Legal Issues and User Experience in Ubiquitous Systems from a Privacy Perspective

Patricia C. de Souza(✉) and Cristiano Maciel

Laboratório de Ambientes Virtuais de Aprendizagem, Instituto de Computação, Universidade Federal de Mato Grosso, Cuiabá, Brazil
{patriciacs, cmaciel}@ufmt.br

Abstract. Guaranteeing privacy in digital systems is an effort that moves several computing areas such as computer security, cryptography, computer networks, safe protocols, system design and human-computer interaction. One of the hypotheses in our work is that many users of mobile applications are not aware of the risks they run of their data being accessed by intruders, mainly because they do not know what they are exposed to and then, because the terms used in access policies are difficult to understand, too long for a dynamic reading and offer little or no flexibility to allow users to make adjustments according to their preferences. Improving users' experience means verifying if the implementation of new ways of interaction that provide freedom and flexibility in the control of privacy settings as well as access policies for mobile applications has allowed for higher levels of security and reliability on the users' side.

Keywords: Privacy · User experience · Legal aspects · Ubiquitous systems

1 Introduction

Privacy issues have become a growing concern among those who entrust their data to IT systems, especially considering the numerous reports of security flaws in systems that had been considered safe; for example, sensitive data stolen or compromised by hackers and digital espionage scandals.

This is the reason why the trust relationship between a user who wishes to store his sensitive data and a service that offers storing has become more unstable. It can be noticed, in modern society, that the very concept of what is private has undergone transformations and suffered from influences according to the context, be it in the offline world or the online world.

Many studies have focused on human behavior regarding privacy in online social networks [1–3] and in ubiquitous applications [6, 8–10]. Some discussion can also be found on the influence of cultural and emotional issues, on values and awareness concerning confidence and on privacy awareness as a reflection of users' attitudes.

One of the hypotheses in our work is that many users of mobile applications are not aware of the risks they run of their data being accessed by intruders, mainly because they do not know what they are exposed to and then, because the terms used in access policies are difficult to understand, too long for a dynamic reading and offer little or no

T. Tryfonas and I. Askoxylakis (Eds.): HAS 2015, LNCS 9190, pp. 449–460, 2015.
DOI: 10.1007/978-3-319-20376-8_40

flexibility to allow users to make adjustments according to their preferences. In this sense, two support fronts for users of ubiquitous applications can be envisioned: digital education and improving users' experience. The first one involves issues of behavior related to values and knowledge, specific to each individual, learned at home or through formal education. Digital education also involves creating regulations to protect citizens against the use of private information. An example of this is the Marco Civil da Internet (Civil Rights Framework for the Internet) a law passed by the Brazilian federal government. This law establishes principles, guarantees, rights and responsibilities for the use of Internet in Brazil (Lei N^{o} 12.965, 2014).

Improving users' experience means verifying if the implementation of new ways of interaction that provide freedom and flexibility in the control of privacy settings as well as access policies for mobile applications has allowed for higher levels of security and reliability on the users' side. In this case, a study on the process of applications re-designing must be developed along with different types of tests. In this sense, the objective of this research was to analyze issues related to privacy, in regard to legal aspects and user's experience, based on the assessment of design products in mobile Apps.

2 Background

2.1 Privacy

Privacy is a fundamental right guaranteed by the Universal Declaration of Human Rights, which was adopted and proclaimed by the United Nations General Assembly and states in its Article XII that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks" [12].

The legal field in Brazil provides specific definitions in different spheres regarding privacy and public life. Reference [13] defines a triad of legal rights without which privacy cannot be guaranteed: (1) the right not to be monitored; (2) the right not to be registered and (3) the right not to be recognized. The author states that any information that is judged irrelevant for a system, should not be required or stored, and this includes photographs as well as unauthorized video and audio recordings. The right not to be recognized is understood as the right not to have photographs, videos or other records published in the media.

According to Durlak in [14] privacy is a human value consisting of four elements he calls rights. Reference [14] divides these rights into two categories. The first category includes three rights that an individual can use to fence off personal information seekers: solitude, anonymity and intimacy. The second category contains those rights an individual can use to control the amount and value of personal information given out: reserve (methods of dissemination controling one's personal information).

