The Journal of Systems & Software 195 (2023) 111523

Contents lists available at ScienceDirect

The Journal of Systems & Software

journal homepage: www.elsevier.com/locate/jss

The perspective of Brazilian software developers on data privacy☆

Mariana Peixoto [a,*], Dayse Ferreira [a], Mateus Cavalcanti [a], Carla Silva [a], Jéssyka Vilela [a], João Araújo [b], Tony Gorschek [c]

[a] Centro de Informática, Universidade Federal de Pernambuco (UFPE), Recife, Brazil
[b] NOVA LINCS, Departamento de Informática, Faculdade de Ciências e Tecnologia, Universidade NOVA de Lisboa (UNL), Lisbon, Portugal
[c] Software Engineering Research Lab (SERL), Software Engineering Department, Blekinge Institute of Technology (BTH), Karlskrona, Sweden

ARTICLE INFO

Article history:
Received 1 October 2021
Received in revised form 26 July 2022
Accepted 27 September 2022
Available online 3 October 2022

Keywords:
Privacy requirements
Software development
Empirical study

ABSTRACT

Context: Maintaining the privacy of user data is a concern in software development to satisfy customer needs or to comply with privacy laws. Recent studies have shown that software development approaches still neglect non-functional requirements, including privacy. Concern about privacy may increase in the period between when a privacy law is initially announced and when it is passed into law. During this period, companies will be challenged to comply with the new law. Research has shown that many developers do not have sufficient knowledge to develop privacy-preserving software systems.
Objective: We investigate the level of knowledge and understanding that developers possess regarding privacy. We explore the personal, behavioural, and external environmental factors affecting a developer's decision-making regarding privacy requirements.
Methods: We replicated a study by means of in-depth, semi-structured interviews with thirteen practitioners at six companies. Our data analysis is based on the principles of 'grounded theory codification'.
Results: We identified nine personal factors, five behavioural factors, and seven external environment factors that are relevant to how software developers make decisions regarding.
Conclusion: Our identification of factors that influence the development of privacy-preserving software systems can be seen as a contribution to the specification of effective methods for securing privacy.

© 2022 Elsevier Inc. All rights reserved.

1. Introduction

Demands with respect to compliance with data protection laws and the safeguarding of personal information are forcing companies to consider the development of privacy-friendly products and services (Spiekermann and Cranor, 2009; Hadar et al., 2018). In this regard, the European Union's passing of the European General Data Protection Regulation (GDPR, 2018) a regulation that introduced fundamental rights and freedoms for European citizens and rules regarding the protection and processing of their personal data. Due to the increasing need of data protection laws, Brazil approved, in August 2018, the General Personal Data Protection Law 13.709/2018 (in Portuguese, Lei Geral de Proteção de Dados or 'LGPD') (LGPD, 2018). After LGPD was approved, authorities started a 'vacancy period', which corresponds to the period between the date when a law is published and the date when the law is in force. This vacancy period ended in 1 August 2021.

Given the above scenario regarding the regulation of privacy, developers[1] are obliged to design and implement privacy-preserving software systems. One approach to the development of such systems is to follow the Privacy by Design (PbD) (Cavoukian, 2009) that lists the fundamental privacy principles that should be dealt with within the very early stages of the software development process (Cavoukian, 2009; Hadar et al., 2018), i.e., from the Requirements Engineering (RE) phase (Del Alamo et al., 2018; Kalloniatis et al., 2008). However, many developers do not have sufficient knowledge and understanding of privacy, nor do they know how to develop a privacy-preserving software systems (Hadar et al., 2018). This lack of knowledge and understanding can lead to developers misinterpreting the concepts of

☆ Editor: Kelly Blincoe.

* Corresponding author.
E-mail addresses: mmp2@cin.ufpe.br (M. Peixoto), dmmf@cin.ufpe.br (D. Ferreira), mcl2@cin.ufpe.br (M. Cavalcanti), ctlls@cin.ufpe.br (C. Silva), jffv2@cin.ufpe.br (J. Vilela), p191@fct.unl.pt (J. Araújo), tony.gorschek@bth.se (T. Gorschek).

[1] We generalize the term developer to refer to any individual who works with software development because we found no differences in the responses across the different roles we interviewed.

https://doi.org/10.1016/j.jss.2022.111523
0164-1212/© 2022 Elsevier Inc. All rights reserved.

'privacy' and 'security', leading to, for example, incorrect design decisions (Hadar et al., 2018; Gharib et al., 2017) and stakeholders may even go so far as to believe that security is the same as privacy (Abu-Nimeh and Mead, 2009; Gharib et al., 2020). Whilst there is a significant difference between the two, if privacy is implemented or used correctly, it can enable security. For example, if the system does not collect sensitive data (since it has been designed not to need such data), then a malicious person cannot access said data.

Examining the aforementioned challenges regarding security and privacy in the context of data protection laws, Hadar et al. (2018) report that privacy concerns from the perspective of software users have been widely studied. However, less attention has been given to the developers' perspective on security and privacy. Successful PbD projects demand knowledge of how developers ensure their customers' data privacy during the software development phase of the project.

Research has been conducted into how developers deal with privacy by using surveys and questionnaires (Sheth et al., 2014; Dias Canedo et al., 2020; Bu et al., 2020), interviews (Hadar et al., 2018; Ribak, 2019; Bednar et al., 2019; Spiekermann et al., 2018), and controlled tasks (Senarath and Arachchilage, 2018a). These studies show that there is still limited awareness amongst developers regarding the importance of privacy and what the concept of 'privacy' means. In the case of non-functional requirements (NFRs), privacy is usually neglected completely or receives scarce attention (Kasauli et al., 2017; Wagner et al., 2018; Curcio et al., 2018).

In this study, we investigated how Brazilian developers deal with privacy when developing software intensive products and services in a time period that corresponded to the vacancy period of LGPD. Therefore, software development organizations were struggling to come into compliance with this law and we found an opportunity to understand this phenomenon and gather more information that could be used to develop processes, tools and techniques focused on guiding Brazilian organizations in the compliance of data protection laws. We also aimed to bring evidence on the differences and similarities between Brazilian developers and foreign developers regarding their development practices related to the development of privacy-preserving software systems. Our study results are also significant for developing countries such as Brazil, which have a large domestic software market and are still making efforts to improve software processes aiming to compete in international markets (Menolli et al., 2015). For example, during this study period, Brazil represented 1.8% of the global IT market (ABES, 2020).

To achieve our goal, we replicated a previous study conducted by Hadar et al. (2018). A replication of an empirical study is regarded as an essential activity to increase and consolidate knowledge in Software Engineering (Da Silva et al., 2014) and for achieving greater validity and reliability in research results (Cruz et al., 2020). For example, a replication can provide confirmation, refutation, or deepen the conclusions drawn from an earlier study (Da Silva et al., 2014). Thus, in this study, our goal is to conduct a replication to increase knowledge concerning the area of data privacy in software development, in addition to promoting the consolidation of knowledge by comparing our results with the results of other studies.

We conducted thirteen in-depth, semi-structured interviews with practitioners from six companies. The interviews were transcribed and analysed by using the coding principles presented in the Grounded Theory (GT) (Strauss and Corbin, 1998) and in light of *Personal*, *External Environment* and *Behavioural* factors from the Social Cognitive Theory (SCT) (Bandura, 1986). This paper is an extension of our previous study (Peixoto et al., 2020) in which we argue that *Personal factors* affect how developers interpret and perceive privacy requirements. In the present paper, we consolidate our analysis concerning *Personal factors*, and also include the other two SCT factors, namely *External Environment* and *Behaviour*. These two factors were also included in the analysis because SCT assumes that the behaviour, personal and environmental factors operate as interacting determinants and influence each other bidirectionally. We selected SCT as a theoretical framework because it is an insightful and widely-used theory in Information Systems (IS) research (Carillo, 2010). An analysis of these determinants provides us with an understanding of the factors that drive human behaviour to deal with new strategies or technologies (Carillo, 2010). Therefore, our study of SCT factors is primarily focused on understanding how developers deal with privacy. Based on this understanding, we can identify the problems that companies should avoid when they are tasked with developing privacy-preserving software systems. Moreover, we claim that the findings of this study can further define software development methods and techniques that promote user privacy.

The following sections are organized as follows: In Section 2, we describe the central concepts used in the study and discuss related work. In Section 3, we describe our research method. Section 4 presents the results of our study. These results are further discussed in Section 5. In Section 6, we identify several threats to the validity of our study and Section 7 presents a summary of our conclusions and directions for future research in this area.

2. Background and related work

In this section, we briefly review the main concepts that are used in this study in order to promote a better understanding of the theoretical aspects, including an explanation of the 'privacy' concept in a digital environment. We also present results from existing studies on how practitioners address software development requirements, with an emphasis on non-functional requirements, which is the case for privacy. In addition, we present a description of Social Cognitive Theory, which constitutes the theoretical framework used to drive our data analysis. At the end of this section, we compare related work.

2.1. Privacy conceptualization

The concept of 'privacy' has been defined in several different ways in the literature. For example, in the seminal *Harvard Law Review*, Brandeis and Warren (1890) conceptualize 'privacy' as "the right to be let alone". Westin and Ruebhausen (1967) defines 'privacy' as the "claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others". For Altman (1975), 'privacy' is "a boundary regulation process whereby people optimize their accessibility along a spectrum of 'openness' and 'closeness' depending on context". It should be noted that 'privacy' is also regarded as a universal right (Assembly, 1948). Nowadays, details about an individual's activities are typically stored for long periods of time and are available from multiple electronic sources (Spiekermann and Cranor, 2009). Therefore, user privacy can be defined as the right to determine when, how, and for what purpose information about the user is communicated to others (Kalloniatis et al., 2008). Spafford and Antón (2007) and Nissenbaum (2009) indicate, however, that no absolute definition of 'privacy' can be formulated because it means different things to different people. For these scholars, privacy expectations are highly dependent on contextual elements. From this perspective, privacy does not only entail controlling other people's immediate access to oneself but includes reducing the risk that

one's personal information might be used in an undesired way (Spiekermann and Cranor, 2009).

A number of guidelines for managing privacy in electronic sources are available (Gellman, 2017; OECD, 2002). For example, the Fair Information Practice Principle (FIPP) includes the following advice: *Notice* (Inform the data subject that data collection will take place); *Consent* (Individual consent is required for the collection, use, or disclosure of personal information); *Data minimization* (Limit the type of information that can be collected about an individual); *Purpose specification* (Information should be collected and stored for a specific purpose and should not be used for other purposes); *Subjects' access* (Enable individuals to access their personal data); *Rectification rights* (Allow the data subject to require that the data be rectified if it is inaccurate); *Confidentiality* (Personal information should be protected with reasonable safeguards to ensure its confidentiality); and *Data security* (Personal data should be protected by reasonable security safeguards) (Cavoukian, 2009; Gellman, 2017; Hadar et al., 2018; OECD, 2002).

Regarding the concept of 'security', Gharib et al. (2020) mention that most current research deals with privacy requirements as a particular case of security requirements. This type of research usually focuses, for example, on issues related to confidentiality but typically overlooks important privacy issues such as anonymity, pseudonymity, and unlinkability. Consequently, developers may well be inclined to make incorrect design decisions due to an insufficient understanding of the concept of 'privacy'. According to Spiekermann and Cranor (2009), the FIPP can be implemented by adhering to 'security best practices', which are covered extensively in SE. In the present study, we are primarily concerned with developing a deeper understanding of 'privacy' and establishing whether there is an overlap between the concepts of 'privacy' and 'security' in practice. In this context, we acknowledge the presence of privacy solution strategies that are based on the FIPP, including concepts, such as: *Decentralization* (There is no single central access point for all of the data); *Anonymization* (Process data to remove or modify information that can identify a person); *Transparency* (Inform the user about the personal information that is available on the system); *Encryption* (Use of encryption technologies); *Data deletion after use* (The system enables users to delete personal information); and others (Hadar et al., 2018; Spiekermann and Cranor, 2009).

Starting from the assumption that privacy is an NFR, we will discuss how companies deal with this type of requirement in the next section.

2.2. Requirements in software development

According to Sommerville (2011), Requirements Engineering (RE) consists of a process that is instantiated by four high-level activities: (i) assessing whether the system is useful to the business (feasibility study), (ii) performing requirements discovery (elicitation and analysis), (iii) converting the requirements into a standard format (specification), and (iv) verifying whether the requirements actually define the system that the customer wants (validation). Separate from, but related to, the above, we find the process of understanding and controlling changes to system requirements (i.e., system management).

In the present study, we are interested in examining the requirements specification phase of NFRs. In this context, requirements specification is the process of recording the user and system requirements in a so-called requirements document (Sommerville, 2011).

Wagner et al. (2019) have investigated requirements documentation in a study that included 228 organizations from across ten different countries. They noticed that the most frequently used representation formats for requirements documentation are (i) free-form textual domain or business process models, (ii) free-form textual structured requirements lists, (iii) use case models presented as text with constraints, and (iv) NFRs that are textually documented. Another format used lies on the (v) user stories technique and their acceptance criteria (Wagner et al., 2019).

On the other hand, there is a limitation regarding the documentation of NFRs since they are often not prioritized and are not usually documented during the software development process (Behutiye et al., 2017; Ijaz et al., 2019). In addition, agile teams face problems regarding privacy specifications (Canedo et al., 2021). However, it is widely known that the lack of prioritization for NFRs and the neglect to document NFRs lead to the release of a low-quality product or service. Furthermore, high maintenance costs may also result from not prioritizing NFRs (Behutiye et al., 2017; Ijaz et al., 2019; Dabbagh and Lee, 2015). Moreover, if a company is to release efficient and effective software intensive products and services, it should promote the idea of 'continuous integration' (CI). This practice is aimed at continuously verifying quality aspects, both for functional requirements and NFRs (Yu et al., 2020). In this sense, the interview-based study that we conducted aimed at discovering how 'privacy', in the context of NFRs, is considered in the RE methods adopted by the companies of our sample.

In the next section, we present SCT to enable a better understanding of how the collected data was analysed.

2.3. Social Cognitive Theory

According to Bandura (2005), Social Cognitive Theory (SCT) proposes an explanatory social model for human functioning and behaviour. According to this model, three factors (personal, behaviour, and environment) influence each other bidirectionally and impose limits on and offer resources for personal development.

