Stakeholder Inclusion and Value Diversity: An Evaluation Using an Access Control System

Alidoosti, Razieh; De Sanctis, Martina; Iovino, Ludovico; Lago, Patricia; Razavian, Maryam

published in
European Conference on Software Architecture
2023

document version
Publisher's PDF, also known as Version of record

Stakeholder Inclusion and Value Diversity: An Evaluation Using an Access Control System

Razieh Alidoosti[1,2], Martina De Sanctis[2], Ludovico Iovino[2], Patricia Lago[1], and Maryam Razavian[3]

[1] Vrije Universiteit Amsterdam, The Netherlands
{r.alidoosti,p.lago}@vu.nl
[2] Gran Sasso Science Institute, L'Aquila, Italy
{martina.desanctis,ludovico.iovino}@gssi.it
[3] Eindhoven University of Technology, The Netherlands
m.razavian@tue.nl

Abstract. Software systems bring great benefits to people's lives. Nevertheless, they can cause issues in terms of social and ethical implications toward individuals and society, and compromise their ethical values. Therefore, it is crucial to consider all potentially-concerned stakeholders during the system design process, as they are the primary source of value- and requirements identification. In this study, we aim to evaluate the effect that two ethics-driven instruments we have created (*i.e.,* a stakeholder map and a value model) may have on supporting ethical considerations (such as stakeholder and ethical value), using the case of a model-driven access control system. The paper presents the insights gained from this evaluation, performed as a retrospective study.

Keywords: Stakeholder · Ethical value · Software system · ACS.

1 Introduction

With the growing digitalization and the increasing reliance on software systems, ethics in software engineering has gained significant attention. This is because of the social and ethical implications these systems have on individuals and society. Software systems can undermine ethical values, leading to issues such as restrictions on personal freedom and violations of privacy. Such issues, therefore, reinforce the need to focus on software systems and architectures from an ethical standpoint. As pointed out in [1], it is essential to focus on ethical considerations, such as stakeholder, ethical concern, ethical value, and ethical decision, at the early stages of system design (*e.g.,* when making architecture design decisions).

With these premises, stakeholders play a critical role in incorporating an ethical perspective in software systems, as they are the primary source for value and requirements elicitation [3]. Accordingly, it is important to account for the plurality of values in design decision making, especially when there are various stakeholders who software systems may directly or indirectly impact. For

instance, consider the case of facial recognition technology in access control systems used at airports [6]. In such cases, there is a tendency to overlook the needs of specific groups, such as people of color or those with disabilities, as the focus is primarily on security benefits. This can result discrimination and potential biases against these individuals. Thus, it is crucial to equip software designers with instruments that facilitate the inclusion of a wide range of stakeholders and their values by focusing on software systems' ethical and social implications. These instruments should enable designers to explore various potential stakeholders of the system, either affecting or being affected by it, and prompt designers to explore different aspects and scenarios in which they can be affected by the system from an ethical perspective.

To this end, we introduced two ethics-driven instruments, namely a *stakeholder map* and a *value model* [2]. The stakeholder map outlines the three overarching stakeholder roles that may directly or indirectly receive benefit/harm from the system. The value model is a classification of values usually considered in software design and a representation of relations among values. In this work, we evaluate these instruments with a retrospective study examining the effects of utilizing them on stakeholder inclusion and value diversity within the context of a model-driven Access Control System (ACS) [4] (Sect. 2). The selection of the ACS as the case of our evaluative reflective study is justified by its critical role in controlling users' access to resources and services, which can have significant ethical implications, such as privacy violations and threats to autonomy [9]. Specifically, this study investigates the ethical considerations associated with the ACS and evaluates which considerations could have been supported if the instruments had been employed during the system design process. We conducted two focus group sessions involving pertinent stakeholders (Sect. 3). Results indicate that the instruments effectively facilitated the identification of stakeholders with different roles, their ethical concerns and values, and ethical decision making (Sect. 4). We further discuss threats to the validity of our results, and we conclude the paper with future directions (Sect. 5).

