

The answers to these questions are depicted in Figure 2. As can be observed in the graph, users' perceptions of the

effectiveness of current privacy protection mechanisms (**Q1**) suggest a moderately low overall opinion. However, when evaluating the ease of use of the device-provided solutions for security and privacy protection (**Q2**), the opinion appears even lower, with two participants giving the minimum score on the Likert scale. Conversely, responses were overwhelmingly positive regarding the interest in having greater control over privacy and security management by the device and applications (**Q3**).

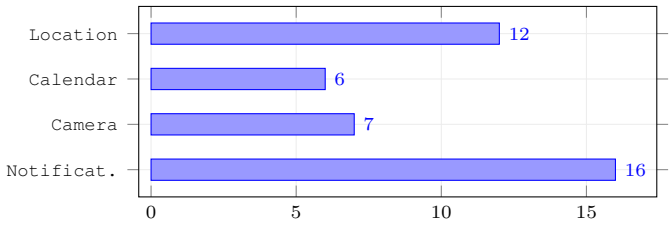


Fig. 3. Permissions chosen by the participants when creating a security rule

Later, during the **week of application usage**, participants collectively created 25 security rules. The number of rules created by each user ranged from a minimum of 1 to a maximum of 12, and most users (5 out of 8) created only one security rule. These rules were quite heterogeneous in terms of the monitored permissions. Generally, it is found that users have preferred to monitor a single permission per rule (72% of cases), likely the one they deemed most relevant. Among the individual permissions that users preferred to monitor, as shown in Figure 3, the highest preferences were for notifications and location (36% and 24%, respectively).

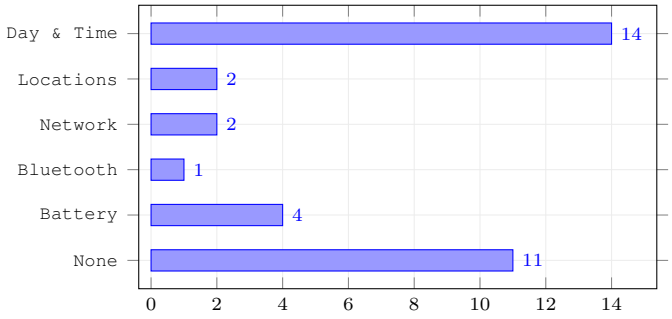


Fig. 4. Conditions defined by the participants when creating a security rule

When it comes to the conditions chosen during the creation of the security rules, as can be seen in Figure 4, a significant majority is observed for the parameter related to the time slot. Alternatively, users have often opted not to add any conditions, thus enabling continuous monitoring upon rule activation.

Furthermore, from the collected data, we observed that the users' week of usage amounted to 24 actions intercepted by the Privacy Manager application, and notifications caused a percentage of 75% of these interceptions. Conversely, the least reported permissions are calendar and camera, both reported only once. The summary of reported interceptations is depicted in Figure 5. Such data emphasizes the prevalence of notification reporting. Nevertheless, it is important to consider that notifications were the most monitored permission by users, especially at the expense of the calendar and camera, which consequently report minimal interceptions.

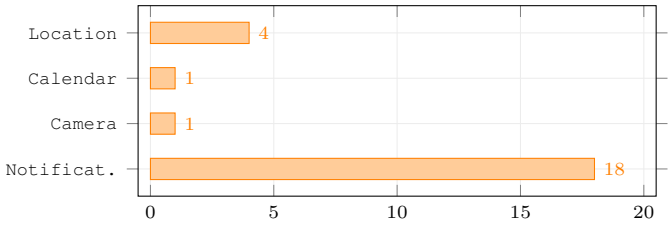


Fig. 5. Applications' actions intercepted by the security rules

Lastly, regarding the **final questionnaire**, done through the SUS assessment, Privacy Manager was rated with an average score of 76.56. Such a result exceeds the average value of 68 provided as a reference by the scale, indicating a general appreciation for the application's usability. Regarding the additional questions in the SUS questionnaire, there is a noteworthy appreciation for the tutorials guiding users on how to start using the application. Participants were asked to rate the usefulness of these initial tutorials on a 5-point Likert scale ranging from 'Not at all' (1) to 'Very much so.' Out of the respondents, 5 participants rated the tutorials as 4, while 3 participants rated them as 5.