We use SCT (Bandura, 1986), to observe factors that affect a developer's decision-making process with regard to privacy. According to Bandura (1986) and Hadar et al. (2018), the factors included in SCT can be characterized as:

- Personal (P). This factor is used to refer to the elements that constitute human cognition. These include the ability of the human being to memorize, plan, and judge. For example, cognitive skills allow for the selection of events that will have the most value. However, cognition does not present itself in isolation because it does not function independently of the other two established variables: behaviour and environment. Therefore, we consider our findings related to developers' perceptions of 'privacy' and their interpretation of this concept.
- Behaviour (B). This factor is used to refer to an individual's personal conduct, excluding the behaviour of others. This includes our observations concerning the developers' self-reported behaviour with respect to their dealings with information privacy (i.e., privacy within a digital environment).
- External Environment (E). This factor refers to the external environment of the person, i.e., objects, other people, and organizational climate. The External environment also interacts with Personal (P) as well as Behaviour (B). Therefore, this factor informs our findings of this research concerning the developers' work environment, namely the organization in which they operate and its privacy-related practices.

SCT is a model that can be described in terms of a triadic reciprocity in which behavioural factors, personal factors, and environmental factors operate as interactive determinants with

respect to each other. Consequently, our use of SCT in this study is an indication of our recognition of the claim that the integration of both the individual and the environment can be used to predict an individual's behaviour (Carillo, 2010).

SCT, thus, will allow us to understand the mutual influence of personal, behavioural and external environment factors on the developers' perceptions and understanding of privacy.

2.4. Previous research on the topic

In this section, we comment on previous research that considers 'privacy' as a very significant factor in software development. We will also comment on research that provides us with an understanding of how privacy is taken into account in software development.

This information provides us with a point of departure in discussing how Brazilian developers address privacy requirements during the 'vacancy period' associated with the introduction of the LGPD data protection law. Developers' perceptions of privacy have been explored in recent research (Hadar et al., 2018; Sheth et al., 2014; Dias Canedo et al., 2020; Bu et al., 2020; Ribak, 2019; Bednar et al., 2019; Spiekermann et al., 2018; Senarath and Arachchilage, 2018a; Senarath et al., 2019; Senarath and Arachchilage, 2018b). Dias Canedo et al. (2020), for example, performed a survey with Brazilian information and communication technology practitioners. They found that their participants lacked comprehensive knowledge of privacy requirements, as outlined in the LGPD. In addition, these researchers found that their participants were not able to work with the prevailing laws and guidelines that govern data privacy.

Tahaei et al. (2021) conducted twelve interviews with the so-called champions in privacy (people who strongly care about advocating privacy). They found barriers during software design. For example, negative privacy culture, internal prioritization tensions, limited tool support, unclear evaluation metrics, and technical complexity.

Waldman (2017) presents the results of an ethnographic study on how technologists consider the thinking about privacy. As a result, the author provides a narrative where privacy is narrow, limited and barely factored into design.

Sheth et al. (2014) conducted an online survey with 408 users and developers. They found that users often reduce the concept of 'privacy' down to a concept of 'security' (data sharing and data breaches are the biggest concerns). Users are more concerned with the content of their documents and their location data than their interaction data. On the other hand, developers prefer to focus on technical measures, including data anonymization. Developers think that privacy laws and policies are not effective. Moreover, the authors noted that people from different countries have different concerns with regard to data privacy. For example, people from Europe are more concerned about data breaches than people from North America.

Ribak (2019) conducted interviews with employees at a late-stage startup and enquired about their perceptions of privacy. Ribak's analysis suggests that the globalization aspects of the startup globalization favoured the implementation of development practices related to protecting user information privacy.

Senarath and Arachchilage (2018a) observed 36 software developers working on a software design task who were provided with instructions to embed privacy in their software design. The authors wished to identify the problems the developers faced when they designed the software. The authors noted that: (i) the participants complained that the specified privacy parameters contradicted the system's requirements; (ii) the participants found it challenging to relate privacy techniques with system requirements; (iii) the participants found that it was difficult to verify their work; (iv) the participants' personal opinions affected the way they embedded privacy into the design of the software; and (v) the participants lacked in-depth knowledge of privacy techniques.

Bednar et al. (2019) interviewed six senior engineers who worked at global corporations and research institutions to investigate their motivation and ability to comply with privacy regulations. Their study shows that they identified behaviours, perceptions, and beliefs for the engineers that were contradictory. For example, some of the participants confirmed that it is possible to implement privacy in software design, whilst others stated that it was unclear whether this is possible. Notwithstanding this, their study provided three results that should be highlighted: first, many engineers perceive privacy demands as a burden; second, engineers are deeply divided with regard to their control over and responsibility for the implementation of privacy. Third, the engineers had to deal with lawyers because of information privacy issues.

Bu et al. (2020) performed an empirical study, based on a survey, with 253 information system engineers. These scholars wished to observe how these engineers adopted PbD practices in their work by exploring how factors associated with their individual and organizational contexts influenced their work. The results of this study demonstrated that: (i) appropriate incentives are critical to the successful implementation of PbD; (ii) the existence of a suitable organizational and technical infrastructure will benefit the successful implementation of PbD; (iii) the systems engineers' awareness of PbD had a notable impact on their performance in this area of software development.

Senarath et al. (2019) conducted a study with 149 software developers to investigate the factors that affect their intention to follow privacy engineering methodologies. Their results reveal that a developer's perception of the usefulness of privacy is the most substantial contributor to a developer's intention to follow a privacy engineering methodology. In addition, (i) the degree of compatibility of the privacy methodology with their way of working and (ii) how the method demonstrates its results when used were also found to be significant factors determining whether a developer would follow a privacy engineering methodology.

Spiekermann et al. (2018) present the results of an empirical study with 124 engineers to examine the development of ethical systems regarding privacy and security engineering. They found that engineers suffer from a lack of time and the autonomy necessary for building ethical systems. Moreover, these scholars note that many organizations' privacy and security norms are often too weak (in terms of supporting an ethical system) or even go so fast as to oppose value-based design, thus putting engineers in conflict with the companies that employ them.

Hadar et al. (2018) conducted 27 interviews to investigate privacy from the point of view of software design and software architects. Their study also used the SCT framework (Personal, Behaviour, and External environment). They concluded that developers do not have sufficient knowledge about and understanding of privacy.

Senarath and Arachchilage (2018b) conducted a study with 54 participants, based on an application scenario, to compare the developers' assumptions on user privacy expectations with the user's actual privacy expectations, which represents a new perspective of understanding how developers perceive privacy. Their findings indicate significant differences between what developers assume the user expects in relation to privacy and what the user really expects regarding privacy as privacy priority and expectations are higher from the user's point of view than from the developer's point of view when he/she is playing the user role. This reinforces the need to consider and understand the user's actual privacy expectations when developing software intensive services and products.

The studies that we presented in this section (Summarized in Table 1) demonstrate that Information Technology (IT) practitioners do not have enough knowledge about privacy and also how to deal with privacy issues during software development. Thus, it is necessary to understand more deeply the reasons that lead to this situation. Therefore, our present study should be viewed as a further development of the studies presented in Table 1 because we investigated more deeply how the entire development team considers privacy according to the personal, behavioural and environmental factors. Moreover, the fact that the Brazilian data protection law is coming into force motivated us to perform an empirical investigation with Brazilian software developers.

Even though we have mentioned the work of Hadar et al. (2018) previously, the reader should note that the present study is a replication of their original study. Thus, whilst this work is a replication study that employs in-depth interviews with developers during the vacancy period of the Brazilian data protection law, we noticed that this is a period when companies are making an effort to change their procedures to achieve legal compliance.

In this context, refer to Carver (2010); Carver et al. (2014), Cruz et al. (2020), Da Silva et al. (2014) and Santos et al. (2021) who all argue for the importance of the replication of empirical studies in the field of Software Engineering. Indeed, replication is useful for verifying previous results (Santos et al., 2021) and is essential to achieving greater validity and reliability in research results (Cruz et al., 2020).

3. Research method

The aim of the present study is to **analyse** personal, behavioural and environmental factors, **for the purpose of** identifying their influence on software development **with respect to** the developer's decision-making process regarding privacy in software development. Our analysis takes **the point of view of** software developers, **in the context of** software developers working at a Brazilian, namely, Recife.

Given the above aim, we pose the following Research Questions (RQ):

RQ1 — What personal factors influence developers' perception and interpretation of privacy in software development?

RQ2 — What influences developers in making decisions related to privacy during the software development process?

RQ3 — What organizational characteristics and procedures influence developers' decision-making processes with respect to privacy during the software development process?

The above RQs are both descriptive and exploratory in nature (Easterbrook et al., 2008). This type of question is asked when we have an exploratory objective, when we want to understand the phenomena (Easterbrook et al., 2008). Given these RQs, we adopt a constructivist philosophical stance corresponding to the belief that scientific knowledge is socially constructed and is relative to a context (Easterbrook et al., 2008).

In this context, we chose to develop a replication study to investigate the phenomenon of how privacy is taken o account by software developers in the Brazilian context when a data protection law is coming into force (vacancy period). When choosing to do such a study, it is necessary to consider the different types of replication, which guide the methodological choices. Gómez et al. (2014), for example, classify replication as literal and conceptual (the idea of repetition and reproduction of the initial study) or operational (uses the original study as a basis, which is modified to introduce appropriate changes). This choice impacts the methodological procedures. This replication study was performed in a new context and also proposed changes within the original data collection instrument (the addition of two questions in the interview script). At the same time, we used the procedures of the original study as, for example, the Grounded Theory in light of the SCT factors to analyse the data.

In addition to the fact we are conducting a replication study, we justify our choice of using SCT as it is a theory already consolidated in the IS area because it helps understanding the influence of (personal, behavioural and environmental) factors when dealing with new strategies or technologies (in our case, dealing with privacy) (Carillo, 2010).

We present more details on the differences and similarities between our study and the original study in Section 5.

Moreover, when performing empirical research, it is necessary to consider triangulation. According to Runeson and Höst (2009), triangulation means taking different angles towards the studied object and, thus, providing a broader picture. Four different types of triangulation may be applied: Data (source) triangulation; Observer triangulation; Methodological triangulation; and Theory triangulation. We used the data triangulation when we researched different types of development team roles and different domains. We used the methodological triangulation when we applied quantitative and qualitative analysis. In addition, in Section 5. we have a discussion comparing our results with the results of other studies.

3.1. Study design and procedures

Participants Selection. It is a generally accepted practice to collect data from only a fraction of a total population, namely a 'sample', instead of from every member of the population since that is often impractical (Kitchenham and Pfleeger, 2008). For the present study, the total population can be described as every Brazilian software company involved in developing software-based products that deal with personal information about the products' users. However, we have limited our sample to companies that are located in Recife. Notwithstanding this, we did not limit our sample population with regard to the participant's level of experience, their role, the software company's, or the company's domain. Nevertheless, we consider the population demographics homogeneous as the participants are from the same city and same IT ecosystem.

Once we were confident that our target population was appropriate, we decided to use a rigorous sampling method. We were faced with the choice of a probabilistic sampling (a simple random sample, stratified random, and systematic sampling) or a non-probabilistic sampling (convenience sampling or 'snowball' sampling) (Kitchenham and Pfleeger, 2008). We chose non-probabilistic convenience sampling because it would have been impractical to identify every member of the target population (i.e., all Brazilian software developers), unlike the original study (Hadar et al., 2018), which sought people through the social network LinkedIn . Our recruitment took place through contact invitation via email (or social network) of predefined practitioners. The selection of the participants was based on industrial contacts who were known to us and who were available and willing to participate in the study.

We interviewed a total of thirteen participants from six different companies. Table 2 shows an overview of the participants in terms of their professional role, education, years of experience, as well as the size and domain of the company where they work. This indicates that the interviewees constitute a sample that includes significant variation in terms of the participants' professional role and level of experience.

We observed that seven interviewees claimed to have experience involving a team or project leadership position. Eleven interviewees had direct experience with the development of systems involving the user or customer's personal information. We

Table 1
Comparison of related work.

Research	Year of study	Research type	Country	Development paradigm	Number of participants	Main results
Dias Canedo et al. (2020)	not informed	Survey	Brazil	Agile teams, Unified Process, and traditional models (Waterfall model)	68	Participants are not able to work within the laws and guidelines that govern data privacy.
Tahaei et al. (2021)	2020	Interview	North America, Asia and Europe	not informed	12	Negative culture regarding privacy, internal prioritization tensions, limited tool support, unclear evaluation metrics, and technical complexity.
Waldman (2017)	2016–2017	Ethnography	not informed	not informed	80	Privacy is narrow, limited, and little considered in design.
Sheth et al. (2014)	2012–2013	Survey	North America, Europe, Asia, South America, and Africa	not informed	267	Different privacy preoccupations among people of different places.
Ribak (2019)	2017–2018	Interview	Israel	not informed	2	Globalization favours privacy.
Senarath and Arachchilage (2018a)	not informed	Software design task with a post-task questionnaire	Australia	not informed	36	Developers experience practi cal issues when they attempt to embed privacy into software applications.
Bednar et al. (2019)	not informed	Interview	not informed	not informed	6	Developers perceive privacy as a burden, are confused about their responsibility towards privacy and faces frustration in their interactions with the legal world.
Bu et al. (2020)	2018	Survey	China	not informed	253	Appropriate incentives are critical to the implementation of privacy.
Senarath et al. (2019)	2018	Survey	not informed	not informed	149	Perception of the usefulness of privacy is the strongest motivation for developers to use it.
Spiekermann et al. (2018)	not informed	Survey	German speaking countries, United States, Italy, and 29 nationalities	not informed	124	The developers' perception of responsibility determines most of their involvement with ethics, security, and privacy.
Hadar et al. (2018)	2013–2014	Interview	not informed	not informed	27	Designers and architects do not have sufficient knowledge about privacy according to personal, behavioural and environmental factors.
Senarath and Arachchilage (2018b)	not informed	Application scenario	not informed	not informed	54	Privacy priority and expectations are higher from the user's point of view than from the developer's point of view when he/she is playing the user role.
Our study	2019	in-depth, semi-structured interview	Brazil	Development Team	13	Different roles in the development team do not have sufficient knowledge about privacy according to personal, behavioural and environmental factors, and this impacts on how they deal with privacy.

also had participants who had worked with payment systems, an investment platform or their company's internal system. The diversity of this study sample in terms of the participants' professional experience range allows us insight into how privacy is treated in different contexts of software development. Considering these different roles and work contexts, we concluded that there is no difference when it comes to privacy. This circumstance lends itself to the configuration of a good empirical research strategy, according to Gürses and del Alamo (2016).

Note that for the sake of anonymity, we do not identify differences in participant responses in terms of the participant's experience or role.

Data Collection. For data collection, we used the interview questions used in the original study by Hadar et al. (2018).

Table 2
An overview of the study's participants.

