Defining Inspection Techniques for Detecting Privacy Problems in Online Social Networks

Andrey Rodrigues
Institute of Computing
Federal University of Amazonas
Manaus, Brazil
andrey@icomp.ufam.edu.br

Natasha M. C. Valentim
Department of Informatics
Federal University of Paraná
Paraná, Brazil
natasha@inf.ufpr.br

Eduardo Feitosa
Institute of Computing
Federal University of Amazonas
Manaus, Brazil
efeitosa@icomp.ufam.edu.br

***Abstract*—In the last few years, Online Social Networks (OSN) have experienced growth in the number of users, becoming an increasingly embedded part of people's daily lives. Privacy expectations of OSNs are higher as more members start realizing potential privacy problems they face by interacting with these systems. Inspection methods can be an effective alternative for addressing privacy problems because they detect possible defects that could be causing the system to behave in an undesirable way. Therefore, we proposed a set of privacy inspection techniques called PIT-OSN (Privacy Inspection Techniques for Online Social Network). This paper presents the description and evolution of PIT-OSN through the results of a preliminary empirical study. We discuss the quantitative and qualitative results and their impact on improving the techniques. Results indicate that our techniques assist non-expert inspectors uncover privacy problems effectively, and are considered easy to use and useful by the study participants. Finally, the qualitative analysis helped us improve some technique steps that might be unclear.**

***Index Terms*—user privacy, privacy evaluation, privacy inspection, social network, empirical study**

I. Introduction

The growth of Online Social Networks (OSN) and its different forms of interaction and exploration of relationship dynamics has encouraged the use of good design and evaluation practices to ensure their social acceptability and quality of use [1] [2] [3]. According to [4], it is not an exaggeration to say that privacy in an OSN has become one of the determining quality factors since discrepant privacy mechanisms/interfaces can negatively influence the appropriation of these applications by the user.

Difficulties in finding the desired option or the inability to perform a certain task in relation to privacy do not always occur as a consequence of improper privacy management by the user. On the contrary, such disparities may be the result of the system being based on a restricted model or mechanism of rules that fail to meet the users' needs and intentions [2] [5], causing unwanted privacy defects.

In the last few years, some technologies have been proposed to support the design and evaluation of OSNs with a focus on user privacy, so that such technologies can be easily articulated and applied by the designers/evaluators of these systems [2] [6] [7] [8]. Many of these previously proposed approaches have been developed to address specific privacy issues in OSNs, such as photo and information management, access control, and data sharing. However, such approaches do not detect potential defects that can affect the user privacy interaction in these systems.

One way to identify and list defects in system is through inspection techniques [9]. For example, to inspect a software artifact, the inspector can use three different techniques: ad hoc, checklist, and reading techniques. While ad hoc and checklist techniques are intuitive and based on non-systematic procedures, the reading techniques have explicit, focused and systematic procedures [10]. According to [9], reading techniques are a specific type of inspection technique with a number of procedures that can be adopted by an evaluator to understand the artifact under inspection, providing a systematic guide for defect identification. A literature review was performed and we identified the lack of inspection techniques that specifically assess privacy aspects in online social networks context. [11].

In this way, it is important that privacy-specific inspection techniques exist because, just like usability, privacy is also a holistic property of interactive systems that includes the people who use them. This belief is based on the fact that an entire system can be compromised if there is a poorly implemented privacy component that shares sensitive user information [4] or a discrepant interface in which users cannot understand its privacy elements. From this perspective, reading-based inspection techniques can provide benefits that: (i) support non-specialist professionals learning about privacy inspection; (ii) maintain the quality of use of an online social network interface regarding privacy aspects, and (iii) provide an effective evaluation with emphasis on low cost, speed, and ease of application.

Therefore, we propose the first version of a set of inspection techniques specifically developed to detect privacy defects in OSN interfaces, which we called PIT-OSN (*Privacy Inspection Techniques for Online Social Network*). Herein, the term privacy problem/defect is used with the same meaning to discover situations where OSN behaves incorrectly, undesirably or corruptly in relation to user privacy. These privacy problems/defects can lead to consequences such as unwanted interactions, incorrect processing or user data corruption. In this way, we consider these techniques important for the Human-Computer Interaction area, since evaluation by inspection, besides being an efficient and inexpensive mechanism to identify defects, can provide gains in relation to time and costs because the inspector does not have to invest a lot of time to apply it [9]. Thus, inspection can be an effective mechanism for quality control of privacy in a OSN system.

To define these techniques, three basic assumptions were considered: (1) using privacy aspects of related works already existing in the scientific literature; (2) using a set of guidelines to help inspectors reflect on the discrepant situation to find privacy defects [9]; and (3) using a preliminary study to evaluate and refine the set of techniques so that they are actually useful and easy to use.

The following sections include the theoretical foundations in which the techniques are grounded and the related works to this research. Subsequently, we describe the proposed set of inspection techniques. Then, the preliminary study and its results are shown. Finally, we present conclusions and future perspectives for this research.

II. Background

The search for improving privacy in digital systems is an effort that moves many areas of Computer Science, including the Human-Computer Interaction (HCI) area. According to [4], the HCI area has good design and evaluation practices that improve user privacy and ensure their privacy in computing systems. In order to better characterize the theme in question, we present the theoretical foundation in which techniques are grounded in the next subsection. Moreover, we present the main definitions regarding software inspection and inspection techniques as an interface evaluation tool.

A. *Privacy Regulation Theories*

According to the privacy regulation theory presented by Altman [12], privacy is defined as a selective control of access to the individual. Altman´s theory presents three relevant elements for dealing with privacy aspects, namely: control, state (level) and context.

Privacy control is associated with the access regulation process as addressed in Altman's privacy theory [12]. In the physical world, this kind of control is usually obvious, since a particular individual knows who they are talking to and how they can control their information. However, controlling these access limits in an OSN environment may be more complex due to the peculiar characteristics of these applications.

State of privacy, also related to Altman's theory, refers to the ability of a given individual to increase or decrease their access limits to achieve their desired privacy level. For Altman [12], there is a continuum point of privacy levels that can be achieved by the user, ranging from a low (minimum) privacy level, where all information is accessible to a wide audience, to a high privacy level, where no information may be shared about the user.

The contextual nature of privacy is related to the dynamics in which privacy levels and controls are modified. In this sense, we must allow different aspects and decisions related to privacy to be considered in different contexts and domains [12] [13].

Nissebaum [13] addressed the contextual nature of privacy by introducing the contextual integrity theory. The author emphasizes that privacy does not have a universal concept and can be understood according to a certain context, that is, there are no universal norms for privacy and the term is different for each situation or context. Nissebaum [13] considers that the access limits pointed out by Altman [12] are governed by a set of related norms: the social adequacy and flow of information dependent on the context. The standard of social adequacy determines what kind of personal information is appropriate to share in a particular situation or in a particular social environment. Information flow rules help define relationships by the amount of information that is shared between people. Then, people share more personal information with more intimate friends and more general information with acquaintances who they are not intimate with.

According to Nissebaum's theory [13], the rules guiding the standards mentioned above change over time, for example, what was appropriate to share at a certain time may no longer be considered appropriate afterwards. This issue is exemplified by behavioral changes of social network users regarding the way they share their personal information, caused by previous positive or negative experiences in relation to the context in which they are inserted.

B. *Software Inspection*

Michael Fagan defined inspection in the computational context in 1976, inspired by the statistical methods of quality used in the hardware manufacture. Fagan basically formalized the practice of questioning a co-worker if everything was working correctly in a software project into a process [14].

In this context, while developing his work in a company, Fagan created the inspection to increase the quality of software and to improve the programmers' productivity. This type of method initially was focused on detecting defects in the program code structures. Subsequently, the inspection was extended to other software artifacts as software requirements documents, architectures, models, interfaces, among others.

The HCI area defines inspection as a specific type of evaluation method that allows the evaluator to examine (or inspect) an HCI solution to detect potential interaction and interface problems that could compromise user experiences. When inspecting an interface, the evaluators try to represent a user with a certain profile and try to find problems that they would experience. In addition, they also try to judge possible problematic points that could cause difficulties to users [15].

C. *Inspection Techniques*

One of the decisive factors in the planning and results of a system inspection is defining the inspection technique to be used. To inspect an artifact, the inspector (professional who performs the inspection) may use different techniques, such as Ad hoc, Checklist, and Reading Techniques.

An ad hoc inspection, as the name implies, is based exclusively on the evaluator's experience; there is no technology, direction or focus on how to proceed or what should specifically be verified during the inspection activity [14]. According to [16], one of the main problems inherent in this type of technique is related to the inspector's skill, knowledge, and experience regarding defect identification activity.

The checklist-based inspection receives a structure in which ”yes/no” questions must be answered by evaluators while they inspect a given artifact [17]. In general terms, the checklist technique uses a list of questions whose answers help the inspector to identify defects.

According to [9], a reading technique is a specific type of inspection technique that contains a series of steps for an individual analysis of a software product to achieve the understanding required for a specific task. Such techniques have a higher formality degree and rely less on the inspector's experience to achieve good results. The main requirements for designing a reading-based inspection technique are [9]: (1) Being associated with a type of artifact (such as an interface for example) and the notation in which the artifact is described (as a natural language); (2) Being adaptable according to the intrinsic characteristics of the application; (3) Being thorough, providing a well-defined inspection process; and (4) Being evaluated experimentally to determine its viability and its degree of effectiveness in the defects detection.