Based on the analysis of the definition provided by the Houaiss dictionary for the term *private* [15] "3. that which belongs to an individual in particular; 4. that which is personal and not to be expressed in public; 5. restricted, reserved to the rightful owner; confidential", several situations can be identified where these concepts are abused. The unauthorized use of users' data, the disclosure of their information and third-party

publication without the user's consent, or even when the user himself discloses personal information due to unawareness or negligence are examples of situations where the right to privacy is violated. In this sense, privacy is a concept closely linked to the concept of anonymity regarding the wish to remain unidentified or even be noticed.

Reference [14] introduces a classification of the different types of privacy:

- Personal privacy involves the privacy of personal attributes.
- Informational privacy: the protection of unauthorized access to information itself. It includes: personal information, financial information, medical information, information related to transactions over the Internet.
- Institutional privacy: it refers to the custody of organizational private data (marketing strategies, data on sales and products) as well as information on the business itself.

Vianna's concept introduces a vision of greater control regarding data, defining data protection as something essential [13, 16] offers a complementary opinion suggesting that the current society has different views on privacy. Driven by a desire to achieve recognition, members of our society reveal private issues via computational systems. Reference [16] raises the issue of the value of privacy in modern society where he considers that, for some subjects, privacy is an irrelevant concept when people in general give up their private life for the sake of recognition and prominence.

According to [17], the very concept of privacy is changing due to modern life and the advent of technology. Even if people try to keep their life intimate and private, many of their actions are registered, such as credit card payments, online shopping, mobile phone calls and Web searching among others [14, 17].

It can be noticed that the concept of privacy is subjective and can vary among different individuals and cultures. Whatever is acceptable for some people might be considered a violation to privacy for others. Privacy is also determined by the environment, the individual time and confidence awareness, which may or not encourage a person to reveal more or less information.

2.2 Brazilian Efforts Towards Preserving Privacy

The Brazilian Constitution [19], when listing Citizens' Individual and Collective Rights and Responsibilities, states in its 5th Article, Paragraph X, that "intimacy, privacy, honor and the image of people are inviolable, being the right to compensation guaranteed for property or moral damages resulting from their violation".

Still, Brazil has been concerned, along recent years, about the recurrent digital privacy and espionage problems and has consequently taken some initiatives to regulate these issues. The Internet Governance Act (Law nº 12.965, 2014) establishes principles, guarantees, rights and responsibilities for the use of Internet in Brazil. This law comprises three major aspects of Internet use: neutrality, privacy and freedom of expression. The Law states in its 8th Article that "the guarantee of the right to privacy and to freedom of expression in communication is a pre-requisite for the full exercise of the right to internet access…".

There is such a great concern about these issues in Brazil that, in a democratic way, a public debate (http://participacao.mj.gov.br/dadospessoais/) is being carried out on the preparation of a draft for a Data Protection Bill. Any person, not necessarily a Brazilian citizen, can participate with suggestions on the minutes. There is an English version available online (http://participacao.mj.gov.br/dadospessoais/2015/02/texto-do-anteprojeto-disponivel-em-ingles/).

The bill draft on data protection intends to ensure control and transparency for citizens about which data corporations and government are dealing with and how they are dealing with them. It is expected that this regulatory bill will protect citizens in all instances and sectors in which personal data are managed, establish bases for addressing issues related to surveillance and monitoring of the Internet and its applications, be aligned with international standards and, furthermore, according to principles of security and responsibility, provide for eventual user's compensation for damages.

Another initiative was triggered by the Special Commission for Human-Computer Interaction that is linked to the Brazilian Computer Society (SBC). During the IHC 2012 symposium (XI Brazilian Symposium on Human Factors in Computational Systems) a panel entitled "Great HCI Research Challenges in Brazil – Gran DIHC-BR" was put up to receive proposals from the HCI community. According to the report that summarizes the proposals [20], the great challenges that resulted from the panel "represent the HCI community's reflection on the field, likely to inspire and guide the course of HCJ research in the country for years to come. We hope that these Great Challenges serve as a guiding principle for the development of projects to produce significant scientific advances, with social and technological applications".