(Cpy.)/ Id[a]	Cpy. size[b]	Domain	Role/ (Years of experience)/ Academic education
(1)/ 1	Medium	Marketing	CEO/ (5)/ Computer Science Bachelor
(2)/ 2	Very small	Software factory	CEO/ (9)/ Computer Science Bachelor
(3)/ 3	Large	Several[c]	Software Engineer/ (5)/ Computer Science Bach- elor
(3)/ 5	Large	Several[c]	Software Engineer/ (5)/ Computer Science Bach- elor
(3)/ 8	Large	Several[c]	Software Engineer/ (16)/ Computer Science Bach- elor
(3)/ 9	Large	Several[c]	Software Engineer/ (10)/ Computer Engineering Bachelor
(3)/ 11	Large	Several[c]	Software Engineer/ (3)/ Computer Engineering Bachelor
(3)/ 12	Large	Several[c]	Software Engineer/ (4)/ Computer Science Bach- elor
(3)/ 13	Large	Several[c]	Software Consultant/ (20)/ Computer Science Bachelor
(4)/ 4	Medium	Security	Software Analyst/ (3)/ Computer Science Bachelor
(4)/ 7	Medium	Security	Software Engineer/ (5)/ Computer Science Bach- elor
(5)/ 6	Very Large	Several	Developer/ (10)/ Information Systems Bachelor
(6)/ 10	Very Small	Aug. Reality	Developer/ (2)/ Information Systems Bachelor

[a]Interviewee Id.
[b]Number of employees: Very small <10; Small <100; Medium <500; Large <1000; Very Large >1000.
[c]Offers services, maintenance, software creation, training courses.

The original interview questions contains a list of thirty-eight questions separated into sections corresponding to the RQs. We added two questions to the original interview questions because the original interview questions did not address RE practices as closely as we might have wished. However, we decided to use the thirty-eight questions of the original interview because we did rounds of discussion among the authors for a deep understanding of the original study's questions, and we concluded that the questions were sufficient to achieve our research objective. Only two additional questions (about RE practices) were included because we needed to collect more evidence to understand the context of RE when considering privacy (Hadar et al., 2018; Dias Canedo et al., 2020).

The interview contained two types of questions that serve our exploratory and descriptive intention:

(i) Open-ended questions: These are questions to which the respondents were asked to frame their own reply based questions (Kitchenham and Pfleeger, 2008). This is the most frequently occurring type of question in the interview questions.
(ii) Closed questions: The respondents were asked to select an answer from a list of predefined choices (Kitchenham and Pfleeger, 2008).

In some cases, we combined both types of question, for example, in cases where the answer to a closed question needed further clarification. The interview questions can be found under 'Supplementary Material'. Questions were divided in ten sections: 1 — Background information; 2 — Privacy definition; 3 — Information sources; 4 — Guidelines; 5 — Cases and examples; 6 — Familiarity and use of privacy strategies; 7 — FIPPs; 8 — Responsibility; 9 — Elicitation and Specification of Privacy Requirements (Included by the authors); and 10 — Open discussion. All ten sections provided inputs to answer the three RQs, given the depth of the answers. Mostly, questions from different sections were used to answer each RQ, but, in some cases, questions from just one section were enough to answer one RQ, as is the case of Section 2 — privacy definition, which helped to answer especially RQ1.

According to Kitchenham and Pfleeger (2002), we must have previous information about the phenomena we are studying to assure precision and reliability. We can obtain such information from: option 1 — previous studies (if they exist); or option 2 — a pilot study (Pilot study is usually conducted with a smaller number of participants) (Kitchenham and Pfleeger, 2002). Assuming that the questions had already been used in the original study (option 1), we decided to conduct the pilot study with as many participants as necessary until we had an adequate understanding of the instrument (option 2). However, after conducting the first pilot interview, the authors concluded that it was sufficient to obtain an adequate understanding of the questions. The pilot interview was conducted with a member of a software development company and allowed us to verify the respondent's comprehension of the questions (in the only pilot, the respondent did not indicate any lack of understanding) and to measure the time that was needed for each interview (forty minutes on average).

The interview type was cross-sectional since the interviewees were requested to answer the questions that were asked of them at a specific moment (Kitchenham and Pfleeger, 2008). Once these preliminary steps had been completed, two of the authors met thirteen practitioners at their respective companies, between January 2019 and May 2019, and conducted detailed, in-depth, face-to-face, semi-structured interviews with these practitioners. This means that each interview followed the format of the researcher asking the question and the interviewee answering it. After the thirteenth interview, we observed that no new information had been mentioned Therefore, after discussions between the authors about the transcripts of the interviews, we chose to indicate that a theoretical saturation occurred, although we did not follow any predefined method existing in the literature. We then determined to end the data collection phase of our study. Each interview lasted 37 min, on average, and resulted in 8 h and 11 min of audio time.

Data Analysis. Once the data had been collected, two of the authors transcribed the interviews. Transcripts can be accessed under 'Supplementary Material' and are thus available to other researchers who may wish to replicate the present study. Two of the authors coded the transcribed material. These two authors, plus a third author, then re-assessed and made a number of improvements to the set of codes. The data analysis was informed by: A descriptive analysis: i.e., a quantitative, descriptive statistical analysis of frequencies and percentages of the answers provided for the closed questions. A coding analysis: consisting of the qualitative coding principles of GT (Open coding; Axial coding; and Selective coding) (Strauss and Corbin, 1998) as applied to both types of question (i.e., open-ended questions and closed questions).

According to the procedures indicated for data analysis, provided by Strauss and Corbin (1998), we began the coding process by performing 'open coding', whereby we created codes for a number of extracts taken from the text. Once this was completed, we started 'axial coding', therefore, we took further readings in the transcripts and the created codes (from open coding). Thus, we identified other text extracts and also grouped similar codes or created new ones. Finally, during our analysis's 'selective coding' phase, we identified higher-level categories that represented

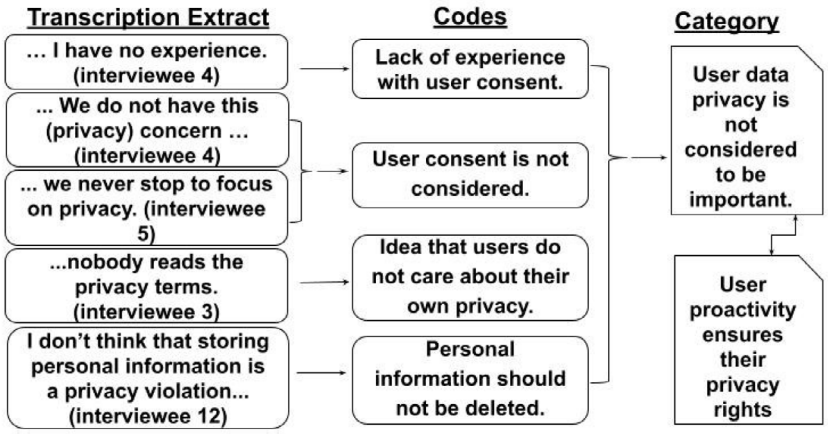

Fig. 1. Steps for the qualitative data analysis for creating the factors influencing developers about privacy.

a grouping of codes. During the 'selective coding' phases of our analysis, we note that these categories can influence and be influenced by other categories.

The categories that we created were then grouped together according to SCT (it means that we grouped the codes according to personal, behavioural and environmental factors). At this step of the analysis, we identify these categories as being the factors that affect how developers take privacy into account in development. We present an example of our coding procedure in Fig. 1 in which the 'User data privacy is not considered to be important' category was identified during selective coding. This category is based on four codes that we grouped together during the axial coding step of our analysis, once they had been identified during open coding. Moreover, the category 'User data privacy is not considered to be important' can influence and be influenced by the category 'User proactivity ensures their privacy rights'. This relationship means that developers who do not consider user's privacy important are influenced by the perception that the user needs to be proactive to have their privacy rights. The coding process was performed using atlas ti software (cloud.atlasti.com), Google Docs, and Google Sheets (docs.google.com).

3.2. Ethical considerations

When a research project involves human participants, a number of ethical considerations need to be made. For example, when the interviews were scheduled, the participants were informed of the research objective, they were asked about if they agree to participate in the research, and also they were informed that they could ask to withdraw of the research at any time. The participants were also informed that their identities and the identity of their respective companies would be kept confidential. The recruitment text can be found in the Supplementary Material. Because of this initial contact, at the beginning of each interview, we collected just the participant's verbal consent to their participation. To the best of our knowledge, consent by writing is not the only valid format. This consent was included in the audio recording before starting the interview.

4. Results and analysis

In this section, we present our answers to each of the RQs posed in this study. Regarding our analysis of the interview transcripts, we identified nine Personal Factors (PF), five Behavioural Factors (BF), and seven External Environment Factors (EF) that influence developers in their implementation of privacy safeguards in the work that they produce (See Fig. 2). We also identified a number of secondary factors that have either a positive influence or a negative influence on the three primary factors. With respect to Personal factors, we identified 22 Secondary Personal Factors (SPF). In our analysis of Behavioural Factors, we identified 9 Secondary Behavioural Factors (SBF), and with regard to the External environment, we identified 18 Secondary External Factors (SEF). The secondary factors are listed in the next Section.

The factors listed in the next subsection provide an overview of the personal, behavioural, and environmental factors that affect a developer's decision-making process with regard to privacy. The material was developed during T's coding. In the rectangles that can be seen in the figures provided in the next subsections, we show the factors hat either positively (+) or negatively (-) affect the developer's decision-making in this regard (identified in selective coding). The arrows that appear between the categories represent the fact that these categories can influence each other (identified in selective coding). The arrows thus represent the interrelationships between the factors. We also found several secondary factors (represented as a statement with an arrow to a category) which can positively (+) influence a factor (i.e., corroborate or support a factor), or negatively (-) influence a factor (i.e., oppose or undermine a factor) (identified in axial coding). We also show extracts of texts to explain factors according to respondents' answers (identified in open coding).

4.1. Sample characterization

We note that certain companies are likely to have a more significant number of protocols and rules regarding privacy. As Interviewee 6 (I6) said: *"Today, I work in a large company that has a number of protocols and many hard rules, a very different reality that I had when I was a freelancer or employee of smaller companies where they did not exist"*. This result may be linked to the larger size of the company. However, we need to do more research to confirm this result. We also observed with respect to every company that was represented by our data sample that the use of agile methodologies and practices (for example, Scrum and Kanban) are often adapted to suit the needs of each product and the service development process. This observation is supported by Klünder et al. (2019), who note that there are several reasons why a company might change its development approach, including improved product quality, shorter development pace, and improved adaptability. This suggests that companies seek to integrate agile methods and practices to improve their development processes.

The respondents reported that the customer/stakeholder could be internal to the company or external to the company. In some

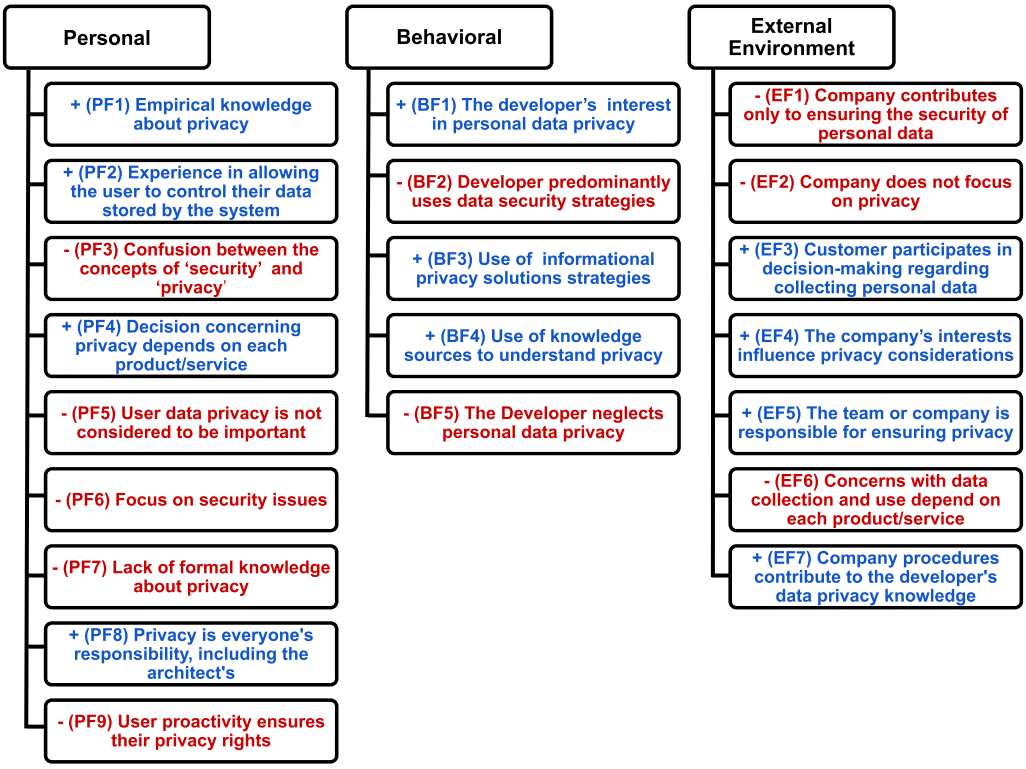

Fig. 2. Factors that influence developers with respect to the implementation of privacy safeguards in their software products.

cases, the customers were in countries outside Brazil. It was also noted that sometimes the customer was responsible for identifying system requirements, which often led to poor documentation or a lack of documentation. Potential problems regarding system requirements documentation are often increased by a lack of communication between the client and the project team. Regarding this, I6 said: *"We only get it [requirements] and do it [requirements implementation]. We have contact with the client to ask questions [about the system], but we do not see the requirements in conjunction with the client"*. We thus observed the different ways that companies in Recife organize and deal with different types of clients and contracts. The problems and challenges associated with software development in the domain of requirements integration and support remain a topic of interest and give rise to a number of questions. For example, in this context, one might ask whether there is a Product Owner or is someone else responsible for talking to the customer to find out what the customer's requirements are? Who then provides this information to the development team? Does this role actually exist in the companies that participated in this study?

4.2. A characterization of personal factors (RQ1)

In Fig. 3, we present our findings with respect to RQ1. This question addresses the personal factors that influence developer's perception and interpretation of privacy in an agile software development context. We also argue that actors influence and are influenced by other factors. For example, the fact that developers have **Empirical knowledge about privacy (PF1)** is a factor that influences and is influenced by the developers' **Experience in allowing the user to control their data stored by the system (PF2)** and **Decision concerning privacy depends on each product or service under development (PF4)**. It means that the fact that the developers' Experience in allowing the user to control their data stored by the system and Decision concerning privacy assists to increase Empirical knowledge, and vice versa.

In total, we identified nine Personal Factors that are relevant to a developer's decision-making processes regarding implementation of privacy. These factors are discussed below.

