Third Study: Privacy Mindset of Software Developers

1 - INTRODUCTION

Privacy is a multifaceted concept, and can often be vague and elusive. Privacy can be understood in many ways, related to what you want to keep private (KALLONIATIS et al., 2008; GHARIB et al., 2017). Aligning software to meet privacy needs is a challenging task because there is still unified view on privacy engineering (BECKERS, 2012). Also, it is still unclear how software development processes deal with privacy (HADAR et al., 2018). This lack of clarity regarding privacy engineering can result in much confusion between designers and stakeholders and sometimes can lead to wrong design decisions (GHARIB et al., 2017).

According to Hadar et al. (2018) it is necessary to observe the perception of privacy from the point of view of users and developers. In fact, software users' perceptions and concerns on privacy have been widely studied. However, less attention is given to the perceptions, interpretations, and practices of the developers regarding privacy (HADAR et al., 2018).

In this sense, Hadar et al. (2018) made efforts to understand privacy from developer's point of view. This study is based on the study of Hadar et al. (2018) and aims to investigate the perceptions and interpretations of privacy and practices to deal with privacy in agile software development projects.

2 - METHOD

The Research Questions (RQ) to be investigated are in Table 1.

Table 1: Research questions and motivations.

Item	Motivation
(RQ 1) How does the work environment help the developer deal with privacy?	The purpose of this question is to understand which organizational practices help the developer deal with privacy concerns.
(RQ 2) How do developers perceive and interpret the concept of privacy in their daily work?	This question aims to observe how developers understand privacy.
(RQ 3) What are the practices developers use to	This question is intended to detect which

deal with privacy?	privacy practices the developer uses at work.

To answer these research questions, it will be conducted in-depth interviews with developers of privacy-sensitive software projects.

Data analysis will be performed qualitatively according to the Grounded Theory (STRAUSS and CORBIN 1994, 1998). Additionally, data classification, according to the Social Cognitive Theory (SCT) (BANDURA, 1986) will be used to propose a conceptualization of the factors that influence and are influenced by the privacy practices of developers. Therefore, factors such as:

- External Environment (E) reside the findings related to the work environment of the developers, namely the organization in which they operate, with its privacy-related characteristics. (Answer RQ 1);
- Personal factors (P) reside the findings related to developers' perceptions of privacy and their interpretation of this concept. (Answer RQ 2);
- Behavior (B) reside the findings related to the developers' (self-reported) behavior when encountering informational privacy concerns during software development. (Answer RQ 3).

APPENDIX : INTERVIEW GUIDE

Part 1: Profile/Background

- What is your academic background?

  O University Graduate O Master

  O Ph.D. O Others
- Do you work for a company that uses agile software development? What kind of agile development (Example: XP, Scrum)?
- What agile artifact does the company you work for adopting? (Example: kanban board, mockup, burndown charts, story map).
- What development domain are you currently working on?
- What is your current role in the company?

  O System Analyst O Tester

O Developer O Project Manager

O Other ______________________________

- How many years of experience do you have in this role?
- Have you been involved in the development of information systems that handle personal information about users? If so, please describe your role in each project.
- Have you acquired knowledge/education specifically related to privacy concerns in information systems? If so, please describe how you have acquired this knowledge.

<u>Part 2: Privacy Mindset</u>

<u>Personal and Behavioral Factors</u>

- What is informational privacy?
- What is the difference between security and privacy?
- What laws are you familiar with, in the context of informational privacy?
- What organizational procedures regarding informational privacy are you familiar with?
- What norms are you familiar with, in the context of informational privacy?
- What sources of information do you use in order to address privacy concerns that you need to deal with?
    - (Internet / what sites? Organizational procedures? Managers? Other employees? Literature (which)?)
- When you encounter a privacy concern, what do you do about it?
- Can you describe three examples of projects you were involved in, in which privacy concerns were discussed? What aspects of privacy did you handle?
- When developing a system, do you consider potential risks scenarios regarding privacy?
- What strategies are you familiar with as solutions for privacy concerns?
    - (Give examples)

Table. 1 List of privacy strategies

Strategy	Familiar with	Uses
Decentralization of data so there is no central access point for all data		
Collected data is regularly deleted after usage		
Providing users control over privacy settings: What would be revealed to other users or		

system operators		
Optional turn off of overall data collection for a certain time frame		
Encryption technologies		
Data anonymization for management and analysis purpose		
User transparency about his/her information that is available in the system		
Systems that enable users to access personal information about them, which resides within the system		
Systems that enable users to delete personal information about them, which resides within the system		
Automatic expiration of personal information		