2 Background

A Model-driven Access Control System. An ACS supports to check entries via controlled gates (*e.g.,* doors equipped with a lock mechanism) to restricted access areas [8]. We selected, as our case, an ACS implementing a model-driven approach enabling the communication between an IoT infrastructure (*e.g.,* Near Field Communication (NFC) readers and tags, relays, led, alarms) and an access management platform to authenticate users [4]. The ACS has been deployed and evaluated in a fitness center (in L'Aquila, Italy). The ACS architecture aligns with the conventional access control framework [14] and its components, reported in *italic* in this section. The user requests access via an NFC tag through the *Policy Enforcement Point (PEP)* embedded in a NFC reader installed on the gate. The PEP will forward the request to the *Policy Decision Point (PDP)* that evaluates the access request against the authorization policy, by querying

a policies repository and replying to the PEP. The PEP will then grant or deny access to the user for the specified resource, *i.e.,* a room. A *Policy Information Point (PIP)* can optionally be used to enrich the authorization request, *e.g.,* with user rights. Lastly, the *Policy Administration Point (PAP)* manages the authorization policies. We refer to [4] for the detailed ACS architecture.

Ethics-driven Instruments. Our Systematic Literature Review of software engineering ethics (SE ethics) [2] led to the creation of two ethics-driven instruments (see Fig. 1) described below.

The Stakeholder Map. It visualizes three overarching stakeholder roles: *system users*, *system development organization*, and *indirect stakeholders*, each comprising various role types (Fig. 1 (left)). For example, the role of "system development organization", in the ACS, includes role types such as "IoT experts" and "architects". The stakeholder map focuses on three key aspects: (i) the different relations of stakeholders with the system, *i.e.,* using it, building it, or being impacted by it, (ii) the system's implications on stakeholders, *i.e.,* benefits and harms, and (iii) the ways in which stakeholders receive benefits and harms from the system, *i.e.,* directly or indirectly. This map helps software designers in the system design process, to identify a comprehensive range of stakeholders.

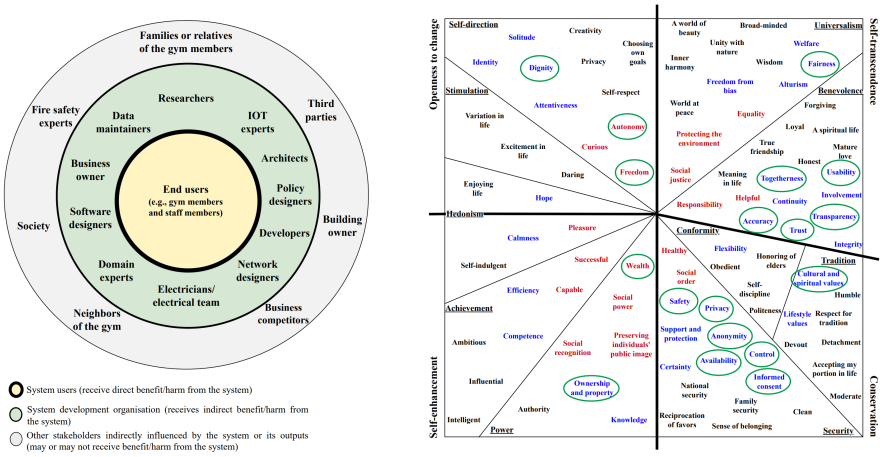

Fig. 1. Ethics-driven instruments [2]: (left) a stakeholder map and (right) a value model

The Value Model. It categorizes ethical values commonly used in system design, along with the relations among these values (Fig. 1 (right))[4]. This model is based on the Schwartz value structure [12,11], a widely used structure for classifying values in social sciences and ethics [13]. Software designers can utilize this model by following a series of steps. First, they should identify the relevant value categories that align with the system's goal(s), and explore sub-values w.r.t. the relevant stakeholders, assessing whether they are supported or undermined by

[4] The elicited values from our evaluation of the ACS are marked with green circles.

the system. The next step involves determining the relationships among those values, including any conflicts or congruencies. To this aim designers should consider the positions of the values within *two orthogonal dimensions*[5]. For instance, "safety" can be considered a pertinent value for gym members, in line with the system's goal. By examining its position in the value model, it becomes apparent that it conflicts with the value of "freedom", as they belong to non-adjacent categories (in *openness to change vs. conservation* dimension). The model provides designers with a guideline to identify the relevant ethical values and relations among them. This enables them to effectively manage potential conflicts and reinforce the values that align with the system's goal(s).

3 Methodology

In this section, we describe our research objective and questions, the evaluation design and execution, as well as the data collection and analysis.