Empirical knowledge about privacy (PF1) is a positive personal factor that is corroborated by three secondary ors (namely SPF1, SPF2, and SPF4). This indicates that when we enquired about their understanding of the concept of 'privacy', the respondents reported that they possessed practical knowledge about the privacy of personal data. This is evidenced in the following excerpts:

- Knowledge of the concept of 'privacy' comes from practice. For example, I2 reported: *"I have already served as an architect [...] who has dealt with user data"*.
- Knowledge of strategies about implementing informational privacy. With respect to this secondary factor, I6 stated: *"... know what [data] you are going to use, what [data] you are going to protect, and the level of protection for that data"*.
- Familiarity with informational privacy techniques and solutions: Related to this secondary factor, we observed that respondents defined 'privacy' as a type of FIPP or as a type of privacy solution or strategy based on the following FIPPs: *anonymization* (I9), *access control* (I5 and I8), *data exposure* (I7), *data minimization* (I6), *the user's autonomy* (I2 and I1), *purpose specification* (I12), *the developer's questioning what should be protected* (I6), *confidentiality* (I4 and I6), and *use limitation* (I13 and I12). For example, with respect to *access control*, I5 said: *"When you have control over your data"*.

The above observations imply that developers do understand privacy concepts. This is related to what Bednar et al. (2019) claim, namely that more recent research has indicated that the level of concern that systems engineers have privacy protection has grown over the past few years. Moreover, this growing concern has occurred precisely a time when privacy laws have been introduced to the country and, perhaps more pertinently, at a time when users e more concerned with the privacy of

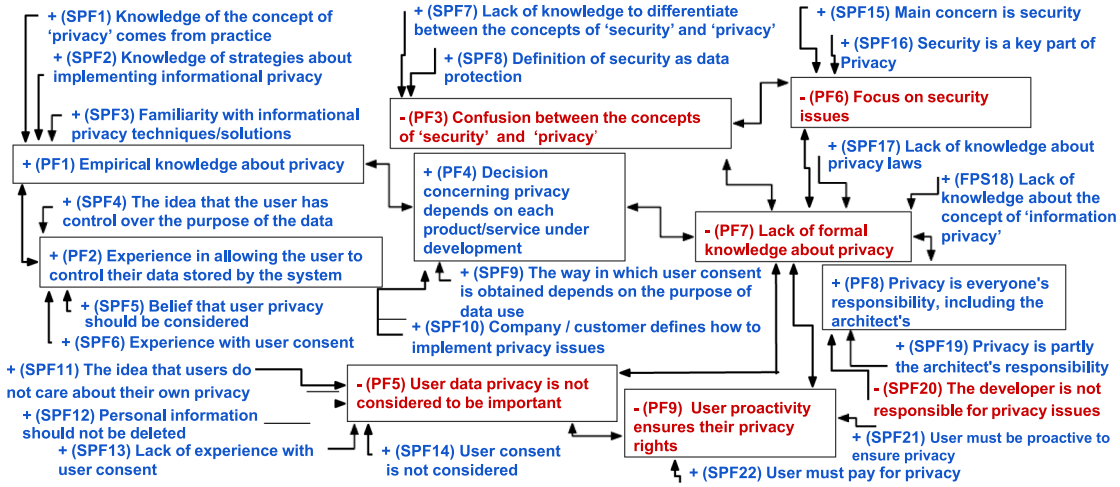

Fig. 3. Personal factors influencing the interpretation and perception of privacy.

their personal data. In addition to privacy preoccupations, ethical discussions also arise (Bednar et al., 2019). In this regard, this observation lends support to the concept of "value levers", as proposed by Shilton and Greene (2019). This concept refers to situations where particular work practices that are shared across different development teams can prompt discussion of social values (for example, privacy) that, in turn, become relevant to software design and influence ethical decisions about the values that developers support.

Empirical knowledge about privacy (PF1) influences and is influenced by other positive personal factors (PF2 and PF4). For example, **Experience in allowing the user to control their data stored by the system (PF2)**, in particular, is positively influenced by three secondary factors (SPF4, SPF5, and SPF6), indicating that the developers who participated in this study showed concern about the user having autonomy regarding control over their data. This observation suggests that there is a need for transparency in the collection and use of personal information. Transparency, in turn, is an issue relevant to the GDPR and the LGPD.

- The idea that the user has control over the purpose of the data: The respondents believed that the user must have control over their data or that this control is the user's right. For example, I8 argued: *"The user should have complete control over this [the user's data]"*. And, I13 reported: *"I think they should have the full right... I think it [control over data] is the most important [issue]"*.
- Belief that user privacy should be considered: In relation to this secondary factor, I12 stated: *"I think it is very important to tell [the user] what we will do with the information"*.
- Experience with user consent: Regarding this factor, I12 claimed: *"I think for all kinds of information I collect, the user has to give me consent"*.

This remark is in agreement the definition of 'privacy engineering' proposed by Bednar et al. (2019), about the activities undertaken by an engineer, which are namely: "(iii) to give users complete information about what happens to their personal data (i.e., transparency), and (iv) to give users real choice whether they consent to the processing of their personal data or not". Furthermore, this position is corroborated by Greene and Shilton (2018), who analysed discussions about the topic of privacy on developer forums. They found that privacy was defined as "individual control over personal data" and the most frequent topic of discussion in the context of defining privacy was establishing transparency with the users, particularly in the form of notice and consent. This suggests that developers often come across personal data and are convinced that personal data should be collected since users are informed.

Decision concerning privacy depends on each product or service under development (PF4) is a positive personal factor that influences and is influenced by two other factors (namely, PF1 and PF7). This personal factor is corroborated by two secondary factors (SPF9 and SPF10), a circumstance which allows us to observe consistency across the participants' answers related to how privacy should be dealt with.

- The way in which user consent is obtained depends on the purpose of data use: In relation to this secondary factor, I3 responded: *"How to get user consent depends on the purpose .."*.: *"I think it also changes according to the business rules"*.
- Company/customer defines how to implement privacy issues: Regarding this factor, I12 reported: *"[...] it depends on each company, the way it deals with its users"*.

This statement is in accordance with the observation we make with respect to the analysis of the characterization of the sample (Section 4.1), where companies adopt particular practices and processes to improve their software development process. On the other hand, this point is supported by the research of Szekely (2011) on what IT professionals think about surveillance. Szekely (2011) found that IT professionals will follow ethical standards if they are asked to do so by their organizations. However, this author also noted that IT professionals typically comply with decisions taken by their employers, regardless of whether these decisions are in line with what the IT professionals considered to be ethical conduct or not (Bednar et al., 2019; Szekely, 2011). This suggests that developers may not have the autonomy to make decisions.

Lack of formal knowledge about privacy (PF7) is a negative personal factor that influences and is influenced by six other factors (namely, PF3, PF4, PF5, PF6, PF8, and PF9). In addition, this factor is corroborated by two secondary factors (SPF17 and SPF18), indicating a lack of awareness regarding the relevant laws and a definition of 'privacy'.

- Lack of knowledge about privacy laws: In this context, I4 reported: *"I have not had this contact [with the law] yet"*.
- Lack of knowledge about the concept of 'information privacy': I7 claimed: *"In fact, privacy is a subset of security, these are two closely related things, but security is bigger"*.

These observations are corroborated by other studies (Hadar et al., 2018; Bednar et al., 2019; Senarath and Arachchilage, 2018a; Bu et al., 2020; Senarath et al., 2019) and thus suggest that, despite possessing some common-sense knowledge about privacy, which is primarily informed by new demands in society, the software developers who participated in this study still lack formal knowledge about privacy. This state of affairs may be due to privacy not being introduced in educational curricula for computer programming or IT courses. For example, the standard textbooks used in computer science education in Brazil do not offer engineering students knowledge about Privacy or PbD (Bednar et al., 2019). Notwithstanding this, we argue that training with respect to safeguarding privacy will ensure that development teams have the latest privacy policies in mind, understand advances in PbD, and consciously integrate PbD into their workflow (Bu et al., 2020). We thus support the position of Hadar et al. (2018) by stating that there is an urgent need to outline ways and strategies by which content about privacy can be included in computer science programs. For example, by creating a curriculum that includes training in privacy engineering.

Confusion between the concepts of security and privacy (PF3) is a negative personal factor because 'security' and 'privacy' are two distinct concepts. This personal factor (i.e., the confusion that people experience over this issue), in turn, influences and is influenced by two other factors (PF6 and PF7). This factor is corroborated by two secondary factors (namely, SPF7 and SPF8), indicating that our respondents defined 'privacy' by using terms related to the concept of 'security'.

- Lack of knowledge to differentiate security and privacy: One comment relevant to this secondary factor was provided by I13, who remarked: *"When you give permission to use your data, and that application eventually leaks the data [...], it's also a matter of privacy, but I don't know if it's a security issue".*
- Definition of security as data protection: In relation to conflating 'security' as 'data protection', I5 stated:
  "Security refers to the protection of personal data from external environments".

In this regard, Abu-Nimeh and Mead (2009) argue that, despite the overlap between engineering requirements for privacy and engineering requirements for security, each set of requirements addresses a different set of problems. Security engineering includes, for example, the implementation of authentication and authorization systems. However, privacy engineering is related to procedures that are focused on data collection and data protection. The significant difference between 'security' and 'privacy' is that threats to individual privacy may arise from authorized users of the system. In such cases, security is not breached (since the users are authorized to use the system), but privacy is breached (Bijwe and Mead, 2010).

Therefore, this observation about the confusion between the concepts of 'privacy' and 'security' is in agreement with what Hadar et al. (2018) found in their work, which was that developers use their understanding of 'security' to address issues related to privacy. Not unexpectedly, this can lead to them making incorrect decisions with regard to safeguarding privacy. For example, one respondent stated that the user should be proactive in ensuring privacy. However, according to data protection laws, the user has several rights and the premise of transparency. Nowhere is it mentioned that the user should act under the premise that the user is responsible for being proactive with regard to the user's privacy.

Focus on security issues (PF6) This factor influences and is influenced by two other factors (namely, PF3 and PF7) and is corroborated by two secondary factors (SPF15 and SPF16), thus indicating the respondent's primary concern is security, not privacy.

- Main concern is security: regarding this secondary factor, I4 stated: *"We need to make sure our software is secure [...]"*. I13 echoed this sentiment by reporting: *"So, this [security] is our main concern"*.
- Security is a key part of Privacy: This factor is supported by the following statements: *"Security would be more comprehensive"*. (I6) and *"Privacy for me is part of data security"*. (I5).

(PF6) is similar to another personal factor about **Confusion between the concepts of 'security' and 'privacy' (PF3)** as mentioned by Hadar et al. (2018). Because developers associate 'privacy' with 'security', and because they believe that they have a good understanding of the concept of 'security', they focus on making decisions based on their conceptualization of 'security'. However, the more practitioners understand the concept of "privacy', the more effective they will be in improving security. If practitioners take steps to safeguard a user's privacy, they will also improve the security of the software. For example, if personal data is not required for a service or product to function, then the service or product should not request said personal data. Less damage will then be inflicted if a security problem occurs.

The respondents reported that **Privacy is everyone's responsibility, including the architect's (PF8)**. SPF19 corroborates this personal factor and SPF20 stands in opposition to this factor. Our observations regarding this category demonstrate that our respondents think that the architect, clients, and the team should be responsible for ensuring privacy in a software application.

- Privacy is partly the architect's responsibility: for example, I12 said: *"The architect does not carry this [responsibility for privacy] alone"*.
- The developer is not responsible for privacy issues: Some respondents did not believe that the responsibility for ensuring privacy in a software product lies with the developer. For example, I12 observed: *"Privacy issues do not come [to the developer] very much. These security issues are linked to development, but privacy issues are not"*.

This research carried out 15 years ago by Lahlou, Langheinrich and Röcker (2005) found that engineers believed that privacy was not their problem but one for politicians, lawmakers, or, more vaguely, society. In addition, in 2011, Szekely (2011) found that developers think they bear no responsibility to ensure the legality of the systems they work on. In Szekely's study, it was reported that the responsibility lies with either the software company's management team or with the client. We thus note that our findings are in opposition to previous findings. In fact, they reveal a marked difference in developers' thinking about who is responsible for ensuring privacy in a software product. Again, our findings reiterate the fact that developers hold different ideas about privacy and security. For example, in PF6, we observed that developers primarily focus on security.

User proactivity ensures their privacy rights (PF9) is classed as a negative personal factor with two corroborating factors (namely, SPF21 and SPF22). In some cases, the participants argued that the right to privacy is equally proportional to how proactive the user is in ensuring their privacy or claiming their right to privacy. This type of reasoning goes against current data protection laws that state that the user does not need to be proactive. Both GDPR and LGPD represent a step forward in this regard; even when the user is not proactive, the law protects the user to the extent to which companies are obliged to be transparent. In addition, companies must also notify users if their privacy is violated.

- User must be proactive to ensure privacy: Regarding this secondary factor, I3 said: *"If I point out the company side, I could say that it is better not to be explicit [about privacy] and that the user has to look for it"*.

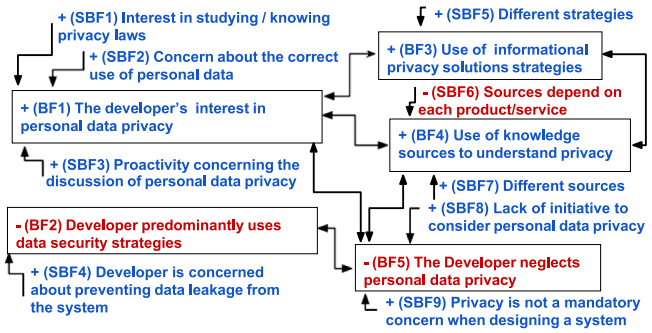

Fig. 4. Behavioural factors that influence developers' decision-making with respect to privacy.

- User must pay for privacy: For example, I2 reasoned: *"If the application is free, you have to accept that you are the product".*

In contrast to the factor that suggested that **Privacy is everyone's responsibility (PF8)**, PF9 indicates that developers believe that the right to privacy should be earned by the user or be monetized. This finding is partially similar to what Greene and Shilton (2018) observed, where mobile application developers believe that users should make use of privacy-enhancing tools to protect their data. We thus note that responsibility for the privacy of the user's personal data has been relegated to the user.

User proactivity ensures their privacy rights (PF9) is a personal factor that influences and is influenced by **User data privacy is not considered to be important (PF5)**, which is also a negative factor. PF5 has four corroborations (SPF11, SPF12, SPF13, and SPF14) that are related to the belief that data should be captured by the system, regardless of whether the user has granted consent to this and regardless of the risk that a breach of the user's privacy may entail.

- The idea that users do not care about their own privacy: This claim is supported by a remark made by I3, for example: *"Nobody reads the [privacy] terms".*
- Personal information should not be deleted: Regarding the idea that personal information should not be deleted, I12 claimed: *"I don't think that storing personal information is a privacy violation because with this [by storing the user's personal information]. I make user's life more comfortable".*
- Lack of experience with user consent: In relation to dealing with user consent, I4 said: *"I, as a developer in the case, I have no experience [with user consent]".*
- User consent is not considered: For example, I4 admitted: *"We don't have this concern [user consent]".*

Factor PF5 is corroborated by previous findings (Bednar et al., 2019; Sheth et al., 2014; Greene and Shilton, 2018). For example, Bednar et al. (2019) observed in their research that privacy was not an important concern for everyone in their sample population. The following two views were expressed: (i) "people don't care" if their privacy is breached and people think no one is interested in a "nobody" or a "general person" like them; and (ii) "for the majority of the people, privacy is not an issue".