Moreover, a reading-based inspection technique consists of two main components: (i) procedures to guide the evaluator with the specific inspection objectives; and (ii) questions that lead the evaluator to reflect on the discrepant situation in order to find defects [9]. The term ”reading” was chosen to emphasize the similarities with the mental process that people use when trying to understand the meaning of a text [18].

III. Related Works

In order to support the proposed set of techniques definition, we sought to apply concepts based on an evidence-based methodology [19], such as conducting a secondary study (which can be a literature review or systematic review or systematic mapping review). Herein, we use a literature review and an empirical study to validate the proposed techniques. From the literature review, we identified the lack of technologies that support privacy evaluation by inspection [11].

Therefore, we collect indicators that could assist in formulating techniques using the privacy regulation theory defined by Altman as a starting point [12]. This theory has exerted relevant influence on how HCI researchers consider privacy in the context of interactive social systems, as used by [2] to design a privacy model for OSN.

From the definitions introduced by Altman, we sought to collect evidence of proposals from the scientific literature by identifying which privacy aspects such proposals focused on. This collection allowed the identification and analysis of several criteria that are considered relevant to privacy.

To address the privacy level aspect, Villela and Prates [2] proposed the Privacy Design Model (PDM). PDM is an epistemic tool to support the design and evaluation of personal information sharing in OSN, with a focus on user privacy.

To derive the privacy characteristics for personal information sharing, the PDM used the elements presented in Altman's theory [12]. The elements are presented directly in the model through the privacy control and privacy level, and indirectly through the context. The model is structured through privacy dimensions that reflect different aspects that impact users' privacy and which designers must reflect. Control is related to who has the power to decide which values will be assigned to each privacy dimensions in the model. The context is not addressed directly in the PDM. However, it plays a key role in guiding the designer's decisions about how to deal with the privacy dimensions as to how the values will be attributed to them. With PDM, it is possible to analyze online social networks to identify the privacy level that they offer to their users and not the ”privacy options” offered to them [2].

To improve the privacy control provided by online social network sites, some authors focused on developing technologies that emphasize different privacy aspects to be considered in the access control. In the papers presented by Anthonysamy et al. [20] and Wisniewski et al. [21], the authors sought to highlight the impasse of managing access to a user's personal information by third-party applications. Both authors stress the importance of restricting information shared in such applications, because both the application developer and a malicious component may have access to a user's private data, which can lead to a privacy problem.

Other authors such as Christin et al. [22] and Rodrigues et al. [23] have investigated the location services of online social networks. These authors highlight the risks that this type of service can pose by allowing third-party applications or other sites to obtain or use information about the user's location. The user needs to have broad control over these services so as not to impact his/her privacy.

For treating cultural privacy issues specific to online social networking controls, Ur and Wang [24] proposed a framework focused on cultural issues, such as norms regarding the use of pseudonyms or posting of photographs. The authors' framework discusses legal issues in cross-cultural privacy, including data-protection requirements and questions of jurisdiction. In this sense, the framework can help researchers, regulators, and designers reason systematically about cultural differences related to privacy control in social media.

Gurses et al. [3] presented heuristics that can be used in OSN privacy design. In this way, the authors developed a conceptual framework that encompasses heuristics that can be used systematically during the privacy controls engineering of an online social network. Such heuristics cover the following themes: privacy law, usability, data transparency, internal separation of identities, and confidentiality. These heuristics that make up the framework structure are interdependent and they highlight different aspects of privacy that can pose a risk to users, impacting his/her privacy. The proposal is based on features extracted from works from the scientific literature and also about the online feedback given by users about privacy violations. Other identified works [25] [26] [27] also address and discuss aspects similar to those presented by [3], highlighting the importance of these heuristics for the OSN privacy control.

Rodrigues et al. [23] identified different aspects of privacy by performing an exploratory study conducted with online social network users. In that study, the aspects found by the authors demonstrated that the decisions adopted by the evaluated social network did not reach the users' preferences regarding privacy, impacting the user interaction with the system. The identified aspects highlight points that, based on the opinion of the study participants, cause unwanted privacy-related problems such as: lack of user privacy in search activity, lack of blocking mechanisms, unwanted comments and poor location controls.

As in the work of Rodrigues et al [23], Shi et al. [28] investigated users' privacy needs and expectations through a qualitative study. Their results highlight the tension between users' social needs and the interpersonal privacy that involves peers' information privacy. Moreover, the authors provide preliminary conceptual and empirical insights in terms of design implications to address the tensions in interpersonal information privacy management.

Nagaraj and Bryant [29] analyzed several factors that affect user-to-system trust with respect to privacy management, providing an overview of techniques used to build privacy statements and privacy controls. In this way, the authors review existing design models and factors in the context of privacy management and propose methods to improve transparency and control for users.

In another look, Pereira and Prates [30] proposed a conceptual framework to support the designers of Digital Legacy Management Systems (DLMS), by describing the dimensions that are relevant to these systems and the values they can take. The DLMS allows users to define the digital data future, once they have decreased. This issue has a strong influence on the privacy of users' data/identities regarding the destination of their post mortem digital legacy.

The privacy policy informs the user of several issues about his/her data privacy, such as information regarding collection and processing data and server location. Furthermore, Yamauchi et al. [31] discuss several privacy issues that arise from the terms of use and mobile application privacy policies. Guidelines for the establishment of trust and privacy are presented in order to guide designers in mobile social network development. Some guidelines presented by these authors discuss the collection, use and data disclosure, clarity, and current legislation. These guidelines served as one of the bases to compose the structure of one of the techniques proposed in this paper.

From this same perspective, Lichtenstein and Swatman [32] Anthonysamy et al. [33] and Yu et al. [34] have sought to add value to the privacy policies aspect through the development of guidelines, approaches, and methods. Yu et al. [34] point out the importance of anonymity and confidentiality as points that must be specified by policies to establish trust and ensure user privacy. The authors emphasize that policy documents should explicitly explain how users' personal information, which is provided in login or financial transactions, are protected, and under what circumstances these applications may disclose such information, i.e., in cases required by law.

Lichtenstein and Swatman [32] and Anthonysamy [33] believe that privacy policies should explain how they treat the involvement of children or minors in online social networks. In this sense, it is possible for privacy policies to protect children's privacy by informing practices for parental consent, collecting information and disseminating information provided by younger children, and general tips on protecting children's privacy.

Based on these works from the literature review, we observed that three main characteristics are systematically emphasized regarding the privacy structure in an OSN, such as level and privacy control, corroborating the Altman theory [12], and privacy policies, which is a criterion of quality that is not considered in the context of Altman theory. Each paper focuses on one of these characteristics, which we call privacy categories. Table I presents each related work identified, indicating which categories these references focus on.

TABLE I
PRIVACY CATEGORIES CONSIDERED BY EACH REFERENCE

References	**Categories**		
	Level	***Control***	***Policy***
Anthonysamy et al. (2012)		x	
Anthonysamy et al. (2014)			x
Christin et al. (2013)		x	
Gurses et al. (2008)		x	
Lichtenstein and Swatman (2003)			x
Nagaraj and Bryant (2016)		x	x
Pereira and Prates (2017)		x	
Rodrigues et al. (2016)		x	
Shi et al. (2012)		x	
Ur and Wang (2013)		x	
Villela and Prates (2015)	x		
Wisniewski et al. (2017)		x	
Yamauchi et al. (2016)			x
Yu et al. (2006)			x

Based on this theoretical contribution and on analyzes made from the works cited above, we developed a set of privacy techniques for inspecting privacy defects in three general OSNs categories: levels, controls and privacy policies. Each technique in the set directs its inspection considering one of the categories above: PIT-OSN 1 for levels; PIT-OSN 2 for controls; and PIT-OSN 3 for inspecting privacy policies. We present the definition and context of use of the proposed set of techniques in the following section.

IV. Privacy Inspection Techniques

Privacy Inspection Techniques for Online Social Network (PIT-OSN) is a set of read-based techniques that detect privacy defects in online social network interfaces. Such techniques guide the inspector to create a privacy defect diagnosis of levels (PIT-OSN 1), controls (PIT-OSN 2), and policies (PIT-OSN 3).

For performing an inspection with PIT-OSN, the set provides verification items (practical guidelines) grouped into privacy dimensions. The dimensions highlight general privacy aspects and the verification items are used to interpret such dimensions, as well as to evaluate if the inspected system interface obeys them or not. For each verification item violated, the inspector should describe the defect, thus signaling the need to or convenience of changing the interface element to ensure user privacy. The verification items were elaborated based on the knowledge acquired in the literature review and by the practical identification of several privacy defects related to the mentioned dimensions. Fig. 1 presents an illustration of the set and its categories for privacy inspection.

