Knowledge as an effective tool to protect ICT users' privacy. The layered informed consent as 'opt-in' model

El conocimiento como arma más efectiva para proteger la privacidad de los usuarios de las TIC. El consentimiento informado activo por capas

Amaya Noain Sánchez. Universidad Complutense de Madrid. (amayanoain@ucm.es)

Abstract:

The present study contributes to the research on communication processes and privacy issues in Social Networks Sites (SNS) and the specific implications for individuals' informational self-determination in these types of technical environments. The central aim of this project is to investigate whether users are in a position to achieve their desired privacy level with the technical tools and information provided by these online social spaces, to delineate the potentially dangerous context for their privacy and to design an efficient way of introducing new European Commission's regulation on informed consent in those scenarios. For this purpose, we use an ethnographic approach in conjunction with technical modelling tools. In a first phase of study, we tested competences and knowledge of a group of users of SNS, especially focusing on their attitudes towards privacy and their own protection strategies. The initial empirical findings of this phase suggest that despite their privacy concerns, users tend to show risky practices when introducing their private information on the Net. To assess if this fact is due to information shortage and coevaluate the importance a correct flow of information has to prevent privacy breaches, in the second phase we will provide participants with an informed consent tool.

Key words:

Privacy; new technologies; Social Network Sites; informed consent; ethics.

Resumen:

El presente estudio contribuye a la investigación en procesos de comunicación y dilemas concernientes a la privacidad en las Redes Sociales, así como las posibles implicaciones específicas que condicionan la autodeterminación informativa del usuario en el ecosistema digital. El propósito específico es investigar cuándo los usuarios están en posición de obtener un nivel de privacidad deseado haciendo uso de las herramientas técnicas proporcionadas por dichos espacios sociales en la Red, delinear los contextos potencialmente peligrosos para su privacidad y diseñar una manera eficaz de introducir, en dichos escenarios, el consentimiento informado propuesto por la Comisión Europea. Para ello, utilizaremos una aproximación etnográfica junto con herramientas tecnológicas. En una primera fase, hemos evaluado las competencias, conocimiento y prácticas de un grupo de usuarios de Redes Sociales incidiendo especialmente en sus actitudes y estrategias de protección. Los resultados de la fase inicial sugieren que, a pesar de sus preocupaciones, los usuarios tienden a realizar prácticas que ponen en peligro su privacidad. Para analizar si este hecho se produce por falta de conocimiento y evaluar el papel que un correcto flujo de información tiene para prevenir dichas intromisiones, en una segunda fase de estudio proporcionaremos a los participantes una herramienta de consentimiento informado.

Palabras clave:

Privacidad; nuevas tecnologías; redes sociales; consentimiento informado; ética.

1. Introduction

Managing the boundary between private and public information on the Internet can be quite controversial since the limit is neither universal nor static. The same happens with privacy concepts which depend on each culture and uses (Capurro, 2005: 37). Additionally, privacy protection, that is to say, the right to privacy is often expressed in terms of a dichotomy - private and public sphere. This distintion, however, is highly useful in the fields of Philosophy and Law, although inefficient in online scenarios where the limits are not so clear.

Still, as online privacy expert Nissenbaum has noted, many theories of privacy fall short of properly addressing the problem of privacy in public spaces, either dismissing it or ignoring it altogether (Nissenbaum, 1998: 560). Nissenbaum argues that in order to understand privacy issues in public environments we have to take into consideration that privacy depends on 'contextual norms' which are the basis for an individual deciding when, where, and under which circumstances information provided should be accessible (Nissenbaum, 2004: 120).

Nevertheless, since the arrival of SNS, understanding informational norms has become not so easy. Besides, although offline privacy is mediated by highly granular social contexts, SNS lack much of this granularity and thus users find themselves incapable of exercising their right to informational self-determination (Latulipe, Hull & Lipford, 2010: 289) Moreover, the ambiguity of some SNS such as Facebook, make it difficult for users to determine whether it is a public space or not (Young & Quan-Hasse, 2013:482) and even when users are aware of that, third party developers create added functionalities that would break the contextual norms described by Nissenbaum (Latulipe, Hull & Lipford, 2010: 289). Therefore, to use efficiently the informational norms mentioned in this theory and be able to decide whether they put their personal data on the Internet, users need to receive a correct flow of information, hence, the importance of informed consent.