The proposals discussed in the panel were divided into five thematic groups. The G4 - Human Values, considers "Privacy within the Connected World" as one of the challenges, bringing forward issues such as: "What information is collected and what can it, directly or indirectly, expose about the users? How can users be allowed to anticipate the combination of parameters in terms of what information about them is visible and to whom? How can harmonious levels of sociability and privacy be guaranteed?" [21].

The report proposes the discussion and publication of articles within the field and the survey of design products (hardware, software, websites, etc.) that explicitly consider these aspects, among other strategies to deal with this challenge. One of the difficulties and barriers for the success of the mentioned studies is "the difficulty in aligning research and the creation of legal regulations, due to the lack of communication between the academic and the legislative spheres. Those who make laws is not necessarily involved in or knowledgeable about the research studies in the area." In this sense, the discussion proposed in this paper articulates the elements above, comparing concepts and legal regulations with technical aspects related to privacy in mobile applications.

2.3 Related Works

Privacy exposure is critical in ubiquitous and or pervasive systems. This is due to the fact that applications need to capture and share context data from users to be able to

take advantage of their features. According to [6], there are growing concerns about the misuse of location data by third parties, which fuels the need for more privacy controls in such services. Reference [5] state that "the pervasive computing paradigm raises the level of the challenge to protect privacy of end-users, mainly due to the fact that devices operating in such an environment will be embedded in the fabric of the everyday life and will exhibit enhanced tracking and profiling capabilities".

In the authors' view, basic characteristics introduced by these systems generate the new Privacy Enhancing Technology (PET), since "appropriate mechanisms that are able to evolve with the needs of the users and interact with them in order to meet their privacy requirements" are necessary. Reference [10] argue that "when sensors capture data about people, and digital systems interpret and respond to that data below the line of user visibility, two fundamental questions arise. First, are current notions of consent relevant in the emerging class of pervasive systems and, secondly, what are the practical consequences of dealing with consent for such environments?".

According [8], we live in a world where people often decide to sacrifice their informational privacy for useful or free services. The author's opinion is that "privacy is a right, but security is a primary state function" since "a loss of privacy can result immediately in a loss of security when data become public or leak". He then adds: "we must ensure that our social norms reflect not only the pleasure we get from visibility to the network, but also the important benefits that protecting privacy will produce for society as a whole. This can't be a matter of regulation, but rather depends on us all taking our responsibilities seriously."

With the emergence of more lenient privacy protection laws, those who develop systems should pay attention to the compliance of legal requirements and users' satisfaction. Reference [7] proposed a technique called Privacy Interface Analysis where "the human factors requirements for effective privacy interface design can be grouped into four categories: (1) comprehension, (2) consciousness, (3) control, and (4) consent". This technique shows how interface design solutions can be used when developing a privacy-enhanced application or service.

Reference [9] conducted an online study aimed at understanding the preferences and practices of LSS users in the US. The authors found that the main motivations for location sharing were to connect and coordinate with one's social and professional circles, to project an interesting image of oneself, and to receive rewards offered for 'checking in.' In this study, there are design suggestions, such as delayed disclosure and conflict detection, to enhance privacy-management capabilities of LSS. They are:

- Delayed disclosure: this usage suggests that it may be possible to mitigate many location-sharing regrets and privacy violations simply by decoupling the time of location broadcast from the time of the decision to share location (e.g., by daily or weekly batching).
- Special handling of purpose-driven sharing. In cases where location disclosures serve an immediate and specific purpose, specialized handling could provide better privacy depending on the purpose. In the way of example, the authors mention recommendations made in situations which might be published later on.
- Conflict detection. Over 20% of research respondents who experienced location-sharing regrets mentioned that the regret was caused by being caught lying.

For example, a user might be cautioned before sharing location if his or her calendar indicates a conflicting event at another location.

Luger and Rodden [10], through a review of multidisciplinary perspectives on consent and technology, offer a set of recommendations to designers as considerations for future systems design: (i) electronic consent mechanisms (ECMs) must cease to be designed around 'moments in time' and allow for negotiation; (ii) systems should enable establishment of user expectations and development of norms; (iii) systems should be sensitive to third-party interactions; and (iv) we should move beyond designing for user control towards designing for user autonomy.