These observations suggest that people do not care about their privacy in the context of software applications. Consequently, according to our results and the findings of previous studies, privacy is not seen as an issue of such importance that it has to be considered in software development.

4.3. Behaviour characterization (RQ2)

We show in Fig. 4, our observations in response to RQ2 about behavioural factors that influence the decision-making process of software developers with regard to privacy. We identified five behavioural factors in our data, classified as follows. We also argue that factors influence and are influenced by other factors. For example, **Developer predominantly uses data security strategies (BF2)** is a factor that influences and is influenced by the fact that **The Developer neglects personal data privacy (BF5)**. This relationship means that developers neglect privacy because they believe that using security strategies is enough to guarantee privacy, and vice versa.

The developer's interest in personal data privacy (BF1) is a positive behavioural factor which is corroborated three secondary factors (SBF1, SBF2, and SBF3), thereby indicating that there the respondents have an interest in privacy of personal data.

- Interest in studying/knowing privacy laws: For example, I4 made the following remark concerning privacy laws: *"This [law] is something that I really need to see".*
- Concern about the correct use of personal data: Regarding the correct use of personal data, I11 said: *"In the last project that involved data, the development team raised some problems".*
- Proactivity concerning the discussion of personal data privacy: The respondents corroborated this factor by answering "Yes" to a question about whether they initiate discussions about privacy (Supplementary Material. Question 5.4).

BF1 factor is also corroborated by the personal factor, Empirical knowledge about privacy (Fig. 3), since the issue of privacy is gaining attention from developers. Bu et al. (2020) state that privacy is a promising development tendency in the information industry and is attracting interest from professionals. Spiekermann et al. (2018) have found that engineers believe that privacy engineering is useful, valuable, and important. This trend may encourage other developers to pay more attention to privacy in their development work.

Use of informational privacy solutions strategies (BF3) is a positive behavioural factor, that is, in particular, corroborated by one secondary factor (SBF5) indicating that respondents use different known privacy strategies.

- Different strategies: For example, I4 said about confidentiality: *"We cannot disclose customer data (name, for example)".*

In Fig. 5, we show the number of developers using or familiar with each of the ten privacy solutions. Our findings similar to the findings provided by Hadar et al. (2018), regarding the fact that developers are familiar with more privacy solution strategies than they actually use. The study of Hadar et al. (2018) also shows that developers have some familiarity with privacy solutions as the authors found mentions of, for example, Aggregation, Separation, Anonymization, Pseudonymization, Data Expiry, and Encryption. In addition, the most familiar strategy that was used most often, both in our study and in Hadar et al. (2018), was 'cryptography/encryption'. Our study's least familiar and (perhaps understandably) least used strategy was 'automatic data expiration'. In Hadar et al. (2018), the least familiar strategy was 'temporal data' (equivalent to 'data deletion after use') and the least used was 'data automatic expiration', just like in our study.

Use of knowledge sources to understand privacy (BF4) influences and is influenced by other factors (BF1, BF3, and BF5). In addition, it is corroborated by two secondary factors (one positive (SBF7) and one negative (SBF6)), thereby indicating that the use of knowledge sources to understand privacy depends on each product/service development project. The fact that the source of

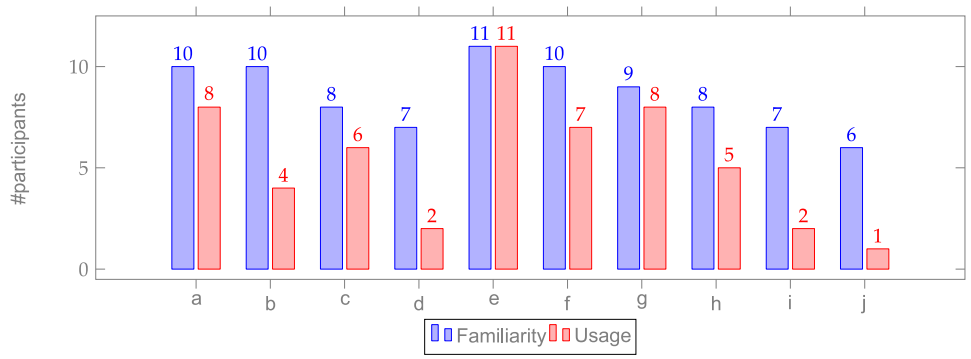

Fig. 5. Developers' familiarity and usage of privacy solutions strategies (Total number of participants, $n = 13$).
Note: a = Decentralization, b = Data deletion after use, c = User control, d = Data turn off, e = Cryptography, f = Anonymization, g = User transparency, h = User personal data access, i = User exclusion, j = Automatic data expiration.

knowledge that is selected depends on each product/service being developed is a negative secondary factor that can indicate a lack of standardization by the company.

- Sources depend on each product/service: In this context, I11 reported: *"in the context of the current project we consult the client"*.
- Different sources: we show, in Table 3, we list the different sources of knowledge that the developers use.

With regard to this factor, we note that the use of knowledge sources depends on the product/service that is being developed. This observation is in agreement with the finding of the sample characterization analysis (Section 4.1) and the personal factor about **Privacy decision depends on each product/service under development (PF4)** (Section 4.2), regarding how companies seek to adopt practices and processes to improve their development process.

A variety of knowledge sources were consulted by the developers. Whilst 'books' were mentioned by 4 respondents, other sources of knowledge included 'colleagues' (4 respondents), 'the internet' (7 respondents), 'blogs' (1 respondent), and 'web articles' (1 respondent). The fact that several sources of knowledge that the developers mentioned are online echoes the finding provided by Greene and Shilton (2018), who observe increasing discussion about privacy in mobile developer forums. However, we must state that if a data protection law is in force in a particular country, companies are obliged to be in compliance with said law. Consequently, the law should be seen as a knowledge source too.

The developer neglects personal data privacy (BF5) is a negative factor that is corroborated by two secondary factors (SBF8 and SBF9) indicating there is a lack of initiative on behalf of the respondents in relation to privacy concerns.

- Lack of initiative to consider personal data privacy: For example, I4 answered: *"I have never questioned myself: why do we need this (personal data)"*.
- Privacy is not a mandatory concern when designing a system: Regarding this secondary factor, I12 responded: *"I think this concern with privacy is always valid, but it is not a discussion that always arises"*.

Despite a growing interest in privacy issues and the fact that many developers are aware of several privacy strategies, developers still neglect privacy in their daily work. However, during our interviews with the developers, it was not clear whether their negligence is due to a lack of feeling responsible for the privacy of the user or whether cultural issues inside the company itself play a determining role with respect to the developers' negligence. This behavioural factor is related to the personal factor that indicates **User data privacy is not considered to be important (PF5)** (Section 4.2). This observation is in agreement with what Spiekermann et al. (2018) found in their study. For example, the vast majority of developers are aware that they should be pursuing privacy and security by design. However, the issue of responsibility is fundamental to understanding the developers' behaviour. The responsibility that a developer feels with regards to privacy is the most influential factor that determines the low priority that developers assign to privacy and security engineering. Despite their purported interest in the issue of privacy, sometimes developers do not put this interest into practice, or they do not feel formally responsible for safeguarding privacy in the software they develop.

Finally, the factor **The developer neglects personal data privacy (BF5)** influences and is influenced by one negative behavioural factor (BF2). In contrast, **Developer predominantly uses data security strategies (BF2)** is a factor corroborated by one secondary factor (SBF4), indicating that participants were more concerned with data security than data privacy.

- Developer is concerned about preventing data leakage from the system: With regard to data leakage, I13 reported: *"The tool I'm working on today is to prevent data leakage"*.

This observation is in agreement with our analysis of the developers' personal knowledge, as noted in the personal factors characterized by **Confusion between the concepts of security and privacy (PF3)** and **Focus on security issues (PF6)** (Section 4.2). Also, in line with the study of Hadar et al. (2018) are our observations concerning the developers' high degree of familiarity with security solutions instead of solutions related to other privacy-related concerns. This point is echoed by the research of Sheth et al. (2014), where they note that their respondents strongly related privacy issues to information security.

Table 3
Developer knowledge sources.

Interviewee (I) ID	Knowledge source
(4, 7, 11, 13)	Colleagues
(9)	Customer
(10)	Team specialist
(12)	Development community
(2, 7, 11, 12)	Books
(12)	Lectures
(2)	Documentation
(13)	Code
(13)	Web articles
(10, 11)	Papers
(1, 4, 7, 8, 9, 12, 13)	Internet
(1)	Blog
(3, 5, 6)	Does not have

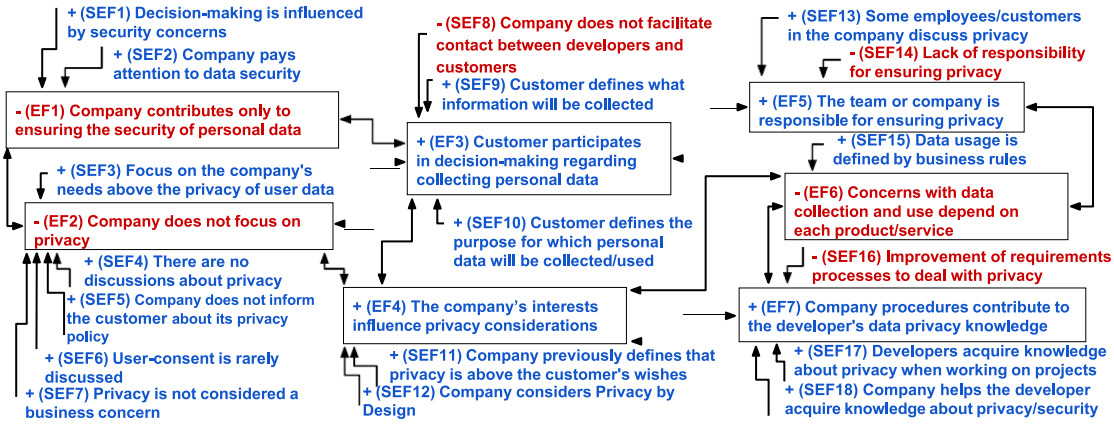

Fig. 6. External environment factors that influence developers' decision-making regarding privacy.

4.4. External environment characterization (RQ3)

In Fig. 6, we list our findings concerning RQ3, which addresses the external environment factors that influence the developers' decision-making process regarding privacy. We identified seven external factors that are relevant to this issue. We also argue that factors influence and are influenced by other factors. For example, **Company contributes only to ensuring the security of personal data (EF1)** is a factor that influences and is influenced by the fact that **Company does not focus on privacy (EF2) and Customer participates in decision-making regarding collecting personal data (EF3)**. This relationship means that there is an influence between the factors in the sense that companies do not focus on privacy, which only contributes to ensuring security. In addition, the focus on privacy occurs when the customer participates in the decision to consider collecting personal information, and vice versa.

Company contributes only to ensuring the security of personal data (EF1). This is a negative external environmental factor with two secondary corroborations (SEF1 and SEF2) indicating that companies show more attention to data security than data privacy.

- Decision-making is influenced by security concerns: In relation to this secondary factor, I12 reported: *"Security is a discussion that always arises"*.
- Company pays attention to data security: Regarding this factor, I7 said: *"Security here is a priority even beyond usability"*.

This factor (EF1) is consistent with the personal factors characterized by **Confusion between the concepts of 'security' and 'privacy' (PF3)** and **Focus on security issues (PF6)** (Section 4.2), and behavioural factor described by **Developer predominantly uses data security strategies (BF2)** (Section 4.3). In this regard, Spiekermann et al. (2018) note that professionals generally comply with organizational expectations with regard to privacy engineering or ethical system designs. Consequently, organizational factors that focus on security can influence a developer's personal and behavioural factors, causing the developer to also focus on security.

The factor **Company contributes only to ensuring the security of personal data (EF1)** influences and is influenced by the factor **Company does not focus on privacy (EF2)**, which is a negative factor. EF1 has five secondary factors (namely SEF3, SEF4, SEF5, SEF6, and SEF7) as a corroborative factor that are related to the company's lack of focus on privacy.

- Company does not inform about its privacy policy: In relation to this factor, I10 responded: *"I do not think so"*.
- User consent is rarely discussed: Regarding the question about whether there is discussion related to user consent within the company (Supplementary Material. Question 7.6), I11 answered: *"Little ... Very little"*.
- There are no discussions about privacy: In relation to this secondary factor, I4 reported: *"About privacy, we don't argue that much"*.
- Privacy is not considered a business concern: Regarding the issue about privacy not being considered a business concern, I4 said: *"I think that, for some purposes, it's good for the company, I don't know for the client"*.
- Focus on the company's needs above the privacy of user data: For example, I5 said: *"Never...in any project I participated in here (company), we focused on that (privacy)"*.

Regarding the factor **Company does not focus on privacy (EF2)**, we saw that, instead, companies are concerned h security. On the other hand, Hadar et al. (2018) and Bednar et al. (2019) found that organizations are concerned h the implementation of their own privacy policy to protect the privacy of the company. However, we did not observe the same attitude in the companies that participated in this study in our work. Regarding companies not informing about their privacy policies, it is not clear whether companies do not have a policy in place or simply do not have an information culture. This suggests that companies are not yet focused on adopting privacy policies informed by the LGPD.

Customer participates in decision-making regarding collecting personal data (EF3) is a positive external environmental factor that is corroborated by three secondary factors (SEF8, SEF9, and SEF10), indicating that there customer involvement in the decisions developers make regarding collecting personal data.

- Company does not facilitate contact between developers and customers: In some cases, the company may not facilitate contact between developers and customers. For example, I6 said: *"We contact the client to answer questions, [developers doubts] but we do not see the [privacy] requirements"*.
- Customer defines what information will be collected: For example, I11 said: *"This concern [collecting personal data] will be decided by the client"*.
- Customer defines the legitimacy for which personal data will be collected/used: In relation to the purpose for which information is collected, I8 said: *"Usually, the customer also defines the purpose"*.

In principle, this factor represents placing responsibility for what decisions are made with respect to privacy on the customer. Such an approach might be considered to be a positive approach in scenarios where customers are increasingly looking for systems that guarantee privacy, according to Bednar et al. (2019).

In this regard, Senarath and Arachchilage (2018a) found that developers believe they should give priority to the client's business requirements. However, the notion of holding the customer accountable with regard to decisions about privacy can create a situation where the developer abrogates their responsibility towards privacy.