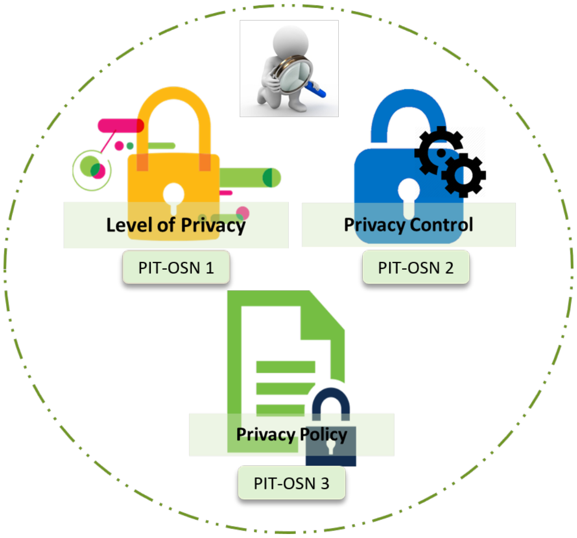


Fig. 1. Inspection Categories of PIT-OSN Techniques.

The main characteristics of the techniques are: (a) Tool independent: the set is not limited to tooling support and is freely distributed; (b) Independent of the development stage: not limited to a specific stage, may also be applied at design time as long as the interface representations are already defined; (c) Comprehensive: not limited to a specific social network domain; and (d) Used by professionals with little knowledge of privacy inspection: any professional involved in design and evaluation of OSN applications can perform the inspection without needing to be experts in interface evaluation.

Moreover, the techniques can be used independently. For example, when an OSN designer or evaluator believes that only the privacy policy scenario can be fragmented, PIT-OSN 3 can be applied separately to improve this scenario. However, when the techniques are performed together, better results can be found as the inspector evaluates and interprets the current privacy situation of the system from a comprehensive point of view. In this sense, an inspection with the whole set can help enrich the identification of needs and opportunities for overall OSN privacy improvement. In the next subsection, we provide a detailed description of the techniques.

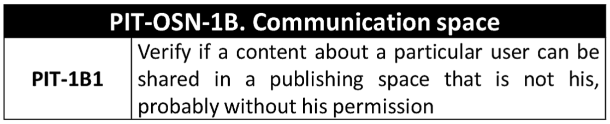
A. *PIT-OSN 1*

PIT-OSN 1 is an inspection technique for evaluating privacy levels of an OSN. The privacy level refers to the access limit provided by the system to a given user information shared. Such sharing may occur either directly, when the user himself shares information about himself in the system, or indirectly, when another user or the system itself takes the initiative to disclose information about the individual. Although information is voluntarily shared by the individual, privacy problems may arise if the user does not have an adequate privacy level to limit the information audience or what can be done with such information.

The inspectors, when using this technique, have the opportunity to evaluate the adequacy of a user's personal information and publications shared in the system. Based on the dimensions presented by [2], the verification items that led the inspector to diagnose a possible privacy defect were originated. A description of the dimensions used in the PIT-OSN 1 structure is presented below:

- **Information source**: refers to who can determine how, when and to what extent information about the individual will be released through the system.
- **Communication space:** refers to where the information about the individual is disclosed within the system.
- **Data content:** refers to the information type about the individual that will be shared in the system, considering their level of individuality.
- **Temporal persistence:** refers to the time period in which information is made available to other users within the system.
- **Audience:** refers to who will have access to the information about the individual within the system. Thus, the broader (and more unknown) the audience is, the lower the privacy level.
- **Feedthrough:** refers to the system suitably informing the individual about other users activities that involves him/her, such as when other users refer to him/her, respond or share his/her post.
- **System's speech:** refers to the system disclosing an individual's personal information to other users.
- **Information dissemination:** refers to the audience being able to share an individual's personal information with other users within the system.

From these definitions, the verification items that determine what should be checked in each dimension are listed. When evaluating privacy from the perspective of levels, the inspector should be concerned that the system provides a continuous point of levels that can be achieved by the individual. So, the main question guiding the category in focus is: "*Can the user achieve his or her desired privacy level?*" In view of this, the initial version of the technique contemplates 17 verification items grouped in the dimensions described above. Fig. 2 provides an excerpt of PIT-OSN 1 with one of its dimensions and a respective verification item.



PIT-OSN-1B. Communication space	
PIT-1B1	Verify if a content about a particular user can be shared in a publishing space that is not his, probably without his permission

Fig. 2. PIT-OSN 1 extract.

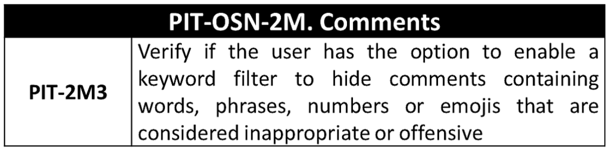
B. PIT-OSN 2

PIT-OSN 2, for its part, focuses on inspecting the privacy controls available in an OSN. Privacy control is associated with the process of regulating access limits as addressed in Altman's privacy theory [12]. An important point to note is that the controls provided by these applications are usually listed through information or represented through elements that indicate how these particular features work.

In this sense, the technique helps inspectors detect a possible defect in these elements, which may not have been well defined or represented through the interface, causing a possible privacy defect. Through the recommendations and technical indicators identified through the related works [3], [29], [24], [28], [21], [23], [20], [30], [22], we defined the dimensions and verification items that guide the inspector to detect potential defects in OSN controls. An explanation of the techniques dimensions in focus is described below:

- **Right of privacy:** the system should provide an option to report an inappropriate profile or content such as nudity, fake accounts or intellectual property violations, for example.
- **Usability and privacy:** the system should provide privacy mechanisms that are easy to use and have as little effort as possible for users to learn efficiently and satisfactorily to manipulate such privacy controls.
- **Data transparency:** the system should provide the user an option to access or review all of their publication history and interactions in the application.
- **Third-party applications:** the system should provide the user an option to make informed data more protected, excluding applications, changing the privacy of these applications and avoiding having their information shared on third-party sites.
- **Friendship requests:** concerns the system that provides mechanisms that allow the user to control all property related to requests for friends or followers.
- **Blocking:** refers to the system presenting options that allow the user to prevent all communications or interactions of people or applications that are inconvenient, for example.
- **Privacy on search:** concerns the system providing the user with an option to restrict or prevent other sources of information from finding their profile based on personal data such as telephone or email address, for example.
- **Privacy negotiation:** refers to the system having a reputation control that allows the user to remove or request the removal of unwanted publications on their behalf.
- **Internal separation of identities:** concerns the system that provides the user an option of making selective publications through personalized lists for the audience.
- **Profile information management:** concerns the system that provides the user an option to control the personal data provided in the profile.
- **Confidentiality:** concerns the system that has resources that allow the user to hide or archive shared publications in the application, without permanently deleting them, being privately accessible to the user.
- **Comments:** refers to the system that provides the user with an option to control who can comment on their publications or even restrict inappropriate comments on publications.
- **Location control:** refers to the system that provides the user with an option to control location services or prevent the application from using its location without permission.
- **Post-mortem digital legacy:** refers to the system that provides a resource to handle the privacy of data and content published by the user in case of death.

Based on these definitions, the items that indicate what should be verified in each dimension have been generated. When evaluating privacy from the control viewpoint, the inspector should be concerned if a particular individual has the ability to properly regulate his or her access control. So, the main question guiding this category is: *"Can the user have adequate control over his or her privacy?"*. Thus, the initial version of PIT-OSN 2 has 35 verification items incorporated in the dimensions defined above. Fig. 3 provides an excerpt of PIT-OSN 2 showing one of its dimensions and a respective verification item.



PIT-OSN-2M. Comments	
PIT-2M3	Verify if the user has the option to enable a keyword filter to hide comments containing words, phrases, numbers or emojis that are considered inappropriate or offensive

Fig. 3. PIT-OSN 2 extract.

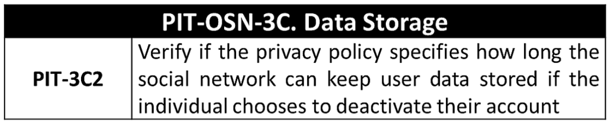
C. PIT-OSN 3

Finally, PIT-OSN 3 directs its inspection of OSN's privacy policies, addressing aspects of privacy that are often neglected. Privacy policies are documents (contracts) that describe terms to ensure the privacy of users' information [33]. To assist in achieving clearer and more consistent privacy policies, PIT-OSN 3 has verification items that help inspectors detect a possible privacy defect in the OSN policy landscape. Based on the theoretical contribution of [31], [20], [33], [34], the dimensions which structure the technique in focus have been formulated, which are described below.

- **Data collection:** concerns the policies that adequately inform the user about the type of data being collected, the method of collection and the purpose for which the data is collected.

- **Use and data disclosure:** concerns the privacy policies that clearly state how the user's data is used and how their information is shared or disclosed.
- **Data storage:** is the policies that specify how they store user data and for how long such content can be stored in the application.
- **Clarity:** concerns the application to present the content of privacy policies clearly, coherently, directly and in a language that facilitates user reading and understanding,
- **Online help:** the privacy policies specifies some way for the user to contact the social network in cases of doubts or complaints.
- **Transaction Anonymity:** refers to the policies specifying how the user personal information that is provided in financial transactions is used and whether the application ensures the confidentiality and protection of user data in such transactions.
- **Confidential data:** refers to policies specifying under what circumstances sensitive user information can be disclosed, such as in cases required by law.
- **Age Restriction:** concerns privacy policies detailing how the involvement of children or minors is treated in the application.
- **Legislation in force:** concerns the privacy policies establishing a regulation or norm for the country in which the application is in use.
- **Advertising services:** concerns the privacy policies explicitly presenting who has targeted the information collected for advertising services and the purpose of this collection and disclosure to third parties.