C. General remarks

During the testing week, users frequently utilized Privacy Manager, as evidenced by the number of security rules created. Analysis revealed that location permissions were among the most sought-after to protect, selected in 48% of rules. Additionally, introducing notifications to the list of monitorable permissions proved effective, with 64% of rules including them. Instead, calendar and camera permissions were less popular, chosen in only 24% and 28% of cases, respectively, suggesting they were perceived as less risky by the participants.

Regarding optional conditions, many participants opted not to include any (44% of cases), preferring continuous monitoring and reporting. However, most users (56%) chose to include a time slot, limiting monitoring to specific times deemed more sensitive. Bluetooth-connected device conditions were rarely chosen. Similarly, examining the most selected applications for security rule creation, social media and banking applications were prominent choices, reflecting participants' concerns about privacy risks associated with these categories.

Finally, although certain preferences were predominant among participants' choices, it is worth underscoring the diverse range of parameters considered in defining security rules. This aspect is particularly significant for us since our proposed approach aimed at empowering users to tailor software components to their specific needs. After all, users possess a unique understanding of what is most effective for their requirements.

V. Conclusion and future work

This article has presented the design considerations, implementation choices, and validation of Private Manager. This mobile application relies on EUD to empower users to protect their privacy and gain better insight into the permissions granted to applications installed on their smartphones. After conducting a one-week validation in the wild with eight participants, utilizing a within-subjects study design, we determined that the goals of providing a tool adaptable to users' personal needs and privacy protection through customized security rules were achieved. For instance, participants found the application to be very useful. However, as this validation phase involved a limited number of participants and a short time window, future work will focus on conducting a more comprehensive testing phase over an extended period. This future validation will involve evaluating various application parameters, such as the frequency of application openings and the duration of application usage, to enhance further its effectiveness in empowering users and ensuring privacy protection.

Acknowledgment

The authors would like to thank Alessio De Gregorio, who contributed to the development and evaluation of the Privacy Manager application as part of his master's thesis. This work was partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.

References

[1] A. Frik, J. Kim, J. R. Sanchez, and J. Ma, "Users' expectations about and use of smartphone privacy and security settings," in *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, ser. CHI '22. New York, NY, USA: Association for Computing Machinery, 2022.

[2] P. Nema, P. Anthonysamy, N. Taft, and S. T. Peddinti, "Analyzing user perspectives on mobile app privacy at scale," in *2022 IEEE/ACM 44th International Conference on Software Engineering (ICSE)*, 2022, pp. 112–124.

[3] C. Fung, V. Motti, K. Zhang, and Y. Qian, "A study of user concerns about smartphone privacy," in *2022 6th Cyber Security in Networking Conference (CSNet)*, 2022, pp. 1–8.

[4] Y. Zhou, A. Raake, T. Xu, and X. Zhang, "Users' perceived control, trust and expectation on privacy settings of smartphone," in *Cyberspace Safety and Security*, S. Wen, W. Wu, and A. Castiglione, Eds. Cham: Springer International Publishing, 2017, pp. 427–441.

[5] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: user attention, comprehension, and behavior," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, ser. SOUPS '12. New York, NY, USA: Association for Computing Machinery, 2012.

[6] M. A. Dar, S. Nisar Bukhari, and U. I. Khan, "Evaluation of security and privacy of smartphone users," in *2018 Fourth International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB)*, 2018, pp. 1–4.

[7] I. Liccardi, J. Pato, D. J. Weitzner, H. Abelson, and D. De Roure, "No technical understanding required: helping users make informed choices about access to their personal data," in *Proceedings of the 11th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, ser. MOBIQUITOUS '14. Brussels, BEL: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2014, p. 140–150.

[8] G. L. Scoccia, S. Ruberto, I. Malavolta, M. Autili, and P. Inverardi, "An investigation into android run-time permissions from the end users' perspective," in *2018 IEEE/ACM 5th International Conference on Mobile Software Engineering and Systems (MOBILESoft)*, 2018, pp. 45–55.

[9] A. Bourdoucen and J. Lindqvist, "Privacy of default apps in apple's mobile ecosystem," in *Proceedings of the CHI Conference on Human Factors in Computing Systems*, ser. CHI '24. New York, NY, USA: Association for Computing Machinery, 2024.

[10] A. Namoun, A. Daskalopoulou, N. Mehandjiev, and Z. Xun, "Exploring mobile end user development: Existing use and design factors," *IEEE Transactions on Software Engineering*, vol. 42, no. 10, pp. 960–976, 2016.

