UNIVERSITY OF PIRAEUS

Privacy in Online Social Networks

Alexandra Michota

Doctoral dissertation

Department of Digital Systems

School of Information and Communication Technologies

October 2017

This doctoral dissertation of Alexandra Michota, entitled “Privacy in Online Social Networks” was examined and approved by the following examination committee:

Sokratis Katsikas, Professor
Department of Digital Systems
University of Piraeus

Costas Lambrinoudakis, Professor
Department of Digital Systems
University of Piraeus

Christos Xenakis, Associate Professor
Department of Digital Systems
University of Piraeus

Stefanos Gritzalis, Professor
Department of Information and
Communication Systems Engineering
University of the Aegean

Christos Kalloniatis, Associate Professor
Department of Cultural Technology and Communication
University of the Aegean

Maria Karyda, Assistant Professor
Department of Information and
Communication Systems Engineering
University of the Aegean

Aggeliki Tsohou, Assistant Professor
Department of Informatics
Ionian University

I would like to dedicate this thesis to my beloved family.

Declaration

I hereby declare that except where specific reference is made to the work of others, the contents of this dissertation are original and have not been submitted in whole or in part for consideration for any other degree or qualification in this, or any other University. This dissertation is the result of my own work and includes nothing, which is the outcome of work done in collaboration, except where specifically indicated in the text.

Alexandra Michota

October 2017

Acknowledgements

First and foremost, I would like to express my special appreciation and thanks to my supervisor Professor Sokratis Katsikas; he has been a tremendous mentor for me. I would like to thank him for encouraging my research and for allowing me to grow as a research scientist. His advice on both research as well as on my career have been priceless. I would also like to thank my committee members, Professor Costas Lambrinoudakis and Associate Professor Christos Xenakis for their time, interest, and insightful comments.

My sincere thanks also go to all my friends who supported me in writing, and incented me to strive towards my goal.

Lastly, I would like to thank my family. Words cannot express how grateful I am to them for all their love and encouragement. Most of all, I would like to express my appreciation to my beloved, encouraging and patient sister Afrodite whose faithful support during all the stages of my PhD and especially in the moments when there was no one to answer my queries was so appreciated. I would like to dedicate this thesis to her.

Alexandra Michota

October 2017

Abstract

The privacy of data that users share over Online Social Networks (OSNs) cannot be taken for granted. A mixture of public and private user profiles create difficulties in preserving the intended privacy levels; privacy conflicts leave a large number of personally identifiable information (PII) exposed to and accessible by unauthorized audiences. Not only the weak privacy preserving architectures of OSNs but also the tendency of the service providers to make publicly available all uploaded content types lead to inability to ensure privacy by design and by default. As a result, privacy management seems to be a hard task even for experienced users; vague guidelines and incorrect perception of the applicable privacy levels may lead to serious privacy breaches.

In this thesis, privacy in OSNs was studied both from an end user and from a provider perspective. User studies were carried out to assess the appropriateness and the adequacy of privacy controls that OSNs offer.

We found that the privacy protection levels that are offered as default by the service providers progressively tend to deactivate any privacy control there is, as multiple types of uploaded data become publicly available, without restrictions. It is also worth noting that the usability of default OSN privacy controls is low. At the same time, the complexity of these settings seems to lead to divergence between the intended and the achieved level of privacy.

We then assessed the privacy risks resulting from a number of popular user interactions with the OSNs, with an eye towards increasing the awareness of such risks among OSN users that will in turn result in motivating them to engage with protecting the privacy of their PII. To this end, we applied risk assessment methods and we proposed the use of visualization techniques to provide the users with a realistic perception of the privacy risks they face. Despite the fact that such visualization may indeed activate the end users, leading them to change their attitude against privacy risks, risk reduction strategies need to be followed by the

end users themselves, rendering them a leading role in decision making with regards to PII privacy management. To this end, we formulated proposals for managing such risks by the end user.

From the provider’s perspective, we investigated the extent of compliance of the OSN privacy protection policies with relevant regulations. We found significant divergence; in order to reduce this, we proposed a common structure for such policies that is based on the PII lifecycle.

Περίληψη

Η ιδιωτικότητα των διαμοιραζόμενων δεδομένων δε θεωρείται δεδομένη για τα ενεργά μέλη στις πλατφόρμες κοινωνικής δικτύωσης. Συνδυασμοί δημόσιων και ιδιωτικών προφίλ δημιουργούν δυσκολίες στη διατήρηση υψηλών επιπέδων ιδιωτικότητας. Οι διαφορετικές και ενίοτε αντικρουόμενες ρυθμίσεις απορρήτου αφήνουν πολλά προσωπικά δεδομένα εκτεθειμένα και προσβάσιμα από μη εξουσιοδοτημένους χρήστες. Όχι μόνο οι αδύναμες αρχιτεκτονικές ιδιωτικότητας των κοινωνικών δικτύων αλλά και η τάση που έχουν οι πάροχοι κοινωνικής δικτύωσης να κάνουν κάθε τύπο δεδομένων που ανεβαίνει στα προφίλ των χρηστών δημόσια διαθέσιμο, αδυνατούν να εγγυηθούν προστασία της ιδιωτικότητας από το στάδιο του σχεδιασμού ή προστασία της ιδιωτικότητας εκ κατασκευής. Αυτό έχει ως αποτέλεσμα η διαχείριση της ιδιωτικότητας να αποτελεί δύσκολη διαδικασία, ακόμα και για τους πιο έμπειρους χρήστες. Επιπρόσθετα, ασαφείς οδηγίες και λανθασμένη αντίληψη των επιπέδων ιδιωτικότητας που εφαρμόζουν οι χρήστες μπορούν να οδηγήσουν σε σοβαρές παραβιάσεις ιδιωτικότητας.

Σε αυτήν τη διατριβή, εξετάσαμε την ιδιωτικότητα στα κοινωνικά δίκτυα τόσο από την οπτική του τελικού χρήστη όσο και από εκείνη του παρόχου υπηρεσιών κοινωνικής δικτύωσης. Πραγματοποιήσαμε μελέτες χρηστών προκειμένου να αξιολογήσουμε την καταλληλόλητα και την επάρκεια των εκάστοτε ρυθμίσεων προστασίας της ιδιωτικότητας που προσφέρουν τα κοινωνικά δίκτυα.

Διαπιστώσαμε ότι τα επίπεδα προστασίας της ιδιωτικότητας που παρέχονται ως προεπιλογή από τον πάροχο κοινωνικής δικτύωσης, χρόνο με το χρόνο τείνουν να απενεργοποιήσουν κάθε ίχνος ιδιωτικότητας των προσωπικών δεδομένων, αφού πολλαπλοί τύποι δεδομένων που αναρτώνται στα κοινωνικά δίκτυα είναι δημόσια προσβάσιμοι, χωρίς περιορισμούς. Επίσης, αξίζει να σημειωθεί ότι η χρηστικότητα

των ρυθμίσεων προστασίας της ιδιωτικότητας στα κοινωνικά δίκτυα είναι χαμηλή. Ταυτόχρονα, η πολυπλοκότητα των επιλογών αυτών φαίνεται να δημιουργεί αποκλίσεις μεταξύ του επιπέδου ιδιωτικότητας που επιθυμούν να εφαρμόσουν οι χρήστες σε σχέση με αυτό που τελικά εφαρμόζεται.

Στη συνέχεια, αξιολογήσαμε και αποτιμήσαμε τον κίνδυνο παραβίασης της ιδιωτικότητας που προκύπτει από συνήθεις ενέργειες χρηστών στα κοινωνικά δίκτυα, προκειμένου οι χρήστες των κοινωνικών δικτύων να ενημερωθούν, να ευαισθητοποιηθούν και κατ' επέκταση να μπορούν να αντιμετωπίσουν πιο ώριμα τον κίνδυνο, καθώς επίσης να αποκτήσουν κίνητρο ενεργού συμμετοχής στη διαχείριση ιδιωτικότητας των προσωπικών τους δεδομένων. Προς τούτο, εφαρμόσαμε μεθόδους αποτίμησης κινδύνου, ενώ παράλληλα προτείναμε τη χρήση εργαλείων οπτικοποίησης των αποτελεσμάτων, προκειμένου να προσφέρουμε ρεαλιστική αντίληψη των επιπέδων του κινδύνου παραβίασης της ιδιωτικότητας στους χρήστες. Παρόλο που η οπτικοποίηση των αποτελεσμάτων αποτίμησης του κινδύνου παραβίασης της ιδιωτικότητας μπορεί να αφυπνίσει τους χρήστες, κάνοντάς τους να αλλάξουν στάση απέναντι στον κίνδυνο που απειλεί την ιδιωτικότητα των διαμοιραζόμενων δεδομένων τους, στρατηγικές μείωσης του κινδύνου πρέπει να ακολουθηθούν ακόμα και από τους τελικούς χρήστες, αναθέτοντάς τους έτσι ηγετικό ρόλο στη λήψη αποφάσεων σχετικά με τη διαχείριση της ιδιωτικότητας των προσωπικών τους δεδομένων. Προς τούτο, διαμορφώσαμε προτάσεις διαχείρισης αυτών των κινδύνων από την πλευρά του τελικού χρήστη.

Από την οπτική του παρόχου, διερευνήσαμε το βαθμό συμμόρφωσης των πολιτικών προστασίας της ιδιωτικότητας των κοινωνικών δικτύων με σχετικές κανονιστικές απαιτήσεις. Διαπιστώσαμε σημαντικές αποκλίσεις, για τη μερική τουλάχιστον άρση των οποίων προτείναμε μία κοινή δομή πολιτικών προστασίας της ιδιωτικότητας, βασισμένη στον κύκλο ζωής προσωπικών δεδομένων.

Contents

List of Figures

List of Tables

Chapter 1 Introduction

This chapter presents this thesis overview; introduces the research questions that were investigated in this dissertation; outlines its scope and objectives; describes the research methodology that was followed in this study; and explains its key contribution.

1.1 Background

Social networking has become very popular in recent years. Users of different age groups are joining daily in one or more online communities depending on their personal needs. Data sharing seems to be innocent when the uploading is limited to what is necessary for maintaining an Online Social Network (OSN) account; however, the oversharing is encouraged by the OSN providers, making the users enrich their profiles with more and more content items. Personally Identifiable Information (PII) treasures are published daily in OSNs, neglecting even their sensitive nature in exchange for enjoying the various OSN services.

Prior research has shown that users are concerned about their PII privacy within the OSNs, but their sharing activities cannot not confirm this; users' behaviors do not match their privacy choices. Thus, multiple types of OSN users' personal information are available to and accessible by third parties; this is attributed to the users' lack of privacy risk awareness on one hand, and to the complexity of the privacy mechanisms, that seems to set barriers in PII privacy management, leading the users into choosing the default privacy settings on the other. This privacy paradox is difficult to explain due to the fact that appropriate usable privacy control mechanisms are missing from OSN interfaces; as a result, the users are restricted in freely deciding and applying the exact privacy levels they would like.

1.2 Research Questions

Sociality has always required some voluntary abandonment of privacy; thus, once the OSN users are engaged to these online communities and have given their direct consent for PII handling, they sacrifice their privacy to a large extent in exchange to reinforcing their social status. Most of the research on privacy in OSNs pertains to the identification of threats and risks; or to users' perceptions, concerns and beliefs; or in proposals for improving privacy, by either proposing entirely new ways of OSN organization and operation or privacy enhancing methods and tools that users may use in addition to the privacy management mechanisms provided by the OSN service providers (OSNSPs). This study focuses on whether and how users' PII privacy protection can be improved by using the existing mechanisms offered by OSNs. Hence, in this study, privacy in OSNs was examined from two viewpoints: the user's perspective and that of the provider.

Towards investigating the former, our first goal was to investigate whether the OSN users are able to use the current privacy mechanisms offered by OSNs effectively and efficiently; secondly, in an effort to support users in actively participating to their PII privacy management by using the existing OSN privacy mechanisms and not relying on the default settings, we identified and assessed the privacy related risks that arise in popular OSN activities aiming to raise their risk awareness. Third, aiming to ensure that users perceive fully and accurately the privacy risks they face, we also assessed such risks and provided a visualization of the risk assessment results.

From the provider's perspective, we investigated gaps in the compliance of OSN privacy policies with privacy standards and how these can be addressed.

Specifically, the open research topics/problems that were investigated in this dissertation are the following:

- Are OSN default privacy control mechanisms appropriate and efficient?

- Do the privacy controls that OSNs offer for content with multi-party ownership always allow for fully matching the users' intentions?
- What are the most common privacy related risks that OSN users face and how can these be mitigated?
- Are OSN privacy policies compliant with privacy related standards?

1.3 Scope and Objectives

The integration of privacy requirements in the design of OSNs as well as in the default privacy levels that are offered to the users once they join OSNs is a challenging task. The objective of this study is to analyze how privacy by design and by default requirements that aim to fulfil the need:

- for compliance with the recommended regulatory frameworks;
- for granting overall control of PII protection in OSNs to the data subjects; and
- for managing the emerging privacy risks stemmed from OSN activities,

are addressed in the development and subsequently in the enhancement of privacy management interfaces. In particular, the objectives of this research are fourfold:

- to examine the appropriateness, the accuracy and the completeness of the default privacy control mechanisms that are offered in OSNs;
- to provide a holistic evaluation of the current OSN privacy "status", to examine whether this reflects the users' intentions and to recommend role-based safeguarding measures for privacy management;
- to analyze the associated privacy risks arising through the use of OSNs; and
- to investigate the relevant key regulatory issues for non-compliant privacy policies and to recommend improvements.

1.4 Research Methodology

Quantitative and qualitative research strategies are widely followed aiming to collect numerical as well as contextual results. The aim of the quantitative research method is to quantify attitudes, opinions or other defined variables in order to generalize results from a population, while the aim of the qualitative research method is focused on explaining the intentions, the reasons and the options of a population's behavior. Various research tools exist for conducting both types of research. Based on the varying nature of the aforementioned research questions, a combination of both research strategies was followed, depending on the research question.

PII privacy management seems not to be an easy and simple task, even for frequent and experienced OSN users. The first research question posed in this study was whether the default privacy control mechanisms are considered to be appropriate and efficient. By monitoring the evolution of the privacy default levels and how these have been formulated year-by-year, it can be easily understood that users should take initiatives in order to protect their PII privacy, as the privacy choices that are recommended by the OSN providers make the majority of users' PII publicly available and make them accessible without any restrictions. Considering the low-levelled protection that is provided by OSNs, we chose to perform a user study aiming to examine how users cope with PII privacy management in their online activities when using OSNs; Facebook and LinkedIn cases were examined.

Research on usability evaluation methods (Hom, 2002) and design practice (Rubin & Chisnell, 2008) shows that user testing is one of the best techniques for acquiring insights into usability problems (Vermeeren, van Kesteren, & Bekker, 2003). Many aspects of usability can best be discovered by questioning the users. Questionnaires are an indirect method (Holzinger, 2005), since this technique does not study the actual user interface but only gathers the opinions of users about the interface. Questionnaires are useful for studying how end users use the system and their preferred features. The method we chose for our study involved asking users to carry out tasks and observing their actions. These tasks cover the main functionalities of the two platforms and simulate expected usage patterns. The results of two usability experiments on the privacy settings of both OSNs, one for Facebook and another one for LinkedIn were collected and reported. This survey was performed in 2013.

Tagged users cannot have full control of the sharing content that is added to their profiles, as the content owners have the role of tagged PII administrators; thus, although the tagged users may restrict the visibility of the tagged content that is interlinked with their profiles, a part of users that are socially connected either with the content owner or with the tagged users may still have access to it. Therefore, the research question posed in this work was whether there exist cases where the privacy controls that OSNs offer for tagged content do not allow for fully matching the users' intentions.

Considering the current absence and the complexity of building a model suitable for theoretically analyzing the problem, we opted to take an empirical approach towards exploring this research question. Furthermore, as the research question was more of a descriptive nature (Yin, 2009), we decided to employ a case study approach. In selecting the case study, we noted that Facebook is by far the most popular OSN, having over 1,5 billion monthly active users (Zephoria, 2015) and that it is also the most popular content sharing platform, with over 350 million photos uploaded daily (Smith, 2013). We therefore decided to base our case study on Facebook. The case study includes a number of possible scenarios that have been designed to allow the exhaustive investigation of possible privacy preference conflicts in tagged multimedia content. Our definition of scenarios was based on the Facebook privacy setting options as they were in 2015.

Although various privacy risks arise in even simple OSN activities, OSN users seem not to act as privacy aware and they still do not adapt their behavior. Thus, the next research question we posed was how the users' privacy maturity can be improved. We considered that this might be achieved by providing a better privacy risk perception to the users in order to raise their privacy risk awareness. The method we used for assessing the privacy related risks in OSNs was based on the recommendations of the ISO 31000:2009 standard for Risk Management (ISO31000, 2009). The proposed Privacy Risk Assessment Method involves the identification of the assets, and the assessment of likelihood and impact of a privacy violation incident. To complete the picture, the risk mitigation strategy that should be followed for treating the identified risks was also provided (Betterley, 2014). The method described herein applies to the case of the most popular OSN, namely Facebook; however, its application to other OSNs is more or less straightforward.

The last research question we posed was whether privacy policies are compliant with the privacy relevant standards; in this study, we investigated whether the OSN privacy policies of five OSNs are compliant with ISO29100:2011 (ISO29100, 2011) that introduces a revised privacy framework. As a structured methodology for assessing conformance to ISO 29100:2011, similar to e.g. the one described in ISO 27007:2011 (ISO27007, 2011) for auditing Information Security Management Systems (ISMS) against the ISO 27001:2013 (ISO27001, 2013) standard does not exist, we examined the conformance of the OSN privacy policies against the principles of the ISO 29100:2011 standard; this evaluation was performed by comparing the statements in each OSN privacy policy part with the adherence criteria stated in the standard. Mapping techniques were used to examine this conformance; this mapping will assist the OSN providers to become compliant with various new privacy requirements as they apply to them, including the data protection by design and by default requirements.

1.5 Thesis Overview

In Chapter 2, the offered privacy architectures and the shared content types that are permitted to be uploaded in the two topmost leading OSNs, namely Facebook and LinkedIn, were analyzed in detail and compared. Then, the changes over the default privacy settings of both OSNs are highlighted, year-by-year. In an effort to examine the competency of the privacy controls provided by the two OSNs, a usability study was performed and the results showed that the challenges the users faced in the privacy related tasks we defined make them keep the default settings that are offered by the OSNs; nevertheless, this is risky as the low levels of the default privacy make users' PII accessible to everyone, thus leaving it exposed to unauthorized misuse. The outcome of the user survey we conducted highlights the need to embed privacy into the design of OSNs in order to enhance the usability of privacy controls.

In OSN profiles, the sharing data is categorized in two classes; users can upload various content types by themselves or content may be added or linked to their profiles by others. The tagging mechanism is one of the most popular features that are provided by the majority of the OSNs. Privacy management for the content that is shared by others seems to be more difficult, as the overall control of the shared content's privacy lies with the content owner i.e. the user who is uploading and sharing the content to an OSN; the tagged user is provided with limited options over the visibility of the content interlinked with her account. In Chapter 3, we focused on examining the privacy of tagged content in Facebook; we assessed the real value of the privacy settings for the tagged content items that Facebook offers, in terms of safeguarding the user's privacy intentions. This was achieved by examining all the information visibility combinations that may be applied between content owners and content heirs, against privacy threats. Privacy conflicts were highlighted as the multi-ownership of different privacy levelled profiles over the shared content creates audience discrepancies. The results of monitoring the privacy in tagged multimedia content highlight the need for taking measures in order to protect even such types of content enriched by using labels.