Following this reasoning, the purpose of the following research is to identify scenarios created by SNS where personal data can be endangered, linking every possibly risk with an informational tool to avoid it. SNS are particularly suited for observing privacy issues because they technically comprise all applications on the web 2.0, and are dynamically structured (Ilyes, Poller & Kramm, 2013: 3). Among all SNS, Facebook seems to lead to many more ethical dilemmas than others since 'it makes what was previously obscure difficult to miss -and even harder to forget- Those data were all there before but were not efficiently accessible' (Boyd, 2008: 15).

For that reason, after describing thematically the variety of vulnerabilities users may suffer, the study will focus on the suitable way to provide people with the amount of information they may need to decide whether or not to put their personal data on the Internet. To fulfil this purpose, we will use a new model of informed consent: layered informed consent as 'opt-in' model. Such is the importance of informed consent that the European Commission will modify the current Data Directive to establish new regulation, which will predictably include it.

2. Methodology and research phases

In the first phase of research, we tested the competences of a group of Communication Ethics students on TIC usage. We used ethnographic observation and interview techniques to collect data on the behaviour of users, focusing on SNS, especially on Facebook. Our study participants gave us permission to observe the actions they took while examining their own Facebook accounts and, after that, they provided us with a detailed description of such actions. (Ilyes, Poller & Kramm, 2013: 3). Thanks to this procedure, they also contributed to show us when and under what circumstances they put new personal material such as, for instance, photos, videos, or decided to share any geographical information on their profiles, as well as the ways in which they allowed others to access the information.

Using ethnographic models and techniques to analyze users' behaviour helped us to identify complex issues related to their privacy concerns when sharing personal data on the Internet. Additionally, the value of this kind of approach has already been demonstrated by several studies and previous research on the topic (Cunningham, Masoodian & Adams, 2010; Kramm, A., 2011). In a second phase of research we will provide users with an application of informed consent as "opt-in" model to examine whether providing a correct flow of information is able to change user's decisions concerning the sharing of private information on SNS.

2.1. Recruitment and demographics

By June 2014, 80 people completed the questionnaire. All of them were university students - all the interviewees came from the Ethics subject of the Communication degree- and the majority of them were under 23 years old. Subsequently, we selected 30 people from this pool to interview. Among the 30 participants, whose ages ranged from 20 to 23, all of them used SNS, particularly Facebook. In fact, 16 of them visited Facebook multiple times per day, 21 of them visited Facebook about once per day and the remaining 3 users visited Facebook less than once per week.

2.2. First phase. Research questions and open interviews

Most previous work focused on users' privacy attitudes and use of privacy settings. At the very beginning of the survey a previous questionnaire was given to balance our interview participants across gender, age, other occupation, frequency of SNS usage and other semantic tools knowledge.

After that, the semi-structured interviews included open-ended questions about users' motivations and use of SNS, personal privacy perceptions and attitudes toward SNS usage and, in particular, towards Facebook privacy settings. In addition to that and to guide this process of ethnographic observations we provided our study participants with a series of open-ended questions they could consider. These questions were divided into the following categories:

(1) Participants' personal concepts of privacy,

(2) General overview and knowledge of SNS,

(3) Strategies they take to protect their privacy on SNS

(4) Facebook usage.

(5) Participants' risk perceptions.

(6) Level of personal satisfaction about privacy protection tools.

Subsequently, interviewees were asked to log into their SNS accounts to have a conversation with the researchers about their experiences.

2.3. Second phase. Application of Informed consent by layers

After analysing the results, we tried to identify whether users' privacy concepts are not at work in practice or whether they simply do not understand the privacy settings provided by SNS. In a second phase of our research, therefore, we will provide our participants with extra information to compare if their final decisions when publishing private information are conditioned by information deficiency.