From these definitions, we formulated the items that guide what should be verified in each dimension of this category. When evaluating privacy under the policy focus, the inspector should observe if the policies content contains clear, consistent and straightforward information that guarantees user privacy. So the main question guiding this category is: *"Does the user have a document that presents specific information that guarantees his/her privacy?"*. A set of 24 verification items integrates the PIT-OSN 3 technique. Fig. 4 provieds an excerpt of one of its dimensions and its verification item.



PIT-OSN-3C. Data Storage	
PIT-3C2	Verify if the privacy policy specifies how long the social network can keep user data stored if the individual chooses to deactivate their account

Fig. 4. PIT-OSN 3 extract.

The full initial version of the PIT-OSN set of inspection techniques proposed in this paper is available online[1]. The main purpose of these techniques is to offer a practice that may not be applied by the professionals involved (designers or evaluators) in the design and development of OSNs, which is privacy evaluation by inspection. The main advantage of PIT-OSN 1 is to show if the social network allows the user to reach their desired privacy level from verification items that guide the evaluator to examine the systems privacy levels. PIT-OSN 2 has the main advantage of showing if an OSN allows the user to have adequate control over their privacy from dimensions that contemplate verification items that are currently in practice. The main advantage of PIT-OSN 3 is to show if the social network contains a document that presents clear and coherent information that guarantees user privacy.

Since PIT-OSN is a set of reading inspection techniques, they instruct inspectors to diagnose privacy problems without requiring them to be experts in an inspection. Although these are evaluation techniques, they can also be applied at design time, as long as the interface representations are already defined. With this, the designer has the opportunity to look for evidence that indicates if the privacy design goals have been reached and if the OSN has the desired quality of use regarding its privacy categories.

One of the main characteristics of these techniques is that they are independent from tooling support, that is, they are not limited by tool availability to carry out their steps. Moreover, these techniques are supported by a set of resources, such as a taxonomy to assist in the classification of detected defects and an application process to provide a better inspection organization. These resources are described in the following section.

D. Defect Classification Taxonomy

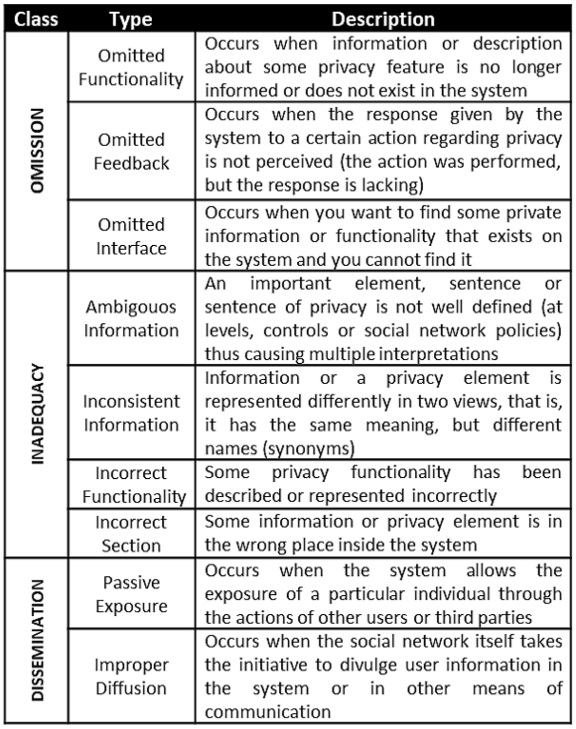
In order to support the PIT-OSN privacy inspection process, a defect classification taxonomy was adopted and adapted [35] [36] to this work context. The taxonomy is organized into three classes: omission, inadequacy, and dissemination. The omission class can be characterized as a type of information or element missing in the privacy categories and can be defined as: omitted functionality, omitted feedback or omitted interface. The defects related to inadequacy can be classified as: ambiguous information, inconsistent information, incorrect functionality or incorrect section. Finally, defects concerning dissemination can be defined as: passive exposure or improper diffusion. Fig. 5 presents a description of defects incorporated in the PIT-OSN set of techniques.

E. PIT-OSN Application Process

To apply the PIT-OSN techniques, we suggest using an application process (a suggested sequence of steps) to provide better inspection organization. To perform this process, we recommend that at least two people participate, as adding more inspectors can increase the chance of finding new defects. The application process consists of five steps, which are described below.

- **Preparation**: The inspection process is prepared and organized in this step. One person, acting as the moderator, defines the inspection process, selects the inspectors, briefly presents about the techniques to inspectors, and

[1] https://bit.ly/2WxrakM



Class	Type	Description
OMISSION	Omitted Functionality	Occurs when information or description about some privacy feature is no longer informed or does not exist in the system
	Omitted Feedback	Occurs when the response given by the system to a certain action regarding privacy is not perceived (the action was performed, but the response is lacking)
	Omitted Interface	Occurs when you want to find some private information or functionality that exists on the system and you cannot find it
INADEQUACY	Ambigouos Information	An important element, sentence or sentence of privacy is not well defined (at levels, controls or social network policies) thus causing multiple interpretations
	Inconsistent Information	Information or a privacy element is represented differently in two views, that is, it has the same meaning, but different names (synonyms)
	Incorrect Functionality	Some privacy functionality has been described or represented incorrectly
	Incorrect Section	Some information or privacy element is in the wrong place inside the system
DISSEMINATION	Passive Exposure	Occurs when the system allows the exposure of a particular individual through the actions of other users or third parties
	Improper Diffusion	Occurs when the social network itself takes the initiative to divulge user information in the system or in other means of communication

Fig. 5. Defect Classification Taxonomy.

distributes the techniques resources to be applied, such as the verification items, the taxonomy for the classification of the possible problems and a spreadsheet to report them.

- **Defect Detection**: In this step, each inspector performs his/her inspection individually, reporting the verification items that were violated, and describing and classifying the possible privacy defects detected in a discrepancy report. A discrepancy represents a possible defect detected during the inspection, but it will only be judged as a real privacy defect in the discrimination step.
- **Collection**: The individual lists of discrepancies (possible defects) produced by the inspectors are integrated into a single list referring to the focus of each technique in this step. One of the inspectors may be responsible for carrying out this integration. After generating the single list, a meeting occurs to eliminate the repeated discrepancies found by more than one inspector, keeping only one record for each discrepancy.
- **Discrimination**: In this step, the inspectors should discuss the discrepancies detected. During this discussion, some discrepancies will be classified as false-positive and others as a real privacy defect. False-positives are discarded because they represent points that the inspector may have reported as a defect, but it is not, either because he/she did not check the social network correctly or because he/she did not fully understand what the verification item requested. Subsequently, the real problems are recorded in a single list of defects generating a consolidated report.
- **Proposed solution**: Finally, inspectors can recommend solutions for detected defects.

V. Empirical Study

The set of PIT-OSN techniques was initially evaluated through a preliminary study aimed to carry out the validity and reliability procedures of the designed techniques and to collect the opportunities for their refinement. The following section presents the study details, including its planning, the execution of the activities related to the evaluation process and the results achieved.

A. Study Planning

The study planning was carried out to evaluate the initial set of PIT-OSN techniques in relation to the type of knowledge generated, time of application, ease of use and utility of each applied technique. We aim to gain new insights and perspectives into the techniques application, also seeking to obtain the possibilities for their refinement.

Three volunteer researchers, chosen by convenience criteria, performed the inspections. The three researchers were doctoral students of a post-graduate program in Computer Science at a Federal Public University. Two participants reported having basic knowledge about interface evaluation acquired in a postgraduate course. One participant stated that they had no experience in interface evaluation. Although the participants are not inspection experts, they produce and dominate the use of technologies, that is, they are prospective inspectors. In this way, we considered the target participants from the perspective of an inspector who is learning about privacy inspection and has the potential to show how these inspectors, who do not know the set of techniques conceived, understood their proposal and application process.

Considering the ethical aspects, a free and informed consent term ensuring the confidentiality and privacy of the data collected was established. Other artifacts were previously defined as a characterization questionnaire that contained questions about participants' experience regarding interface evaluation and other questions regarding privacy knowledge. A post-study questionnaire to collect the participants' opinions regarding the acceptance degree of the set of proposed techniques was also applied. In addition, other resources were defined for the privacy inspections, such as a preparation step, the guidelines for execution of the inspections, a document containing the taxonomy to help in the defect classification and a spreadsheet for reporting and specification of identified discrepancies.

The mobile version of the social network Instagram was chosen as an inspection object. This choice was made using two criteria: expansion and mobility. Regarding expansion, we note the exponential growth of Instagram as a social network service, considering the quantity and diversity of users. Regarding mobility, the mobile version of Instagram shows the trend of use of these applications in smartphones, making it relevant for evaluation by inspection of these mobile social technologies. The application was evaluated in May 2018.

As the participants were not experts in privacy inspection, a presentation was delivered to show the initial idea about the set of techniques. This presentation served as the preparation step for the PIT-OSN application process. In this preparation the inspection objectives, techniques, resources and activities to be performed during the inspection were presented. In addition, a set of slides containing all the contextualization and practical examples of the techniques were presented. For each inspection technique, a possible privacy defect that occurred in a particular OSN was shown. The social networks chosen as an example to illustrate privacy violations during the preparation were not the same ones used as the inspection object, ruling out any bias. All the doubts that arose regarding the techniques were immediately clarified. The total presentation time lasted approximately one hour.