Although privacy enhancements need to be made on the OSN providers' side, it is also important to enhance the users' perception of risks, by monitoring the emerging risks in OSNs and the controls applied to manage privacy; the OSN users should be aware of the possible privacy risks that they may face and how they could mitigate them. In Chapter 4, we assessed the privacy risks we identified in popular OSN activities that can be also managed by end users; then, we proposed visualising the results, aiming to make them more comprehensible even for non-expert users. Last but not least, privacy risk treatment options based on the privacy risk scores were recommended.

If privacy by design and by default were provided in online communities, there would be less need for further action as regards PII privacy assurance. Privacy principles are recommended by laws, regulations and standards aiming to enhance the levels of PII protection. In Chapter

5, the conformance of the OSN privacy policies to the ISO 29100:2011 standard was examined; two case studies were conducted, on Facebook and on LinkedIn. The partial conformance that was found in the majority of the policy parts in both OSNs, highlights the need for restructuring OSN privacy policies. We proposed a prototype privacy policy, based on the PII lifecycle framework and we examined how this could be embedded in the OSN privacy policy structure; the related mapping was performed for five OSN privacy policies.

1.6 Summary of Contribution

The main contribution of this thesis is twofold: increased insight into privacy issues in OSNs from both a users' and a providers' viewpoint on one hand and a set of proposals for enhancing privacy in OSNs by adhering to the privacy by design and by default principles and requirements. Table 1.1 summarizes the contributions of this thesis against the publications that resulted from it. These are also listed in Appendix A.

Table 1.1 – Summary of Contribution of the Thesis

Published Papers	**Research Objective**	**Key Results**
(Michota & Katsikas, 2014b)	To examine the appropriateness, the accuracy and the completeness of the default privacy control mechanisms that are offered in OSNs.	The dominant privacy option for the OSN sharing data is public. Low-levelled usability was identified in privacy control mechanisms.
(Michota & Katsikas, 2015b) **(Michota & Katsikas, 2017a)**	To provide a holistic evaluation of the current OSN privacy "status", to examine whether this reflects the users' intentions and to recommend role-based safeguarding measures for privacy management.	Privacy gaps were identified as audience discrepancies were highlighted over the privacy of tagged content types.
(Michota & Katsikas, 2017b)	To analyze the associated privacy risks arising through the use of social networks.	Critical and high risks identified in OSN interactions.
(Michota & Katsikas, 2014a) **(Michota & Katsikas, 2014c)** **(Michota & Katsikas, 2015a)**	To investigate the relevant key regulatory issues for non-compliant privacy policies and to recommend improvements.	Partial coverage of the privacy principles that are recommended by the ISO29100:2011.

Chapter 2 Privacy by Design and by Default

OSNs tend to make their default privacy settings “public”. In this chapter, we focused on comparing the changes in default privacy settings of the two topmost leading OSNs, on an annual basis, building upon an earlier work (Paul, Puscher, & Strufe, 2011) that started in 2005 and ended in 2010. We also examined the usability of privacy controls in both OSNs. We performed a user survey among Facebook and LinkedIn users, comparing the current interfaces with those of the older versions and performing a usability test for the privacy settings of their latest versions. The results of the user study indicated that OSN privacy settings tend to become progressively more liberal and they also highlighted a great number of usability problems showing that privacy by design is not taken into consideration during the OSN privacy frameworks enhancements.

2.1 Background

OSNs have permeated everyday life and have radically transformed the online behavior of users. People use different OSNs depending on their personal needs. The ultimate goal of the majority of OSNs is to entertain users; some of them have even professional character giving the users the opportunity to be included in social circles of candidate employers. OSNs make the users more and more social; however, sociality has always required some voluntary abandonment of privacy. Thus, OSN users must give up some of their private space so as to share it with others. This space includes treasures of PII that can lead to privacy drifts such as damaging users’ reputation and credibility, security risks (e.g. identity theft) and profiling risks.

Privacy paradox explains the contradictory relationship between the OSN users’ privacy concerns and their PII sharing actions (Barth & de Jong, 2017), (Barnes, 2006) although people are concerned about privacy, most do not do much about protecting it (Kokolakis, 2017). In 2006, Acquisti and Gross measured the accuracy of Facebook users' perception of their level of disclosure on the site by surveying users on the visibility of their profile and then comparing their answers against the amount of data that was available to all members of the participants' university network (Gross & Acquisti, 2005). Joinson found that the users' privacy settings varied based on their motivation for using Facebook (Joinson, 2008). This can be attributed to many reasons, including the lack of privacy controls available to the user, the complexity of using the controls and the burden associated with managing these controls for large sets of users. In fact, members of OSNs are often under an illusion of privacy, underestimating the privacy risks related to their personal information published in their profiles. Data and security breaches have been highlighted in most OSNs. According to the Sophos Security Threat Report 2012 (Sophos, 2012), data loss is usually caused by human errors or negligence. Risks arise when personal information is leaked, improperly discarded or gets into the wrong hands. Data leakage is usually caused by unprotected technical equipment and email communication. As social media marketing techniques are widely used, OSN sharing data is vulnerable to a wide range of digital threats, which are becoming increasingly sophisticated and damaging. Identity theft, and consequently credit card theft, has major financial and reputation consequences for both the individual whose identity is stolen and the company from which the data was obtained. While most of the published work on privacy in social networks has identified and analyzed privacy and security exposures of current OSNs (Bonneau, Anderson, & Danezis, 2009), some recent works also propose solutions to these exposures by enhancing the infrastructure or even by developing entirely new social networking platforms (Paul, Puscher, & Strufe, 2011), (Al-Badi, Michelle, Al Roobaea, & Mayhew, 2013).

The users seem to be incapable to master the settings (Lipford, Besmer, & Watson, 2008) due to lack of proper privacy awareness (Vemou, Karyda, & Kokolakis, 2014). Since most of the users are not aware of the necessity for changing the default privacy preferences, it is essential to improve the privacy levels for the default settings so that these settings meet the users' expectations and essential demands as much as possible. Only a small percentage of users tend to change the default privacy preferences that are highly permeable (Mackay, 1991). Hence, OSNSPs need to offer user-friendly guidelines that help the users to change the privacy settings successfully (Sanghvi, 2009) (Bilge, Strufe, Balzarotti, & Kirda, 2009). However, OSN providers have access to all users' private information, and thus they can use it for several purposes, not always with the explicit consent of the users (Feldman, Blankstein, Freedman, & Felten, 2012). Massive targeting advertisement and behavior analysis by using data mining techniques are just examples. The OSN providers can also share social networking users' information with large companies or research groups, or provide access for governments for surveillance purposes (Mont, Pearson, & Bramhall, 2003).

Mark Zuckerberg, the founder of the most popular OSN namely Facebook said that the reason why Facebook's default privacy settings changed from private to public is his consideration that privacy is no longer a social norm; everyone should be allowed to see and search for Facebook profiles by accessing personal information such as names, gender, city etc. This statement is in contrast with many sociological theories (Levine, 1971) that support that the online privacy is considered to be a strong social norm. According to the sociological theory of privacy, every individual is the center of many social circles composed of people they know from different parts of their life. Different circles have different norms for what is acceptable or non-acceptable behavior or what is publicly visible and what is kept private. OSNs consist of many social circles and as a result of many different norms. Privacy is difficult to be achieved when different social circles have different norms. Not only do the default privacy settings tend to be more liberal but the frequent updates of the privacy related user interfaces of both OSNs also raise barriers that inhibit the users from reflecting easily and accurately their privacy preferences on the privacy settings.

Usability is not a single "one-dimensional" property of a user interface. There are many usability attributes that should be taken into consideration and measured. Shneiderman proposes four attributes that influence the acceptance of a product, namely "effectiveness", "learnability", "flexibility" and "attitude" (Shneiderman, 1991). Nielsen introduces some different usability attributes based on a "system acceptability model" (Nielsen,1993). The word "usability" also refers to methods of improving ease of use during the design process (Nielsen, 2003). It has also been described as the acceptability of a system and its ease of use for a specific set of users performing specific tasks in a precise setting (Holzinger, 2005).

While new privacy setting interfaces are presented aiming to help users in OSN privacy management, the upgrades in the default privacy settings seem to be more confusing, as they do not readily allow the users to grasp the effect of their changes. Thus, not only is this an issue regarding users' intentions but it also concerns the continuous changes in the default privacy controls of the existing interfaces that make the users do experience problems in correctly adjusting these settings (Paul, Puscher, & Strufe, 2011). On the other hand, LinkedIn is a business oriented social networking tool that shares some features with Facebook but its interface seems to be less user-friendly (Furnell & Botha, 2011).

Strict default privacy levels could protect users' PII from unintentional exposure to unknown audiences. Not only are differences highlighted in OSNs' nature but differences are also met in the default privacy levels that are provided by each of them. Among the popular OSNs, we selected two in order to investigate the default privacy they offer to their audiences and to examine whether its customization is considered to be an easy task for the users.

This chapter offers a comparative analysis between the default privacy offered by Facebook and LinkedIn. While Facebook is particularly focused on facilitating personal self-presentation, LinkedIn's interface caters towards the need for professional self-promotion. Both platforms use similar principles of connectivity and strategies that can be successfully revealed in recent interface changes. This similarity is the subject of research interest and has been the reason why we selected to study these particular OSNs. Further, usable security and privacy are two critical components that have received a fair amount of research attention as they influence users' PII protection. In this chapter, we focus on satisfying the need for a usable access control mechanism for end users of both platforms. We approach the problem by researching how end users cope with managing the privacy controls they need in their online activities when using Facebook and LinkedIn. To this end, we report on the results of two usability experiments on the privacy settings of both OSNs, one for Facebook and another one for LinkedIn. On the one hand, the evolution of the default privacy settings that tend to reveal more and more PII of the OSN users and on the other hand, the changes in the structure of the privacy setting menus highlight the need for reframing security problems that may lead to better usability.

The chapter is structured as follows: Section 2.2 presents the privacy settings and sharing content for both OSNs we used in this study. Section 2.3 discusses the usability of privacy controls in these OSNs based on the results of this study. Finally, in Section 2.4 summarizes our findings.

2.2 Privacy Settings & Sharing Content

Figure 2.1 depicts in detail the design of the “Privacy Settings” according to the current interface in Facebook. The “Privacy shortcuts” menu that was added for the first time on December 2012 in the Facebook page gave the users quick access to the privacy controls, with certain settings that are also available in the submenus of the three major choices of the “Privacy Settings” menu.

Common settings between the “Privacy Shortcuts” menu and the “Privacy Settings” menu are highlighted in bold frames in Figure 2.1. Meanwhile, LinkedIn takes a completely different approach with regards to privacy settings; it controls what a viewer can see according to whether she has a paid or a free account. In this study, we focus on the default privacy settings of a free account. In Figure 2.3, one can observe in detail the design of the “Privacy Settings” in LinkedIn (Furnell & Botha, 2011).

In Figures 2.2 and 2.4, the abundance of information that can potentially be shared among users that maintain profile pages in Facebook and LinkedIn respectively can be clearly seen. The naming that was used for the description of the users’ sharing data follows the available choices on the interface of the corresponding social network (Schneier, 2010).

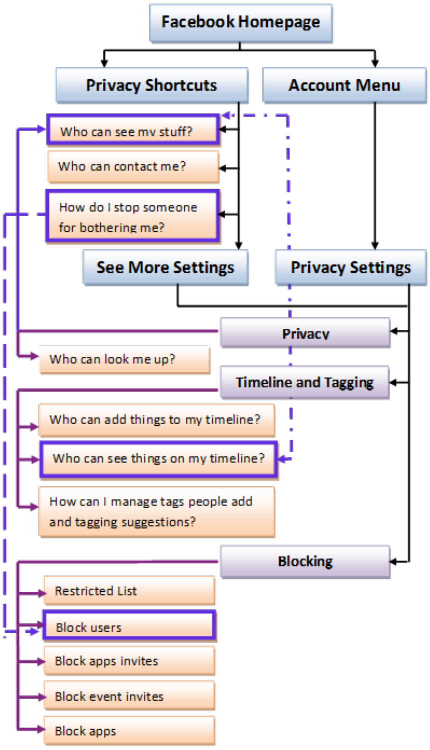


Figure 2.1– Architecture of Privacy Settings in Facebook

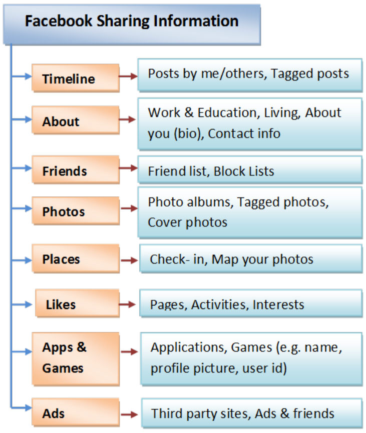

Facebook Sharing Information
Timeline
Posts by me/others, Tagged posts
About
Work & Education, Living, About you (bio), Contact info
Friends
Friend list, Block Lists
Photos
Photo albums, Tagged photos, Cover photos
Places
Check- in, Map your photos
Likes
Pages, Activities, Interests
Apps & Games
Applications, Games (e.g. name, profile picture, user id)
Ads
Third party sites, Ads & friends

Figure 2.2– Sharing Content in Facebook

Figure 2.5 presents a comparative analysis of the default privacy level of the shared content in Facebook and LinkedIn. As far as Facebook goes, over 80% of the content items are shared with default privacy settings; this means that they are visible to millions of Facebook users. In order to quantify the differences among privacy settings, we mapped the possible settings to numerical (on a percent scale) exposure levels. The audience selector in both OSNs allows the users to choose a specific audience for sharing their data. As it can be seen in Table 2.1, the visibility of the shared content in Facebook and in LinkedIn is classified in five levels. A numerical value for each exposure level can be derived by mapping visibility levels to equally distributed percentage values, with an increment step of 20% between levels. Thus, the "Only me" option corresponds to the minimum content exposure (20% on the numerical scale) and the default setting "Everyone/public" corresponds to the maximum content exposure level of 100%.

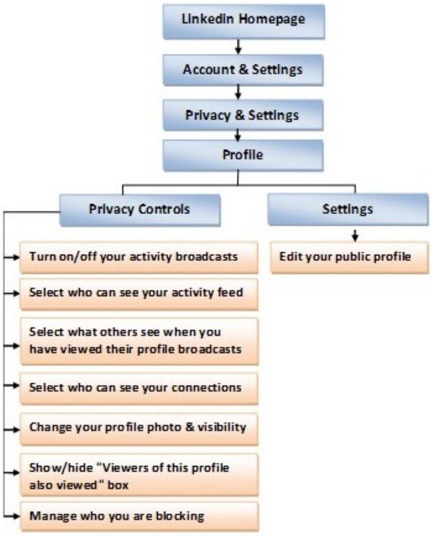

Linkedin Homepage
Account & Settings
Privacy & Settings
Profile
Privacy Controls
Settings
Turn on/off your activity broadcasts
Select who can see your activity feed
Select what others see when you have viewed their profile broadcasts
Select who can see your connections
Change your profile photo & visibility
Show/hide "Viewers of this profile also viewed" box
Manage who you are blocking
Edit your public profile

Figure 2.3– Architecture of Privacy Settings in LinkedIn

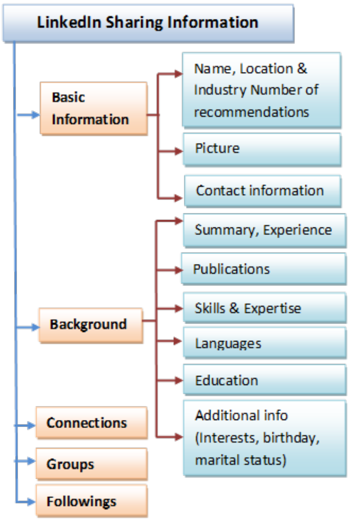


Figure 2.4– Sharing Content in LinkedIn

Table 2.1 – Exposure Levels in Facebook and LinkedIn Privacy Settings

Facebook setting	LinkedIn setting	Exposure level
Only me	Only me	20
Friends	Your connections	40
Friends of friends	Your network	60
All Facebook users	All LinkedIn users	80
Everyone/public	Everyone	100

We observe that, with the passing of time the default privacy settings of each type of shared content in Facebook tend to approach or to reach the exposure level of 100% (that corresponds to the “public” choice). Since 2005 until 2013 that this study was carried out, the exception to the rule in the default privacy settings was for the visibility of birthday and contact details that were not accessible to the public audience. On the other hand, LinkedIn privacy policies seem to be more conservative. The analysis of the default privacy controls of the shared content in LinkedIn reveals that the data exposure level is lower than that of Facebook. By using the same scale with the corresponding choices in LinkedIn, we observe that the setting “Your connections” represents exposure level of 40% and seems to be the dominant choice (Schneier B., 2010).

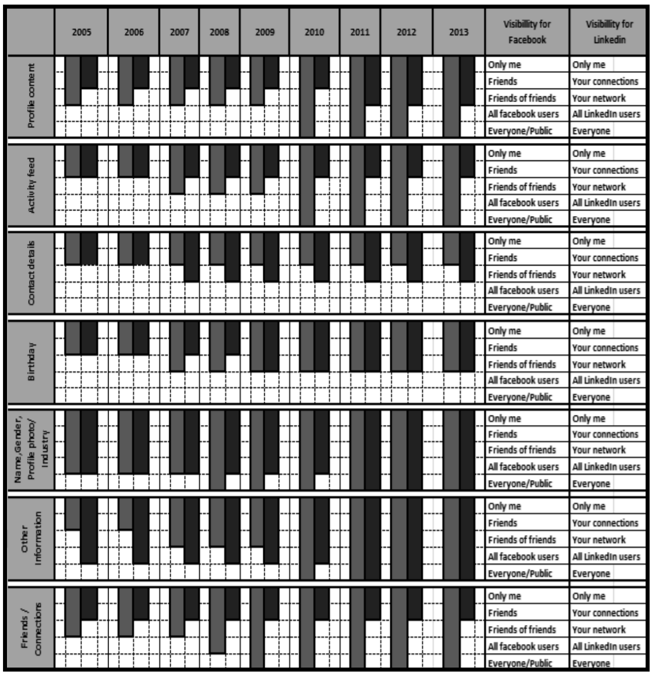


Figure 2.5– Default Privacy Settings of Facebook (Grey columns) and LinkedIn (Black columns)

2.3 Usability of Privacy Controls

Two usability experiments on the privacy settings of both OSNs were performed, one for Facebook and another one for LinkedIn. The workflow for both usability tests is presented below.

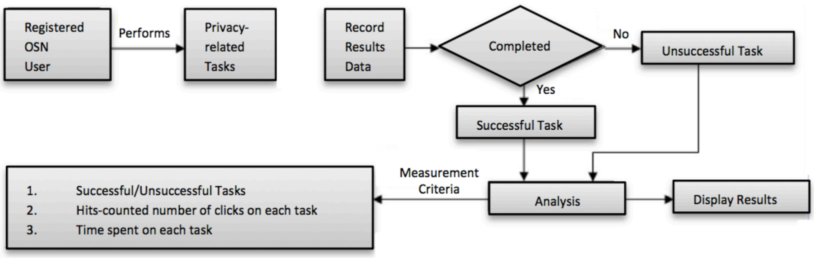


Figure 2.6– Work Flow for Usability Tests

The selection process for the participants used sampling within categories of OSN users with similar age groups but with various user behaviors on OSN sites. It was essential to include users with active roles in the social media cloud; users who are familiar with creating, sharing and reacting to web content, as well as users who are mostly passive OSN users; users with poor activity through these online communities; usually beginners can be characterized as "habitual" users. Hence, the selection of the sample was based on the following criteria: (i) the Facebook and LinkedIn profiles have to be real, (ii) the test users have to belong to the targeted age groups (iii) participants with variation in levels of activity have to be included in both OSNs, in order for the results to be as unbiased as possible.