The factor **Customer participates in decision-making regarding collecting personal data (EF3)** is related to **The company's interests influence privacy considerations (EF4)**, which is a positive factor. **(EF4)** has two secondary factors (SEF11 and SEF12) indicating that when the company considers Privacy by Design, they refer back to previously defined privacy principles.

- Company previously defines that privacy is above the customer's wishes: In cases where the company has previously defined what privacy is, over and above the customer's wishes, I13 said: *"[...] the pre-sale did not go forward. Because of these privacy issues [client did not accept the company's recommendations]".*
- Company considers Privacy by Design: In cases where the company considered using PbD, I1 reported: *"We appreciate this [privacy] as I said, there is an area just for that, and today we try to make all products with privacy by design".* The same respondent continued: *"[W]e define what we are going to do with the data [...] Data collection must also be correct".*

We observed that privacy has already become a topic of conversation in the company and has thus begun to influence the company's decision-making process regarding privacy. However, we did not observe a clearly established method or guide for addressing issues related to privacy, even though Hadar et al. (2018) found these in their work. For example, in our study, the developers claimed that their companies had very clear guidelines that they were asked to follow regarding their privacy work or held workshops that dealt with issues related to privacy and the protection of information. In this context, Sheth et al. (2014) report that establishing procedures, for example, in the form of published guidelines, can be a good start to raise interest in the concept of 'privacy'. Establishing an explicit procedure that developers can follow in safeguarding privacy can be a positive factor that will bring issues related to privacy to the fore in the context of the software development process.

The team or company is responsible for ensuring privacy (EF5) is a positive external environmental factor that is corroborated by one positive secondary factor (SEF13) and opposed by one negative secondary factor (SEF14), indicating that although there is a lack of responsibility regarding privacy on behalf of developers, there are some employees and customers who consider privacy.

- Some employees/customers in the company discuss privacy: Regarding this secondary factor, I7 stated: *"[...] privacy [is considered] especially with external customers".*
- Lack of responsibility for ensuring privacy: for example, I5 said: *"The customer has to make [privacy concerns] explicit".*

The team or company is responsible for ensuring privacy (EF5) corroborates the personal factor described by **Privacy is everyone's responsibility, including the architect's (PF8)** (Section 4.2) and the external factor characterized by **Customer participates in decision-making on collecting personal data (EF3)** EF5 is also supported by observations made by Lahlou et al. (2005) and Szekely (2011). Given the above, we observe a certain contradiction with respect to whose responsibility it is to consider privacy.

The factor **The team or company is responsible for ensuring privacy (EF5)** influences and is influenced by **Concerns with data collection and use depend on each product/service (EF6)**, which is a negative factor. **(EF6)** has one secondary factor (SEF15) indicating that, in some cases, data usage is defined by the business rules of each product or service without general rules defined by company.

- Data usage is defined by business rules: For example, I11 said: *"I think [privacy consent] depends on the scope of the system".* Similarly, I12 reported: *"In some situations, I don't see that much need [of privacy consent]".*

Concerns with data collection and use depend on each product/service (EF6) corroborates with another external factor, **The company's interests influence privacy considerations (EF4)**, reflecting the fact that the companies that participated in the study lack explicit privacy guidelines and procedures. Also, **(EF6)** corroborates with the personal factor about **Decision concerning privacy depends on each product/service under development (PF4)** (Section 4.2). This implies that although some companies may be starting to consider their decision-making processes with respect to privacy, they still do not have a general privacy procedure.

Company procedures contribute to the developer's data privacy knowledge (EF7) is a positive external environmental factor corroborated by two positive secondary factors (SEF17 and SEF18) and is opposed by one negative secondary factor, indicating that although it is necessary to improve the requirements process with respect to privacy, some companies already have clear procedures for data caring. These procedures will assist developers in making enquiries about privacy.

- Improvement of requirements processes to deal with privacy: In relation to the improvement of requirements processes to deal with privacy, I11 said: *"Definitely [we need to improve the requirements process for dealing with privacy].*"
- Developers acquire knowledge about privacy when working on projects: With regard to this secondary factor, I12 reported: *"This project I'm working on nowadays, I'm acquiring a lot of knowledge on privacy issues".*
- Company helps the developer acquire knowledge about privacy/security: With regard to the role played by the company, I6 reported: *"The company checks who is not following the company's rules".*

Previously, regarding the factor about **Concerns with data collection and use depend on each product/service (EF6)**, it has been observed that companies do not have a general procedure on how to deal with privacy, as noted. However, **(EF7)** demonstrates that companies are open to considering privacy in their organizational climate, as evidenced by how companies take privacy into account depending on the product/service. This openness is often considered a positive factor since it improves developer's behaviour and adds personal protection with respect to safeguarding the customer's privacy (Hadar et al., 2018).

5. Discussion

Software development companies, including Brazilian ones, face a scenario in which people are increasingly connected with each other via software apps as they carry out their daily activities. In this scenario, people are starting to worry about how their personal information is used by digital media, especially at this crucial moment with respect to the 'vacancy period' associated with the Brazilian LGPD privacy law. Also, studies that we reported on show that developers are not aware of the meaning of the concept of 'privacy' since they do not know much about privacy and often do not consider privacy issues when developing software (Hadar et al., 2018; Ribak, 2019; Senarath and Arachchilage, 2018a; Bednar et al., 2019). Given this scenario,

Table 4
Comparison between the original study and our replication.

Comparison	Original study	Replication study
Research question	One main question and two sub-questions about SCT factors *	Three questions about SCT factors
Participant selection	Recruitment via social network	Recruitment via industrial contacts
Audience	Architects	Developers
Data collection	Interview questions with thirty- eight questions	Interview questions with thirty-eight questions plus two questions on the elicitation and specification of privacy requirements
Data collection year	2013–2014	2019
Data analysis	Coding principles of GT (Open coding; Axial coding; and Selective coding) (Strauss and Corbin, 1998) in light of SCT	Coding principles of GT (Open coding; Ax- ial coding; and Selective coding) (Strauss and Corbin, 1998) in light of SCT
Main conclusions	(i) Software developers are actively discouraged of making informational privacy a priority;(ii) Many developers do not have sufficient knowledge about privacy and there is a lack of understanding of the concept of 'privacy', but they are highly familiar with security solutions.	(i) Although there is not an active discouragement of prioritizing privacy, companies and development teams do not have a strategy to consider privacy and lack a professional culture that promotes the implementation of a privacy;(ii) Even in this context, developers have practical knowledge about privacy, although there is a confusion between the concepts of privacy and security; (iii) Developers realize the importance of addressing privacy, but it is not made clear to them who (which role in the development team) is responsible for this.

*Note: The research questions of Hadar et al. (2018) were as follows: Main RQ — What are the perceptions of privacy among developers involved in the design of software systems? Two sub-questions — How do developers interpret the concept of privacy in their daily work and working environment, in light of the privacy concept as explained by the regulators? — Given that developers typically work within organizations and are evidently influenced by them, how are the organizational characteristics and procedures translated into the developers' privacy decisions?

the literature indicates that a good starting point with respect to privacy is to promote PbD. This entails creating a culture of thinking about privacy from the very conception of a software application. Our research seeks to take us one step forward in this direction by examining the factors that influence how developers deal with privacy in their daily work. Therefore, to achieve this objective, we carried out a replication of the study of Hadar et al. (2018). In Table 1 (Section 2), we present a summary comparison between our replication study and others (including Hadar et al., 2018). We presented, for example, that, unlike Hadar, we focus the investigation on the entire development team (not just with designers and architects). In Table 4, we provide more information highlighting some of the differences between the original study of Hadar et al. (2018) and our replication study.

In our replication study, we observed details that were not present in the original study (as well as in the other studies presented in Section 2). Also, several findings from the original study are not present in the findings of the replication study. For example, with respect to the first finding of the original study depicted in Table 4, our replication study did not find active discouragement with respect to the implementation of privacy safeguards in the software produced by the companies who participated in the study. Nonetheless, we found a lack of a privacy strategy and a lack of a privacy culture. Regarding the second finding of the original study, our replication study found that developers could make a confusion about privacy and security, although they have a working knowledge of privacy. Our replication study also found that the developers are aware of the importance of addressing privacy, although it is not clear who in the development team is in charge of this.

Moreover, we interviewed participants who hold different roles and who work for companies of different sizes and domains (from the same country). We note that certain companies have more procedures in place to deal with privacy. This result may be related to the size of the company, but we still have to gather more evidence to support it. Nevertheless, Balebako et al. (2014) found that larger mobile application companies adopt privacy and security practices to a greater degree than small companies.

Our observations regarding **Personal Factors (RQ1)** indicate that developers possess empirical knowledge about privacy, which indicates that they have some concerns about privacy. However, most of the developers whom we interviewed do not know how to interpret privacy requirements correctly. Furthermore, many of them do not possess formal knowledge about privacy issues. This finding may be related to the fact that university curricula for Computer Science degree programs lack mandatory content on privacy, as shown by Bednar et al. (2019).

Although empirical knowledge about privacy is a positive point, the fact that developers do not have formal knowledge about privacy can be seen as problematic, especially in countries where data protection laws are coming into force, such as Brazil. Even in this context, we found that the developers who participated in our study possess a certain knowledge of privacy strategies (see Fig. 5). This finding is also supported by other studies, such as the study provided by Senarath and Arachchilage (2018b), who found that developers who participated in their study also use techniques to ensure privacy. In addition, our study also shows that the developers' knowledge of privacy strategies can compromise their interpretation of what privacy is, as, for example, by viewing privacy exclusively in terms of anonymization.

The developers suggested that privacy can be implemented by using practices that are meant for the implementation of security. However, we claim that this suggestion is based on their confusion between the definitions of 'privacy' and 'security. It may be the case that this confusion between the concepts of 'privacy' and 'security' is a significant problem for software development companies. This claim is similar to what Hadar et al. (2018) argue. They noted that developers use the vocabulary of

'security' to address 'privacy' challenges. Consequently, their use of this vocabulary limits their perceptions with regard to 'privacy'. In fact, many developers described 'privacy' in terms of other definitions, including definitions that are more properly associated with ' access control'. Although the developers who participated in this study demonstrated that they possessed some knowledge of privacy-related practices and are of the opinion that users should have transparent control over data, some respondents stated that they do not intend to use privacy practices (for example, the deletion of personal data when it is no longer needed), even though they recognize how important these practices are. The developers also mentioned that their use of privacy practices depends on what product or service is being developed.

The respondents believed that the responsibility for safeguarding the software user's privacy is everyone's responsibility. This observation contrasts with previous research that had shown that developers did not believe that they were solely responsible for ensuring user-privacy (Lahlou et al., 2005; Szekely, 2011). On the other hand, research has shown that developers do not feel personally responsible for privacy, a somewhat contradictory finding. Developers believe that privacy is negotiable, because a lack of privacy is sometimes justified by the provision of a better service. We also note a lack of concern with regard to restricting the collection of personal data to a minimum for the functional operation of the software. Unfortunately, unrestricted data collection can become a serious problem if a security breach occurs. This factor may be a negative influence on the incorporation of PbD, which recommends the implementation of privacy practices at the initial software design stage. However, it is important to note that there are no concrete PbD guidelines at present that can be used to encourage the adoption of PbD.

Our findings concerning **Behavioural Factors (RQ2)** indicate that developers have an interest in the privacy of customers' personal data. This finding echoes other research studies claiming that privacy is a promising trend (Bu et al., 2020). However, we noted on occasion that the developers' interest in privacy actually began during the interviews that we conducted with them. In other words, a simple conversation was enough to stimulate interest.

Another positive trend in the developers' attitudes towards privacy is related to their increasing use of different strategies that can be deployed to safeguard privacy, although the number of developers who actually use such strategies is lower than the number of developers who are familiar with them. Developers also use different sources of knowledge regarding privacy. Although we found that they refer to several different sources of knowledge, we also observed that individual developers do not use a wide range of sources, as we can see in Table 3.

We observed that the concept of 'privacy' remains somewhat neglected because the respondents predominantly use strategies that are related to security strategies. They do this in the belief that security techniques are sufficient to the mitigation of privacy problems. In contrast, no solutions that were specific to privacy policies or data protection laws were reported to us by the developers who participated in our study. In this regard, Hadar et al. (2018) state that developers prefer to employ solutions informed by the principle of privacy-by-policy instead of solutions that implement privacy-by-architecture. The findings of Hadar et al. (2018) may indicate the presence of a problem since it suggests that developers lack the required knowledge to design applications that safeguard the user's privacy effectively. We observe that, in addition to their misguided use of security strategies for issues related to privacy, developers are not yet suitably aware of the privacy policies that the LGPD will establish.

Our findings regarding **External Environment (RQ3)** Factors indicate that companies are concerned with the user's personal data security, but they do not demonstrate the same concern for the user's privacy. Unfortunately, since the companies are concerned with security, they erroneously believe that they are also concerned with privacy. Because of the confusion between the two issues there is little very discussion within the companies about privacy and privacy practices; for example, there is no talk about informing users about privacy policies, what strategies they have to safeguard the privacy of the user, or any discussion of obtaining the user's consent. According to Sheth et al. (2014), the reason why not a great deal of attention is paid to issues related to privacy is because concern with respect to online privacy are a relatively recent phenomenon. Given its newness, developers are not sure which approach to dealing with privacy will be the best approach and provide the largest number of benefits in the long run.

In some cases, we observed that the developer's customers of the participate in deciding on which data will be to be collected to ensure the functionality of the product or service provided. However, in many other cases, this approach to privacy was not taken by the companies included in this study. Allowing the customers to provide input regarding what data will be collected was considered to be a positive factor, but it is worth reflecting on the question of whether customers genuinely care about what data is collected or whether they understand the all the issues that are pertinent to the privacy of user data in the products and services that they use.

In general, we observed that the development team is responsible for safeguarding the privacy of the users' data and that the data that is collected depends on each product or service that is developed. Companies contribute positively to this situation with knowledge about privacy because they have concerns regarding the care with personal data. However, this contribution is still very much related to security procedures when compared to privacy procedures.

6. Threats to validity

With respect to the threats to the validity of this study, we refer to the guidelines provided by Runeson and Höst (2009) to address four different areas related to the validity of this study, namely, construct validity, internal validity, external validity, and the reliability of the study.

Construct validity threat reflects the extent to which the operational measures that are implemented in the study actually represent what the researcher has in mind. This is reflected by what we investigated in response to the three RQs that the research poses. In the present study, the participants may have felt inclined to speak well of the topic of 'privacy' because of the influence of participatory bias. We mitigated this threat by ensuring that the identities of the participants and companies would not be disclosed in this paper. In addition, prior to the interviews, we informed the interviewees of the purpose of our study. Consequently, the participants would feel free to talk about the issue of privacy without fear of any future embarrassment. We also addressed the issue of construct validity when we constructed and tested the interview guide considering: methodological triangulation (quantitative and qualitative analysis);and data (source) triangulation (different types of development team roles and different domains).