In the analysis of specific studies on privacy in social networks [1–3], it is evident that there is a common concern about understanding human attitudes related to the behavior when faced with privacy issues: security awareness, confidence awareness, the influence of cultural issues, the influence of knowledge about the risks related to a high exposure of private information as well as the necessary skills to maintain protection.

3 Methodology

The issues discussed in this article are part of a research project in an international partnership between France and Brazil[1] in which an architecture that supports the development of ubiquitous applications called Devices, Environments and Social Networks Integration Architecture (DESIA) [18] was proposed. The concepts of the proposed DESIA architecture are detailed in terms of services, requirements and architecture. The main services offered by DESIA are: collection, storage and query of context information; situation inference; user and environment interfaces; and integration with external sources of data. The functional requirements were grouped in seven different categories including Location-related requirements; Privacy; and Security and permissions. Examples of Privacy-related requirements are:

PRIV-01. The architecture must permit setting the user's privacy options.
PRIV-03. The architecture must permit defining rules to obtain third parties' information, considering confidentiality, reputation mechanisms and information classification, for example.
PRIV-05. The system must include documents detailing the Terms of Use and Privacy Policy of the application, which must be available for users and these must be explicitly notified about any alteration.
PRIV-06. The system must provide dynamic solutions aligned with the application features so that users may choose what information they desire to be visible or to be shared in which contexts, so as to safeguard their privacy.

Associated Non-functional requirements are:

[1] Sponsored by Fapemat, Brazil.

NFR-03. The system developers must use techniques according to usability regulations.
NFR-04. The architecture must consider cultural aspects.
NFR-05. The architecture must provide Terms of Use and Privacy Policy according to existing laws in each country.

The efforts committed to this stage of the research, of an exploratory character and qualitative approach, are included in the detailed explanation of these functional and non-functional requirements. They are based on: (1) the analysis of how applications have implemented terms of use and privacy policies; (2) studies related to the study object in the area of HCI; and (3) the study of regulations, considering the need to understand the whole context and the ease of use of the systems. In order to achieve this, concepts on privacy and the legal apparatus in this area in Brazil were analyzed, especially in the Marco Civil da Internet [11] (Brazilian Internet Governance Act) and in the Data Protection Bill.

Aiming to analyze privacy features and settings of the applications, five applications were inspected, along with their terms of use and privacy policies. Based on the survey of the applications' design products, problems and solutions are discussed in order to improve user experience from the perspective of privacy.

The results of this stage will help elaborate guidelines in favor of the quality of user experience in ubiquitous systems from a privacy perspective, being this a future stage in the study.

4 Exploratory Study

The exploratory study involved the analysis of the Terms of Use and Privacy Policy of five randomly chosen applications: Viber (text messaging and phone calls), Waze (community-based GPS), Facebook Messenger (instant messaging). Snapchat (picture-based messaging) and Google Now (intelligent personal assistant). This resulted in a report offering a critical analysis of the privacy problems found and suggestions to improve users' experience.

Among the applications that were analyzed, Snapchat, Viber and Waze do not present the text for the Access Policy and/or Terms of Use in Portuguese, which makes reading difficult and probably leads the user to simply agree having no idea of what is written. Other applications, even though they present a Portuguese version of the Terms of Use, make it clear that, in case of divergence, the English version is the only one that will be considered.

In some cases, the labelling is in Portuguese, but the section's contents are in English. Depending on the users' literacy level, these issues may interfere with the use of the application causing doubts as they go against usability principles such as ease of use, consistency and standardization.

Reference [23] state that in Human-Centered Informatics "it is important to understand people's situated interactions with information, in other to help us understand how to better support them". The authors propose a model with core elements of an anticipation-based information journey, with thinner arrows indicating feedback,

anticipating demands. Anticipating the demands of interpretation and validation, it is possible to select sources in which they have confidence while also selecting topics (or reinterpreting a question) in order to minimize the interpretation demands.

Moreover, this kind of situation could have been foreseen in legal rules of the countries where the applications are used; in the case of Brazil, the Internet Governance Act should discredit any application that does not make the Terms of Use text available in the country's native language.

In general, the Terms of Use and/or Privacy Policy are long texts to be read on a smartphone's interfaces. In some applications such as Waze and Facebook Messenger the interfaces are offered with a summary data and services that the application can access. However, it can be noticed that these interfaces are purely informative and they do not allow any type of choice on the user's part. Application users are nowadays made hostages considering that in order to use the application the user must accept the Terms of Use and other policies in full.