Table 2.2 – Tasks in Usability Tests

TASKS	TASKS IN FACEBOOK	TASKS IN LINKEDIN
A	Hide photo albums	Limit the audience of profile photo view
B	Hide basic info (About)	Hide basic info
C	Hide your friend-list	Hide your connections
D	Hide a timeline post	Limit the audience of a sharing post
E	Using the activity log, review your tagged posts	Turn off your activity broadcasts
F	Hide application posts	Don't allow sharing your data to third party apps
G	~~**Blocking**~~	Hide info from your public profile
H	~~**Profile search**~~	Select who can send you invitations to connect
I	Select what other people see on my timeline (View as…)	
J	Select who can send you friend requests	

Accordingly, based on a locally implemented showcase and real Facebook and LinkedIn profiles, we performed two user studies: the first in Facebook with 100 Greek young adults, aged between 18 and 34 and the second in LinkedIn with 45 Greek adults in the same age group who are studying or working at the University of Piraeus. It is important to mention that the majority of the test users were female and only 38% were male. This survey was performed on November 2013, almost one year after the implementation of the new privacy shortcuts menus in Facebook.

The users were requested to complete some tasks related to controlling privacy and then to answer three questions on their experience with each task. The tasks of the practical part of the user studies were designed to address everyday needs, like changing privacy settings for a given attribute. The registered users in Facebook had to accomplish ten different privacy related tasks while those in LinkedIn had to accomplish eight. This was because Facebook offers a wider variety of services as compared to LinkedIn. The tasks of the practical part of the user study in LinkedIn were designed to be comparable with those in Facebook. Table 2.2 describes in detail the tasks that users were requested to perform.

In both usability tests the performance shown by the test participants was measured with regard to effectiveness and efficiency (Ivory & Hearst, 2001), (Otaiza, Rusu, & Roncagliolo, 2010) (Bevan & Spinhof, 2007). Effectiveness refers to the extent to which a task goal is successfully achieved (e.g., percentage of users that complete a task) while efficiency is associated with the level of resources deployed to achieve a task goal (e.g., task completion time, number of user inputs). These were assessed by means of the three questions the users had to answer after carrying out each task.

The first question is related to the user‘s ability to accomplish each task successfully or not. In the second question, the user is requested to fill in the number of clicks she needed to find the appropriate setting in order to finish each task and, in the third question of each task, the user is asked to select one of the given choices that best describes the time she took to perform each task. For the second and the third question of each task, three choices were given. Each choice describes the minimum, median and maximum number of clicks or seconds of time correspondingly. In addition to the analysis of the results, in order to count the user inputs, the actual number of clicks and the actual time taken to complete the task were measured, for each participant. The results of these measurements are depicted in Figures 2.9-2.12.

As seen in the following charts (Figures 2.7-2.8), the majority of Facebook participants (75,6% - 97,1%) and LinkedIn participants (77,8% - 100%) were successful in changing the privacy settings of each content item as requested;

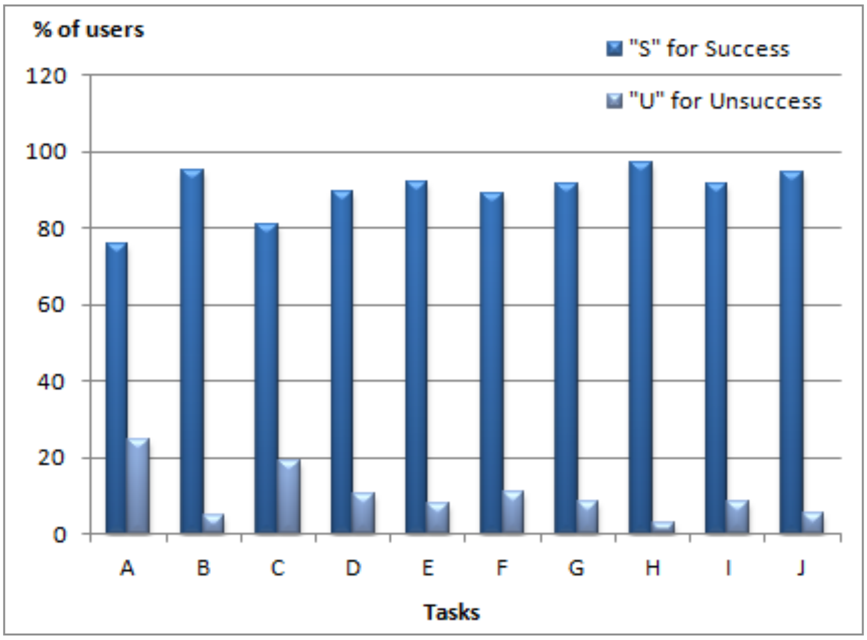


Figure 2.7– Task Accomplishment in Facebook

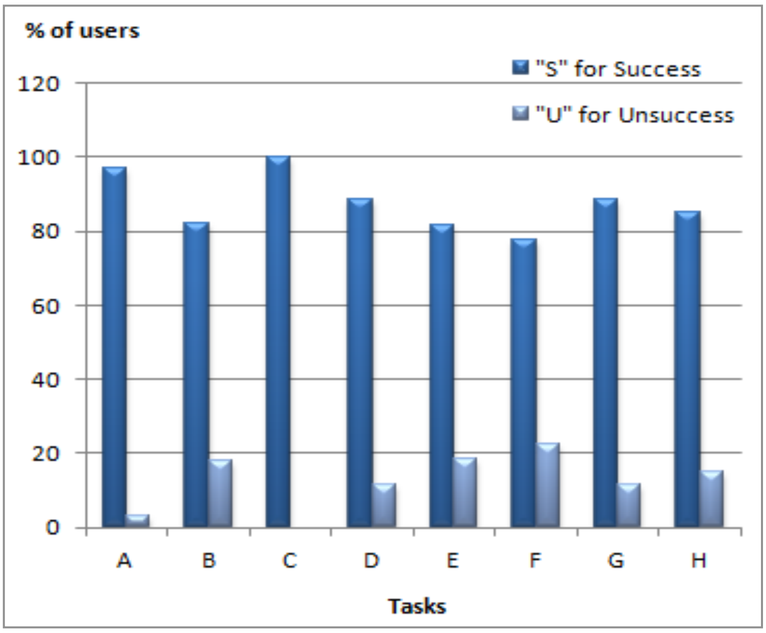


Figure 2.8– Task Accomplishment in LinkedIn

It is apparent from the four charts below (Figs. 2.9-2.12) that the LinkedIn users experienced some difficulties in completing some of the tasks, as they spent more time and they accessed many more pages than necessary. It is noticeable that the time taken and the clicks taken varied widely, because of the differences in the users' behavior; thus, there is no dominant answer. On the contrary, the participants' answers span the full range of the three given choices (minimum, median and maximum).

Accordingly to Figures 2.10 and 2.12, the LinkedIn's task solving was slightly more difficult than that in Facebook; to complete tasks E, F, H, the participants needed to consume the maximum available time as well as to spend the maximum amount of clicks.

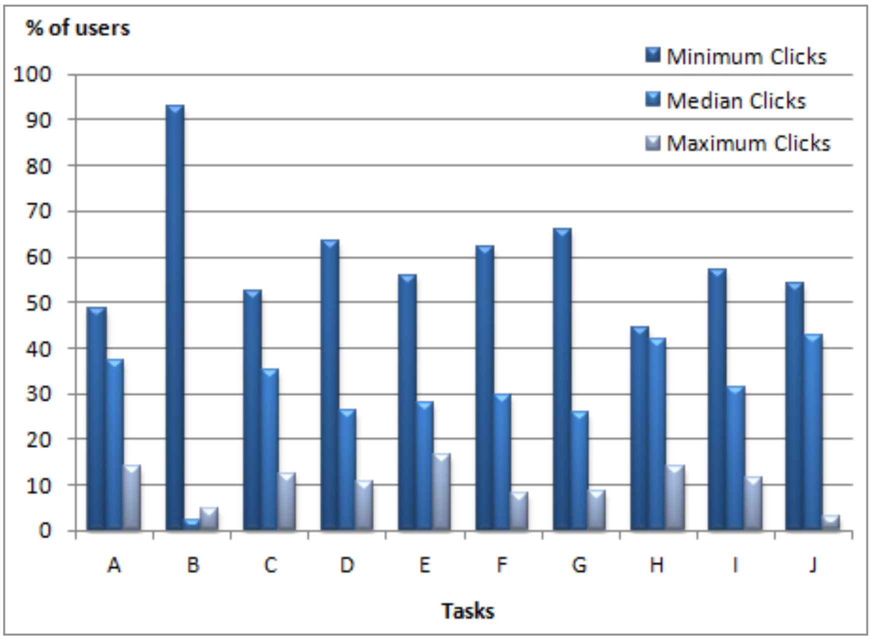


Figure 2.9– Number of Clicks in Facebook

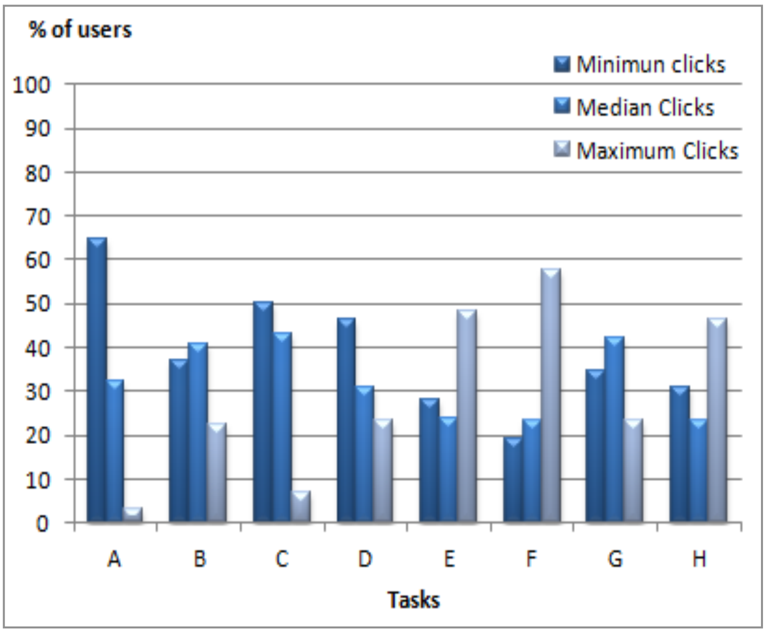


Figure 2.10– Number of Clicks in LinkedIn

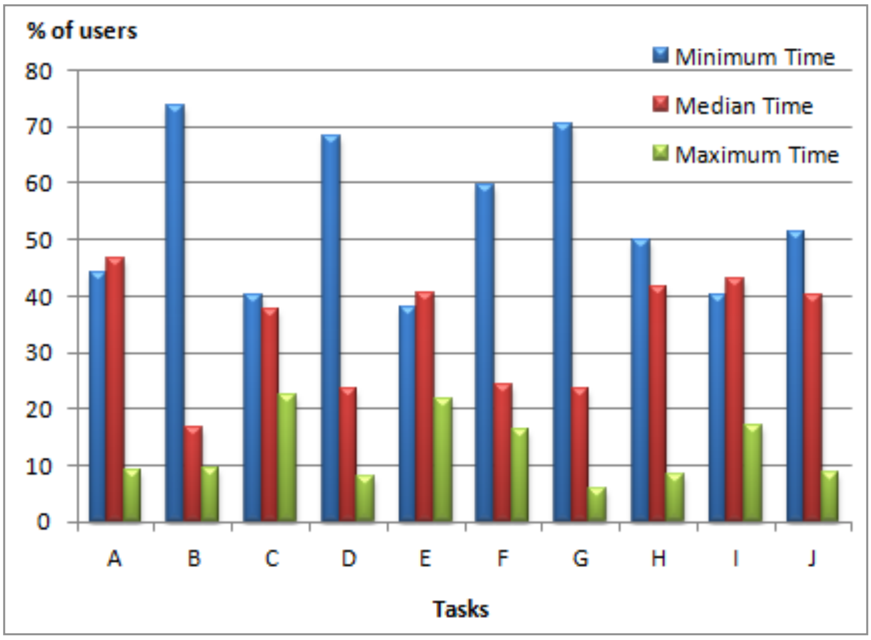


Figure 2.11– Time (sec) Needed in Facebook

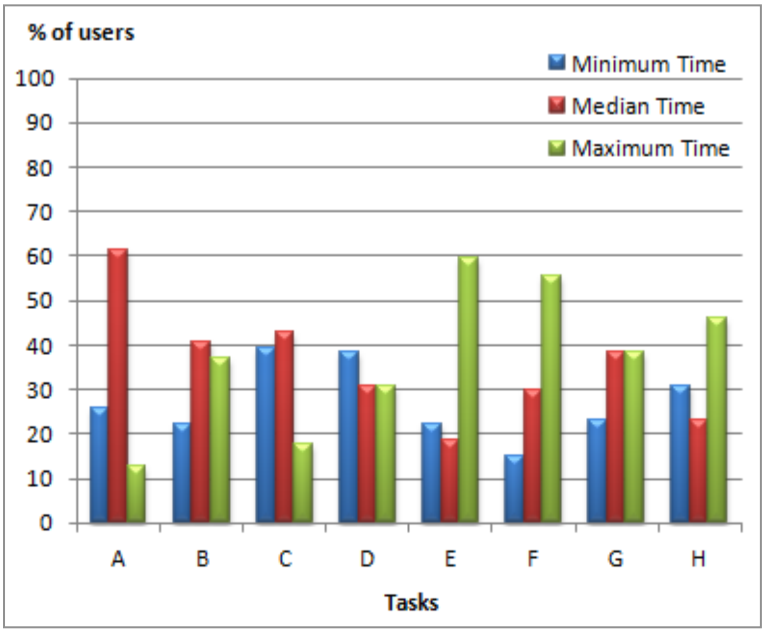


Figure 2.12– Time (sec) Needed in LinkedIn

These results indicate that although the majority of the users managed to accomplish successfully all the tasks, they had slightly more difficulty in performing some of them. This is evident from the long time they spent on specific tasks and from the high number of clicks they needed for searching and finding the right menus and choices to perform them.

Even though we did not explicitly explore that in the studies we conducted, it seems reasonable that the situation would be better if both OSNs could use the same naming for identical data types. For instance, Facebook users are familiar with the term “Friend” instead of the term “Connection” that is used in LinkedIn. In LinkedIn user study, in Task H, users were asked to find the appropriate preference in order to choose who can be included in their connections. More specifically, LinkedIn users were requested to apply the setting that will allow them to receive invitations only by people who know their email addresses or appear in their "Imported Contacts" list. The corresponding task in Facebook was the task of restricting the audience allowed to send friend requests to the users. We can easily observe that different terms with the same meaning are used in the social networking communities and this may be confusing for the users.

It would also be desirable to categorize the data types that are published in OSNs based on their content, For instance, the category “About” in Facebook and the categories “Basic info” and “Background” in LinkedIn include the same content types. It is difficult for the users to remember different categories for the same data types depending on the social network they have logged in, when they are trying to restrict their content visibility. Task B seemed to be a challenging task for the users, as such difficulties were highlighted when they were asked to change the visibility of their basic information. In the case of Facebook, users were asked to restrict the audience who can see their date of birth and in case of LinkedIn, users were requested to change how their name appears in order their full surname to be invisible (appearance of the first letter only).

Further, it would be useful to improve link placements. For instance, in LinkedIn, the “Privacy Settings” link position should be positioned within easy view of the user on the profile page along with the other links and not within the setting menu (Figure 2.3), thus making the task easier to perform.

2.4 Results and Discussion

As the web-based technologies become more accessible and easy to use, social networks likewise make personal information more accessible to the public audience. Since privacy settings are the means offered to the users for controlling and managing their privacy in the social networking platforms, users’ perspective should be taken into consideration during their design. Changes in default privacy settings for OSN users’ PII become more and more permissive over time with the “Public” option to be dominant in the most sharing data fields. Even if LinkedIn‘s privacy policy is considered to be more “conservative” and restrictive for the sharing data exposition, it also follows the OSN providers’ trend for liberation of personal information.

The changes in privacy settings for both OSNs seem not to make the privacy control management easier for the users. We confirmed that by empirically evaluating how Facebook and LinkedIn users utilize the available privacy controls in order to implement privacy restrictions for their shared content and we showed that many users did not manage to match the privacy settings with their sharing intentions.

In conclusion, no trace of privacy by default is provided in both OSNs as users' PII is becoming visible to the public audience in a timely manner. More effort and time are requested by the users in order to restrict the audience that will be authorized to access their PII; usability factor should be taken into consideration during the enhancements of OSN privacy architectures that should be aligned with privacy by design requirements aiming to simplify the access management procedures. The recommendations made herein for privacy interfaces were based on the findings of our usability study.

Chapter 3 Customized Privacy Limitations

Tagging services in OSNs allow users to connect online resources based on their characteristics in addition to their URLs. The semantic interoperability creates authorization conflicts when accessing the tagged shared content; as a result, privacy requirements cannot be fully satisfied. In this chapter we investigate the privacy implications of unauthorized audience discrepancies in tagged multimedia content that are due to the different privacy restrictions that users apply to their PII. By examining all the possible visibility combinations in a two-level social relationship scale for different anonymized real user profiles, according to the offered choices that are provided by the privacy mechanisms in OSNs, we identified the cases where there exist audience discrepancies that can cause privacy breaches. Our findings indicate that the current privacy mechanisms of OSN users' tagged multimedia content are insufficient, as they cannot fully match the users' privacy intentions.

3.1 Background

OSNs have permeated everyday life and have radically transformed the online behavior of users. OSNs, popular as they are, they come also with a number of privacy issues; these have attracted considerable research interest (Kaiser, 2010), (Krishnamurthy & Wills, 2008). As the use of OSN services spans across multiple facets of daily life, privacy unaware users may find themselves facing grave problems with information about themselves that they willingly uploaded to an OSN but was revealed to third unintended parties. Such misuse may be exercised by other users and includes cyberstalking (Madejski, Johnson, & Bellovin, 2011), identity theft (Acquisti, Gross, & Stutzman, 2014), (Thompson, 2010) and discrimination

(Johnson, 2009); it may also be exercised by third parties. Many incidents of users being fired because of sensitive content which they considered to be private, but nevertheless was accessed by their employers have been reported (Bort, 2013), (Did the Internet Kill Privacy?, 2011) and checking up job applicants online during the hiring process is not unusual; Acquisti and Fong (Acquisti & Fong, 2015) revealed that information found in OSNs may be used to discriminate against applicants. The CrossTab survey (Cross-Tab Marketing Services, 2010) found that 70% of recruiters in the US have rejected candidates due to information they found online.

Tagging allows users to annotate uploaded multimedia content with those who appear in them, by using labels that provide links to the OSN users' accounts. Tagging is also referred to as social tagging, when tags are shared with an OSN community and different OSN users are allowed to tag the same content item. Tag is a popular feature of many OSNs, even though it is most pronounced in Facebook. Facebook that is by far the most popular OSN, having over 1,5 billion monthly active users (Zephoria, 2015) provides the greatest variety of OSN services comparing with other OSNs. Within one month of the launch of the service in Facebook, 85% of the subscribed users were tagged at least once (Kirkpatrick, 2010). The most characterizing example of tagging is multimedia tagging and more specifically photo tagging. Facebook is also the most popular content sharing platform, with over 350 million photos uploaded daily (Smith, 2013). The tagged content is also added on the participating members' Timelines. *Video tagging* is also possible, but tags usually cannot be added to the video file itself; they are rather used for classifying it in a category with similar videos, thereby facilitating the process of finding it. It is also used to specify what the video is about and to prepare the viewer on what she is going to watch. *Hashtags* are usually used as in photo tagging and in video tagging, in order to make these content items searchable in popular topics. Hashtags classify the different content items based on related topics of common interest. The Facebook hashtag service drives its users to a page that aggregates all the related posts. For instance, videos that are accompanied with hashtags help the users who are looking for videos similar to the ones that they have shared.