The threat of **internal validity** demands that we consider whether there are factors in addition to the factors that we discuss in our study that might influence the results of our study. To mitigate this type of threat, we selected a sample of individuals who have different professional roles and have different levels of experience. The sample was also drawn from companies of different sizes and domains (Our research project included six

different companies). The fact that seven of our participants ($n = 13$) worked at the same company can be seen as a threat to the internal validity of the study. In some cases, the participants stated that they were interested in the concept of 'privacy', but this merely appeared to have been prompted by the interview process. This fact could indicate a limitation to our study. However, we mitigated against this problem when we conducted an in-depth interview into each of the participants' prior knowledge regarding (i) their concept of 'privacy', (ii) methods that can be used to mitigate privacy issues, and (iii) sources of knowledge that they to address privacy issues. On the other hand, although we have reached saturation in a joint decision between the researchers, we can indicate as a threat that we have not followed any predefined method to indicate such saturation.

External validity threat is concerned with the extent to which the results of this study can be generalized. We cannot assure that the results of this study can be generalized because it is a qualitative study that was carried out with only a limited number of participants and companies in a single city. Nevertheless, results presented here are similar to findings provided by other studies (Hadar et al., 2018; Sheth et al., 2014; Bu et al., 2020; Ribak, 2019; Bednar et al., 2019; Spiekermann et al., 2018; Senarath and Arachchilage, 2018a; Senarath et al., 2019).

Reliability threat is concerned with the extent to which the data and the analysis are dependent on a specific researcher. To mitigate this threat, we followed a clearly articulated method and we conducted several rounds of discussion before and after the interviews. In addition, the interviews and data analysis were carried out by more than one author.

7. Conclusions and future work

In this paper, we have presented the results of a qualitative study on how developers make decisions regarding privacy in the development of software products and services.

We conducted our exploratory study at six companies in Recife, Brazil. The number of employees at each of these companies varied from less than 10 to more than 1000. The application domain includes Marketing, Software factory, Augmented reality, security, and companies operating in several domains. We interviewed thirteen employees who had experience in the industry ranging from 2 years of experience to 20 years of experience. These participants were employed in different professional roles at the companies.

We identified nine Personal factors, five Behavioural factors, and seven External environment factors that positively or negatively affect developers' decision-making with respect to privacy. The interviews were conducted with the three research questions in mind that allowed us to make some indications, as follow:

RQ1 related to the *personal factors that influence developers' perception and interpretation of privacy in agile software development*. The results of our analysis of the interviews indicate that the employees who participated in the study have practical knowledge of privacy instead of theoretical knowledge of privacy. These developers were more concerned with issues related to security in the software that they developed. Furthermore, whilst many developers recognized the importance of using privacy practices in their work, some of them indicated that they had no intention of using these practices. **First Indication -** Companies should encourage their employees to achieve knowledge about the importance/concepts of privacy.

RQ2 related to the *behaviours that influence the developers' decision-making process regarding privacy during software development*. Our responses to this RQ indicate that the developers' concern for security overrides their limited interest in privacy. For example, the developers primarily use data security strategies over privacy strategies. It was also noted that developers neglect the concept of 'privacy' in their development work since privacy is not viewed as a mandatory concern during the development of a product or service. However, we did note that whilst they are somewhat familiar with specific strategies that can be used to safeguard privacy, they do not use these strategies in practice. **Second Indication -** Companies should encourage their employees to consider privacy a responsibility of the entire team during the development of their products and services.

RQ3 related to the *the organizational characteristics and procedures that influence the developers regarding their decision-making related to privacy during their software development.* Similar to the previous two research questions, we observe that companies are more concerned with security than privacy. However, we note that companies do consider the privacy of personal data in some instances, depending on the products and services that they offer. **Third Indication -** Companies must include a culture of privacy through general guidelines that can be adapted to the particularities of each team.

The findings of our research are relevant to understanding how privacy is taken into account in the agile development of products and services. In this context, we argue that companies are able to encourage positive factors and mitigate negative ones by proposing new plans or strategies.

The authors used these results to develop and evaluate a requirements specification method that is designed to guide developers to consider privacy from the beginning of the agile software development process (Peixoto, Silva, Lima, Araújo, Gorschek and Silva, 2019). The method includes a process that can be inserted into the development process while the development team performs the system requirements specification activity, which can occur in each new iteration throughout the software development lifecycle. This method promotes the three factors examined in this paper, namely: Personal factors, Behavioural factors, and the External environment (as per SCT). For example, with regard to Personal factors, our requirements specification method includes extensive materials that provide developers with formal knowledge about privacy. Also, our method is intended to addressing difficulties in understanding the difference between 'security' and 'privacy', since our method presents many other concepts that are related to privacy. With respect to Behavioural factors, we provide a guide for developers so that they might not neglect privacy requirements whilst encouraging them to use several 'privacy strategies'. Finally, regarding the External environment, companies are provided with a specific strategy focused on privacy to be used during the development of a software intensive product or service.

Several approaches have been proposed to deal with privacy in the earlier phases of the software development process, such as RE and design. For example, an ontology is provided by Gharib et al. (2017), whereas methods to include privacy in the RE process were proposed (Bijwe and Mead, 2010; Deng et al., 2011; Ayala-Rivera and Pasquale, 2018; Kalloniatis et al., 2008), several modelling languages were used to capture privacy requirements, such as Business Process Model and Notation (BPMN), Non-Functional Requirement Framework (NFR), Tropos, and iStar (Labda et al., 2014; Kalloniatis et al., 2009; Mouratidis et al., 2005, 2013), as well as privacy specification methods were defined to be used in conjunction with specification techniques already broadly used by the software industry, namely User Stories (Bartolini et al., 2019; Peixoto et al., 2019), to cite some works. Regarding design, we can cite approaches to develop privacy policies (Lobato et al., 2009; Caramujo et al., 2019), design strategies to implement privacy (Kalloniatis et al., 2008; Hoepman, 2014; Baldassarre et al., 2020), among other works. Therefore, we consider it is relevant to conduct an exploratory

study focused on how the software development industry adopts these and other strategies to develop privacy-preserving software systems. Another study that we consider relevant to conduct is a replication of the study of Senarath and Arachchilage (2018b) regarding the comparison among developers' privacy expectations when playing the user role, the developers' assumptions on users' privacy expectations and the actual users' privacy expectations.

As ongoing work, we designed and applied an in-depth survey to practitioners working in IT companies located in many countries to investigate their perception and understanding on privacy and how they deal with privacy during software development activities. In this case, we will have a bigger and more diverse sample and we will be able to compare this replication study's results with the results that will emerge from the ongoing in-depth survey study.

The authors hereby declare that they have no known competing financial interests or personal relationships that may appear to influence the study reported on in this paper.

CRediT authorship contribution statement

Mariana Peixoto: Conceptualization, Methodology, Validation, Formal analysis, Investigation, Supervision, Writing – original draft, Writing – review & editing. **Dayse Ferreira:** Conceptualization, Methodology, Validation, Formal analysis, Investigation. **Mateus Cavalcanti:** Conceptualization, Methodology, Validation, Formal analysis, Investigation. **Carla Silva:** Conceptualization, Methodology, Validation, Formal analysis, Investigation, Supervision, Funding acquisition, Writing – original draft, Writing – review & editing. **Jéssyka Vilela:** Conceptualization, Methodology, Validation, Investigation, Writing – original draft, Writing – review & editing. **João Araújo:** Conceptualization, Methodology, Validation, Supervision, Writing – original draft, Writing – review & editing. **Tony Gorschek:** Conceptualization, Methodology, Validation, Supervision, Funding acquisition, Writing – original draft, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

We have shared the link to our data in the supplementary material.

Acknowledgements

Part of this study was funded by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior — Brasil (CAPES) (Finance Code 001), and the KKS foundation Profile Project ReThought.se. It was also supported by NOVA LINCS Research Laboratory (Ref. UID/CEC/04516/2019).

Supplementary materials

The supplementary materials associated with this article can be found at: https://docs.google.com/document/d/1Ety1YLNJeZDXSP5z--i3GRSjimWw-cAjrMGIgGaJX24/edit

References

ABES, 2020. Mercado brasileiro de software: Panorama e tendências. URL: https://abessoftware.com.br/wp-content/uploads/2021/08/ABES-EstudoMercadoBrasileirodeSoftware2021v02.pdf.

Abu-Nimeh, S., Mead, N.R., 2009. Privacy risk assessment in privacy requirements engineering. In: 2009 Second International Workshop on Requirements Engineering and Law. IEEE, pp. 17–18. http://dx.doi.org/10.1109/RELAW.2009.10.

Altman, I., 1975. The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding. ERIC, United States.

Assembly, U.G., 1948. Universal declaration of human rights. UN General Assembly 302.

Ayala-Rivera, V., Pasquale, L., 2018. The grace period has ended: An approach to operationalize GDPR requirements. In: 2018 IEEE 26th International Requirements Engineering Conference. RE, IEEE, pp. 136–146. http://dx.doi.org/10.1109/RE.2018.00023.

Baldassarre, M.T., Barletta, V.Santa., Caivano, D., Scalera, M., 2020. Integrating security and privacy in software development. Softw. Qual. J. 28, 987–1018. http://dx.doi.org/10.1007/s11219-020-09501-6.

Balebako, R., Marsh, A., Lin, J., Hong, J.I., Cranor, L.F., 2014. The privacy and security behaviors of smartphone app developers. In: Workshop on Usable Security. USEC'14, The Internet Society, http://dx.doi.org/10.14722/usec.2014.23006.

Bandura, A., 1986. Social Foundations of Thought and Action. Englewood Cliffs, NJ.

Bandura, A., 2005. The evolution of social cognitive theory. In: Smith, K.G., Hitt, M.A. (Eds.), Great Minds in Management. Oxford University Press, pp. 9–35.

Bartolini, C., Daoudagh, S., Lenzini, G., Marchetti, E., 2019. GDPR-based user stories in the access control perspective. In: Piattini, M., Rupino da Cunha, P., García Rodríguez de Guzmán, I., Pérez-Castillo, R. (Eds.), Quality of Information and Communications Technology. Springer International Publishing, Cham, pp. 3–17. http://dx.doi.org/10.1007/978-3-030-29238-6_1.

Bednar, K., Spiekermann, S., Langheinrich, M., 2019. Engineering privacy by design: Are engineers ready to live up to the challenge? Inf. Soc. 35, 122–142. http://dx.doi.org/10.1080/01972243.2019.1583296.

Behutiye, W., Karhapää, P., Costal, D., Oivo, M., Franch, X., 2017. Non-functional requirements documentation in agile software development: Challenges and solution proposal. In: Product-Focused Software Process Improvement. Springer International Publishing, Cham, pp. 515–522. http://dx.doi.org/10.1007/978-3-319-69926-4_41.

Bijwe, A., Mead, N., 2010. Adapting the Square Process for Privacy Requirements Engineering. Tech. Rep. CMU/SEI-2010-TN-022, Software Engineering Institute. Carnegie Mellon University, URL: https://resources.sei.cmu.edu/asset_files/technicalnote/2010_004_001_15185.pdf.

Brandeis, L., Warren, S., 1890. The right to privacy. Harvard Law Rev. 4, 193–220.

Bu, F., Wang, N., Jiang, B., Liang, H., 2020. "Privacy by Design" implementation: Information system engineers' perspective. Int. J. Inf. Manage. 53, 102124. http://dx.doi.org/10.1016/j.ijinfomgt.2020.102124.

Canedo, E.D., Toffano Seidel Calazans, A., Cerqueira, A.J., Teixeira Costa, P.H., Seidel Masson, E.T., 2021. Agile teams' perception in privacy requirements elicitation: LGPD's compliance in Brazil. In: 2021 IEEE 29th International Requirements Engineering Conference. RE, pp. 58–69. http://dx.doi.org/10.1109/RE51729.2021.00013.

Caramujo, J.a., Rodrigues Da Silva, A., Monfared, S., Ribeiro, A., Calado, P., Breaux, T., 2019. RSL-IL4Privacy: A domain-specific language for the rigorous specification of privacy policies. Requir. Eng. 24, 1–26. http://dx.doi.org/10.1007/s00766-018-0305-2.

Carillo, K.D., 2010. Social cognitive theory in IS research – literature review, criticism, and research agenda. In: Prasad, S.K., Vin, H.M., Sahni, S., Jaiswal, M.P., Thipakorn, B. (Eds.), Information Systems, Technology and Management. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 20–31. http://dx.doi.org/10.1007/978-3-642-12035-0_4.

Carver, J.C., 2010. Towards reporting guidelines for experimental replications: A proposal. In: Proceedings of the 1st International Workshop on Replication in Empirical Software Engineering Research. RESER, pp. 1–4, [Held during ICSE 2010].

Carver, J.C., Juristo, N., Baldassarre, M.T., Vegas, S., 2014. Replications of software engineering experiments. Empir. Softw. Eng. 19, 267–276. http://dx.doi.org/10.1007/s10664-013-9290-8.

Cavoukian, A., 2009. Privacy by design: The 7 foundational principles. Information and privacy commissioner of ontario. Canada 5. URL: https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf.

Cruz, M., Bernárdez, B., Durán, A., Galindo, J.A., Ruiz-Cortés, A., 2020. Replication of studies in empirical software engineering: A systematic mapping study, from 2013 to 2018. IEEE Access 8, 26773–26791. http://dx.doi.org/10.1109/ACCESS.2019.2952191.

Curcio, K., Navarro, T., Malucelli, A., Reinehr, S., 2018. Requirements engineering: A systematic mapping study in agile software development. J. Syst. Softw. 139, 32–50. http://dx.doi.org/10.1016/j.jss.2018.01.036.

Da Silva, F.Q., Suassuna, M., França, A.C.C., Grubb, A.M., Gouveia, T.B., Monteiro, C.V., dos Santos, I.E., 2014. Replication of empirical studies in software engineering research: a systematic mapping study. Empir. Softw. Eng. 19, 501–557. http://dx.doi.org/10.1007/s10664-012-9227-7.

Dabbagh, M., Lee, S.P., 2015. An approach for prioritizing NFRs according to their relationship with FRs. In: Lecture Notes on Software Engineering, vol. 3, pp. 1–5. http://dx.doi.org/10.7763/LNSE.2015.V3.154.

Del Alamo, J.M., Martín, Y.S., Caiza, J.C., 2018. Towards organizing the growing knowledge on privacy engineering. In: Privacy and Identity Management. the Smart Revolution: 12th IFIP WG 9.2, 9.5, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Ispra, Italy, September (2017) 4-8, Revised Selected Papers. Springer International Publishing, Cham, pp. 15–24. http://dx.doi.org/10.1007/978-3-319-92925-5_2.

Deng, M., Wuyts, K., Scandariato, R., Preneel, B., Joosen, W., 2011. A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requir. Eng. 16, 3–32. http://dx.doi.org/10.1007/s00766-010-0115-7.