- Does the organization inform its users about its privacy policy?
- During your work, have you ever needed to address concerns of notifying users about ongoing operations or information theft? If so, how? At what stage?
- In your opinion, to what extent is it important to receive consent from users prior to collecting private data about them?
- In your opinion, to what extent do the users have the right to choose how, when and what information is gathered about them (that is, the freedom to design the information that is collected about them)?
- Do you think that user consent for data collection should be opt-in (default is lack of consent, and requires active action to give consent) or opt-out (default is agreement, and requires active action to deny consent)?
- Have you ever dealt with user consent in this context? In what stage of the development? Who raised the need? Is the topic of user consent discussed during projects?
- Do you, or the customer (for whom the system is designed), define the purpose for which the information is collected by the system?

- How do you decide what information is collected by the system? What are the considerations? Are they determined according to customer requirements? According to common practices? Some other criteria?
- Is the legitimacy of the purpose for which personal information is collected by the system discussed? Do you ever ask yourself if a specific purpose of collecting personal information is legal/problematic in any sense?
- In your opinion, should personal information accumulated about users in the system be deleted? If so, after how much time should it be deleted? (Immediately after the use of the information? after one month? three months? one year? two years? five years? ten years?)

External Environment Factors

- Are privacy concerns considered, in projects you are involved with? If so, can you describe these privacy concerns? What are the roles involved in this project?
- Does the organization encourage taking precautions with privacy?
- Tell me how identification/elicitation of requirements occurs in your organization? What privacy concerns were considered?? Is privacy considered? How is privacy considered? Do you agree with the current practices? How could they be improved?
  - What are the techniques used to elicit requirements? What about privacy requirements?
  - What are the roles/functions of those involved in the organization that participates in the elicitation of requirements? What about privacy requirements? Are stakeholders involved in the process?
- Who is involved in the decision about privacy requirements inclusion/exclusion?
  - How do you handle conflicting requirements (clients and stakeholders)? What about conflicts involving privacy requirements?
- Tell me how specification/documentation of requirements occurs in your organization? Is privacy considered? How is privacy considered? Do you agree with the current practices? How could it be improved?
  - What are the techniques used to specify/document requirements? What about privacy requirements?

    - What are the roles/functions of those involved in the organization that participates in the specification process of requirements? What about privacy requirements? Are stakeholders involved in the process?
- What are the tools used to support requirements activities? What about privacy requirements? What are the benefits these tools provide?
- Does the company have concerns regarding the General Regulation of Protection of Data (GDPR) European legislation that came into force in May 2018?
- How is the company preparing to comply with the GDPR?
    - Who is responsible for verifying whether the system complies with the GDPR?
- Can you describe the procedure to define Privacy Policies for systems developed in the company?
    - Who is responsible for this definition?
- Do you have any other thoughts about informational privacy you would like to share?

REFERENCES

1. KALLONIATIS, C.; KAVAKLI, E.; GRITZALIS, S. Addressing privacy requirements in system design: the PriS method. Requirements Engineering, [S.l.], v. 13, n. 3, p. 241-255, 2008.
2. GHARIB, M.; GIORGINI, P.; MYLOPOULOS, J. Towards an Ontology for Privacy Requirements via a Systematic Literature Review. In: Mayr H., Guizzardi G., Ma H., Pastor O. (eds) Conceptual Modeling. LNCS, p. 193-208, 2017.
3. BECKERS, K. Comparing privacy requirements engineering approaches. In: Availability, Reliability and Security (ARES), 2012 7th International Conference on. IEEE, 2012, Prague. Proceedings. . . Prague: IEEE. p. 574-581.
4. HADAR, I.; HASSON, T.; AYALON, O.; TOCH, E.; BIRNHACK, M.; SHERMAN, S.; BALISSA, A. Privacy by designers: software developers' privacy mindset. Empirical Software Engineering, v. 23, n. 1, p. 259-289, 2018.
5. BANDURA, A. (1986) Social foundations of thought and action: a social cognitive theory. Prentice-Hall, Englewood Cliffs.

6. STRAUSS, A.; CORBIN, J. (1994) Grounded theory methodology: an overview. In: Denzin NK, Lincoln YS (eds) Handbook of qualitative research. Sage, Thousand Oaks, pp 273–285.
7. STRAUSS, A.; CORBIN, J. (1998) Basics of qualitative research: techniques and procedures for developing grounded theory. Sage Publications, Thousand Oaks.