Tagging has raised serious privacy concerns, as it has been shown to enable the disclosure of

PII, even sensitive information, without the concerned user's consent or even knowledge. OSNs allow their users to be policy administrators of the protection of user data (Hu, Ahn, & Jorgensen, 2013). Hence, users can restrict data sharing to a set of people they choose to give access to their PII. Nevertheless, interlinking profile information may be risky. The question of whether it is possible to identify users across systems based on their tag-based profiles has attracted some research interest (Iofciu, Fankhauser, Abel, & Bischoff, 2011). Tagged data includes information such as captions, comments and photo tags; the combination of publicly available data and face recognition services are sufficient to disclose the identities of OSN users appearing in a photo (Acquisti, Gross, & Stutzman, 2014). When OSN users add id-tags on their sharing content in Facebook, they unintentionally put their friends' or even their own privacy at risk (Krishnamurthy, 2010). Collateral damage is the term used to describe this kind of problems. Tagging has also been shown to provide a convenient mechanism for launching attacks aiming at the security of the services used by the tagged user rather than her privacy (Irani, Balduzzi, Balzarotti, Kirda, & Pu, 2011), as well as for spreading malware (Botezatu, 2015).

Privacy concerns with sharing multimedia content over OSNs have attracted considerable research attention (Ahern, Eckles, Good, King, Naaman, & Nair, 2007) (Besmer & Lipford, 2008), (Johnson, Egelman, & Bellovin, 2012), (Klemperer, et al., 2012), (Liu, Gummadi, Krishnamurthy, & Mislove, 2011), (Squicciarini, Xu, & Zhang, 2011). One direction of research in this field aims at ascertaining users' attitudes. Early work in this direction has reported that users are concerned about their privacy and tend to avoid publishing photos or any other private information publicly (Strater & Lipford, 2008). User concerns related explicitly to photo tagging are reported in (Besmer & Lipford, 2010), where explicit requests by users for deletion of photos, or users un-tagging themselves, are thought to be complicated issues. These can lead to social tension and are a source of anxiety for users, who may abstain from such actions to ensure the stability of their social relations (Strano & Queen, 2012). The authors in (Henne & Smith, 2013) study user awareness of privacy issues concerning the sharing of media including media shared by others and the perception of metadata privacy. Furthermore, they discuss the concept of a privacy tradeoff and how this can be used to enable users to regain control of their media privacy.

Possible threats and attacks leveraged by content sharing ability against the privacy of users or the security of the services they use or of the OSN itself, as well as recommendations for countermeasures is another direction of research, where a wealth of literature exists. Several privacy leakage scenarios are described in (Ilia, Polakis, Athanasopoulos, Maggi, & Ioannidis, 2015), where a proposal for changing the granularity of access control as applied to photos is made in an attempt to thwart the privacy leakage scenarios. An analysis of how photo tags can be used to help predicting some of the attributes of PII is provided in (Pesce, Las Casas, Rauber, & Almeida, 2012). The authors therein argue that it is also very important for the tagged users to be aware of the possible threats that they are exposed to in addition to be able to predict exposure of PII to unknown or unintended audiences through shared multimedia content. The authors in (Besmer & Lipford, 2010) argue that the tagged user is offered with limited options in order to restrict the privacy of her tagged content by hiding it from a workplace and she is forced to set an all-or-nothing option with any particular user group. Malware has been known to spread through the tagging services (Botezatu, 2015). The legal problems associated with tagging have been identified in (Kosta, Kalloniatis , Mitrou, & Gritzalis, 2010), and self-regulation of the OSNs has been highlighted as a promising way forward in this respect. However, none of these works explores in detail possible cases of conflicts among the privacy preferences of OSN users and their impact in terms of violation of such preferences.

In this chapter, we focus on examining the privacy of tagged content in Facebook. This was achieved by examining all the information visibility combinations that may be applied between two users, against security and privacy threats that may be concealed in tagged content. We further propose measures to restrict or remediate the resulting impact if a threat succeeds. The remainder of the chapter is structured as follows: In Section 3.2 the privacy control mechanisms that Facebook offers for the protection of tagged content and their limitations are described. Section 3.3 presents the scenarios we examined for monitoring privacy in tagged multimedia content and discusses our findings. This chapter concludes with Section 3.4.

3.2 Privacy Controls for Tagged Content

OSNs offer specialized privacy control mechanisms to their users, in order to allow them to limit the visibility of their tagged content items. The option that is widely used by the majority of the users for limiting the visibility of their PII is to remove a tag. “Timeline Review” is offered for all the content types by Facebook and allows the users to choose whether the tagged content will appear on their timelines or not. In case that a user changes her mind and then she decides to hide this content from her timeline, she can apply the corresponding setting. However, both options do not remove the content from Facebook; this still remains visible in “News feed” or “Search” of the Facebook home page.

The audience selector in OSNs allows the users to choose a specific audience for sharing their data. The visibility of the shared content in Facebook even for the tagged content types is classified in four levels; the most common visibility choice that is widely used by the majority of OSN users is the “Friends” option when the content owner wishes to share her content items only with the users who belong to her friend list; the second visibility level corresponds to the “Public” option that seems to be dominant in the default privacy settings offered by the OSN providers as mentioned in (Michota and Katsikas, 2014b); the third available visibility level is the “Only me” option that is set when the content owner decides no one can see her shared content; the fourth level offers the OSN users the option to customize their content visibility based on their personal preferences; herein users can exclude specific user lists or users from the audience that is allowed to see their content. Tagged content items are shared by default with anyone tagged in them. Facebook users are offered with the option to exclude the friends of tagged.

Depending on the type of tagged content items that are interlinked with OSN users’ profiles, different privacy concerns arise. Table 3.1 presents examples of privacy consequences in tagged data categories that may be caused by data breaches. Video tags are included in the “Mention Tag” category, as tags cannot be added to the file directly and appear as part of a sharing post.

Table 3.1 – Examples of Privacy Consequences in Tagged Data Categories

Tagged Data Types	Privacy Consequences
Photo Tags	Disclosure of real names even for unregistered users to OSNs
Mention Tags	Disclosure of private user profiles
Geo Tags	Disclosure of users' location in the physical world
Hashtags	Users' data disclosure in publicly available posts

Geotagging is provided by Facebook through the service named Facebook Places; the visibility of geospatial metadata can be restricted through the offered privacy settings. When Instagram is used via mobile devices, in case a user takes either a photo or a video while connected via Wi-Fi or 3G, her phone logs the coordinates where this multimedia file content was taken. Using this information, a user can add that multimedia file to a Photo/Video Map. This is an easy way to add context to these content types and see photos and videos other Instagram users have taken nearby. By default, adding location is turned off for all photos and videos a user uploads to Instagram. However if a user shares this multimedia file on Facebook, this will be visible by her friends by default.

Hashtag-related privacy settings are vague; if an OSN user publishes a post on her profile to friends only and the post contains a hashtag, the hashtag will be accessible and it will just open and will show the publicly available posts with that tag on Facebook. Due to the privacy restrictions, only friends are allowed to see that post, even though it appears in hashtag searches.

Among multimedia content that is allowed to be shared in OSNs, video sharing is not offered by all OSN platforms. Once Instagram was acquired by Facebook in 2012, a new feature was added namely "Video-Sharing" that allows their users to record a 15-second video.

In Instagram, as in Facebook, although tagging in photos is applied directly on the content element, tags on videos are added only as mention tags that also correspond to specific users' profiles and are received as notifications that inform them when someone mentions them in a tagged post.

Sharing tagged content items in Facebook via other OSNs is possible, but it raises privacy concerns for the users. Tags are not transferred from one OSN to another; instead, tagging should be applied again by using the tagging mechanisms that are offered by the secondary OSN in which the tagged content is also shared. Furthermore, privacy limitations that have been set in the OSN the user has logged in and shared primarily the content are not transferred. If an Instagram user has set her profile to be private, the multimedia files she uploads and accordingly her tagged multimedia files will be visible only to her followers; however, a multimedia file of a user who has not made her profile private will be publicly accessible by anyone who has access to its direct link. The "Privacy & Safety Center" specifies that an Instagram user can make her profile private so that only approved followers can see her posts. Sending a follower request is required for getting access to private profiles' posts.

OSNs that support registration via plug-ins provide access to the specific Instagram multimedia files for each registered user of the corresponding OSN to see. Thus, it is necessary for any OSN user to check the privacy settings on the connected accounts. For instance, if a user has her Instagram connected to Facebook, she should confirm that her sharing settings on Facebook are not set to "Public" but to "Friends". This setting can be applied via the Instagram app in her Facebook applications settings where she can set the visibility per application.

Reporting services have also been developed by the OSNSPs, aiming to face the malware and virus penetration in their online communities. In most cases, reporting is used as a corrective action after an incident has been occurred; however, reporting tools have also been used in cases where suspicious content may look like with a threat.

In March 2011, Facebook presented a tool called "Social Reporting" that enables the users to report suspicious content not only to the Facebook providers but also to the members who belong to their friend list. When a Facebook user reports a tagged content item, they declare that they do not like the corresponding tagged content by clicking the "I don't like this post" option. Then, the users are requested by Facebook to help its providers understand what has happened by explaining the reason why they made the report. Four options are offered to the users, namely "It's annoying or not interesting", "I 'm in this tagged content and I do not like it", "I think it should not be on Facebook" and "It's spam". After choosing one of these options the users are transferred to a new page that allows them to decide what they can do after the reporting. Removing a tag and hiding it from the tagged users' timeline are the most popular actions that the users select in such cases. They can also choose to block, unfollow or unfriend the user who tagged them in the related post. Users are also offered with the option to give feedback directly to the content owner via Facebook messenger. If a user declares that they do not like the tagged photo, they have to explain the reason why this is the case; they should specify whether the related content is inappropriate, embarrassing or dissatisfying. After this step, they can perform one of the suggested actions mentioned before.

If a user considers that this content should not be on Facebook, they have to justify their option. First, they should report whether the tagged content is nudity or pornography; second, they should specify whether they or their family are willing to share this content on Facebook or not; third, they should explain whether this post humiliates them or someone they know; they can choose the last option if the tagged content is inappropriate, annoying or not funny. In the next step, an extra action is given in these cases that allow users to submit to Facebook for review.

If the tagged post is spam, with an eye towards helping the OSN providers understand the reasons for their reporting, extra options such as "It's a spammy post", "User's account has been hacked", and "This is a fake account" are offered to the users. Similarly with the previous cases, the users are then provided with the suggestions mentioned above and they can choose either to block their friend's account or to unfollow her or to unfriend her or simply to remove the tag.

A customized option is offered to the users, if none of the above reasons can describe why they would like this content to be removed from Facebook. If the users select this option, they are transferred to a new page with five extra reasons that may match in their incident. The first choice presents the case that the tagged content insults or attacks someone based on her religion, ethnicity or sexual orientation; the second choice describes the case that the tagged content advocates violence or harm to a person or an animal; the third choice pertains to the case that the tagged content displays someone harming herself or planning to harm herself; the fourth choice pertains to incidents of buying or selling drugs, guns or related products; last but not least, in the fifth choice, the case of unauthorized use of the tagged users' intellectual property is presented.

Privacy conflicts that lead to data leakage by letting users' PII exposed to unknown audiences occur due to the fact that multiple connected users may have different privacy limitations over their sharing, on one hand, and due to the lack of collaborative privacy controls on the other (Madejski, Johnson, & Bellovin, 2011), (Squicciarini, Shehab, & Paci, 2009). How the lack of joint privacy controls over content can inadvertently reveal sensitive information about a user including preferences, relationships, conversations, and photos is discussed in (Thomas, Grier, & Nicol, 2010). It is also proposed therein to mitigate this threat, by adapting Facebook's privacy model to enforce multi-party privacy.

Summing up, both sharing content owners and tagged users need to manage the visibility of their content to different, in some cases overlapping groups.

3.3 Privacy Settings for Tagged Multimedia Content Cannot Fulfil Users' Privacy Intentions

3.3.1 Scenarios

In order to identify possible privacy gaps in multimedia files in general, i.e. in photos and videos, the most common multimedia files that are added to OSN user profiles by using tags, we performed all the visibility options that are offered in Facebook's privacy settings and can be applied between the content owner and the content heir, i.e. the user who is tagged in the content. We used the scenarios we had designed and used in our previous study (Michota & Katsikas, 2015b) when examining the privacy gaps for tagged photos in Facebook.

Real Facebook user profiles were used for this study, which contain their private information, uploaded resources and other types of resources, but have been anonymized in the interest of privacy by using the terms "User *" instead of real names. Without considering a specific friend list, we chose a friend that User A and User B have in common, namely User C to examine the visibility levels by applying all the possible options in privacy settings for each user; then, we investigated the interactions they had with the profiles they are socially connected to.

We use a two level scale social relationship management in both scenarios we examined; Figures 3.1, 3.2 depict this relationship. As seen in Figures 3.1 and 3.2, the tagged content is shared with two social circles namely "Friends" that includes friends of User A and B and "Friends of Friends" that includes the friends of their friends. The "Friends of Friends" social circle includes the friends of tagged by default. The first level allows the data owner to share its content with her friends; the second level is her social circle that allows the owner to interact with her friends. In this level, the friends of her friends develop a relationship with the data owner and they grant indirect and partial access to her resources. The permissions that users have on a tagged content item depend on their roles.

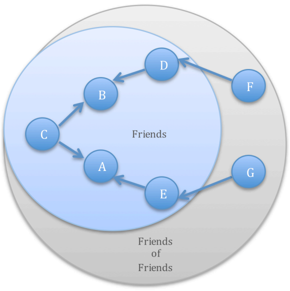


Figure 3.1– Social Graph I

Scenario A: We assume that User A is socially connected with User B in Facebook. Recently, User A found an interesting multimedia file on the web and decided to share it with User B. User A copied the link of the related content and shared it in her profile. Then, User A would like to share this content with User B and tagged her in the uploaded content type.

Thus, in this scenario, we assume that User A is the data owner, i.e. the person who shared the multimedia file and then she tagged it; User B is the tagged user, i.e. the person to whom the multimedia file was added to her profile. As seen in Figure 3.1, in this Scenario, User C is the friend that User A and B have in common in "Friends" social circle, while there are no mutual friends in "Friends of Friends" social circle. We examined eight cases in this scenario namely Case A.1, where User A sets the "Friends" privacy option, Case A.2 where User A sets the "Public" privacy option, Case A.3 where User A sets the "Only me" privacy option and Case A.4 where User A customizes the audience that will be allowed to see the content she uploaded; these cases are presented in the Tables 3.2 - 3.8. Note that in all cases we examined in both scenarios the privacy option of User A remains unchanged, whereas User B's privacy options vary aiming to cover all the possible visibility combinations that may be applied for tagged content types.

Scenario B: We now assume that User H is a mutual friend of User A's and B's friends. As seen in Figure 3.2, the only difference with Scenario A is that here the "Friends of Friends" social circle includes a friend who is a common friend of User A's and B's friends, i.e. a mutual friend of User D and E, namely User H. We examined two cases in this scenario where User A applies customized privacy settings; these are presented in cases namely Case B.4.2 (i) where User A sets the "Friends of Friends without Friends of Tagged" privacy option and Case B.4.2 (ii) where User A applies the "Friends of Friends" privacy option.

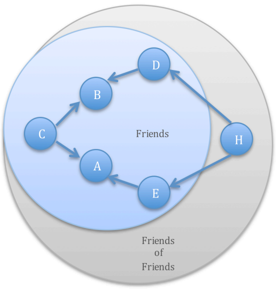


Figure 3.2– Social Graph II

3.3.2 Results

The results of this examination are presented in Tables 3.2 - 3.8. Each table is divided in two main vertical parts; the left part includes the privacy options that the data subjects we selected to examine from the social graph of Figure 3.1 applied for their sharing content, while the right part presents the visibility results collected by this examination.

For instance, as seen in the left part of Table 3.2, the data owner i.e. User A selects her "Friends" as the audience she wishes to share her content with. The tagged user i.e. User B may select any of the offered audience options she wishes to share her tagged content with. The right part of this table then shows who can see this content on either User A's or B's Timelines or on both.

The results of the eight cases namely Case A.1, A.2, A.3, A.4.1, A.4.2 (i), (ii), A.4.3 and A.4.4 we examined in Scenario A are presented below.

Case A.1: User A chooses the tagged content she uploaded to be viewed only by her friends. She has also chosen by default this to be visible by the friends of tagged people, i.e. the friends of User B. Subsequently, as seen in Table 3.2, User B applied all the possible privacy levels that are offered by Facebook for the content that is added to her profile through tags. Based on User A's and B's privacy options, we performed all the privacy visibility combinations that are allowed by Facebook; the results are shown in Table 3.2. These results show that in most cases, User A's friends, i.e. Users B, C, E are allowed to see this content in both timelines; only the customized settings of User B, namely "Only me", "Apart from User C" or "Only User C" restrict the visibility of the tagged content in User B's profile. It should be noted that this might in fact be protective for User B's audience, if the multimedia file was infected with malicious content, as they would not be tricked to watch it. However, despite her intention, it is not possible for User B to make the tagged content item visible to the friends of her friends, as the data owner has granted access only to their friends.

Table 3.2 – Case A.1 - Visibility Combinations for the Tagged Content

Shared with	Data Subjects			Visible to	Who can see the content on	
	User A, Data Owner	User B, Tagged User			User A's Timeline	User B's Timeline
	Friends	Friends			Users A, B, C, E	Users A, B, C, D, E
		Public				Users A, B, C, D, E
		Only me				User B
		Custom	Friends of Friends			Users A, B, C, D, E
			Friends apart from User C			Users A, B, D, E
			Friends of Friends apart from User C			Users A, B, D, E
			Only User C			Users B, C

Case A.2: Now assume that User A changed the visibility of the multimedia file she shared from "Friends" to "Public". The public option has two different meanings for the Facebook audience. If a user has turned on the setting for profile link with search engines, it is easy for everyone on the web to find this user's timeline in search results. If later she changes this setting to off, it may take a while for search engines to stop showing the link to her timeline. Subsequently, User B applied all the possible privacy levels that she can choose for the tagged content.

As it can be seen in Table 3.3, the results in this case show that the sharing content is visible to everyone on User A's timeline. The audience to which the tagged multimedia file on timeline B is made visible is defined according to the privacy settings that User B has applied. In this case, the content owner, i.e. User A has not applied any restrictions to the visibility of tagged content, and User B chooses to whom the tagged content item will be visible regardless of User A's privacy choices.

Table 3.3 – Case A.2 - Visibility Combinations for the Tagged Content

Shared with	Data Subjects			Visible to	Who can see the content on	
	User A, Data Owner	User B, Tagged User			User A's Timeline	User B's Timeline
	Public	Friends			Everyone/ Public	Users A, B, C, D, E
		Public				Everyone/ Public
		Only me				User B
		Custom	Friends of Friends			Users A, B, C, D, E, F
			Friends apart from User C			Users A, B, D, E
			Friends of Friends apart from User C			Users A, B, D, E, F
			Only User C			Users B, C

Case A.3: User A has now changed the visibility of the tagged multimedia file and chose the "Only me" option. This restriction does not allow User B's audience to see the tagged content at all in any timeline. As can be seen in Table 3.4, regardless of what privacy level User B applied, no access to the tagged content was allowed to her audience; User B, who is the tagged user, was also not allowed to see this content on User A's timeline.

Table 3.4 – Case A.3 - Visibility Combinations for the Tagged Content

Shared with	Data Subjects			Visible to	Who can see the content on	
	User A, Data Owner	User B, Tagged User			User A's Timeline	User B's Timeline
	Only me	Friends			User A	Users A, B
		Public				User B
		Only me				Users A, B
		Custom	Friends of Friends			Users A, B
			Friends apart from User C			Users A, B
			Friends of Friends apart from User C			Users A, B
			Only User C			User B

Case A.4: User A used applied customization for the visibility of the tagged content she shared. Customized privacy settings are offered by Facebook when a user is not willing to share her PII with the preselected groups that have been defined in the visibility options in Facebook. Here it is worthwhile to mention that when a user applies customization, two parts should be filled in; in the first part, the user should select with whom she would like to share her tagged content and in the second part she should select who she would like to exclude from the audience who has access to her tagged content. There is a notice in both parts mentioning that anyone tagged will be able to see this post. Cases A.4.1 and A.4.2 examine whether privacy violations occur in the second level of the social relationship scale.