Research Objective and Questions. The objective of this study is to explore the effects of the two ethics-driven instruments in supporting ethical considerations in the case of the ACS represented in Sect. 2. To achieve the research objective, we drive the study with the following research questions (RQs):

(RQ1) *How could the proposed instruments affect the identification of stakeholders with different roles and their ethical concerns?*
(RQ2) *How could the instruments affect the identification of ethical values and the potential relations among them?*
(RQ3) *How could the instruments enable decision-making to support ethical considerations?*

Evaluation Design and Execution. We conducted a retrospective study through a small-scale evaluation of the ACS [4] case. Following the guidelines proposed by Robson [10], we designed the evaluation in two steps: *initial evaluation* and *secondary evaluation* (the asked questions can be found in Appendix A[6]).

In the former we used the focus group research method to explore the effects of the instruments on supporting ethical considerations. In the latter we also employed a focus group to evaluate the findings from the initial evaluation.

Initial Evaluation. The focus group study was conducted in March 2023 as an online session involving four participants who had actively contributed to the design and development of the ACS. The session began with an introduction to the study objective and fundamental concepts in the context of SE ethics. The session was organized as a semi-structured discussion in two parts, lasting a total of three hours. In *part* 1, participants were asked predetermined questions categorized based on our RQs. In *part* 2, participants were introduced to the ethics-driven instruments and were asked questions regarding their usage.

[5] These two dimensions are (i) self-enhancement vs. self-transcendence and (ii) openness to change vs. conservation.

[6] All appendixes are available in the GitHub repository `https://github.com/S2-group/ECSA23-SIVD-rep-pkg.git`

The session served a twofold aim. First, understanding the current state of the ACS in terms of ethical considerations, such as stakeholders and ethical values. Second, using the instruments to uncover ethical considerations that could have been supported in the design of the ACS but were overlooked.

Secondary Evaluation. The focus group study was conducted in May 2023 as an online session lasting one and a half hours. It included two participants from the initial focus group and three additional participants who were end users of the ACS and members of the fitness center exposed to the case.

This evaluation aimed to discover the opinions and expectations of system users, regarding the ethical aspects of the ACS. The results from this phase served as an indicator of the effectiveness of the instruments in identifying ethical considerations related to the system.

Data Collection and Analysis. Focus group sessions in both evaluations were video-recorded and transcribed for further analysis. We analyzed the transcript of each session by using transcript coding as our qualitative data analysis method. Following the approach suggested by Miles and Huberman [7], we created an initial list of codes based on the RQs, including stakeholders, ethical concerns, ethical values, value relations, and ethical decisions. Throughout the analysis process, we further expanded and refined this code list.

4 Results

In this section, we outline our research findings, by discussing the possible relation with the components making the architecture of the ACS (Sect. 2).

4.1 The Initial Evaluation Results

Finding 1. In *part* 1 of the session, participants discussed those individuals or groups who were explicitly considered in the design of the ACS, such as *the business owner* (the ACS contractor) and *the building owner*. During the stakeholder identification process, only individuals with direct relationships with the system were considered, *e.g.,* those involved in the ACS implementation, infrastructure, and usage. The participants recognized the end users of the ACS as one of the most crucial stakeholder, being the primary beneficiaries of the system. In *part* 2 of the session, as the ethics-driven instruments were introduced, the participants noted that certain stakeholders had been overlooked during the ACS design process. These stakeholders included individuals who could have a significant impact on the ethical implications of the system by, *e.g.,* establishing ethical standards and providing oversight and regulation, such as *policy designers* and *fire safety experts*. Policy designers could be directly involved in designing and implementing the PDP and policy repositories. Additionally, some could be indirectly influenced by the system's ethical implications, such as *the entire society* and *the families of end users*. The only part of the system in which the involvement of the end users and relatives (*e.g.,* visiting the facility) maybe required is the PEP since it serves as the external interface of the ACS with the users. Section 3 in Appendix B reports the identified stakeholders.

Finding 1 (RQ1): We observed that utilizing the ethics-driven instruments broadened the participants' perspectives on the ethical implications of the system and its interactions with various stakeholders. This helped identify overlooked stakeholders that should be considered in the ACS design process.