In this sense, the active informed consent by layers or 'opt-in' model is the central improvement research in progress introduces. Usually, informed consent is provided as an 'opt-out' model which is based on a notion of passive consent and does not protect users from being tracking or targeting. Nonetheless, settings by default should assure the highest level of privacy, for that reason we propose to implement a new model of consent to ensure that users control their data from the beginning.

In our study, informed consent will be provided to participants in two layers: the first will show basic information about the consequences of improving the visibility of some kind of personal data while the second will supply deeper information, illustrating with examples or simulations such consequences. The results of this second phase will allow us to understand whether users' decisions are due to information shortage or intention.

3. Results and discussion

First phase: The wide majority of users tend to behave in risky ways when using Social Network Sites, often due to lack of knowledge and sometimes because of their low risk perception. Following this assumption and, after analysing all the data collected, we identified several risk factors:

-Users' actions and use of privacy settings led to the 'privacy paradox':

The majority of our interviewees claimed to be aware of their privacy information, checking their privacy settings on Facebook. The majority of participants reported that they only shared information with people they already knew, customizing by default settings and rejecting friend requests if they did not know or recognize the person.

Nonetheless, we could observe users' paradoxical behaviour relating to privacy concerns on SNS, in line with Barnes' 'privacy paradox' (Barnes, 2006). For example, only some of them reported having checked their privacy settings regularly. Moreover, the majority of worries were not about privacy protection: users only showed regrets when there had been a possible breach in reputation. (Lampe *et al.* 2008:720; Madden & Smith, 2010: web; Young & Quan-Hasse, 2013: 483)

-There is a huge gap between competences or information users receive and their privacy protection attitudes. As an overall trend, interviewees were not aware of the quantity of privacy and personal information about them is available on the Net. Nevertheless, those with more knowledge seemed to show strategies of self censorship in order to have their privacy protected and even showed mental models and protection strategies (Gross & Acquisti, 2005: web; Lampe *et al.*, 2008:723; Boyd & Hargittai, 2010: web) Moreover, the results suggest that users at different life stages tend to have different mental models to separate their professional sphere from their personal sphere (Wang *et. al.*, 2011: 10).

In a second phase we will try to determine whether a correct flow of information is able to change users' decision when introducing privacy information in SNS such as Facebook.

3.1. Research limitations

The main drawback of analysing the phenomenon of New Information and Communication Technologies is its changing character and its multidisciplinary nature, since this subject is always renewing. Additionally, we can underline the following limitations:

- Methodological limitations: the use of ethnographic approach is linked to limitations such as difficulty in identifying privacy concerns, particularly those which come from deeply personal conceptions or those which are "too private" for users to be showed (Cunningham & Masoodian, 2010: 35) and, therefore, be observed in the interview.

- Survey size: Our survey participants were recruited from Communication Sciences, thus our results and findings may not necessarily be representative of the whole population using SNS. The results of the study, therefore, can only be generalized to university students.

4. Expected results and spreading possibilities of the research and conclusion

This research was designed to identify users' privacy concerns when using SNS and to evaluate the leading role of a correct flow of information in such scenario. Needless to say, future research could seek to expand the analysis by evaluating other users groups to compare results; however the present approach aims to set a precedent or model for future research on the topic. As a result, the findings of the present project can build a bridge to connect users' privacy needs with computer developers.

As a conclusion and to analyse the conflict between data protection and the capabilities of new technological applications, we must start from admitting a premise: privacy problems have two realities depending one on another, the technical side and the users' action. Therefore, we must affirm that those theories focusing on 'sociotechnical privacy' (Petra & Ochs, 2013:75) will play an essential role when identifying privacy concerns in the future. Moreover, privacy will keep on playing an essential role in the design of information technology, for that reason our understanding of what privacy is and how it operates might become as sophisticated as the technologies involved (Palen & Dourish, 2003: 130).

Therefore, and taking into account that the main actor of new tools is undoubtedly the citizen, all the agents involved are duty bound to improve a culture of privacy (Buchmann, 2013: 22) particularly, since the correct use of New Information and Communication Technologies is a key concept to promote and preserve the values of a democratic society.