Case A.4.1: User A excluded the friends of the tagged user that are included by default when the "Friends" visibility option is exercised by a Facebook user. Similarly with the previous cases, User B applied every possible privacy option she is allowed to choose.

Table 3.5 – Case A.4.1 - Visibility Combinations for the Tagged Content

	Data Subjects				Who can see the content on	
	User A, Data Owner	User B, Tagged User			User A's Timeline	User B's Timeline
Shared with	Friends (without Friends of Tagged)	Friends		Visible to	Users A, B, C, E	Users A, B, C
		Public				Users A, B, C
		Only me				Users B
		Custom	Friends of Friends			Users A, B, C
			Friends apart from User C			Users A, B
			Friends of Friends apart from User C			Users A, B
			Only User C			Users B, C

As shown in Table 3.5 regardless of which option User B sets for her tagged content visibility, the multimedia file appears on User A's and B's friends; the exception of the friends of the tagged user is only applied for content that appears on User A's timeline without including the mutual friends of User A and B. Consequently, even when User A has selected User B's friends not to see the tagged content item on Timeline B, their mutual friends can have access to it. Hence, User C, who is a common friend of A and B, can see the tagged multimedia file on both timelines. The restrictions that are selected by User B change the visibility of the tagged multimedia file for their mutual friends only to her own timeline. Only when User B excludes User C from the authorized audience, User C will not have access at all to this content item.

Case A.4.2: Two subcases were examined in this case; the first assumes that User A applied the "Friends of Friends without Friends of Tagged" visibility option, whilst the second assumed that she applied the "Friends of Friends" visibility option that includes by default User B's friends to the audience that is authorized to see the tagged multimedia file.

When User A sets the option "Friends of Friends without Friends of Tagged", she excludes the friends of tagged, i.e. the friends of User B from viewing the tagged content. As seen in Table 3.6, although User A has chosen to limit her content visibility, not only the mutual friends of User A and B, i.e. User C, but also all User B's friends, i.e. User D can see the content on both timelines. However, restrictions are applied only in User B's timeline, when

User B sets customized options such as "Friends apart from User C", "Friends of Friends apart from User C" and "Only User C".

Table 3.6 – Case A.4.2 (i) - Visibility Combinations for the Tagged Content

	Data Subjects				**Who can see the content on**	
	User A, Data Owner	User B, Tagged User			User A's Timeline	User B's Timeline
Shared with	Friends of Friends (without Friends of Tagged)	Custom	Friends of Friends	**Visible to**	Users A, B, C, D, E, G	Users A, B, C, D, E, F
			Friends apart from User C			Users A, B, D, E
			Friends of Friends apart from User C			Users A, B, D, E, F
			Only User C			User B, C

No differences in visibility results exist when User A and B both set the option "Friends of Friends". As seen in Table 3.7, although privacy restrictions may be applied by User B, the tagged content item is visible to the users who are friends of both A and B.

Table 3.7 – Case A.4.2 (ii) - Visibility Combinations for the Tagged Content

	Data Subjects				**Who can see the content on**	
	User A, Data Owner	User B, Tagged User			User A's Timeline	User B's Timeline
Shared with	Friends of Friends	Custom	Friends of Friends	**Visible to**	Users A, B, C, D, E, G	Users A, B, C, D, E, F
			Friends apart from User C			Users A, B, D, E
			Friends of Friends apart from User C			Users A, B, D, E, F
			Only User C			User B, C

Case A.4.3: User A applied the same privacy settings as she had set in the previous cases, having excluded a friend she has in common with User B, namely User C. Similarly with the previous cases, User B applied all the possible privacy options for the tagged content. The results of the last case of Scenario A show that when User A has set the option "Friends without Friends of Tagged apart from User C" for the multimedia file she shared, User C is not allowed to see the content on either timeline; The content owner exclusively decides who is authorized to see what she has shared.

Table 3.8 – Scenario A.4.3 - Visibility Combinations for the Tagged Content

Shared with	Data Subjects			Visible to	Who can see the content on	
	User A, Data Owner	User B, Tagged User			User A's Timeline	User B's Timeline
	Friends (without Friends of Tagged) apart from User C	Custom	Friends of Friends		Users A, B, E	Users A, B, E
			Friends apart from User C			Users A, B, E
			Friends of Friends apart from User C			Users A, B, E
			Only User C			User B

Case A.4.4: No differences in the visibility results are noticed, when User A sets the option "Friends of Friends without Friends of Tagged apart from User C".

The results of the two cases namely Case B.4.2 (i), (ii), we examined in Scenario B are presented below:

Cases B.4.2 (i), (ii): By repeating the process followed for Cases A.4.2 (i), (ii) for Scenario B we had designed, we conclude that due to the fact that User H belongs to the lists of User A's and User B's friends of friends, she can see the tagged content item on both timelines. The occurrence of a friend who may belong simultaneously in both "Friends of Friends" lists is not noticed by the users unless a "Like" or a "Comment" appears on the activities feed that is related to the tagged content. Based on the current privacy settings of Facebook, although the visibility restrictions may be applied for the "Friends of Friends", there is no provision for the mutual "Friends of Friends". Thus, without knowing the social relationships that connect users in Facebook, although User B may have chosen her tagged content not to be visible to the friends of her friends, i.e. the content not to be visible to User H who belongs to User D's friends, she may unwillingly reveal her content to User H; the reason why this happens is because User H also belongs to User A's "Friends of Friends" list and "Friends of Friends" is the option that user A set for the multimedia file's visibility.

To sum up, privacy violations occur, even when the content owners have limited the content visibility for the audience of their tagged friends. Mutual friends and friends who belong to "Friends of Friends" lists are special categories whose members have access to the tagged content items although privacy limitations had been put in place. Both categories belong to the groups whose profiles are highly possible to be infected, as they may be tricked by the content that appears in their home pages and be driven to the attackers' pages.

3.4 Results and Discussion

The aim of this chapter was to examine whether the privacy controls that OSNs, in particular Facebook, offer for tagged content match the users' intentions. We approached this issue by examining an exhaustive list of scenarios for privacy settings applied to tagged content, identifying and analyzing the related privacy vulnerabilities. The results of our analysis indicate that privacy violations exist that let the users' PII exposed to unauthorized audience, even if the users have applied settings that limit their content's visibility. The role of content owner seems to be more important than the role of content heir, allowing the former to decide who can see the content she uploaded although this content's visibility may be limited by the latter. Furthermore, the results of this examination indicate that conflicts in privacy preferences arise due to the social relationships that are created among OSN users.

The weaknesses we identified in current privacy management of PII that is added by others highlight the need for taking measures in order to protect the PII that is shared through OSNs. Such measures may include the addition of mechanisms for setting intended audiences with higher granularity; the additional mechanisms should aim to minimize the possibility for privacy conflicts and should let the users select the audience who will have access to their shared content. The privacy intentions of tagged users regarding the sharing content that is added by third parties in their OSN profiles should be fully reflected in the privacy restrictions they apply. Users' privacy intentions should be primarily taken into account when privacy setting menus are designed; these should provide simple and precise controls for PII privacy management. Moreover, data governance improvements are necessary for ensuring data quality, easier access, and managed data security and privacy. The implementation of data governance models facilitates the specification of decision rights and provides an accountability framework that encourages desirable user behavior in all PII lifecycle stages; processes, roles and standards that ensure the effective and efficient use of users' PII are defined in data governance models. Last but not least, the data subjects should be allowed to make all decisions regarding the settings of the privacy of their data; they should determine and approve access and use of their PII; in general, they should approve all governance actions that may have privacy risk impact on their PII.

Chapter 4 Privacy Risk-based Review

Empirical privacy evaluation in OSNs may provide a better understanding of the effectiveness and the efficiency of the default privacy controls and those customized by the users. Proper user perception of the privacy risk could restrict possible privacy violation issues by enabling user participation in actively managing privacy. In this chapter, we assess the current state of play of OSN privacy risks. To this end, a new data classification model is first proposed. Based on this, a method for assessing the privacy risks associated with data assets is proposed, which is applied to the case when the default privacy controls are assumed. Recommendations on how the resulting risks can be mitigated are given, which reduce the risk level.

4.1 Background

Privacy expectations may be influenced by the users' sharing activity with the OSN audiences; by each OSN user's privacy preferences; and by the terms of and agreements with the OSN provider. The challenge of sustaining high privacy levels in OSNs is of great importance in an era when data oversharing has exploded (Hicks, 2009). Privacy risk scores daily increase due to the fact that OSN users are publishing willingly their PII treasure; in most cases they also fail to use the privacy features in a manner consistent with their intentions. This is not only attributed to the providers' neglect of designing usable privacy setting interfaces, but also to back-end privacy breaches and vague privacy policy guidelines (Koops, 2014).

The types of risks vary depending on the nature of affected assets; as different types of information are published in online communities, it would be very useful to classify all this data. In (Schneier, 2010), a general taxonomy for social networking data is presented. Then, based on the nature of the data and the reason why this is shared, a different approach is investigated in (Beye, Jeckmans, Erkin, Hartel, Lagendijk, & Tang, 2012); herein, a classification of different types of OSNs and different data contained in OSNs is provided. A privacy framework that classifies users' data, associates privacy concerns with data, classifies viewers of data, determines privacy levels and defines tracking levels is presented in (Ho, Maiga, & Aïmeur, 2009); the cases of Myspace, Facebook and LinkedIn are examined. Beyond the new taxonomy of data types that is proposed in (Richthammer, Netter, Riesner, Sänger, & Pernul, 2014), a metric to assess their privacy relevance is developed for the topmost leading social networks namely Facebook, Google+, Twitter, LinkedIn and Instagram. Serious concerns about which types of PII is processed highlight the need of creating customized groups for this content; in this study, the data taxonomy we recommend is an extension of the classification presented in (Årnes, Skorstad, & Michelsen, 2011).

Privacy grading systems aim to provide detailed information for enhancing users' awareness (Racz, Weippl, & Seufert, 2010). A framework to compute a privacy score of an OSN user is proposed in (Liu & Terzi, 2009). Several studies over the relationship between the social network graph topology and the achievable privacy in OSNs were presented in (Cutillo, Molva, & Onen, 2011) but much work has still to be done. In (Symeonids, Beato, Tsormpatzoudi, & Preneel, 2015), a new model and a privacy scoring formula are proposed that aim to calculate the amount of PII that may be exposed to Facebook Apps. Moreover, a useful tool in order to detect and report unintended information loss in OSNs that also quantifies the privacy risk attributed to friend relationships in Facebook was presented in (Becker & Chen, 2009). In (Ananthula, Abuzaghleh, Alla, Chaganti, Kaja, & Mogilineedi, 2015), an innovative suggestion inserted the Privacy Index and the Privacy Quotient to measure a user's privacy exposure in an OSN and to measure the privacy of the user's profile.

A quantitative analysis approach is necessary in order to assess privacy impact for OSNs and that is what was provided in (Nepali & Wang, 2015). However, the risk identification seems not to be enough to avoid possible emerging threats that may be concealed in OSN interactions. Privacy policy visualization tools have been proposed presenting the users' privacy issue in a manner more comprehensible than this has used before (Schneier, 2010), (Beye, Jeckmans, Erkin, Hartel, Lagendijk, & Tang, 2012), (Ho, Maiga, & Aïmeur, 2009), (Richthammer, Netter, Riesner, Sänger, & Pernul, 2014), but they have been proved insufficient as they do not cover every aspect of privacy in OSNs. Based on the predicates of a privacy policy model, a privacy policy visualization model for the Facebook case was presented in (Ghazinour, Majedi, & Barker, 2009); this aimed to help both the data providers and the data collectors to better understand the content of designed policies. Three different approaches are inserted in (Birge, 2009) that highlight the need for usable privacy and security field. The effects of visualization on security and privacy were investigated in (Becker & Chen, 2009) and showed that visualization may influence positively the users who can better comprehend the applied safeguarding measures for their PII and make them trust the providers. However, due to the fact that the mobile applications are becoming more and more popular, the need for enhancing users' awareness over possible privacy risks that may arise when installing applications in their mobile devices is apparent. A privacy meter that visualizes such risks through mobile applications on Android devices was presented in (Kang, Kim, Cheong, & Huh, 2015) and seems to make the privacy management easier for the users. Beyond other OSNs, Facebook aims just to make the users keep in mind to choose an audience before they share their content with it. Facebook checkup is a tool that was added in Facebook in 2014 and consists of an audience selector that enables users to review their privacy practices and settings. (What's the Privacy Checkup and how can I find it?, 2015) Although, privacy strength estimators seem to provide acceptable privacy guidelines by helping the users to keep their accounts protected (Burr, Dodson, Newton, Perlner, Polk, Gupta, & Nabbus, 2011), research on the OSN privacy more often than not remains at the level of identifying and analyzing privacy problems, rather than proposing solutions.

In a privacy evaluation framework, the most difficult procedure is to select the proper metrics in order to meet the objectives of the evaluation. A wide variety of privacy metrics has been proposed in the literature to rank the level of protection offered by OSNs. Although OSN users seem to personalize their privacy of the PII they are sharing via their OSN accounts, privacy assurance cannot be guaranteed in various cases (Michota & Katsikas, 2015b), as the privacy control mechanisms seem not to reflect their real privacy intentions. Not only the lack of privacy risk awareness but also the misconception that the privacy controls they set are sufficient to prevent unauthorized access and misuse of their shared PII may cause serious privacy leakage.

To this end, the sharing data is categorized and classified in a common base data model, according to their potential for privacy invasion when sharing them in OSNs. Furthermore, with a view towards creating a common risk register for OSN privacy, we considered the ten most popular Facebook actions (Most popular activities of Facebook users worldwide as of 1st quarter 2016, 2016) and we identified the accordant privacy risks in case of an incident. Then, a visualized risk scoring matrix was designed, aiming to provide awareness to the data subjects that willingly share their PII treasure via their daily social networking interactions.

The aim of this chapter is to propose a simple and easy-to-use method for identifying and analyzing privacy risks in OSNs and then to suggest corrective action plans for them. Privacy risk is defined as the “potential loss of control over personal information” (Featherman & Pavlou, 2003). In this study, the privacy risk is defined as the potential for PII exposure when the privacy levels do not meet or exceed the agreed audience visibility that could result in embarrassment of the data subject. We focus on the privacy risks incurred when a user leaves the default privacy settings unchanged.

Thus, in this study we first intended to assess all the privacy risks that arise through the most common OSN users’ activities and it is highly possible the users to be faced with during their experience in the topmost leading social network i.e. Facebook; and second, to evaluate whether the default privacy controls are sufficient for users’ PII privacy protection. The results of this examination identified and assessed these risks, and then we further proposed risk treatment actions.

The remainder of this chapter is structured as follows: in Section 4.2 we introduce a data classification model to be used for identifying and classifying critical PII. Section 4.3 describes the proposed method for assessing privacy risks and its application to the case of Facebook. Section 4.4 summarizes our conclusions.

4.2 Data Classification

Our proposed classification builds upon (Årnes, Skorstad, & Michelsen, 2011) and extends the taxonomy proposed by Årnes et al. for the personal data processed by Facebook; it also aims to amend deficiencies highlighted in existing taxonomies (Beye, Jeckmans, Erkin, Hartel, Lagendijk, & Tang, 2012), (Schneier, 2010), (Richthammer, Netter, Riesner, Sänger, & Pernul, 2014) that have been proposed for OSN data. First, an overall data analysis and review of the common data categories as they are defined in each OSN were performed. Then, a user-oriented approach was followed by analyzing data that is used in the 10 most popular OSN activities.

Based on the deficiencies we identified in the aforementioned taxonomies, this classification was built around three core pillars:

a. **User-friendly terminology**. Vague terms and inaccurate naming of classes may create wrong perception to the users regarding the content of each class. The ultimate goal of the proposed classification was the users to be familiar with namings that were used in this classification. For instance, OSN users can easily understand a term such as “meta tags” comparing to “metadata” used by Årnes, as the tag feature is one of the most popular functions of Facebook and prepares the users for the data types expected to be included in such a category.

b. **High granularity**. Existing taxonomies present lack of granularity in the definition of data categories; this creates difficulties in verifying what data may be included in these categories.

c. **Completeness.** Previous taxonomies do not cover all available OSN data types, such as missing data related to "Third Party Data" and "Communication Data".

The data categories we defined are the following:

- **Registration Data** is the data that a new user should give to an OSN provider in order to become a member of an OSN and use it.
- **Enriched Profile Data** includes data types that are not mandatory to be completed for retaining an OSN user account, but it is recommended the related data sets to be filled in for enhancing users' OSN activities. This category contains a. text-based data, b. multimedia and c. data that is shared in OSN pages, e.g. contact information, familial information, education information, employment information, visual information etc.
- **Social Graph Data** is the data that describes users' social interaction or declares her ratings/interests such as connection relationship, public endorsement of pages, group membership etc.
- **Publish Sharing** category includes all the data that an OSN user shares on her own pages or what other OSN users share on her pages; OSN user may have control over the content once she shares it or not;
- **Meta-Tags** is the data that is added by others by using labels over sharing content and discloses which users are interlinked with this content. More specifically, this category includes status tagging, photo tagging, geo tagging, hashtagging (Michota & Katsikas, 2015b)
- **Third Party Data** includes the data types that are used when an OSN user enjoys the Facebook integrated third party services like applications, games etc.

- **Financial Data** is any type of purchase data such as credit card information.
- **Connection Data** is the data that shows the activities that are associated with users' Facebook accounts.
- **Communication Data** includes the data that is used to provide communication between two OSN users.

Table 4.1 depicts our proposed data classification for the case of Facebook. The second column aggregates all the data derived from Facebook data analysis; and the last column presents the data categories we classified, identifying them with a Data ID, from D1 to D9.

Table 4.1 – Proposed Data Classification for Facebook

Proposed Data Classification	**Facebook Data Items**	**Data ID**
Registration Data	Display Name, Verified Email, Birthday, Gender, Verified Mobile Phone, Password	D1
Enriched Profile Data 1. Text-based 2. Multimedia 3. Pages	1. Work, Education, Professional Skills, Places you have lived, Contact info (phone, address, other OSN profiles, website, email), Basic info (birthday, gender, nameday, interested in, languages, religious views, political views) Other names, Relationship, Family members, About you, Favorite quotes 2. Photos, Videos 3. Pages	D2, SD2
Social Graph Data	Connections, Groups, Likes, Followings, Events	D3
Publish Sharing	Status/Post (that can be enriched by adding photos, tag, url, what you are up to, check-in)	D4
Meta Tags	Tagged Photos/Videos and Facial Data for tag suggestions status/comments mentions, check-in	D5
Third Party Data	Facebook-integrated Games, Applications, and Websites you and your friends use	D6
Financial Data	Billing Information (Name of banking institution, credit card number)	D7
Connection Data	Log files, Cookies, IP address, Browser type, Device type, GPS location, Time zone	D8
-	-	-
Communication Data	Messenger, Poke, Call	D9

Subcategories are also defined for the cases that sensitive[1] information is included in the main categories; a prefix "S" derived from the term sensitive precedes the Data ID was used for these subcategories in order to be distinguished. Due to the fact that the D2 category also includes political and religious PII, we classified this PII in subcategory SD2.

It is worthwhile to mention that although the "Name" belongs to the contact information category, in this study we will not include it in this area. The reason why this content item is excluded from the scoring matrix is due to the searchability feature that has been embedded in each OSN that makes the name public by default. The provision of the name is the critical element when an individual decides to sign up in an OSN.