Dias Canedo, E., Toffano Seidel Calazans, A., Toffano Seidel Masson, E., Teixeira Costa, P.H., Lima, F., 2020. Perceptions of ICT practitioners regarding software privacy. Entropy 22, http://dx.doi.org/10.3390/e22040429.

Easterbrook, S., Singer, J., Storey, M.A., Damian, D., 2008. Selecting empirical methods for software engineering research. In: Guide to Advanced Empirical SE. Springer, London, pp. 285–311. http://dx.doi.org/10.1007/978-1-84800-044-5_11.

GDPR, 2018. General data protection regulation. https://eugdpr.org/. (Accessed 24 March 2022).

Gellman, R., 2017. Fair information practices: A basic history. Available at SSRN 2415020.

Gharib, M., Giorgini, P., Mylopoulos, J., 2017. Towards an ontology for privacy requirements via a systematic literature review. In: Conceptual Modeling. Springer International Publishing, Cham, pp. 193–208. http://dx.doi.org/10.1007/978-3-319-69904-2_16.

Gharib, M., Mylopoulos, J., Giorgini, P., 2020. COPri - A core ontology for privacy requirements engineering. In: International Conference on Research Challenges in Information Science. Springer International Publishing, Cham, pp. 472–489. http://dx.doi.org/10.1007/978-3-030-50316-1_28.

Gómez, O.S., Juristo, N., Vegas, S., 2014. Understanding replication of experiments in software engineering: A classification. Inf. Softw. Technol. 56, 1033–1048. http://dx.doi.org/10.1016/j.infsof.2014.04.004.

Greene, D., Shilton, K., 2018. Platform privacies: Governance, collaboration, and the different meanings of privacy in iOS and android development. New Media Soc. 20, 1640–1657. http://dx.doi.org/10.1177/1461444817702397.

Gürses, S., del Alamo, J.M., 2016. Privacy engineering: Shaping an emerging field of research and practice. IEEE Secur. Priv. 14, 40–46. http://dx.doi.org/10.1109/MSP.2016.37.

Hadar, I., Hasson, T., Ayalon, O., Toch, E., Birnhack, M., Sherman, S., Balissa, A., 2018. Privacy by designers: Software developers' privacy mindset. Empir. Softw. Engg. 23, 259–289. http://dx.doi.org/10.1007/s10664-017-9517-1.

Hoepman, J.H., 2014. Privacy design strategie. In: ICT Systems Security and Privacy Protection. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 446–459. http://dx.doi.org/10.1007/978-3-642-55415-5_38.

Ijaz, K.B., Inayat, I., Bukhsh, F.A., 2019. Non-functional requirements prioritization: A systematic literature review. In: 2019 45th Euromicro Conference on Software Engineering and Advanced Applications. SEAA, IEEE, pp. 379–386. http://dx.doi.org/10.1109/SEAA.2019.00064.

Kalloniatis, C., Kavakli, E., Gritzalis, S., 2008. Addressing privacy requirements in system design: the PriS method. Requir. Eng. 13, 241–255. http://dx.doi.org/10.1007/s00766-008-0067-3.

Kalloniatis, C., Kavakli, E., Gritzalis, S., 2009. Methods for designing privacy aware information systems: A review. In: 2009 13th Panhellenic Conference on Informatics. IEEE, pp. 185–194. http://dx.doi.org/10.1109/PCI.2009.45.

Kasauli, R., Liebel, G., Knauss, E., Gopakumar, S., Kanagwa, B., 2017. Requirements engineering challenges in large-scale agile system development. In: 2017 IEEE 25th International Requirements Engineering Conference. RE, IEEE, pp. 352–361. http://dx.doi.org/10.1109/RE.2017.60.

Kitchenham, B.A., Pfleeger, S.L., 2002. Principles of survey research part 2: Designing a survey. SIGSOFT Softw. Eng. Notes 27, 18–20. http://dx.doi.org/10.1145/566493.566495.

Kitchenham, B.A., Pfleeger, S.L., 2008. Personal opinion surveys. In: Guide to Advanced Empirical Software Engineering. Springer London, London, pp. 63–92. http://dx.doi.org/10.1007/978-1-84800-044-5_3.

Klünder, J.A., Hohl, P., Prenner, N., Schneider, K., 2019. Transformation towards agile software product line engineering in large companies: A literature review. J. Softw. Evol. Process 31, http://dx.doi.org/10.1002/smr.2168.

Labda, W., Mehandjiev, N., Sampaio, P., 2014. Modeling of privacy-aware business processes in BPMN to protect personal data. In: Proceedings of the 29th Annual ACM Symposium on Applied Computing. Association for Computing Machinery, New York, NY, USA, pp. 1399–1405. http://dx.doi.org/10.1145/2554850.2555014.

Lahlou, S., Langheinrich, M., Röcker, C., 2005. Privacy and trust issues with invisible computers. Commun. ACM 48, 59–60. http://dx.doi.org/10.1145/1047671.1047705.

LGPD, 2018. Lei Geral de Proteção de Dados Pessoais. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. (Accessed 24 March 2022).

Lobato, L.L., Fernandez, E.B., Zorzo, S.D., 2009. Patterns to support the development of privacy policies. In: 2009 International Conference on Availability, Reliability and Security. Vol. 74, IEEE, pp. 4–749. http://dx.doi.org/10.1109/ARES.2009.114.

Menolli, A., Cunha, M.A., Reinehr, S., Malucelli, A., 2015. Old theories, new technologies: Understanding knowledge sharing and learning in Brazilian software development companies. Inf. Softw. Technol. 58, 289–303. http://dx.doi.org/10.1016/j.infsof.2014.07.008.

Mouratidis, H., Giorgini, P., Manson, G., 2005. When security meets software engineering: a case of modelling secure information systems. Inf. Syst. 30, 609–629. http://dx.doi.org/10.1016/j.is.2004.06.002.

Mouratidis, H., Islam, S., Kalloniatis, C., Gritzalis, S., 2013. A framework to support selection of cloud providers based on security and privacy requirements. J. Syst. Softw. 86, 2276–2293. http://dx.doi.org/10.1016/j.jss.2013.03.011.

Nissenbaum, H., 2009. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press, USA, URL: https://dl.acm.org/doi/abs/10.5555/1822585.

OECD, 2002. Organisation for Economic Co-Operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. OECD Publishing, France.

Peixoto, M., Ferreira, D., Cavalcanti, M., Silva, C., Vilela, J., Araújo, J., Gorschek, T., 2020. On understanding how developers perceive and interpret privacy requirements research preview. In: International Working Conference on Requirements Engineering: Foundation for Software Quality. Springer, pp. 116–123. http://dx.doi.org/10.1007/978-3-030-44429-7_8.

Peixoto, M., Silva, C., Lima, R., Araújo, J., Gorschek, T., Silva, J., 2019. PCM tool: Privacy requirements specification in agile software development. In: 10th Brazilian Software Conference: Theory and Practice. CBSoft'19, SBC, Salvador, BA, pp. 108–113. http://dx.doi.org/10.5753/cbsoft_estendido.2019.7666.

Ribak, R., 2019. Translating privacy: developer cultures in the global world of practice. Inf. Commun. Soc. 22, 838–853. http://dx.doi.org/10.1080/1369118X.2019.1577475.

Runeson, P., Höst, M., 2009. Guidelines for conducting and reporting case study research in software engineering. Empir. Softw. Eng. 14, 131. http://dx.doi.org/10.1007/s10664-008-9102-8.

Santos, A., Vegas, S., Oivo, M., Juristo, N., 2021. Comparing the results of replications in software engineering. Empir. Softw. Eng. 26, 1–41. http://dx.doi.org/10.1007/s10664-020-09907-7.

Senarath, A., Arachchilage, N.A., 2018a. Why developers cannot embed privacy into software systems?: An empirical investigation. In: Proceedings of the 22nd International Conference on Evaluation and Assessment in Software Engineering 2018. ACM, pp. 211–216. http://dx.doi.org/10.1145/3210459.3210484.

Senarath, A.R., Arachchilage, N.A.G., 2018b. Understanding user privacy expectations: A software developer's perspective. Telemat. Inform. 35, 1845–1862. http://dx.doi.org/10.1016/j.tele.2018.05.012.

Senarath, A., Grobler, M., Arachchilage, N.A.G., 2019. Will they use it or not? Investigating software developers' intention to follow privacy engineering methodologies. ACM Trans. Priv. Secur. 22, 1–30. http://dx.doi.org/10.1145/3364224.

Sheth, S., Kaiser, G., Maalej, W., 2014. Us and them: a study of privacy requirements across north america, asia, and europe. In: Proceedings of the 36th International Conference on Software Engineering. pp. 859–870.

Shilton, K., Greene, D., 2019. Linking platforms, practices, and developer ethics: Levers for privacy discourse in mobile application development. J. Bus. Ethics 155, 131–146.

Sommerville, I., 2011. Software Engineering, ninth ed. ISBN-10 137035152.

Spafford, E.H., Antón, A.I., 2007. The balance of privacy and security. In: Science and Technology in Society: From Biotechnology to the Internet.

Spiekermann, S., Cranor, L.F., 2009. Engineering privacy. IEEE Trans. Softw. Eng. 35, 67–82. http://dx.doi.org/10.1109/TSE.2008.88.

Spiekermann, S., Korunovska, J., Langheinrich, M., 2018. Inside the organization: Why privacy and security engineering is a challenge for engineers. Proc. IEEE 107, 600–615.

Strauss, A., Corbin, J., 1998. Basics of Qualitative Research Techniques. Sage publications, Thousand Oaks, CA.

Szekely, I., 2011. What do IT professionals think about surveillance? In: Internet and Surveillance: The Challenges of Web 2.0 and Social Media. Vol. 16, Routledge, UK.

Tahaei, M., Frik, A., Vaniea, K., 2021. Privacy champions in software teams: Understanding their motivations, strategies, and challenges. In: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. pp. 1–15.

Wagner, S., Fernández, D.M., Felderer, M., Vetrò, A., Kalinowski, M., Wieringa, R., Pfahl, D., Conte, T., Christiansson, M.T., Greer, D., Lassenius, C., Männistö, T., Nayebi, M., Oivo, M., Penzenstadler, B., Prikladnicki, R., Ruhe, G., Schekelmann, A., Sen, S., Spínola, R., Tuzcu, A., De La Vara, J.L., Winkler, D., 2019. Status quo in requirements engineering: A theory and a global family of surveys. ACM Trans. Softw. Eng. Methodol. 28 (9), http://dx.doi.org/10.1145/3306607.

Wagner, S., Méndez-Fernández, D., Kalinowski, M., Felderer, M., 2018. Agile requirements engineering in practice: Status quo and critical problems. CLEI Electron. J. 21 (15), http://dx.doi.org/10.19153/cleiej.21.1.6.

Waldman, A.E., 2017. Designing without privacy. Hous. L. Rev. 55, 659.

Westin, A.F., Ruebhausen, O.M., 1967. Privacy and Freedom, Vol. 1. Atheneum New York, New York.

Yu, L., Alégroth, E., Chatzipetrou, P., Gorschek, T., 2020. Utilising CI environment for efficient and effective testing of NFRs. Inf. Softw. Technol. 117, 106199. http://dx.doi.org/10.1016/j.infsof.2019.106199.

Mariana Peixoto is a Postdoctoral Researcher and Temporary Professor at the Center of Informatics of the Universidade Federal de Pernambuco (CIn-UFPE), Brazil, since 2021. She received her Ph.D degree in 2021 in Computer Science from UFPE. She has been involved with extension projects and research and development projects. Her research interests are Software Engineering, Requirements Engineering, Legal Compliance and Agile Software Development. Occasionally, she serves as a reviewer for scientific journals and conferences, such as IET; JCL; SBTI; MoDRE; ISD.

Dayse Ferreira is a software developer graduated from Center of Informatics of the Universidade Federal de Pernambuco (CIn-UFPE).

Mateus Cavalcanti is a software developer graduated from Center of Informatics of the Universidade Federal de Pernambuco (CIn-UFPE).

Carla Silva is an Associate Professor at CIn-UFPE. She earned a Ph.D. in Computer Science from UFPE in 2007. For the past five years, she has been researching topics on privacy requirements specification, legal compliance and agile practices in safety-critical systems. She has been serving as a Program Committee member of conferences, such as RE, ICSE, EASE, ACM SAC RE Track, CibSE, CBSoft and WER. Occasionally, she serves as a reviewer for scientific journals and has reviewed papers for the EMSE, JSS, JSERD, CLEIej and IST.

Jéssyka Vilela is Adjunct Professor at Universidade Federal de Pernambuco (UFPE). Previously, she held an Associate Professor position at Universidade Federal do Ceará (UFC) from 2017–2019. She received her Ph.D. degree in 2018 and M.Sc. degree in 2015 both in Computer Science from UFPE. Graduation in Computer Engineering from Universidade Federal do Vale do São Francisco — UNIVASF (2012). She has been involved with extension projects as well as research and development projects with public organizations. Her main research lines include Software Engineering, Requirements Engineering, Safety-Critical Systems, and Information Security.

João Araújo is a professor at the Department of Informatics at the Universidade Nova de Lisboa, Portugal and a full member of the Portuguese research center NOVA LINCS. He holds a M.Sc. from Universidade Federal de Pernambuco and a Ph.D. from Lancaster University, UK, both in the area of Software Engineering. His principal research interests are Requirements Engineering (RE), Advanced Modularity, Model-Driven Engineering (MDE), and Software Product Lines (SPL), where, he has published several papers on these topics in journals, international conferences, and workshops. Within these subjects he has also been involved in several projects, such as: AMPLE (funded by the European Union), Aspects for Space Domain (funded by ESA), SOFTAS and BATIC3S (both funded by FCT/MCTES in Portugal). He has served in the organization of several conferences such as RE, MoDELS, ICSE, ECOOP, AOSD. He has been a co-founder of the series of Early Aspects workshops which has been held at AOSD, OOPSLA, SPLC and ICSE conferences since 2002. Recently, he has launched the series of workshops on model-driven RE (MoDRE) that has been held in RE conference.

Tony Gorschek is a Professor of Software Engineering at Blekinge Institute of Technology — where he works as a research leader and scientist in close collaboration with industrial partners. Dr. Gorschek has over fifteen years industrial experience as a CTO, senior executive consultant and engineer. In addition, he is a serial entrepreneur — with five startups. At present he works as a research leader and in several research projects developing scalable, efficient and effective solutions in the areas of Requirements Engineering, Product Management, Value based product development, and Real Agile™ and Lean product development and evolution. Dr. Gorschek leads the SERT profile (Software Engineering ReThought) - Swedens largest software engineering research initiative, developing the next generation of applied empirical research movements to meet the challenges of the next generation of software intensive products and services.