As the initial purpose of this study was to validate the proposed set of techniques and to collect opportunities for refinement, the participants were not required to perform an inspection using the three techniques together, that is, each participant applied one type of technique. This indicates that, in practice, only one evaluation of each technique was performed. A partial inspection was initially chosen to allow participants to capture the maximum potential of results from each applied technique to provide more critical and comprehensive information and, above all, to analyze the plausibility and interpretive processes of each PIT-OSN technique.

B. Study Execution

One of the techniques developers acted as moderator during the study and was responsible for assisting in and answering questions about the technique's application process, being careful not to influence the inspection activity. As the study counted on the participation of three participants, each inspector received a type of inspection technique established through a lottery. From this, the participants were classified as P1, P2, and P3. Participant P1 received the PIT-OSN 1 technique to inspect privacy levels, the participant P2, in turn, stayed with the PIT-OSN 2 for inspecting privacy controls. Finally, participant P3 received the PIT-OSN 3 for detecting defects in privacy policies. Each participant received the support material for his or her specific inspection technique. The individual evaluation of the interface was performed. Participants used their own mobile device and social network to perform the evaluation. After the inspection, a post-study questionnaire was administered.

After the study was carried out, the lists of discrepancies produced by the inspectors were subsequently reviewed in the defect discrimination step. The collection step was discarded in this study because there were no duplicate discrepancies due to individual inspections. The study participants could have carried out all steps of the application process, however, to avoid a prolonged and costly study, two other researchers carried out the discrimination step separately.

In the discrimination step, researchers ranked the discrepancies produced by the inspectors as false-positive or as privacy defect. False positives were discarded as they represent the identified points that were "not real" privacy defects and the real problems were recorded in a single list of defects.

VI. Study Results

Herein, we present the general results from the evaluation performed through the privacy inspection techniques.

A. Privacy Level Inspection

Table II presents the overall result of the inspection performed for Instagram privacy level. In this table, the first column (Part.) represents the participant who applied the PIT-OSN 1. The second column (EIA) indicates the participant's experience in interface evaluation. The third column (ND) shows the number of discrepancies (possible defects) identified. The fourth column (FP) shows the number of false positives. The fifth column (ND) indicates the number of real privacy defects detected (ranked after the discrimination step). The sixth column (T(h)) shows the total time spent by the participant during the inspection. Finally, the seventh column (D(h)) indicates the number of defects per hour.

TABLE II
Inspection results with PIT-OSN 1

Part.	*EIA*	*ND*	*FP*	*ND*	*T(h)*	*D(h)*
P1	S	07	0	07	1,32	4,07

We observed that PIT-OSN 1 fulfilled its main purpose in helping detect privacy defects in the OSN privacy levels used as inspection object. A total of 7 defects were detected and the inspector took 1h32min for the inspection.

Four types of defects related to privacy levels were identified, which were classified by the inspector as: omitted functionality, omitted feedback, passive exposure, and improper diffusion. The most frequently found problems were omitted functionality and passive exposure, evidencing that many functions regarding privacy levels do not exist in the system. In addition, the social network allows the passive exposure of a particular individual through the actions of other users, which can generate unwanted privacy problems. Two problems identified by the inspector in the evaluated OSN are exemplified in Fig. 6.

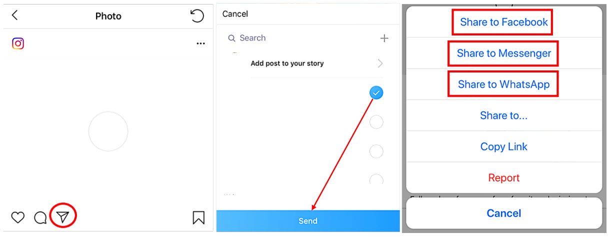


Fig. 6. Examples of defects identified with PIT-OSN 1.

Based on Fig. 6, we noticed that the social network allows another user to share a publication about a certain individual, in another communication space that does not belong to the post owner and probably without his permission. This other publishing space can be Instagram Direct, as shown in the figure 6, which allows the publication to be directly sent to specific friends or groups of friends of the user who shared and also allows sharing in other spaces outside the social network such as Facebook, WhatsApp, and Messenger, for example. This issue shows that the ”Communication Space” dimension and one of its verification items has been violated, revealing a passive exposure problem.

In addition, Fig. 6 presents that by allowing another user to share a particular individual’s publication via direct, the social network also violates the ”Feedthrough” dimension and one of its verification items as it does not provided the individual (owner of the post) notification of this disclosure made by another user through the direct resource. This issue reveals an omitted functionality defect because the system does not notify the subject of this interaction. This result may be an indication of (re)design decisions because, in order for the user to have an adequate privacy level, the system must provide complete notification so that the user is aware of what is being accessed by other users. Thus, the more a user is notified, the greater the chance that user will be more restrictive in relation to the information they share or with their privacy settings.

B. Privacy Control Inspection

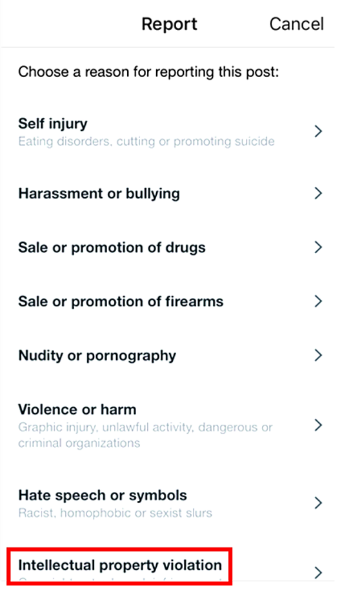
Table III presents the overall result of the inspection performed in Instagram privacy control. The descriptions of the column items in Table III are the same as described in section VI-A. Observing Table III, we note that the PIT-OSN 2 technique also fulfilled its general purpose of supporting defect diagnosis in the privacy controls made available by the inspected OSN. A total of 13 privacy defects were diagnosed. It took 2h14min to apply the technique.

TABLE III
INSPECTION RESULTS WITH PIT-OSN 2

Part.	*EIA*	*ND*	*FP*	*ND*	*T(h)*	*D(h)*
P2	S	16	3	13	2,14	5,12

The inspector who used PIT-OSN 2 identified two types of defects: omitted functionality and incorrect section. This shows that an important information or a privacy element for the system interface are missing from the OSN’s privacy controls. In addition, the incorrect section problem also demonstrates that some information or privacy elements are embedded in incorrect locations in the inspected social network, causing this type of defect reported, as shown in Fig 7.

By inspecting Instagram from the dimension ”Right of Privacy” and its respective verification item 2A1 ”*Verify is the social network allows the user to request the removal of information, image or video that violates their privacy rights*”, the inspector detected an incorrect section defect. Although the social network allows the user to report an intellectual property violation, this option is not found in the system privacy settings. When searching for this option, the user is directed to help center and has to go through the interface to search for this functionality. That is, the user needs to consult the online help to know how to report this issue. This path reflects a defect because, considering the profile of a user who does not know the system well, it is difficult to find this option related to a privacy action.



Report Cancel

Choose a reason for reporting this post:

Self injury
Eating disorders, cutting or promoting suicide

Harassment or bullying

Sale or promotion of drugs

Sale or promotion of firearms

Nudity or pornography

Violence or harm
Graphic injury, unlawful activity, dangerous or criminal organizations

Hate speech or symbols
Racist, homophobic or sexist slurs

Intellectual property violation

Fig. 7. Example of defect identified with PIT-OSN 2.

C. Privacy Policy Inspection

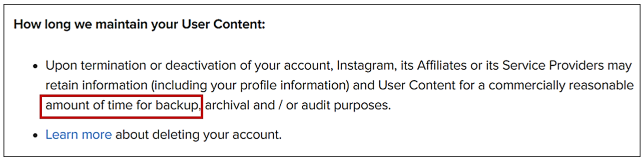
Table IV presents the overall result of the inspection performed in the Instagram privacy policy. The descriptions of the column items in Table IV are the same as described in section VI-A. Based on the results of Table IV, we found that the PIT-OSN 3 technique also fulfilled its purpose to identify defects in this system scenario. A total of 10 defects were detected in the privacy policies using this technique, with an application duration of 1h36min.

TABLE IV
INSPECTION RESULTS WITH PIT-OSN 3

Part.	*EIA*	*ND*	*FP*	*ND*	*T(h)*	*D(h)*
P3	N	11	1	10	1,36	5,68

The most reported defects by inspector were omitted functional and ambiguous information. Thus, we note that some OSN functionality that could be stated in the system policies has not been defined or is omitted in this scenario. In addition, other information contained in the privacy policies is ambiguous, that is, several interpretations can be derived from privacy policy, leading the user to have a dubious understanding of what is being exposed or requested to protect them in the system interaction. An example of ambiguous information detected by the inspector is shown in Fig. 8.

Based on Fig. 8, we note that the social network informs how long it stores the user’s content. However, when evaluating this information through the ”Data Storage” dimension



How long we maintain your User Content:

- Upon termination or deactivation of your account, Instagram, its Affiliates or its Service Providers may retain information (including your profile information) and User Content for a commercially reasonable amount of time for backup, archival and / or audit purposes.
- Learn more about deleting your account.