4.3 Assessment of Privacy Risks

As mentioned in Section 1.4, the method proposed in this study was based on the ISO 31000:2009 standard. The scope of this risk-based privacy review involves evaluating the privacy levels that are offered by default in OSNs in conjunction with the different types of data that are shared to theses online communities by examining popular OSN actions, starting from the creation of an OSN account until its deletion.

The approach follows four steps:

- risk identification based on possible privacy issues.
- assessment of impact.
- assessment of likelihood
- assessment of privacy related risks

In this study, we first identify the privacy related risks that are met often in OSNs; these are presented and analyzed in section 4.3.1. Section 4.3.2 describes the impact and the likelihood assessment for this study. Impact evaluation was based on two factors, first, the nature of the data that is used in OSNs (see Table 4.4) and second, the type of incident that may occur (see

[1] Article 9 (1), (2): http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

Table 4.3) and we considered three levels, namely low, moderate and major; likelihood evaluation was based on the default visibility levels that are offered in Facebook and we considered three levels, namely low, moderate and high. Last but not least, by applying the results of section 4.3.2, we evaluated the privacy risks (see Table 4.6) that are presented in Section 4.3.3.

4.3.1 Risk Identification

As seen in Table 4.2, we identified the Asset Risks (ARs) for the most common social networking activities and we considered the corresponding privacy issues that may arise during them. We assumed that when an OSN user performs a social networking action, at least one data category as defined in Table 4.1 is affected. For the D2 and D7 data categories that include sensitive data, we considered OSN activities including users' sensitive information as affected assets. The privacy issues identified in association with each OSN action were taken as indicative examples. It should also be noted that this study is not an exhaustive analysis that aggregates the total number of risks that may be concealed in OSNs; it rather presents part of them and highlights the likely repercussions that privacy violations may have to users' PII.

Despite the fact that OSN users may feel protected when they apply strict privacy settings, it is highly possible that privacy breaches may occur. As seen in Table 4.2, risks were identified in the most frequent OSN actions, from the stage of account creation as described in AR1 when examining the case that transparent policy terms and conditions are not provided to the user, until its deletion, as described in AR10 when examining the case of fake reports. In the latter case, after clicking "Report" in Facebook, two options are offered to the user, namely "Report content shared" or "Report this account". Then the user is requested to explain the reasons why she reports an account and suggestions for resolving this problem appear in a new window. Based on the complaint the user described, the options that are recommended include "Unfollow", "Unfriend", "Block", and "Submit to Facebook for Review". Until Facebook evaluates the related reports, the user's PII remains visible in her profile.

Table 4.2 – Asset Risk Matrix in Facebook

OSN Action	Data Category	Privacy Issue	Asset Risk	Risk ID
Create a FB Account	D1	Non transparent policy terms and conditions	Use and disclosure of PII with OSN users' direct consent without providing alternative	AR1
Update your religion and political views	SD2	Collection of data not required for the specified purpose	Misuse of sensitive PII	AR2
Like a page	D3	Selling of users' public endorsement	Unauthorized access of PII to unknown audiences and excessive processing for use	AR3
Update a status by adding mood, location and photo	D4	Excessive collection due to the sharing & merging of datasets	Privacy requirements of the data are not satisfied for the PII combination sharing; PII disclosure occurs.	AR4
Tagged in a photo	D5	No proper implementation of privacy control mechanisms	Unintentional PII disclosure to unknown audiences	AR5
Play a game by installing the suggested app	D6	Sharing of data with Third Parties	Excessive disclosure of PII	AR6
Pay for a page ad	SD7	Operator - side data leakage	Breach of official secrecy during processing of sensitive data	AR7
Remember the device you last logged in	D8	Non anonymity due to identifiers' collection and storage	Disclosure of users' location data/ users' physical presence	AR8
Send a private message	D9	Tracking users' communication	Unauthorized use and access to private discussions	AR9
Deleted content	D4	Fake reports	PII loss	AR10

Missing legal grounds for the processing of users' sensitive data creates serious risks. According to AR2, the update of users' political and religious opinions would be preferable to be avoided.

The public endorsement in OSN pages seems to help advertisers to satisfy their commercial goals. It is not a coincidence that targeted suggestions for pages with content similar to that an OSN user is reading on the internet are created, due to the keyword scanning mechanisms that are used by OSNs. AR3 focuses on the excessive and unauthorized access to the users' PII.

In the case of Facebook, "Nearby friends" is a new feature that was added recently on the top of users' friend list that provides information about users' location and is available through the Facebook mobile application. However, the most popular feature for users' location declaration remains the "check-in". When we tried to combine different content types in a sharing post, we ended up that according to AR4, the most important risk is highlighted because the privacy limitations of the data are not satisfied for the whole dataset.

Even when a user is not willing to share one's PII to one's OSN profile, data disclosure may be achieved from one's friends OSN actions, and as a result private things about one may become visible to unknown audiences. In most cases, users' PII is discovered by content that is added by others, such as tagged data (Michota & Katsikas, 2015b). AR5 describes a similar case with unintentional PII disclosure due to possible conflicts during the implementation of different privacy options between the user who tags the content and the tagged user.

In order to play a game in Facebook, the users are requested to install the suggested app. Users' PII is given to third parties through these applications. According to (Wüest, 2006), when a user accepts the installation of such an app, she gives her permission for accessing her public information, her profile information; she accepts receiving related emails to the registered email address; she is granting access to her posts in "News Feed", to her family and relationship information, to her photos and videos, to her friends' information. AR6 focuses on the excessive collection of users' PII and on the data economy that is not respected during the processing of PII.

When a user buys a page advertisement, the service providers (SPs) collect and process her PII for the financial transaction. Users' payment information includes her credit/debit card number, expiration date, security code, authentication data, billing, shipping and contact information. (Facebook Data Policy, 2017) AR7, the risk that arises in this case, is a possible breach of privacy during processing of sensitive data, assuming that the relevant operator is responsible for the data leakage.

AR8 describes a feature that provides users with direct and quick access to their accounts by giving them the choice of remembering the device they last logged in. However, the collection of identifiers creates risks, as anonymity is not ensured. As seen in AR8, users' location data as well as their physical presence are disclosed.

Facebook messenger is now also available as an independent application for access via mobile devices. However, the content of private messages known as inboxes seems not to be invisible for all Facebook stakeholders. Data mining when links are contained to these messages is a usual phenomenon. As described in AR9, the unauthorized use and access to sensitive discussions create threats for the PII protection when communications are monitored.

Facebook reporting helps the users to protect the social network from any digital threats that can harm the users' privacy. The OSNSP team is available to face incidents and problems such as pornography, hate speech, threats, graphic violence, bullying and spam. After a report has been submitted to the OSNSP team, it is reviewed, and its conformance to the Facebook policies and statements is examined; then, it is decided whether the reported content will be removed or not. Furthermore, notices are received by the users who have shared these content types; actions after reporting include revocation of users' ability; disablement of certain profile features for the user; cancelation of a Facebook account; reporting to law enforcement. Sometimes users' sharing content is deleted due to a number of fake reports. AR10 describes such a case, and as a result PII loss is possible. (OWASP, 2017)

4.3.2 Impact and Likelihood Assessment

According to (Brooks, Garcia, Lefkovitz, Lightman, & Nadeau, 2017), the privacy risk equals the likelihood of an incident occurring times its impact.

The level of impact from a privacy related incident e.g. privacy breaches due to data leakage is the magnitude of harm that results from the consequences of unauthorized disclosure modification, destruction, or loss of PII. The likelihood of a privacy related incident's occurrence is a risk factor that is estimated by analyzing the probability that a given threat is capable of exploiting a given vulnerability.

The nature of the data was used for assessing the impact and the current default privacy controls were used for assessing the likelihood; the stricter the default privacy levels are, the lower the likelihood of PII disclosure is and the more accessible the PII is to bigger audiences, the more possible the PII disclosure is.

For the purpose of our approach, we considered four levels of impact, namely Low, Moderate, Major and Critical, as shown in Table 4.3 below. As stated above, the level of impact is correlated to the repercussions that a possible data breach may have to the PII of the data subjects involved. For instance, loss of tangible PII assets, be they sensitive PII or not is considered to have major impact for the privacy risks we have defined in our study, as there is no possibility of individual access and participation of data subjects to recover their PII. However, in case of unauthorized access and disclosure of PII, data subjects may apply stronger privacy restrictions, in order to mitigate such a type of risk; as a result the impact will be assessed as low.

Table 4.3 – Impact Levels

Potential Impacts	**Impact Levels**	
	PII	**Sensitive PII**
Access/Disclosure	Low	Major
Modification	Moderate	Major
Misuse	Moderate	Major
Loss/Destruction	Major	Major

As seen in Table 4.4, a classification of the data categories we defined in Table 4.1 according to their nature is presented. Whether this PII is sensitive or not was based on the recommendation presented in Directive 95/46/EC (European Parliament and Council of the European Union, 1995).

Table 4.4 – PII Asset Categorization

Data Assets	**Data ID**
PII	D1, D2, D3, D4, D5, D6, D8, D9
Sensitive PII	D2, D7

The assessment of likelihood is based on the default visibility levels namely “Public”, “Friends of friends”, “Friends”, “Only me” that was considered per data category. Three levels were defined, namely Low, Moderate and High. High likelihood means that many people are allowed to see the OSN sharing content; this corresponds to the “Public” option.

Table 4.5 – Likelihood Levels

Default Visibility Levels	Likelihood Levels	
Public/ Everyone	**High**	Users’ content is visible to everyone.
Friends, Friends of Friends	**Moderate**	Users’ content visibility is restricted to specific audiences.
Only Me	**Low**	Users’ content is visible only to the content owner.

Having assessed the impact in case of a data breach and the likelihood of this happening, the evaluation of risk is possible; the assumption of the worst-case scenario with highest possible impact on the data subjects was made.

4.3.3 Risk Assessment

By applying the results of section 4.3.2, the following table 4.6 results:

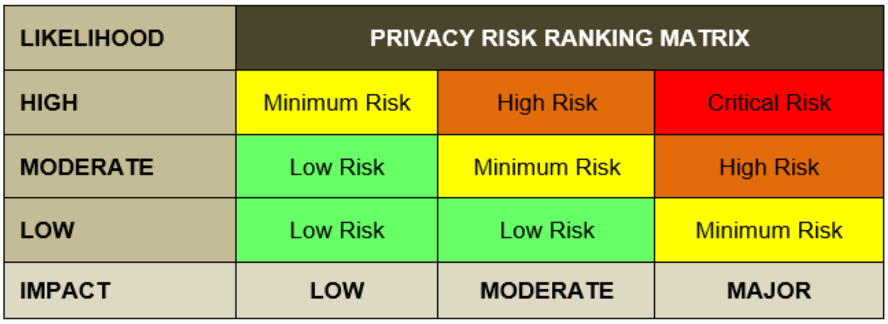
Table 4.6 – Privacy Risks in Facebook

Risk ID	Affected PII Assets	Asset Value	Default Visibility Level	Impact	Likelihood	Risk
AR1	D1	P	F/P	Moderate	Moderate / High	Minimum / High
AR2	D2	S	F	Major	Moderate	High
AR3	D3	P	P	Moderate	High	High
AR4	D4	P	F	Moderate	Moderate	Minimum
AR5	D5	P	FoF	Moderate	Moderate	Minimum
AR6	D6	P	F	Moderate	Moderate	Minimum
AR7	D7	S	M	Major	Low	Minimum
AR8	D8	P	M	Moderate	Low	Low
AR9	D9	P	M	Moderate	Low	Low
AR10	D2, D4	P, S	F	Major	High	Critical

For the Asset Value, we used “P” for Personal information and “S” for Sensitive information. For the visibility level, we considered the four choices that are offered by Facebook. “Only me” (M) is the strictest privacy level that declares that no one can see the sharing PII apart from the content owner. The “Public” (P) choice corresponds to the minimum privacy level and declares that the sharing content is visible to everyone. The intermediate levels are the “Friends” (F) and “Friends of friends” (FoF) privacy choices.

As seen in Table 4.6, two levels were considered for the default visibility level of D1 because a combination of PII is used for the users’ registration. Specifically, while the majority of the information that should be provided for the registration process is visible to users’ friends, the display name and the registration email address are visible to everyone on Facebook. Furthermore, on May 2014, Facebook changed the default post privacy setting from “Public” to “Friends”.

The last column in Table 4.6 shows the risk level of the privacy related incident scenarios. The risk is measured on a three-value qualitative scale and is calculated according to the rules shown in Figure 4.1. The meaning of each value of risk is explained in Table 4.7.



LIKELIHOOD	PRIVACY RISK RANKING MATRIX		
HIGH	Minimum Risk	High Risk	Critical Risk
MODERATE	Low Risk	Minimum Risk	High Risk
LOW	Low Risk	Low Risk	Minimum Risk
IMPACT	LOW	MODERATE	MAJOR

Figure 4.1– Privacy Risk Matrix

Table 4.7 – Risk Levels

Privacy Risk	
Risk level	**Meaning**
Low	Satisfactory privacy levels can ensure PII protection.
Minimum	Privacy levels cannot ensure PII Protection.
High	Unsatisfactory privacy levels for PII protection; corrective action plans should be designed.
Critical	Unacceptable privacy levels for PII protection; catastrophic consequences without recovery chance.

4.3.4 Risk Management

The majority of the risk assessment results show that the privacy levels need improvements; thus, risk management activities should be undertaken in order to address the identified privacy risks. Risk treatment options include modification, retention, avoidance and sharing.

As seen in Table 4.8, we recommend risk treatment actions for the asset risks we identified in Table 4.2. For the asset risks' treatment, the active participation of the user is necessary.

Table 4.8 – Risk Treatment

Risk Treatment Option	OSN User Action
Risk modification	Customization of visibility levels
Risk retention	Direct consent
Risk avoidance	No PII sharing
Risk sharing	Individual PII insurance

Risk modification is the risk mitigation that can be achieved by reducing either the incident's likelihood or its impact. In this study, due to the fact that risk impact was defined based on the PII sensitivity, it is not possible to reduce impact; thus, we selected to reduce the risk likelihood by amending the visibility level.

The majority of the default settings in Facebook tend to make the users' content visible to the public audience (Michota & Katsikas, 2014b). Thus, as seen in Table 4.9, when a user customizes her privacy settings by selecting limited audiences, she can decrease the privacy score without letting her PII exposed to everyone. This grading component is a dynamic field as it can easily change by the user's initiative. Figure 4.2 depicts the new risk scores as decreased after customizing the visibility level.

Benchmarking of best practices also recommend monitoring of changes that would impact individuals' privacy as well as monitoring of the effectiveness of implemented privacy controls.

Table 4.9 – Mitigated Risks in Facebook

Risk ID	**Affected PII Assets**	**Asset Value**	**Default Visibility Level**	**Customized Visibility Level**	**Impact**	**Likelihood**	**Risk**
AR1	D1	P	F/P	**F**	Moderate	**Moderate**	**Minimum**
AR2	D2	S	F	F	Major	Moderate	High
AR3	D3	P	P	**F**	Moderate	**Moderate**	**Minimum**
AR4	D4	P	F	F	Moderate	Moderate	Minimum
AR5	D5	P	FoF	**F**	Moderate	Moderate	Minimum
AR6	D6	P	F	F	Moderate	Moderate	Minimum
AR7	D7	S	M	M	Major	Low	Minimum
AR8	D8	P	M	M	Moderate	Low	Low
AR9	D9	P	M	M	Moderate	Low	Low
AR10	D2, D4	P, S	F	**M**	Major	**Low**	**Minimum**

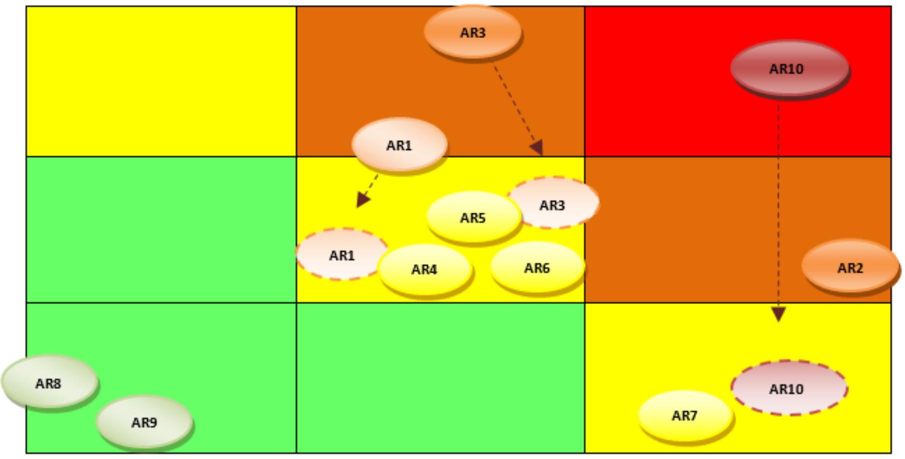


Figure 4.2– Asset Risk Visualization

Risk retention is the handling of risks that cannot be avoided. Additional controls should be implemented in case that risk levels are higher than those assessed based on the risk acceptance criteria. The risk acceptance criteria include: a cost-benefit analysis that compares the estimated benefit with the estimated risk; different risk management techniques for different risk levels; provision for future additional treatment, when it is necessary. When the level of risk does not meet the risk acceptance criteria, the establishment of a retention program that could cover possible privacy gaps through corrective action plans is required. The main goal of this treatment option is the maintenance of consistency with retention practices. As seen in Table 4.8, when we cannot avoid a risk, guidelines that make stakeholders aware of the best practice techniques for the retained risks are recommended.

Risk avoidance means elimination of risk. This can be achieved in two different ways; either the likelihood or the impact of the risk to be set to zero. As seen in Table 4.8, we recommend no sharing of sensitive PII in Facebook or the implementation of "Only me" visibility option for such content types.

When sharing the risk with another party or parties insurance arrangements are performed; insurance partners are used in order to spread responsibility and liability. A risk can be shared either in whole or partially.

4.4 Results and Discussion

The main purpose of this study was to show that when OSN accounts are managed fairly, efficiently and effectively, the privacy risk of breaches may be managed. The research objectives were to assess whether the current framework of privacy controls offered for the management of OSN PII is appropriate and consistent with the users' needs. The results of this examination provide detailed and simple information that allows a non-technical or non-privacy aware person to understand how their PII privacy might be invaded.

The need for enhancements in the current default privacy controls provided by Facebook became evident, as high and critical privacy risks were identified. In view of the reluctancy of the service provider to increase the default privacy levels, users should take the initiative to increase the privacy levels on their sharing PII by following the provided recommendations.

Chapter 5 Privacy Policy

The privacy policies of OSNSPs are criticized as falling short of satisfying their users' privacy expectations letting huge quantities of their PII exposed to unknown audiences. The purpose of this chapter is twofold: to assess the conformance of the privacy policies applied in the five topmost leading OSNs to an internationally acknowledged benchmark such as the ISO 29100:2011 standard, and to propose improvements based on the findings of the assessment. Further, as serious mismatches between these privacy policies and the adherence criteria set out in the ISO 29100:2011 standard were identified, a data lifecycle model is proposed as the basis for an improved OSN privacy policy. A restructuring of the existing policies according to the data lifecycle model will allow them to enjoy characteristics other than actual content that are known to be important in forming users' perceptions.

5.1 Background

Surveys on concerns about general privacy, consumer privacy, medical privacy, and other privacy related areas, as well as indices that allow inferring related trends over time have appeared in the literature since the 70's (Kumaraguru & Cranor, 2005). In a general online service context, a prototype of an online interactive tool embedding features of the concept of online interactive privacy in generic online services, was presented and evaluated in (Kani-Zabihi & Helmhout, 2012). The findings therein suggest that online interactive privacy features increase users' privacy awareness and encourage users to find out more about the uses of their PII. Coles-Kemp and Kani-Zabihi argue in (Coles-Kemp & Kani-Zabihi, 2010) that online SPs and service users want to engage in privacy and consent dialogue and explore how a socio-technical approach should ideally form the basis of the design and implementation of any dialogue system.