The installation of the Facebook Messenger application for messaging has recently become mandatory for Facebook users. It is very likely that thousands of Facebook users have not bothered to read the Messenger Terms of Use. Furthermore, when modifying the decoupling of the application to the social network, many users became confused with alterations such as: the request to access the camera or the microphone in the mobile device and published news on the application's permissions on an Android system [22].

In view of this, three items considered problematic in the Terms of Use were chosen to be described:

1. Permission to access the call history in the device, including incoming and outgoing calls. This permission simply creates log files in the device, but other malicious applications can access this information without the user realizing. This kind of permission may challenge security policies, since the creation of log files and the fact that malicious applications may access this information turn the risk of improper use imminent.
2. Permission to access information on the user's contacts, including the frequency with which the user communicates via e-mail or other means of contact. Such an authorization may indicate a breach in security, since as the App scans the user's device looking for other Apps to synchronize information, confidential data might be used without the user's permission. Even when this information is used to improve the user's experience in using the application, the user has no knowledge nor has he consented to this action.
3. Permission to access the user's personal information that is stored on the device, such as contacts' name and data. This means that the company may identify the user and keep a customer database.

Along this short list, two kinds of problem can be identified: first, permission is unrestricted, i.e. the term does not clarify that the application may access the user's whole contact list because it needs this access when the user wants to use a contact to make a call through the App. In this case, the text does not help the user to trust the application. The second problem is that it is difficult to understand the application's real need to access certain data, such as the above-mentioned situations.

Such situations are not only found in Facebook Messenger, but in other applications as well. On the on hand, the user needs the services, agility or convenience the application offers; on the other hand, the application does not help the user to establish an adequate confidence for its use. Even so, there is a concern in the sense that many users simply ignore the risks and terms of use, either because of their need or hurry to use the application or in order to feel part of a social group.

In another application (Viber), privacy policies lead users to understand that their information is protected. Yet, a study carried out on this application by researchers of the UNH Cyber Forensics Research & Education Group at the University of New Haven [24] in the US identified, by testing mobile phones in 2014, that the application sent and stored the users' messages on their servers without encrypting them – including images, pictures, videos, doodles and location. As privacy is linked to data security, the group pointed out, in terms of solution: "Make sure the data is encrypted over a tunnel when it is sent. Also make sure the data is encrypted properly when saved, and authenticated when being accessed".

In order to use the Google Now App, for example, the user needs to authorize the application to collect various personal data. This allows a constant surveillance on the application's part. An interesting design solution in this application is that google makes access to the collected data available to the user so that, in case he does not want this information to be visible, he can simply delete it. In case the user does not want any information to be recorded, he can delete everything and cancel the registration definitely. However, if the user does this, he will not be able to access all the application's features, since the he depends substantially on personal information to be able to act. The Privacy Policy (https://www.google.com/intl/pt-BR/policies/privacy/) is clear concerning the user's collected data, how the company uses this information and how it is protected.

Waze, also Google's, is an application that provides a lot of interaction with/for the user, considering as key features issues involving privacy. It allows the user to share his routes, favorite places, information on accidents and traffic jams, among other data. Accordingly, people may have their personal activities disclosed, also through the integration of social networks. At the same time, the application allows that, in the case the user does not want to share anything, he can just use the GPS in a standard manner. In addition, in order to use the application in all its features, the user should not be bothered by, for example, the sharing of his information on alternative routes, if he did accept and authorize the Terms of Use.

Another interesting solution for these applications, regarding the deletion of users' data, an issue that has been put forward by Internet regulatory laws, is the specification of the maximum latency time that the user data may be stored after canceling the account. Except for cases where the information is part of a lawsuit, the user may be notified when the data has been definitely excluded from the server. Furthermore, applications must be careful not to have user data stored by third-party applications without prior notice, not to cause conflict between Terms of Use and Privacy Policies.

According to Article X in the Internet Governance Act, "the custody and availability of the connection and access logs to Internet applications to which this law refers, as well as that of personal data and the contents of private communications, must meet the preservation of intimacy, private life, honor and image of the directly or

indirectly involved parties". According to the law, "the content of private communications will only be made available by means of a court order".