Finding 2. During *part* 1, participants examined the possible ethical issues associated with the ACS concerning the stakeholders involved. One of the most prominent raised concerns was possible *privacy violations*. All participants were cognizant of this issue and acknowledged its significance in the context of software systems. They also identified other ethical concerns, such as *avoiding identifiability* and *avoiding malicious activities* (see Sect. 4, Appendix B). When the system evaluates an authorization request, the PIP can enhance it with additional information such as user rights, and schedules, while the PAP is responsible for administering the authorization policies. They may be both affected by privacy issues, thus their design must consider these possible threats. In *part* 2, the participants brainstormed the system's ethical implications for different stakeholders. They discussed different scenarios to determine how ethical values in relation to the system could potentially be supported or undermined. They raised ethical concerns regarding the ACS, which they had never thought about or considered their impacts on stakeholders. For example, the risk of *violating dignity* of gym members, *e.g.,* when they are publicly denied access to gym services (by raising the alarm) due to late payment of membership fees. It could lead to feelings of embarrassment and shame. Moreover, they raised ethical concerns focused on indirect system's stakeholders, *e.g., noise pollution* affecting the gym's neighbors, the potential *threats to the sense of togetherness* experienced by gym members and their families. Such implications emphasize the need to consider system users and indirect stakeholders when designing the components of the PEP. It is essential to properly control and configure the loudness of speakers to prevent any violation of dignity when a user is denied entrance and to ensure there are no disturbances to the gym's neighbors.

Finding 2 (RQ1): We observed that using the instruments assisted the participants in considering the possible and far-reaching ramifications of the system and its potential to harm various stakeholders from an ethical perspective. This helped the elicitation of the ethical concerns of the involved stakeholders.

Finding 3. During *part* 1, the participants discussed several values related to the system, including *privacy*, *security*, *welfare*, and *fairness*. Although not explicitly stated, they acknowledged their reliance on use cases to identify these values, guided by the functionalities requested by the business owner. Given the relations among ethical values (see Sect. 5, Appendix B), the participants focused only on the tension between *security and privacy*, and the congruity between *fairness and well-being/welfare*. They emphasized that defining these relations was not straightforward and required reasoning, as there was no clear-

cut solution. During *part* 2, following the introduction of the instruments, the participants identified several new values concerning the system and their relationships. These relations included tensions between values, such as *togetherness and ownership and property*, *freedom and safety*, *freedom and control*, *safety and anonymity*, *cultural values*, and congruity between *cultural values and control*. The ACS components are all tied to the above-mentioned value relations, highlighting the need for their consideration when designing the components.

Finding 3 (RQ2): We observed that the instruments expanded the participants' perspectives on affected values and their relations by prompting the focus on stakeholders' ethical concerns. Participants gained insight into identifying and balancing different ethical values.

Finding 4. During *part* 1, participants focused primarily on privacy-related design decisions (see Sect. 6, Appendix B), such as implementing separate internal and external storage for keeping data. A scenario was derived where a user might require authorization from the PEP following another user. If the PEP includes output devices, *e.g.,* a display, the system must ensure that the PEP can provide information regarding a possible denial without causing ethical harm to the users. This highlights the importance of considering privacy concerns when designing the PDP, PIP, and PAP, even though the PEP could also be exposed. Thus, an important design decision is about how long the reason for the denial of entrance should be displayed on the screen. Alternatively, this private information could even be sent to the user confidentially, *e.g.,* by email. During *part* 2, the participants put forward various design decisions aimed at supporting different ethical aspects. They suggested, *e.g.,* a solution to reduce noise pollution at night, which could have a positive impact on the well-being of neighbors. Other ethical decisions are listed in Appendix B. When designing the PIP for the ACS, it is crucial to consider all the decisions above, as the PIP's role is to enrich the authorization with additional data.

Finding 4 (RQ3): We observed that the instruments raised the participants' awareness regarding the importance of considering ethical values and the ethical implications in the design decision process. This enabled the participants to make ethical design decisions within the context of the ACS.

Further, we observed that using the instruments enabled the participants to propose recommendations grounded in an understanding of the system's ethical implications on the stakeholders (see Sect. 7, Appendix B). These recommendations can be regarded as potential considerations for future design decisions within the context of the ACS.

4.2 The Secondary Evaluation Results

During this session, our main focus was on examining the potential ethical implications of the ACS, discovered in the initial evaluation. We delved into the

opinions and perspectives of system's users (*e.g.,* gym members) regarding these implications (see Sect. 8, Appendix C). We found that participants acknowledged the existence of most of them within the context of the ACS. They specifically emphasized the relevance and importance of the following implications: *noise pollution*, *control*, *violation of physical and emotional well-being*, *violation of dignity*, *threatening togetherness*, *violation of cultural and spiritual values*, *support for usability*, *support for trust*, *support for autonomy*.