[11] D. Fogli, R. Lanzilotti, and A. Piccinno, "End-user development tools for the smart home: A systematic literature review," in *Distributed, Ambient and Pervasive Interactions*, N. Streitz and P. Markopoulos, Eds. Cham: Springer International Publishing, 2016, pp. 69–79.

[12] A. Krishna, M. Le Pallec, R. Mateescu, and G. Salaün, "Design and deployment of expressive and correct web of things applications," *ACM Trans. Internet Things*, vol. 3, no. 1, oct 2021.

[13] H. Lieberman, F. Paternò, M. Klann, and V. Wulf, *End-User Development: An Emerging Paradigm*. Dordrecht: Springer Netherlands, 2006, pp. 1–8.

[14] A. J. Ko, R. Abraham, L. Beckwith, A. Blackwell, M. Burnett, M. Erwig, C. Scaffidi, J. Lawrance, H. Lieberman, B. Myers, M. B. Rosson, G. Rothermel, M. Shaw, and S. Wiedenbeck, "The state of the art in end-user software engineering," *ACM Comput. Surv.*, vol. 43, no. 3, apr 2011.

[15] B. R. Barricelli, F. Cassano, D. Fogli, and A. Piccinno, "End-user development, end-user programming and end-user software engineering: A systematic mapping study," *Journal of Systems and Software*, vol. 149, pp. 101–137, 2019.

[16] D. Tetteroo and P. Markopoulos, "A review of research methods in end user development," in *End-User Development*, P. Díaz, V. Pipek, C. Ardito, C. Jensen, I. Aedo, and A. Boden, Eds. Cham: Springer International Publishing, 2015, pp. 58–75.

[17] A. F. Westin, "Science, privacy, and freedom: Issues and proposals for the 1970's. part i–the current impact of surveillance on privacy," *Columbia Law Review*, vol. 66, no. 6, pp. 1003–1050, 1966.

[18] M. Guerra, S. Scalabrino, F. Fasano, and R. Oliveto, "An empirical study on the effectiveness of privacy indicators," *IEEE Transactions on Software Engineering*, vol. 49, no. 10, pp. 4610–4623, 2023.

[19] H. Zhu, H. Xiong, Y. Ge, and E. Chen, "Mobile app recommendations with security and privacy awareness," in *Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, ser. KDD '14. New York, NY, USA: Association for Computing Machinery, 2014, p. 951–960.

[20] F. Mohsen, U. Rauf, V. Lavric, A. Kokushkin, Z. Wei, and A. Martinez, "On identification of intrusive applications: A step toward heuristics-based adaptive security policy," *IEEE Access*, vol. 12, pp. 37 586–37 599, 2024.

[21] H. Elahi, G. Wang, W. Jiang, A. Bartel, and Y. Le Traon, "A qualitative study of app acquisition and management," *IEEE Transactions on Computational Social Systems*, vol. 11, no. 2, pp. 1907–1925, 2024.

[22] R. Lavranou, S. Karagiannis, A. Tsohou, and E. Magkos, "Unraveling the complexity of mobile application permissions: Strategies to enhance users' privacy education," *European Journal of Engineering and Technology Research*, vol. 1, no. CIE, p. 87–95, Dec. 2023.

[23] B. Ur, M. Pak Yong Ho, S. Brawner, J. Lee, S. Mennicken, N. Picard, D. Schulze, and M. L. Littman, "Trigger-action programming in the wild: An analysis of 200,000 ifttt recipes," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, ser. CHI '16. New York, NY, USA: Association for Computing Machinery, 2016, p. 3227–3231.

[24] R. Liu, J. Cao, K. Zhang, W. Gao, J. Liang, and L. Yang, "When privacy meets usability: Unobtrusive privacy permission recommendation system for mobile apps based on crowdsourcing," *IEEE Transactions on Services Computing*, vol. 11, no. 5, pp. 864–878, 2018.

[25] G. Charness, U. Gneezy, and M. A. Kuhn, "Experimental methods: Between-subject and within-subject design," *Journal of Economic Behavior & Organization*, vol. 81, no. 1, pp. 1–8, 2012.

[26] J. Brooke, "Sus: a retrospective," *J. Usability Studies*, vol. 8, no. 2, p. 29–40, feb 2013.