We expect the findings of current research to supply viable solutions both for users to improve their privacy needs and for promoting a safer use of New Information and Communication Technologies.

Acknowledgements:

We would like to thank Petra Ilyes, Laura Kocksch and Andreas Kramm for their exceptional guidance on ethnographic studies.

5. References

Barnes, S. B. (2006): "A privacy paradox: social networking in the United States", *First Monday*, vol. 11, n. 9. Disponible en: http://firstmonday.org/ojs/index.php/fm/article/view/1394/1312 [Consultado el: 15/05/2013].

Boyd, D. y Hargittai, E. (2010): "Facebook privacy settings: who cares?", *First Monday*, vol. 15, n. 8. Disponible en: http://firstmonday.org/article/view/3086/2589 [Consultado el: 05/06/2013].

Buchmann, J. (ed.) (2013): *Internet Privacy: Taking opportunities, assesing risk, building trust.* (Acatech – Deutsche Akademie der Technikwissenschaften, acatech STUDY), Heidelberg *et al.*: Springer Verlag.

Capurro, R. (2005): "Privacy. An intercultural perspective", *Ethics and Information Technology*, vol. 7, n. 1, pp. 37- 47.

Gross, R. y Acquisiti, A. (2005): "Information revelation and privacy in online social networks", *Proceedings of ACM Workshop on Privacy in the Electronic Society'05*. Nueva York: ACM Press, pp. 71-80.

Hull, G.; Lipford, H.R. y Llatulipe, C. (2010): "Contextual gaps: privacy issues on Facebook", *Ethics and Information Technology*, vol. 13, n. 4, pp. 289-302.

Ilyes, P. y Ochs, C. (2013): "Sociotechnical Privacy. Mapping the Research landscape", *Tecnoscienza, Italian Journal of Science & Technology Studies*, vol. 2, n. 4, pp. 79-91.

Ilyes, P.; Andreas, P. y Kramm, A. (2013): "Designing privacy-aware online social networks - A reflective socio-technical approach" *CSCW '13 Measuring Networked Social Privacy Workshop*, February 23-27, 2013, San Antonio, Texas, United States. Disponible en: http://testlab.sit.fraunhofer.de/downloads/Publications/poller_osn_design_cscw13_workshop_camera_ready_rot.pdf [Consultado el: 25/05/2013].

Kramm A. (2011): "The field site as a tool: mixed methods in social network studies", *Graduate Journal of Social Science*, vol. 8, n. 3, pp. 127-141.

Lampe, C.; Ellison, N. B. y Steinfield, C. (2008): "Changes in use and perception of Facebook", *Proceedings of the 2008 ACM conference on Computer supported cooperative work (CSCW'08)*. San Diego: ACM Press, pp. 721-730.

Madden, M. y Smith, A. (2010): "Reputation management and social media", *Pew Internet & American Life Project*, Washington. Disponible en: http://www.pewinternet.org/files/oldmedia//Files/Reports/2010/PIP_Reputation_ Management.pdf [Consultado el: 15/04/2013].

Nissenbaum, H. (2010): *Privacy in context: technology, policy, and the integrity of social life*, Stanford: Stanford Law Books.

- (2004): Privacy as contextual integrity" *Washington Law Review*, vol. 79 n. 1, pp. 101-139.
- (1998): "Protecting privacy in an Information Age: The problem of privacy in public", *Law and Philosophy*, vol. 17, n. 5-6, pp. 559-596.

Palen, L. y Dourish, P. (2003): "Unpacking "privacy" for a networked world", *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '03)*. New York: ACM Press, pp. 129-136.

Wang, Y. et al. (2011): "I regretted the minute I pressed share': A qualitative study of regrets on Facebook", *Proceedings of the Seventh Symposium on Usable Privacy and Security, SOUPS '11*, New York, n. 10, pp. 1-16.

Young, A.L. y Quan-Hasse, A. (2013): "Privacy protection strategies on Facebook", *Information, Communication and Society*, n. 16, vol. 4, pp. 479-500.