There were also instances where participants expressed that certain implications are not deemed as significant in relation to the ACS. For instance, they believed that the system's *security risks* are not highly impactful since the system does not store sensitive information. Additionally, they believed that the system does not impose *restrictions on their freedom*, and any limitations they experience are primarily due to the gym's security measures. Furthermore, participants raised the ethical concern of *identifiability*, *i.e.,* the state of being identifiable, which had not been previously mentioned. They considered it as the most significant implication that requires to be taken into account during the design process. All the components of the ACS are clearly tied to the highlighted ethical concerns. However, since the user interaction happens through the PEP, it is crucial to design it in a way that instills a sense of trust in the end user.

Finding 5 (RQ1): We observed that the opinions of the system's users regarding its ethical implications align closely with those revealed using the instruments. This suggests that the instruments have the potential to assist software designers in identifying ethical implications of the system that are important from the standpoint of stakeholders with different roles.

5 Threats to Validity and Conclusion

A potential threat to *construct validity* is related to the mediator's bias in data collection. We mitigated it by proposing predetermined questions in the two focus group sessions. A potential threat to *internal validity* is related to the reliability of the data collected from the two focus groups. To mitigate it, we used Atlas.ti [5] to code and cluster notable quotes to reduce bias and ensure reliable results. A potential threat to *external validity* is related to the experience and background of participants involved in the secondary evaluation. To mitigate it, we conducted the focus group involving participants with different experiences. A potential threat to *conclusion validity* is related to the credibility of the final findings. To mitigate it, we all discussed the study findings and drew conclusions.

To conclude, we observed that the instruments effectively helped accomplish the study objective, which involved facilitating the identification of potential stakeholders with different roles, their ethical concerns, their ethical values, and ethical decision making. One potential direction for future research could involve conducting a broader range of studies to comprehensively assess the effectiveness of the instruments.

Acknowledgment

We would like to thank the ACS designers for their contribution to enhancing our understanding of the system from an ethical standpoint. Also, we thank the gym members for their valuable feedback.

References

1. Alidoosti, R., Lago, P., Poort, E., Razavian, M.: Ethics-aware decidarch game: Designing a game to reflect on ethical considerations in software architecture design decision making. In: 2023 IEEE 20th International Conference on Software Architecture Companion (ICSA-C). pp. 96–100. IEEE (2023)
2. Alidoosti, R., Lago, P., Razavian, M., Tang, A.: Ethics in Software Engineering: A Systematic Literature Review. Tech. rep., Vrije Universiteit Amsterdam (2022), `https://tinyurl.com/39crpyn2`
3. Bittner, K., Spence, I.: Establishing the vision for use case modeling, use case modeling. Addison Wesley Professional, Reading (2003)
4. De Sanctis, M., Di Salle, A., Iovino, L., Rossi, M.T.: A technology transfer journey to a model-driven access control system. International Journal on Software Tools for Technology Transfer pp. 1–26 (2023)
5. Friese, S.: Qualitative data analysis with ATLAS. ti. Sage (2019)
6. Leong, B.: Facial recognition and the future of privacy: I always feel like... somebody's watching me. Bulletin of the atomic scientists **75**(3), 109–115 (2019)
7. Miles, M.B., Huberman, A.M.: Qualitative data analysis: An expanded sourcebook. sage (1994)
8. Moreno, M.V., Hernández, J.L., Skarmeta, A.F.: A new location-aware authorization mechanism for indoor environments. In: international conference on advanced information networking and applications workshops. pp. 791–796. IEEE (2014)
9. Neudecker, T., Hayrapetyan, A., Degitz, A., Andelfinger, P.: Consideration of values in the design of access control systems. Informatik 2016 (2016)
10. Robson, C.: Small-scale evaluation: Principles and practice. Sage (2017)
11. Schwartz, S.H.: Universals in the content and structure of values: Theoretical advances and empirical tests in 20 countries. In: Advances in experimental social psychology, vol. 25, pp. 1–65. Elsevier (1992)
12. Schwartz, S.H.: Basic human values: Theory, measurement, and applications. Revue française de sociologie **47**(4), 929 (2007)
13. Schwartz, S.H.: An overview of the schwartz theory of basic values. Online readings in Psychology and Culture **2**(1), 2307–0919 (2012)
14. Sicari, S., Rizzardi, A., Miorandi, D., Cappiello, C., Coen-Porisini, A.: Security policy enforcement for networked smart objects. Computer Networks **108**, 133–147 (2016)