Fig. 8. Example of defect identified with PIT-OSN 3.

and its verification item 3C2 *"Verify if the privacy policy specifies how long the social network can keep user data stored when the individual chooses to deactivate their account"*, the inspector noticed that there is ambiguous information about the time mentioned, since it does not specifically inform the user how long his/her information will be maintained if his/her account is excluded. The phrase "commercially reasonable amount of time" does not clearly specify the length of time that user data will be retained in the system, thus leading to varying interpretations.

D. Type of Knowledge and Generated Explanations

In terms of knowledge required to apply and interpret the set of techniques verification items, we observed that PIT-OSN exempts the evaluator from needing to be a specialist to identify and list problems, as discussed in its formulation. The explanation quality of the diagnosed privacy defects may indicate that the techniques inspection process does not necessarily depend on the inspector knowledge in an interface evaluation.

Regarding the type of knowledge that the set of techniques generated for its application, the PIT-OSN can adequately, technically improve the quality of privacy in OSN projects and evaluations. They can be used both for formative evaluation, that is, giving inputs to the quality of a privacy (re)design and to compare design alterations, as well as in a sommative evaluation, serving as tools that support if the OSN has the desired quality of use levels in terms of their privacy aspects.

Considering the type of explanation generated, the PIT-OSN seeks to foster evaluator reflection and interpretation about the detected privacy problems, since they are qualitative and exploratory techniques. That is because they have verification items linked to practice, as the set of techniques seeks to offer results that generate articulated and consistent explanations about levels, controls and privacy policies.

E. Application time

PIT-OSN 1 showed a good performance in detecting defects, finding 4.07 defects per hour and having an execution time of 1h32min, standing out as the most agile application time for the set of techniques proposed.

PIT-OSN 2, in turn, identified 5.12 defects per hour and had an application time of 2h14min. Despite presenting the longest time spent detecting defects, it fulfilled its general purpose to detect problems regarding the privacy controls of the inspected OSN.

Finally, PIT-OSN 3 identified 5.68 defects per hour and lasted for 1.36 minutes. With this, the technique was also able to detect discrepant information in the privacy policies of the evaluated system. With this, we noted that the time required for applications may be directly related to the interpretive process that each technique generated. The PIT-OSN 1 and 3, while fulfilling their technical aims, are shown as relatively agile and objective inspection techniques. Since PIT-OSN 2 contains the largest number of verification items in the set of techniques, it tends to have a longer interpretive process, as the number of items to be checked can increase the inspection time.

F. Techniques Acceptance Analysis

Participants informed their acceptance degree regarding the set of techniques through a post-study questionnaire. This questionnaire was elaborated based on the TAM (*Technology Acceptance Model*) that has been widely used in several studies [37]. Davis [38] proposed TAM to assess why users accept or reject a particular technology. The indicators used were: (i) perceived ease of use; (ii) perceived usefulness; and (iii) intention to use.

Ease of use defines the degree to which a person believes that using a specific technology is effortless, through the following questions: (F1) My interaction with PIT-OSN was clear and understandable, (F2) Using PIT-OSN does not require much of my mental effort, (F3) I consider PIT-OSN easy to use and (F4) I find it easy to use the PIT-OSN for what I want it to do, supporting the privacy evaluation in online social networks through inspection.

Perceived usefulness defines the degree to which a person believes that the technology could improve their performance through the following questions: (U1) Using PIT-OSN has improved my performance in privacy inspection of social networks, (U2) PIT-OSN has improved my productivity in privacy inspection of social networks, (U3) Using PIT-OSN has increased my effectiveness in privacy inspection of social networks and (U4) I consider PIT-OSN useful to support the process of privacy inspection of social networks.

Intention to use defines the degree to which a person believes that he or she would use the technology in future projects, through the following questions: (I1) Assuming I have access to PIT-OSN, I intend to use it and (I2) the PIT-OSN I predicts that I will use it at other times.

Participants provided their answers on a six-point scale based on the questionnaire applied by [39]. The possible answers were: totally agree, strongly agree, partially agree, partially disagree, strongly disagree, and totally disagree. This scale of responses was considered adequate because there is no intermediate value, that is, it helps avoid the bias of the central tendency in classifications, forcing participants to judge the result as adequate or inadequate.

Fig. 9 presents the participants' perception of ease of use indicator. The vertical axis of the graph represents the affirmatives of the indicator in focus along with the number of the technique. The horizontal axis refers to the degree of participants' acceptance. In the bars, there are codes that symbolize the participants (P1, P2, and P3) of the study and their respective evaluation.

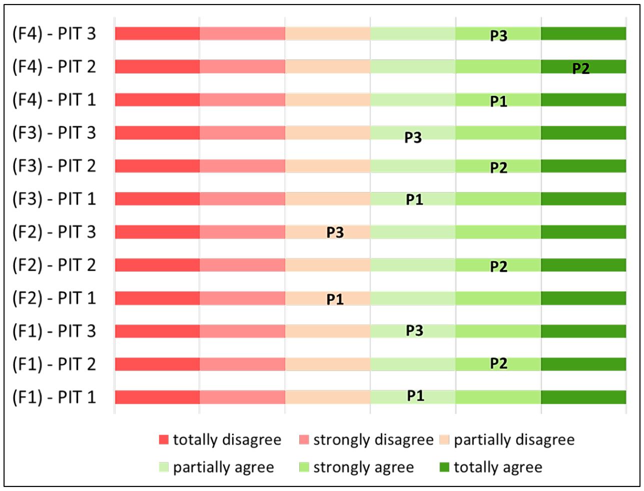


Fig. 9. Participants' perception of PIT-OSN ease of use.

Based on the view provided in Fig. 9, we note that all participants agreed with the statements F1, F3 and F4, indicating that PIT-OSN is easy to use since it presents simple, objective and generic guidelines, which are unrelated to the solid knowledge of the inspector in evaluating interfaces. However, two participants disagreed partially about the affirmative F2. This question probably points to the need for a more in-depth investigation about some points of technology to identify what may be causing mental effort and what can or should be simplified to avoid possible application difficulties.

Fig. 10 presents the participants' perceptions regarding the usefulness indicator. In this perspective, we can verify that the application of PIT-OSN in this study revealed that the techniques were considered useful to identify and list privacy problems in an online social network. This result may be related to the type of knowledge generated by the techniques since they are linked to verification items linked to the practice and allow for an articulated discussion of the results. In this way, the techniques are potentially useful to diagnosis privacy problems in OSN.

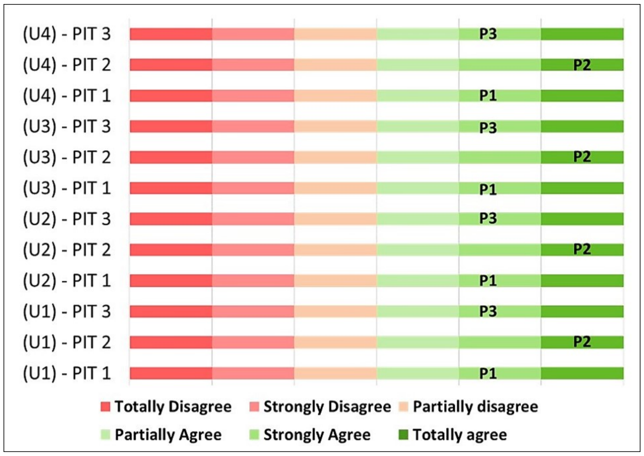


Fig. 10. Participants' perception of PIT-OSN usefulness.

Finally, Fig. 11 points out the participants' perception regarding the intention to use indicator. Following the same interpretation of the previous figures, Fig. 11 demonstrates that participants consider PIT-OSN appropriate to be used in future projects.

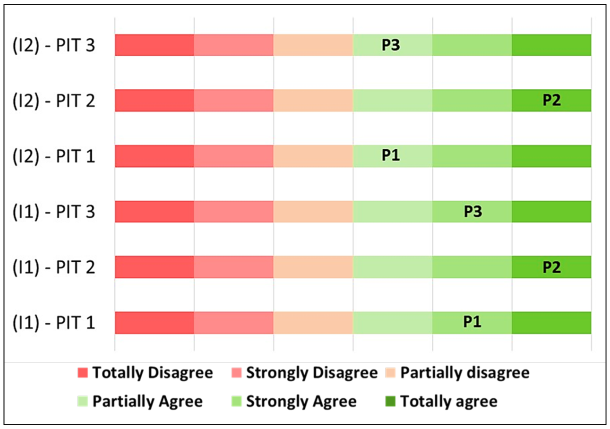


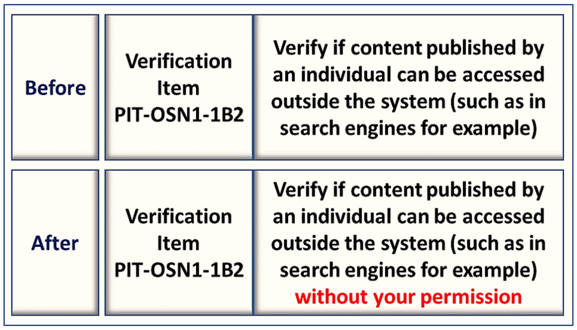
Fig. 11. Participants' perception of PIT-OSN intention to use.