People use different OSNs depending on their personal needs. The availability of information brings convenience to modern life; however privacy breaches are increasingly getting in the spotlight and have caught people's attention, raising valid privacy concerns (Acquisti & Grossklags, 2005), (Boyd & Hargittai, 2010).

Privacy in the specific world of OSNs has been the subject of extensive research efforts in the past decade. Since 2005, when Gross and Acquisti published their findings on the potential risks induced by information sharing in Facebook (Gross & Acquisti, 2005), several studies concerning privacy in the online world have appeared in the literature, which shed light on different aspects of privacy in OSNs.

People are concerned about privacy (Gross and Acquisti, 2005), (Vu et al., 2007), but most do not do much about protecting it. This can be attributed to many reasons, including the lack of privacy controls available to the user, the complexity of using the controls and the burden associated with managing these controls for large sets of users. However, perhaps the most important barrier to user involvement with privacy controls is the fact that individuals lack appropriate information to make informed privacy decisions (Acquisti and Grossklags, 2005). In fact, members of OSNs are often under an illusion of privacy, underestimating the privacy risks related to their personal information published in their profiles due to lack of proper privacy awareness (Vemou et al., 2014).

OSN privacy policies should provide the users with an easy and flexible way to inform and enforce their privacy preferences to other users, to third parties and to the OSNSPs. Unfortunately, in most cases, these policies are not clearly and explicitly stated; they are often long and abstruse, thus virtually impossible to understand, even if the user is willing to invest time for reading them (Kayes & Iamnitchi, 2015). Long as they are, these privacy policies tend to be incomplete (Privacy Commissioner of Canada, 2009), as they often cannot include all the parties to which user's private information will be allowed to flow (such as advertisers). Moreover, since the policies are not documented in a manner easily understandable by the average, non-expert user, the OSN provider can modify them without the users noticing it, thus putting the users at great risk of privacy violations (Dwyer, Hiltz, & Passerini, 2007). The result of all this is that generally people do not read the “Terms of Service” and when they do, they do not understand them (Fiesler & Bruckman, 2014), particularly if they are low-level educated (Strater & Lipford, 2008), (Masoumzadeh & Joshi, 2013). It is also known that individuals are more likely to agree with privacy policies on familiar social media websites (Yang, Ng, & Vishwanath, 2015). Hence, on the users’ side, it is apparent that there is a need for OSN privacy policies that will enjoy a number of characteristics, namely appropriate length, high comprehensiveness, low complexity, accessibility, readability, consistency and accuracy; these are equally important factors aside from the actual content of the policy (Capistrano & Chena, 2015).

If such policies were made available, the OSN users would perceive the social networking platforms as more trustworthy (Han & Maclaurin, 2002). On the other hand, the privacy policy determines the OSN provider’s option to monetize user data. Reduced perceived trust on the user’s side leads to reduced willingness to disclose personal information, which in turn limits the data available for monetization (Gerlach, Widjaja, & Buxmann, 2015). Thus, in addition to the obligation that the OSN providers have, according to the social contract theory, to make their privacy policy known to the general public, they also have a financial interest in making sure that these policies and statements are actually communicated properly to their customers (Yang, Ng, & Vishwanath, 2015).

Despite the importance of privacy policies, research on the privacy of OSNs has mostly concentrated on proposing technological and technical solutions to the problem (Díaz & Ralescu, 2012), (Zheleva & Getoor, 2011), (Kayes & Iamnitchi, 2015). All these approaches, however, focus on privacy as an attribute added to the functionality of OSNs, and are not widely adopted by users (Castelluccia & Narayanan, 2012), (London School of Economics, 2010), (Vemou, Karyda, & Kokolakis, 2014). Additionally, most of these works more often than not propose privacy requirements that OSNs to be developed in the future should fulfil (Chen & Williams, 2009); research on the privacy of existing OSNs more often than not remains at the level of identifying and analyzing privacy problems, rather than proposing solutions.

Among three possible privacy protection regimes commonly chosen by market designers or government regulators, namely caveat emptor, seal-of-approval programs, and mandatory standards, the mandatory standards regime is the most effective way of enhancing consumer trust, even though it can be less efficient than the seal-of-approval programs regime in terms of social welfare, in particular for cases in which few consumers are sensitive to privacy and when their potential loss is small (Tang et al., 2008). Standardization bodies such as the International Standardization Organization (ISO), the American National Standards Institute (ANSI), the Canada's Standards Association and the National Institute of Standards and Technology (NIST), have developed privacy frameworks as organizations with responsibility for personal data may have additional audit requirements like those described in ISO 29100:2011 (ISO 29100, 2011), ANSI X9.99:2004 (ANSI, 2004), NIST SP 800-53, 2013 (JTF, 2013), CAN-CSA-Q830-96 (Canadian Standards Association, 1996). Such requirements stem from the need to ensure that PII is adequately protected in accordance with the principles defined in the ISO/IEC 29100 Privacy Framework. Even the most recently updated ISO standard, namely ISO/IEC 27018 (ISO 27018, 2014) that presents a code of practice for the protection of PII in public clouds suggests a set of controls based on the privacy principles of the ISO/IEC 29100 standard.

The ultimate goal of this chapter is to propose a methodology for improving existing OSN privacy policies. In this chapter, we first focus on comparing the ISO 29100:2011 standard privacy framework that describes privacy safeguarding considerations that should be observed when a privacy policy is designed, to the privacy policies of the five topmost leading social networks. The results of this examination indicate serious mismatches that need to be addressed if the policies are to be improved. We further propose a restructuring of the existing policies according to a data lifecycle model; this will allow them to enjoy some of the desirable characteristics reported in (Capistrano & Chena, 2015).

The remainder of this chapter is structured as follows: The need for privacy by design and by default that is outlined by the privacy framework proposed in the ISO 29100:2011 standard is discussed in Section 5.2. In section 5.3 we introduce the privacy policies of the five most popular OSNs, namely Facebook; LinkedIn; Google Plus; Twitter; Instagram. Their conformance to the ISO 29100:2011 principles is examined in section 5.4. Section 5.5 describes our proposal for redesigning existing OSN privacy policies and Section 5.6 summarizes our results and the recommendations of this examination.

5.2 ISO 29100:2011 Privacy by Design and by Default

Privacy by design describes the philosophy of embedding privacy from the outset into the design specifications of web-based technologies. The privacy by design approach has already been put into practice in different application areas. Regulations and various privacy protection policies impose a set of obligations to organizations. Privacy by design and by default has been proposed as an efficient way for dealing with privacy issues in any IT system, by taking privacy requirements into account throughout the system development process, from the conception of the system through to its realization. The underlying motivation for this approach is that, by taking privacy seriously from the start, the final system will be more usable and privacy friendly. Privacy as the default setting aims to deliver the highest level of privacy by ensuring that PII is automatically protected in any given application. If an individual does nothing, her privacy still remains intact. No action is required on the part of the users to protect their privacy. Privacy by default is defined as the privacy that is built into a web application by default.

Privacy by design and by default constitutes a holistic approach of privacy controls aiming to protect users' PII that is completely different from the traditional privacy frameworks that focus on international standards for information practices and remedies for privacy breaches (ISO29100, 2011). The aim of a privacy framework is to guide organizations towards achieving a positive-sum outcome, a win-win solution for the related actors, by ensuring the protection of individuals' privacy without sacrificing functionality or security. Easy-to-use privacy services are keys for enabling users to maintain control of their private data in the online environment. The current privacy framework that is used by the majority of OSNs seems to be unable to cover all the aspects of the OSN users' privacy. However, normal users have to spend much more time than necessary, especially at the beginning, to understand and configure their privacy settings according to their intentions.

ISO/IEC 29100:2011 provides a privacy framework for handling PII. The standard:

- specifies a common privacy terminology;
- defines the actors and their roles in PII processing;
- describes privacy safeguarding considerations; and
- provides references to known privacy principles for information technology

The standard suggests that it is necessary to integrate into a single framework all the parameters that can have impact on the privacy architecture of a service and its properties. The first parameter is the service to be provided. The second parameter is the set of actors involved and their interaction with all PII. Actors' interactions can express the need for an actor to get access to the information given or to ensure that another actor cannot get access to the information. Figure 5.1 depicts in detail the diversity of OSN users and reflects their relationship to the OSN functionality and possible access to the PII of the OSN users. It also describes the access that OSNSPs and Third Party SPs have to PII (Cutillo, Manulis, & Strufe, 2010)

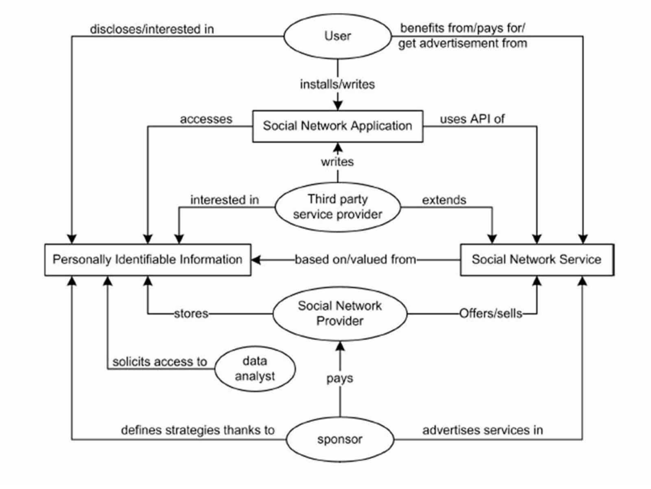


Figure 5.1– Roles and Functionalities in OSNs

OSNSPs play the most important role as they offer social networking services to the users. Sponsors are users who advertise their services to the users through the OSNs. Third party SPs are responsible for extending the content and functionality of OSNs with their own applications. These applications such as quizzes and games are typically executed on the servers under control of these third parties connected to the OSNs via appropriate Application Programming Interfaces (APIs). Often these applications have extensive access to the personal data of OSN users. Last but not least, data analysts are interested in data mining and may also get access to the personal information of users and their activities within the OSNs (Cutillo, Manulis, & Strufe, 2010). Section 5 of the standard focuses on the basic elements of a privacy framework. It discusses actors and roles, interactions, recognizing PII, privacy safeguarding requirements, privacy policies and controls. It identifies four types of actors involved in PII processing, namely the PII principals, controllers, processors and third parties. In most cases, PII controllers and processors are categorized to the OSNSP team. According to the standard, a PII principal does not always have to be identified by name. These different actors (stakeholders) can interact with each other in a variety of ways. The standard includes a table with several different scenarios showing possible information flows between the PII stakeholders. It clarifies how information can be considered as PII e.g. if the information has an identifier that refers to a person, and it regards as PII any information that distinguishes one person from another (e.g., biometric data). The standard clarifies that it may be possible to identify someone even if there is no single attribute that uniquely identifies her. A combination of more than one attributes may be enough to identify the person. Thus, PII is defined as any information that can be used to identify a PII principal (a “data subject”) or that might be linked to a PII principal either directly or indirectly.

Figure 5.2 depicts the data flow for the OSN privacy framework after the ISO privacy compliance examination we performed in our study.

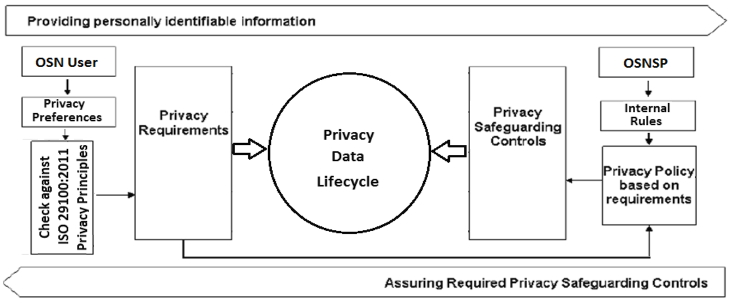

Providing personally identifiable information
OSN User
Privacy Preferences
Check against ISO 29100:2011 Privacy Principles
Privacy Requirements
Privacy Data Lifecycle
Privacy Safeguarding Controls
OSNSP
Internal Rules
Privacy Policy based on requirements
Assuring Required Privacy Safeguarding Controls

Figure 5.2– The Data Flow for the OSN Privacy Framework

In the context of an OSN, the user is the PII principal that provides her PII for processing, gives her consent and determines her privacy preferences for how her PII should be processed. The OSNSP is the PII controller, who determines why and how the PII is to be processed. The OSNSP is also one of the PII processors, who carry out the processing on behalf of the PII controller. Finally, third parties may receive PII from the OSNSP or another PII processor. As privacy safeguarding requirements, we defined the set of requirements (legal, regulatory, contractual, business) that the OSNSP has to take into account with respect to the privacy protection of PII when processing such information. These requirements are met by implementing appropriate privacy controls that are applied throughout the lifecycle of PII, within the context of the privacy policy.

As seen in Figure 5.3, the privacy principles are the motivating force in order to move the wheel that symbolizes the privacy framework that is defined by the ISO standard. However, there is a gap in this “uphill path”, between the ISO standard and the current OSN privacy policy; this gap corresponds to the compliance gap identified in the current privacy policy, as the standard’s privacy principles seem not to be covered. If this gap can be somehow overcome, the ISO 29100:2011 privacy framework will be embedded in the OSN privacy architecture and as a result the privacy principles will be fully implemented into the revised OSN privacy policy.

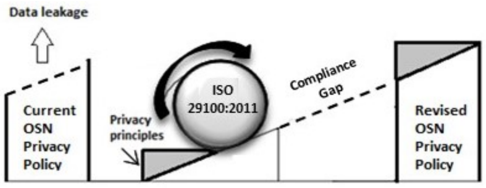


Figure 5.3– ISO 29100:2011 Privacy Framework Incorporation to the OSN Privacy Policy

Figure 5.4 depicts the 11 privacy principles as suggested by the standard; these are to guide the design, development and implementation of privacy policies and controls.

- **Consent and choice:** the PII Principals should be presented with the choice whether to allow or not the processing of their PII, such opt-in and informed consent to be given freely, specific and on a knowledgeable basis.
- **Purpose legitimacy and specification:** the purposes of the processing should comply with the law, and they should be communicated to the PII principals before the PII collection, using clear language.
- **Collection limitation:** collected PII should be limited to what is legal and necessary for the specified purposes.
- **Data minimization:** the PII that is processed should be minimized, as well as the number of entities that have access to it and these entities to be determined on a "need-to-know" principle; interactions and transactions that do not involve the identification of PII principals, reduce the observability of their behavior and limit the linkability of PII should be used; and PII should be deleted and disposed of whenever the purpose for processing it expires.
- **Use, retention and disclosure limitation:** use, retention and disclosure of PII should be limited to what and to when it is necessary for satisfying the specified purposes.
- **Accuracy and quality:** PII must at all times be accurate, complete, up-to-date, adequate and relevant.

- **Openness, transparency and notice:** PII principals must be, at all times, provided with clear, complete and accessible information on the controller's policies regarding the processing of PII.
- **Individual participation and access:** PII Principals should have the ability to simply, quickly and efficiently access and review their PII, to challenge its accuracy and completeness, and to have it modified as appropriate; such modifications have to be communicated to any and all recipients of such PII.
- **Accountability:** PII processing must be performed in ways such that duty of care is demonstrated and practical and concrete measures for its protection must be adopted.
- **Information security:** the security of PII must be ensured with appropriate controls.
- **Privacy compliance:** adherence to privacy safeguarding requirements, laws, and regulations must be verified and demonstrated by means of internal or third party audits and privacy risk assessments.

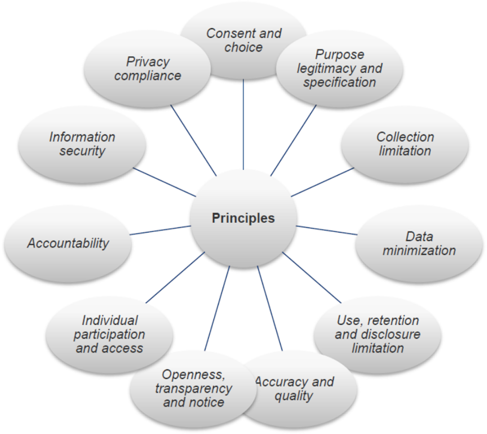

Principles
Consent and choice
Purpose legitimacy and specification
Collection limitation
Data minimization
Use, retention and disclosure limitation
Accuracy and quality
Openness, transparency and notice
Individual participation and access
Accountability
Information security
Privacy compliance

Figure 5.4– ISO 29100:2011 Privacy Principles

5.3 OSN Privacy Policies

Like many websites that collect users information, all OSNs have privacy policies. A privacy policy is a disclaimer informing users about how the OSNSPs deal with users' PII. By accepting the terms of the policy, the users volunteer to relinquish some known rights or privileges they may have by giving their indirect consent to third parties to use their personal data. For example, according to the Facebook's terms of use, the users' uploaded content becomes the property of the OSN. Furthermore, users cannot know if the OSNSP honors its privacy policy. Even if the users apply the strictest privacy settings, they still do not have full control over their personal information. Moreover, the OSNSPs may change their policies at any time.

All OSNs also collect and store other data about their users, such as personal interests; gender; age; education and occupation; and IP addresses. Even after the users delete their profiles, all of their personal information that was collected during their membership is retained for a period of time. For instance, in Facebook, users are simply informed that account reactivation is possible in the future.

It is not a coincidence that the majority of the OSN privacy policies is not only an easy-to understand format policy for other users but also a standardized format policy for SPs and third parties. However, the policy statement is supposed to summarize and disclose data privacy and protection policies, practices and procedures of the sharing content in OSNs.

All OSN privacy policies are structured in parts. The first part explains either in short form or in detail what kinds of information the OSNSPs collect. The remaining parts are not similarly structured.

Facebook's privacy policy (Facebook Privacy Policy, 2016) is also known as the "Data Policy". Facebook has split this policy down to eight parts, namely "What kinds of information do we collect?" (Part I); "How do we use this information?" (Part II); "How is this information shared?" (Part III); "How can I manage or delete information about me?" (Part IV); "How do we respond to legal requests or prevent harm?" (Part V); "How our global services operate?" (Part VI); "How will we notify you of changes to this policy?" (Part VII); and "How to contact Facebook with questions?" (Part VIII).

LinkedIn has split its privacy policy (LinkedIn Privacy Policy, 2016) down to four parts, namely “Information collected” or “What information we collect?” (Part I); “Uses & sharing of personal info” or “How we use your personal information?” (Part II); “Your choices & obligations” (Part III); and the part on “Important information” (Part IV).

Google Plus has split its privacy policy (Google Plus Privacy Policy , 2016) down to twelve parts, namely “Information we collect” (Part I); “How we use information we collect” (Part II); “Transparency and choice” (Part III); “Information you share” (Part IV); “Accessing and updating your personal information” (Part V); “Information we share” (Part VI); “Information security” (Part VII); “When this privacy policy applies” (Part VIII); “Compliance and cooperation with regulatory authorities” (Part IX); “Changes” (Part X); “Specific product practices” (Part XI); “Other useful privacy and security related materials” (Part XII)“.

Twitter recently revised its privacy policy (Twitter Privacy Policy, 2016) and removed two parts; the current privacy policy of Twitter is split down to five parts, namely “Information collection and use” (Part I); “Information sharing and disclosure” (Part II); “Accessing and modifying your personal information” (Part III); “Our policy towards children” (Part IV); “Changes to this policy” (Part V). It is worth pointing out that, in an effort to protect the privacy of the young and to comply with the relevant data protection laws, both Twitter’s and Instagram’s privacy policies include a part on their specific policies towards the collection of children’s PII.

Instagram has split its privacy policy (Instagram Privacy Policy , 2016) down to ten parts, namely “Information we collect” (Part I); “How we use your information” (Part II); “Sharing of your information” (Part III); “How we store your information” (Part IV); “Your choices about your information” (Part V); “Children's privacy” (Part VI); “Other websites and services” (Part VII); “How to contact us about a deceased user” (Part VIII); “How to contact us” (Part IX); “Changes to our privacy policy” (Part X).