The Draft Bill on Data Protection states in its Article 6 nine principles on the processing of personal data. The following two principles serve as example: "I – Principle of purpose, by which the processing must be made according to legitimate, specific and explicit purposes known to the holder; II – Principle of adequacy, according to which the processing must be compatible with the aimed purposes and with the holder's legitimate expectations according to the processing context". Even though the text is still being discussed, it can be noticed how the existing Terms of Use and/or Privacy Policies will need to be improved, considering that they are usually generalist, superficial and not very explicit about the requirements of use and processing of personal and sensitive data.

In addition, the Draft Bill on Data Protection explicitly deals on the difference between personal data, sensitive data and anonymous data. Once approved, even after alterations, the Data Protection Law may become a landmark in Brazil to safeguard fundamental rights such as freedom, intimacy and privacy of a person.

One possibility, during the design or re-design of applications, viewing to meet privacy regulations, is the mapping between the items in the Terms of Use and the application's features in order align them with the systems requirements.

5 Conclusions

Privacy, as a software requirement, needs to be guaranteed by technical and legal means. Understanding privacy as a social and cultural process, it must be delivered to the user in a simple and clear manner, since he will be continuously interacting with computer systems. Privacy modeling is a challenge in mobile applications, especially those that require location-sharing services.

If on one hand we have a wealth of interesting, useful, free solutions, on the other hand we need to produce terms of use and privacy policies that are clear to users and in agreement with legal regulations. Faced with so many privacy-related challenges, the issue is how to structure users' consent to the use of their data. How can the design of applications favor reliability and provide the user with security. How can terms of use be developed in order to make them more interactive?

Another relevant issue is the fact that many companies make their terms of use so that they can protect themselves against users' misuse and not really thinking about the users. Many of the inspected applications make the user a hostage when he must accept the entire terms of use and allow more access to data than he would need so that he can use the application in all its features.

As much as interactive solutions are required, from the perspective of implementation, it is well known that it is challenging to suggest terms of use where users may choose specific items, since such choices might interfere in the system's features. However, intermediate solutions can be thought of. In addition, warnings can be given out to the user while he is using the application, not only in situations where he is disclosing private information, but also as an educational tool.

Privacy protection involves education, technology and rules. In this sense, the creation of regulations, discussing them and analyzing technological solutions must be done constantly. Certainly, these three fronts must be in harmony, since technology provides services that will result in regulations. Education in turn assumes knowledge and skills so that users may use it in the best possible way in order to, for example, understand and have control over the privacy settings of each application.

Future stages of this research will involve interviewing professionals in the fields of sociology, law and computing. The objective is to deepen knowledge on the concept, and social, legal and technological issues surrounding the understanding of privacy and terms related to the establishment of confidence, the social circle among others. A quantitative research will be carried out with users of X, Y and Z-generation ubiquitous applications, as a follow up to works the group has already started [4]. This research intends to understand the behavior of the three different generations faced with the use of mobile technology as well as analyze how they react to the privacy and security issues. Results will help produce guidelines to enhance use experience in ubiquitous systems from the perspective of privacy.