G. Qualitative Results and Improvements

In addition, the participants' comments were analyzed through open questions in the post-study questionnaire. Regarding the positive aspects, the participant's commentary P2 states that: "*[The technique] is very detailed, it uses current approaches and allows us to actually inspect privacy in social networks.*" P3 also notes that "*[The technique allows] the analysis of all major privacy points and it is easy to identify privacy flaws.*" This may indicate that the proposed set of techniques has a good level of detail that forces important subsidies to identify privacy defects.

Considering the disadvantages and difficulties involved in the PIT-OSN application, we emphasize the comment of participant P1 who reported: "*[I had] difficulty in understanding some verification items.*" P3 also expresses difficulty, but not related to the usefulness of the technique specifically, but to the content described by the privacy policies: "*The technique itself is easy to use, the biggest difficulty is in the information interpretation provided by the privacy policy.*" This issue fully reflects the policy problems of its structure and appropriateness, which often include lengthy texts, technical jargon, no writing patterns, and very complex terms. P2, on the other hand, stressed the issue of time as a negative aspect: "*It is a time-consuming inspection. You could standardize and/or reduce [verification] items in the privacy controls technique*". Thus, we observed that there are points that need to be further investigated in the proposed techniques to analyze if the number of verification items influence the application time or not.

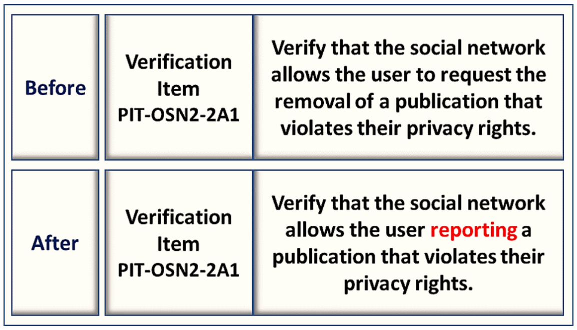
We found that there were some difficulties in the study, one of which is: the understanding regarding certain verification item descriptions. We noticed that some items were not clearly described to detect a potential privacy defect. This happened in the verification item 1B2 description of the PIT-OSN 1 technique, where it asks to verify if content published by an individual can be accessed outside the system. In order for this issue to be seen as a problem that increases the possibility of an individual's privacy being compromised, the content on it must be shared outside the system without their knowledge or consent. This issue best characterizes a real privacy problem, because if the social network does not ask the user to allow their content to be accessed outside the system, we have a potential problem. For this verification item to consider the user's consent, ”without your permission” was included, as shown in Fig. 12.



Before	Verification Item PIT-OSN1-1B2	Verify if content published by an individual can be accessed outside the system (such as in search engines for example)
After	Verification Item PIT-OSN1-1B2	Verify if content published by an individual can be accessed outside the system (such as in search engines for example) without your permission

Fig. 12. PIT-OSN 1 verification item improvement.

Regarding the PIT-OSN 2 technique, we observed that one of the verification items could be confusing in terms of interpretation. This is item 2A1, which asks to verify that the social network allows the user to request the removal of a publication that violates their privacy rights. We noticed that control to request the removal of a post would be a little-used privacy option for social networks. Thus, we modify the phrase ”request removal” by ”reporting”, as shown in Fig. 13. In this sense, if the social network does not provide control to denounce publications that violate the user's privacy rights, there is a possible problem.



Before	Verification Item PIT-OSN2-2A1	Verify that the social network allows the user to request the removal of a publication that violates their privacy rights.
After	Verification Item PIT-OSN2-2A1	Verify that the social network allows the user reporting a publication that violates their privacy rights.

Fig. 13. PIT-OSN 2 verification item improvement.

Likewise, we made improvements in the PIT-OSN defect classification taxonomy. Such improvements mainly occurred in describing some types of defects that might be misaligned in their understanding. Thus, some descriptions have been improved and the nomenclature of one of the defect types about omission class was changed. This is the ”performance omitted” defect. We observed that the study inspectors did not point out this type of defect. So, we explain its definition more thoroughly and changed the name to ”omitted feedback”, that is, the privacy action may have been performed, but the answer is missing.

Regarding PIT-OSN 3, we made some adjustments in the dimensions, for example, dimension 3E was called ”requests” and dealt with the issue of privacy policies to specify ways for the user to contact the social network in case of questions or complaints. We modified the dimension name to ”online contact”, so that the nomenclature is clearer with the description.

In addition, from the responses analysis of the post-study questionnaires and the analysis of the defects pointed out by each inspector, we also verified the need to insert a new procedure in the set of techniques to meet some domain specificities. How privacy is related to the levels, controls, and policies of a particular OSN may be represented in different ways when the social network is for general purpose (e.g. Facebook) or scientific collaboration (e.g. Research Gate). For example, in a general purpose social network, many users like to restrict the temporal persistence of some posts. However, in a scientific collaborative social network, many users want the audience to have access to their entire publication. In this regard, some verification items may be problems in certain OSNs, while they may not be a specific defect in others. Thus, the severity rating was added as a complement applied to detect defect steps, so that the inspectors can judge the detected defects and analyze the severity degree of it in a given domain.

This severity rating was elaborated based on the scale suggested by [40]. These factors influence the severity rating used in the evaluation and can be classified as:

- 0. I do not consider a privacy defect in this social network;
- 1. Only a cosmetic privacy defect - fix only if there is time available;
- 2. Light privacy defect - low priority to fix it;
- 3. Serious privacy defect - high priority to fix it;
- 4. Catastrophic privacy defect - it is imperative to fix it.

VII. Limitations

The study limitations are mainly related to three items: (i) the sample; (ii) the social network used as the inspection object; and (iii) the partial inspection process used in the study, that is, inspection with only one type of technique. In relation to item 1, the small number of participants is not considered ideal from a statistical point of view. Therefore, there is a limitation in the results, which are considered signs and not conclusive. However, this was an initial study to verify the set of techniques validity. Regarding item 2, the social network inspected (Instagram) corresponds to a real system. However, it is not possible to state that the application represents all types of existing social networks. Finally, with respect to item 3, it is noted that with a partial inspection, inputs are gained on the validity of the proposal as inspection techniques that can be applied independently, the knowledge necessary for the application of each technique and the time spent on applications. However, we lost the participants point of view regarding the potential benefits that an integrated inspection would allow us to explore.

In relation to the inspection techniques, one limitation is that they are only applicable in the OSNs context and cannot be performed in other types of systems. Moreover, even if the set of techniques can be applied at design time, this application can only occur after the interface representations choice and cannot be applied in a task model, for example.

VIII. Conclusions and Future Works

Privacy has become a primary concern among social network users. Users can become the victims of privacy problems such as identity theft, stalking or dissemination due to personal data revealed in their profiles. Even if information is voluntarily shared by the user, privacy problems may arise if the user does not have an adequate privacy level to limit the audience information or a privacy mechanism for controlling access to such information. So users have to carefully select the privacy settings for their profile attributes, keeping in mind that they are not exempt from suffering an unwanted privacy problem. Without any support, the OSN can make decisions that lead or expose users to privacy problems.

Therefore, we proposed a set of inspection techniques for detecting privacy problems/defects in OSNs interfaces. For this, the PIT-OSN (Privacy Inspection Technique for Online Social Network) was defined. These techniques were developed from evidence collected in the scientific literature and were evaluated empirically through a preliminary study. With PIT-OSN support, the inspector has the opportunity to evaluate the OSN by considering general privacy aspects (Levels, Controls and Policies). This ensures full coverage of a privacy inspection and also promotes the quality of use to the user while interacting with the system.

This study's main contribution is a new approach to privacy evaluation by inspection. Thus, the techniques can be applied as a tool to diagnose privacy problems, and can also be employed to support the quality of an interface (re)design with respect to privacy categories. Therefore, we hope to help OSN designers and evaluators use the techniques to explore different ideas in design and evaluation alternatives, thus, helping them to elaborate solutions that are more appropriate for the needs and intentions of user's privacy.

However, due to the small sample, it was not possible to consider the study results as conclusive, and a new study with a larger and more heterogeneous sample of participants is needed to evaluate the set of techniques more comprehensively. Based on participants' comments and new ideas that emerged after the analysis of results, new adjustments in techniques will be added to improve them until we find indicators that demonstrate that techniques can feasibly be applied.

As future works, we highlight further studies to test the possibility of using and improving techniques, also aiming to explore the efficiency and effectiveness indicators defined as: Efficiency - the ratio between the number of defects and the time spent in the inspection process; and Efficacy - the ratio of the number of defects detected to the total number of known defects. Consequently, new discrepant items that may arise to evolve the applications of techniques should be observed. For this process of evolution of techniques, exploratory studies, such as interviews or focus groups, should be carried out to explore and explain qualitative data that can enrich the context of the techniques.

Acknowledgment

We thank the undergraduate students who participated in the study. We also thank the Brazilian Symposium on Human Factors in Computer Systems for the invitation to submit an extended version of the paper "*A Set of Privacy Inspection Techniques for Online Social Networks*" to compose a special issue of the JIS-SBC Journal on Interactive Systems. Finally, we would like to acknowledge the financial support granted by CAPES (Foundation for the Improvement of Highly Educated Personnel).

References

[1] D. A. Epstein, B. H. Jacobson, E. Bales, D. W. McDonald, and S. A. Munson, "From nobody cares to way to go!: A design framework for social sharing in personal informatics," in *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*. ACM, 2015, pp. 1622–1636.

[2] M. L. B. Villela and R. O. Prates, "Supporting designers in modeling privacy for social network sites," in *Proceedings of the 14th Brazilian Symposium on Human Factors in Computing Systems*. ACM, 2015, pp. 113–122.

[3] S. Gurses, R. Rizk, and O. Gunther, "Privacy design in online social networks: Learning from privacy breaches and community feedback," *ICIS 2008 Proceedings*, p. 90, 2008.

[4] G. Iachello, J. Hong *et al.*, "End-user privacy in human–computer interaction," *Foundations and Trends® in Human–Computer Interaction*, vol. 1, no. 1, pp. 1–137, 2007.

[5] Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove, "Analyzing facebook privacy settings: user expectations vs. reality," in *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*. ACM, 2011, pp. 61–70.

[6] P. W. Fong, "Relationship-based access control: Protection model and policy language," in *Proceedings of the First ACM Conference on Data and Application Security and Privacy*, ser. CODASPY '11. New York, NY, USA: ACM, 2011, pp. 191–202.

[7] J. Pang and Y. Zhang, "A new access control scheme for facebook-style social networks," *Computers & Security*, vol. 54, pp. 44–59, 2015.

[8] A. S. Teles, F. J. d. S. e Silva, and M. Endler, "Situation-based privacy autonomous management for mobile social networks," *Computer Communications*, vol. 107, pp. 75–92, 2017.

[9] G. Travassos, F. Shull, M. Fredericks, and V. R. Basili, "Detecting defects in object-oriented designs: using reading techniques to increase software quality," in *ACM Sigplan Notices*, vol. 34, no. 10. ACM, 1999, pp. 47–56.

[10] L. He and J. Carver, "Pbr vs. checklist: a replication in the n-fold inspection context," in *Proceedings of the 2006 ACM/IEEE international symposium on Empirical software engineering*. ACM, 2006, pp. 95–104.

[11] A. Rodrigues, "Um conjunto de técnicas de inspeção orientado à avaliação de privacidade em redes sociais online," Master's thesis, Federal University of Amazonas, Brazil, Feb. 2019. [Online]. Available: https://tede.ufam.edu.br/handle/tede/7092

[12] I. Altman, "The environment and social behavior: Privacy, personal space, territory, and crowding." *Brooks/Cole Publishing Company*, 1975.

[13] H. Nissenbaum, "Privacy as contextual integrity," *Wash. L. Rev.*, vol. 79, p. 119, 2004.

[14] H. Ahrefors, “Supporting software inspections through fault content estimation and effectiveness analysis,” Ph.D. dissertation, Lund University, 2002. [Online]. Available: http://lup.lub.lu.se/record/20821

[15] A. Dix, J. E. Finlay, G. D. Abowd, and R. Beale, *Human-Computer Interaction (3rd Edition)*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 2003.

[16] T. Y. Chen, P.-L. Poon, S.-F. Tang, T. Tse, and Y.-T. Yu, “Towards a problem-driven approach to perspective-based reading,” in *7th IEEE International Symposium on High Assurance Systems Engineering, 2002. Proceedings.* IEEE, 2002, pp. 221–229.

[17] O. Laitenberger, K. El Emam, and T. G. Harbich, “An internally replicated quasi-experimental comparison of checklist and perspective based reading of code documents,” *IEEE Transactions on Software Engineering*, vol. 27, no. 5, pp. 387–421, 2001.

[18] F. J. Shull, “Developing techniques for using software documents: a series of empirical studies,” Ph.D. dissertation, Dept. of Computer Science, University of Maryland, 1998.

[19] F. Shull, J. Carver, and G. H. Travassos, “An empirical methodology for introducing software processes,” in *ACM SIGSOFT Software Engineering Notes*, vol. 26, no. 5. ACM, 2001, pp. 288–296.

[20] P. Anthonysamy, A. Rashid, J. Walkerdine, P. Greenwood, and G. Larkou, “Collaborative privacy management for third-party applications in online social networks,” in *Proceedings of the 1st Workshop on Privacy and Security in Online Social Media*, ser. PSOSM ’12, 2012, pp. 5:1–5:4.

[21] P. J. Wisniewski, B. P. Knijnenburg, and H. R. Lipford, “Making privacy personal,” *Int. J. Hum.-Comput. Stud.*, vol. 98, no. C, pp. 95–108, Feb. 2017. [Online]. Available: https://doi.org/10.1016/j.ijhcs.2016.09.006

[22] D. Christin, P. S. López, A. Reinhardt, M. Hollick, and M. Kauer, “Share with strangers: Privacy bubbles as user-centered privacy control for mobile content sharing applications,” *Information Security Technical Report*, vol. 17, no. 3, pp. 105–116, 2013.

[23] A. A. de O. Rodrigues, F. A. S. Clemente, and A. A. S. dos Santos, “An information window about online privacy aspects perceived by social networks users,” in *Proceedings of the 15th Brazilian Symposium on Human Factors in Computing Systems*, ser. IHC ’16. New York, NY, USA: ACM, 2016, pp. 18:1–18:10.

[24] B. Ur and Y. Wang, “A cross-cultural framework for protecting user privacy in online social media,” in *Proceedings of the 22Nd International Conference on World Wide Web*, ser. WWW ’13 Companion. New York, NY, USA: ACM, 2013, pp. 755–762.

[25] F. Bélanger and R. E. Crossler, “Privacy in the digital age: a review of information privacy research in information systems,” *MIS quarterly*, vol. 35, no. 4, pp. 1017–1042, 2011.

[26] H. Krasnova, O. Günther, S. Spiekermann, and K. Koroleva, “Privacy concerns and identity in online social networks,” *Identity in the Information Society*, vol. 2, no. 1, pp. 39–63, 2009.

[27] P. Anthonysamy, P. Greenwood, and A. Rashid, “Social networking privacy: Understanding the disconnect from policy to controls,” *Computer*, vol. 46, no. 6, pp. 60–67, 2013.

[28] P. Shi, H. Xu, L. Erickson, and C. Zhang, “See friendship: Interpersonal privacy management in a collective world,” in *18th Americas Conference on Information Systems 2012, AMCIS 2012*, vol. 4, 12 2012, pp. 2937–2946.

[29] S. K. Nagaraj and A. Bryant, “Factors in building transparent, usable and comprehensive user privacy policy system,” in *11th International Conference on Cyber Warfare and Security: ICCWS2016. Academic Conferences and publishing limited*, 2016, p. 253.

[30] F. H. S. Pereira and R. O. Prates, “A conceptual framework to design users digital legacy management systems,” in *Proceedings of the XVI Brazilian Symposium on Human Factors in Computing Systems*, ser. IHC 2017. New York, NY, USA: ACM, 2017, pp. 1:1–1:10.

[31] E. A. Yamauchi, P. C. de Souza, and D. P. S. Junior, “Prominent issues for privacy establishment in privacy policies of mobile apps,” in *Proceedings of the 15th Brazilian Symposium on Human Factors in Computing Systems*, ser. IHC ’16. New York, NY, USA: ACM, 2016, pp. 26:1–26:9.

[32] S. Lichtenstein and P. M. C. Swatman, “Adding value to online privacy for consumers: remedying deficiencies in online privacy policies with an holistic approach,” in *36th Annual Hawaii International Conference on System Sciences, 2003. Proceedings of the*, 2003, p. 10 pp.

[33] P. Anthonysamy, P. Greenwood, and A. Rashid, “A method for analysing traceability between privacy policies and privacy controls of online social networks,” in *Privacy Technologies and Policy*, B. Preneel and D. Ikonomou, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 187–202.

[34] W. D. Yu, S. Doddapaneni, and S. Murthy, “A privacy assessment approach for serviced oriented architecture application,” in *Proceedings of the Second IEEE International Symposium on Service-Oriented System Engineering*. IEEE Computer Society, 2006, pp. 67–75.

[35] F. Lanubile, F. Shull, and V. R. Basili, “Experimenting with error abstraction in requirements documents,” in *Proceedings Fifth International Software Metrics Symposium. Metrics (Cat. No. 98TB100262).* IEEE, 1998, pp. 114–121.

[36] A. A. Porter and L. G. Votta, “An experiment to assess different defect detection methods for software requirements inspections,” in *Proceedings of 16th International Conference on Software Engineering*. IEEE, 1994, pp. 103–112.

[37] V. Venkatesh and H. Bala, “Technology acceptance model 3 and a research agenda on interventions,” *Decision sciences*, vol. 39, no. 2, pp. 273–315, 2008.

[38] F. D. Davis, “Perceived usefulness, perceived ease of use, and user acceptance of information technology,” *MIS quarterly*, pp. 319–340, 1989.

[39] F. Lanubile, T. Mallardo, and F. Calefato, “Tool support for geographically dispersed inspection teams,” *Software Process: Improvement and Practice*, vol. 8, no. 4, pp. 217–231, 2003.

[40] J. N.-R. L. Mack and J. Nielsen, *Usability inspection methods*. Wiley John & Sons, New, 1995.