References

1. Nosko, A., Wood, E., Molema, S.: All about me: Disclosure in online social networking profiles: the case of FACEBOOK. Comput. Hum. Behav. **26**, 406–418 (2010)
2. Fogel, J., Nehmad, E.: Internet social network communities: risk taking, trust, and privacy concerns. Comput. Hum. Behav. **25**, 153–160 (2009)
3. Shin, D.: The effects of trust, security and privacy in social networking: a security-based approach to understand the pattern of adoption. Interact. Comput. **22**, 428–438 (2010)
4. Borges, G., Ribeiro, T., Maciel, C., Souza, P.C.: Who is this guy who liked my picture? privacy control mechanisms on Facebook for Generations X and Y. In: 15th International Conference on Enterprise Information Systems (ICEIS 2013), France, pp. 179–186 (2013)
5. Dritsas, S., Tsaparas, J., Gritzalis, D.: A generic privacy enhancing technology for pervasive computing environments. In: Fischer-Hübner, S., Furnell, S., Lambrinoudakis, C. (eds.) TrustBus 2006. LNCS, vol. 4083, pp. 103–113. Springer, Heidelberg (2006)
6. Bilogrevic, I., Jadliwala, M., Kalkan, K., Hubaux, J.-P., Aad, I.: Privacy in mobile computing for location-sharing-based services. In: Fischer-Hübner, S., Hopper, N. (eds.) PETS 2011. LNCS, vol. 6794, pp. 77–96. Springer, Heidelberg (2011)
7. Patrick, A.S., Kenny, S.: From privacy legislation to interface design: implementing information privacy in human-computer interactions. In: Dingledine, R. (ed.) PET 2003. LNCS, vol. 2760, pp. 107–124. Springer, Heidelberg (2003)
8. O'Hara, K.: Are we getting privacy the wrong way round?. In: Internet Computing, IEEE, vol.17, no. 4, pp. 89–92, July–August 2013
9. Patil, S., Norcie, G., Kapadia, A., Lee, A.J.: Reasons, rewards, regrets: privacy considerations in location sharing as an interactive practice. In: Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS 2012). ACM, NY, USA (2012)
10. Luger, E., Rodden, T.: Terms of agreement: rethinking consent for pervasive computing. Interact. Comput. **25**(3), 229–241 (2013)
11. Lei N° 12.965: Marco Civil da Internet (2014). http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

12. ONU: Declaração Universal dos Direitos Humanos. http://portal.mj.gov.br/sedh/ct/legis_intern/ddh_bib_inter_universal.htm
13. Vianna, T.L.: Transparência pública, opacidade privada: o Direito como instrumento de limitação do poder na sociedade de controle. Tese de doutorado, Universidade Federal do Paraná (2006). http://www.midiaindependente.org/media/2008/05/419863.pdf
14. Kizza, J.M.: Ethical and Social Issues in the Information Age, 5th edn. Springer, New York (2013)
15. Houaiss, A.: Dicionário Eletrônico Houaiss da Língua Portuguesa. Objetiva, São Paulo (2012)
16. Sibila, P.: La intimidad como espectáculo, 1st edn. Fondo de Cultura Económica, Buenos Aires (2008). http://cmap.javeriana.edu.co/servlet/SBReadResourceServlet?rid=1J2SK927M-22DBXQG-1TB
17. Jennings, C., Fena, L.: Priv@cidade.com – Como preservar sua intimidade na era da internet. Futura, São Paulo, SP (2000)
18. Maciel, C., Souza, P.C., Viterbo, J., Mendes, F.F., Seghrouchni, A.E.F.: A multi-agent architecture to support ubiquitous aplications in smart environments. In: Fifth International Workshop on Collaborative Agents - Research & Development (CARE) - 13th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2014), Paris-France (2014)
19. Constituição da República Federativa do Brasil (1998). http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm
20. Baranauskas, C., Souza, C.S., Pereira, R. (Orgs.): I GranDIHC-BR - Grandes Desafios de Pesquisa em Interação Humano-Computador no Brasil. Relatório Técnico. Comissão Especial de Interação Humano-Computador (CEIHC) da SBC (2014)
21. Maciel, C., Pereira, V., Hornung, H., Piccolo, L.G.S., Prates, R.O.: Valores humanos. In: Baranauskas, Souza and Pereira (orgs.) I GranDIHC-BR — Grandes Desafios de Pesquisa em Interação Humano-Computador no Brasil. Relatório Técnico. Comissão Especial de Interação Humano Computador (CEIHC) da SBC, pp. 27–30 (2014)
22. Fiorela, S.: The Insidiousness of Facebook Messenger's Android Mobile App Permissions (2013). http://www.huffingtonpost.com/sam-fiorella/the-insidiousness-office_b_4365645.html
23. Blandford, A., Attfield, S.: Interacting with information. Synth. Lect. Hum.-Centered Inf., Morgan & Claypool **3**, 1–99 (2010)
24. UNHCFREG: Viber security vulnerabilities: do not use Viber until these issues are resolved (2014). http://www.unhcfreg.com/#!Viber-Security-Vulnerabilities-Do-not-use-Viber-until-these-issues-are-resolved/c5rt/BB4208CF-7F0A-4DE1-92A4-529425549683