5.4 Conformance of the OSN Privacy Policies with the ISO 29100:2011 Standard Privacy Principles

5.4.1 Gap Analysis

Laws and regulations typically carry with them requirements for assessment of compliance, or conformance in the case of standards. In some cases, these are supplemented by methods for assessing conformance that typically lead to certification of conformance. This is, for example the case with some information security standards, such as the ISO/IEC 27002 standard. Unfortunately, it is not yet the case with the ISO/IEC 29100 standard.

The ISO 29100:2011 standard refers to Privacy Impact Assessment (PIA), which is described as that part of risk management that focuses on ensuring compliance with legislation and on assessing privacy implications. According to the standard, privacy safeguarding requirements and PIAs should be part of the organization's risk management framework, and privacy risk management is described as a process. This process should take into account various factors, including legal and regulatory, contractual, business, and others. These other factors include the privacy preferences of PII principals. Organizations should respond to the privacy safeguarding requirements with a set of privacy controls as an outcome of their PIA and treatment. The controls should be embedded in the organization's approach to privacy by design and by default and in its information security management framework.

Many organizations have their own PIA templates but in most cases the topics that should be addressed are common:

- What information is to be collected;
- Why the information is being collected;
- The intended use of the information;
- With whom the information will be shared;
- How the information will be secured;

- What choices the agency made regarding an IT system or collection of information as a result of performing the PIA.

To simultaneously meet their compliance requirements, continuous assessment and adaptation of the privacy controls embedded in OSN privacy architectures are mandatory. This assessment is a typical task of auditing. In summary, to achieve compliance, an organization needs to:

- map abstract controls to concrete control structures and processes;
- enforce the controls in business operations; and
- evaluate the effectiveness of the controls.

Nevertheless, the standard itself does set out the requirements for conformance, by listing in detail criteria for assessing the adherence of a policy to each principle. We evaluated the conformance of the examined OSN privacy policies against the principles of the standard by directly comparing the statements in each policy part with the adherence criteria stated in the standard. Both the policy statements and the criteria are in several cases quite abstract; hence, they can be interpreted in more than one way. Subsequently, the result of the evaluation can only be qualitative. Moreover, full conformance with a principle, as well as full non-conformance is difficult, if at all possible to establish. We have therefore opted for a coarse classification, using two possible outcomes of this evaluation process, namely "largely conformant" and "partially conformant", depending on the (large or some respectively) extent of adherence of a policy (or part of it) to the criteria set out in the standard. When a structured methodology for assessing conformance to ISO 29100, similar to e.g. the one described in ISO 27007:2011 (ISO27007, 2011) for auditing Information Security Management Systems (ISMS) against the ISO 27001:2013 (ISO27001, 2013) standard, becomes available, the use of additional levels of classification will be possible.

For example, adhering to the "Individual participation and access" principle means:

- giving PII principals the ability to access and review their PII, provided that their identity is first authenticated with an appropriate level of assurance and such access is not prohibited by applicable law;
- allowing PII principals to challenge the accuracy and completeness of the PII and have it amended, corrected or removed as appropriate and possible in the specific context;
- providing any amendment, correction or removal to PII processors and third parties to whom personal data had been disclosed, where they are known; and
- establishing procedures to enable PII principals to exercise these rights in a simple, fast and efficient way, which does not entail undue delay or cost.

The third part of Twitter's privacy policy, namely "Accessing and modifying your personal information", states that each user who has created and retains a Twitter account is provided with tools and settings to access, correct, delete, or modify their PII; thus, the ability to simply, quickly and efficiently access and review their PII is given to the PII principals. However, no guarantee is given that amendments will be provided by third parties; hence, the principle is largely conformed to by this policy part.

On the other hand, adhering to the "Openness, transparency and notice" principle means:

- providing PII principals with clear and easily accessible information about the PII controller's policies, procedures and practices with respect to the processing of PII;
- including in notices the fact that PII is being processed, the purpose for which this is done, the types of privacy stakeholders to whom the PII might be disclosed, and the identity of the PII controllers including information on how to contact them;
- disclosing the choices and means offered by the PII controllers to PII principals for the purposes of limiting the processing of, and for accessing, correcting and removing their information; and

- giving notice to the PII principals when major changes in the PII handling procedures occur.

The “How can I manage or delete information about me?” policy part of Facebook does not clearly state where users’ PII is stored; the retention and deletion processing periods are not mentioned; and additional guidelines for account deletion or deactivation are provided, but only via hyperlinks, i.e. in a way that these are not made as easily accessible and visible as possible. Hence, only partial conformance can be established.

5.4.2 Results

The results of the evaluation are comprehensively shown in Tables 5.1 - 5.5. Two symbols are used as entries in these tables. The symbol “+” designates that a policy part is largely conformant with a principle, whereas the symbol “O” designates that a policy part is partially conformant with a principle. The workflow for this examination is presented below in Figure 5.5.

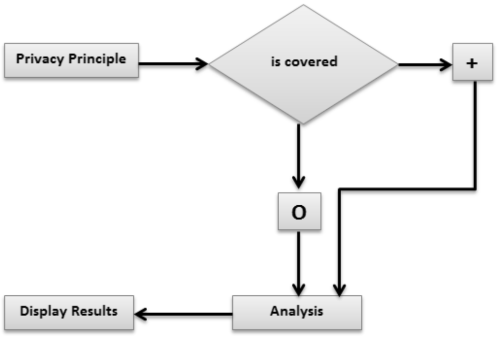


Figure 5.5– Workflow for Mapping Study

Facebook

A new Facebook user is expected to give her consent to share her personal information, otherwise (i.e. if she does not provide all the necessary information or she does not allow the provider to collect it) she will not be allowed to register with this OSN. Thus, her only option for using the service is to accept and agree with all Facebook terms of use. As shown in Table 5.1, the Facebook data use policy part I ("What kind of information do we collect?") satisfies the majority of the ISO privacy principles only to some extent. There are no huge differences in principle coverage between the first and the second part that describe the collection and the processing of the data use policy. Similarly, most of the privacy principles are partially conformed to by the third part of the policy, namely "How is the information shared?". As seen in Table 5.1, no restrictions on the collection and processing of users' PII were highlighted in any policy part. The exception to the rule is the "Accuracy and quality" principle that is applicable to all features of this part. The "Openness, transparency and notice" principle is partially conformed to by half of the policy parts; this is so because the OSNSP seems not to give proper notices about personal data collection and processing, Facebook account maintenance and the overall frameworks that Facebook should follow. The common perception that insufficient protection and security controls are provided by the OSNSP is confirmed by our findings, as the "Information security" and "Privacy compliance" principles are conformed to only partially by all parts of the Facebook Data Use Policy.

LinkedIn

In the case of LinkedIn, similarly with Facebook, if the users do not provide the necessary information, they will not be allowed to create an account on LinkedIn. However, they may still register for a SlideShare account (Slideshare, 2014) and, while they may no longer register for new Pulse accounts (Pulse, 2014), they may continue to use their existing Pulse account. Nothing on Linkedin is performed without the users' consent; thus, the "Consent and choice" principle is largely conformed to by all parts of the Linkedin privacy policy. As shown in Table 5.2, the principles of "Accuracy and quality", "Openness, transparency and notice" and "Individual participation and access" are also largely conformed to in all the LinkedIn privacy policy parts. On the contrary, the "Collection limitation" privacy principle is only partially conformed to by all parts of the policy. This is because not only much data is collected, but the users are also encouraged to share even more PII. There are little differences in principle coverage between the first part ("What information we collect") and the second part ("How we use your personal information") of the privacy policy. The third LinkedIn policy part describes the procedures that are followed when an account is deleted or deactivated. In case of account closing, the logs and backup information that are retained during the deletion process period are depersonalized; thus, adherence to privacy safeguarding requirements is achieved. In case of account deactivation, the policy states that PII retention is possible only when its purpose conforms to LinkedIn's legal obligations and meets the regulatory requirements. The PII retention period is also clearly defined in the policy. The use, the retention and the disclosure of users' PII are limited; hence, the related privacy principle is largely covered by the third policy part of LinkedIn. On the other hand, the "Information security" principle is not largely conformed to in all the parts of the LinkedIn privacy policy. This is because PII integrity, confidentiality and availability are difficult to guarantee when there are interactions of the OSNSP with third parties whose adherence to data protection laws is at least partially unknown.

Google Plus

The findings with regards to the conformance of the Google Plus privacy policy, as shown in Table 5.3, are similar to those with Facebook and LinkedIn. The "Consent and choice" principle is largely conformed to by the majority of its policy parts, letting the user choose whether they allow the Google Plus provider to handle their PII or not. The only ISO29100:2011 privacy principle that is largely conformed to in all the policy parts of Google Plus is the "Accuracy and quality" principle, as all the time the users' PII is accurate and updated. The data subjects seem to be well informed about their PII lifecycle stages as the "Openness, transparency and notice" principle is also largely conformed to in almost all the parts of the policy. Who is accountable in case of PII mishandling is not specified; hence, the "Information security" and the "Privacy compliance" principles are only partially conformed to.

Twitter

User consent, giving the provider the right to collect, transfer, store, disclose its members' PII, is also necessary for using Twitter services. Similarly with other OSNs, the "Consent and choice" privacy principle is largely conformed to. In the case of Twitter, as shown in Table 5.4, the "Collection limitation" and "Data minimization" principles are only partially conformed to in all policy parts. Twitter seems to give clear notices to their data subjects; hence, the "Openness, transparency and notice" privacy principle is largely conformed to in all parts of its policy. Furthermore, Twitter supports the individual participation and access of its users, as it provides the users with mechanisms that allow them to control their PII anytime they want. Similarly with the other three OSNs, before any OSN activity, users should give up some rights in favor of the OSNSP, in order to enjoy Twitter's services. Twitter's privacy policy specifies who is accountable on matters related to the control of its users' PII, depending on the users' location; different contact information is given to residents and to non-residents of the United States. Finally, it is noteworthy that, in contrast to the other four OSNs, all parts of the Twitter privacy policy largely conform to the "Accountability" principle.

Instagram

Only when the Instagram users allow the processing of their PII, i.e. they opt-in, can they become members of this OSN. User consent is necessary for any processing of their PII. The OSNSP seems not to impose any restrictions for PII collection and processing. The use, the retention and the disclosure of PII are also not limited; an exception to this rule is in the special part of the policy that applies to collecting PII of children; this is the only part of the policy that largely conforms to the relevant privacy principle, similarly with Twitter. Furthermore, as seen in Table 5.5, the "Individual participation and access" privacy principle is largely conformed to by almost all the privacy policy parts, as PII principals are able to access and review their PII. Finally, all policy parts other than the "Children's privacy" part, cover the "Information security" and "Privacy compliance principles only partially.

Table 5.1 – Mapping of the Facebook Data Use Policy onto the Privacy Principles of the ISO 29100:2011

		ISO 29100:2011 Privacy Principles										
		Consent and choice	Purpose legitimacy and specification	Collection limitation	Data minimization	Use, retention and disclosure limitation	Accuracy and quality	Openness, transparency and notice	Individual participation and access	Accountability	Information security	Privacy compliance
Facebook Data Use Policy Parts	What kind of information we collect?	+	+	O	O	O	+	O	O	O	O	O
	How do we use this information?	O	O	O	O	O	+	O	O	O	O	O
	How is this information shared?	+	O	O	O	O	+	+	+	O	O	O
	How can I manage or delete information about me?	+	O	O	O	O	+	O	+	O	O	O
	How do we respond to legal request or prevent harm?	O	+	O	O	+	+	+	O	O	O	O
	How our global services operate?	O	O	O	O	O	+	O	O	+	O	O
	How will notify you of changes to this policy?	O	+	O	O	O	+	+	+	O	O	O
	How to contact Facebook with questions?	+	+	O	O	O	+	+	+	+	O	O

Table 5.2 – Mapping of the LinkedIn Privacy Policy onto the Privacy Principles of the ISO 29100:2011

		ISO 29100:2011 Privacy Principles										
		Consent and choice	Purpose legitimacy and specification	Collection limitation	Data minimization	Use, retention and disclosure limitation	Accuracy and quality	Openness, transparency and notice	Individual participation and access	Accountability	Information security	Privacy compliance
LinkedIn Privacy Policy	What information we collect?	+	O	O	O	O	+	+	+	+	O	O
	How we use your personal information?	+	O	O	O	O	+	+	+	+	O	O
	Your choices & obligations	+	+	O	O	+	+	+	+	O	O	+
	Important information	+	+	O	O	O	+	+	+	+	O	O

Table 5.3 – Mapping of the Google Plus Privacy Policy onto the Privacy Principles of the ISO 29100:2011

		ISO 29100:2011 Privacy Principles										
		Consent and choice	Purpose legitimacy and specification	Collection limitation	Data minimization	Use, retention and disclosure limitation	Accuracy and quality	Openness, transparency and notice	Individual participation and access	Accountability	Information security	Privacy compliance
Google Plus Privacy Policy	Information that we collect	+	O	O	O	O	+	O	O	O	O	O
	How we use information that we collect	+	O	O	O	O	+	+	+	O	O	O
	Transparency and choice	+	+	O	O	O	+	+	+	O	O	O
	Information that you share	+	+	O	O	O	+	+	+	O	O	O
	Accessing and updating your personal information	O	+	O	O	+	+	+	+	O	+	O
	Information that we share	+	O	O	O	O	+	+	O	O	O	O
	Information security	+	+	O	O	O	+	+	O	O	+	+
	When this privacy policy applies	+	O	O	O	O	+	+	O	+	O	O
	Compliance and cooperation with regulatory authorities	+	+	O	O	O	+	+	+	O	O	+
	Changes	+	+	O	O	O	+	+	+	O	O	O
	Specific product practices	+	O	O	O	O	+	+	O	+	O	O
	Other useful privacy and security related materials	+	+	O	O	O	+	+	+	O	+	+

Table 5.4 – Mapping of the Twitter Privacy Policy onto the Privacy Principles of the ISO 29100:2011

		ISO 29100:2011 Privacy Principles										
		Consent and choice	Purpose legitimacy and specification	Collection limitation	Data minimization	Use, retention and disclosure limitation	Accuracy and quality	Openness, transparency and notice	Individual participation and access	Accountability	Information security	Privacy compliance
Twitter Privacy Policy	Information collection and use	+	O	O	O	O	+	+	+	+	O	O
	Information sharing and disclosure	+	+	O	O	+	+	+	+	+	O	O
	Accessing and modifying your personal information	+	O	O	O	+	+	+	+	+	O	O
	Our policy towards children	+	+	O	O	+	+	+	+	+	+	+
	Changes to this policy	O	+	O	O	O	+	+	+	+	O	O

Table 5.5 – Mapping of the Instagram Privacy Policy onto the Privacy Principles of the ISO 29100:2011

		ISO 29100:2011 Privacy Principles										
		Consent and choice	Purpose legitimacy and specification	Collection limitation	Data minimization	Use, retention and disclosure limitation	Accuracy and quality	Openness, transparency and notice	Individual participation and access	Accountability	Information security	Privacy compliance
Instagram Privacy Policy	Information we collect	+	O	O	O	O	+	+	+	+	O	O
	How we use your information	+	O	O	O	O	+	O	O	O	O	O
	Sharing of your information	+	+	O	O	O	+	+	+	O	O	O
	How we store your information	+	+	O	O	O	+	+	+	O	O	O
	Your choices about your information	+	O	O	O	O	+	O	+	O	O	O
	Children's privacy	+	+	O	O	+	+	O	+	+	+	+
	Other websites and services	+	O	O	O	O	+	+	+	+	O	O
	How to contact us about a deceased user	+	+	O	O	O	+	+	+	O	+	+
	How to contact us	+	+	O	O	O	+	+	+	O	O	O
	Changes to our policy	+	+	O	O	O	+	+	+	O	O	O

5.4.3 Discussion

The landscape emerging from the above findings does not allow the formulation of patterns consistent to all examined OSNs. However, some comparative observations can be made; these are discussed below.

When a user creates and then retain an account in an OSN, she allows the OSNSP to monitor her online activities. Thus, the provider continues to collect information without any restrictions; this can be achieved through the provider's third-party partners. For instance, third-party advertisement partners may share information, such as a browser cookie ID, URLs of visited sites, a mobile device ID, or the cryptographic hash of a common account identifier, with the OSNSP. This data is processed and personalized content appears on the user's news feed. Unfortunately, such types of PII collection, processing and sharing violate the "Purpose, legitimacy and specification", "Information security" and "Privacy compliance" principles. Not only the OSN users choose and allow the OSNSPs to collect and share their PII with their members, but they also agree to share their PII even with third parties, sites and applications that are embedded in the OSNs and with advertisers. Sites and apps that use instant personalization receive the users' IDs and friend lists when they are visited, despite the fact that there is no explicit consent for such data sharing.

Regarding how the OSNSPs use the information they receive from OSN users' profiles, only the "Accuracy and quality" privacy principle seems to be largely conformed to in all the privacy policies. This is not surprising, as most OSNSPs preserve the accuracy and timeliness of the PII. Openness, transparency and clear notices about the way the users' PII is used are provided by the corresponding policy parts of LinkedIn, Google Plus and Twitter, whilst users' participation and access are offered to these OSN users in case they would like to make changes to match their intentions. The "Accountability" privacy principle is largely conformed to only by the corresponding parts of LinkedIn and Twitter.

Furthermore, the OSN policies for PII processing procedure do not fully adhere to the privacy safeguarding requirements. For instance, the LinkedIn privacy policy states that the OSNSPs may provide, and the users may use, other mechanisms similar to the contacts importer, allowing users to upload individual contacts or their entire address book. The mobile applications may allow the OSN users to synchronize their calendar, email, or contacts apps with LinkedIn to show meeting attendees, email correspondents and contacts. As far as the privacy protection and security by using cookies goes, it is claimed that by allowing cookies users help secure Facebook by letting them know if someone tries to access another user's account or engages in activity that violates their terms of use. However, there is a unique identifying code known as "pixel" that is assigned to the users by the OSN and that can be matched with behavior tracked by cookies. This means that third party SPs, such as advertisers, are able to use information gleaned from the OSN to build a profile of a user's life, including linking browsing habits to one's true identity. LinkedIn has clarified that mobile application identifiers are used rather than mobile device identifiers, to help identify the users across their services. The Google Plus privacy policy states that although Google Plus may combine personal information from one service with information, including personal information, from other Google services in order to make it easier for its users to share things with people they know, Google Plus will not combine cookie information with PII unless it has its users' opt-in consent. Most of the times, when users do not accept the use of cookies, they cannot take full advantage of the online services; thus, users are pushed to give their consent and to allow the use of cookies. Hence, the "Information security" and "Privacy compliance" principles are only partially conformed to. Fortunately, the "Openness, transparency and notice" principle is largely conformed to in the policy parts that describe how the OSNSPs use their members' PII. This is so because the data subjects are informed about the data controller policies, and the OSNSPs give proper notices that personal data is being processed, and provide their users with information on how to access and review their personal data; for instance, when users' PII is used in advertising campaigns. Only Instagram provides vague information and a poor description of its pertinent policy.

The maintenance of OSN accounts is, justifiable, a source of privacy concerns for the users. According to the Facebook data use policy, accounts are permanently deleted from the Facebook database at the request of a user, but some information may remain in backup copies and logs for up to 90 days, as stated in the "What's the difference between deactivating and deleting my account?" part of Facebook's "Help Center" and there is no choice for direct and full deletion even if the user so wished. As stated in the LinkedIn privacy policy, if a user decides to close her account(s), her information will be removed from the service within 24 hours. LinkedIn deletes closed account information and will depersonalize any logs or other backup information within 30 days of the account closure. It is also specified by its policy that even if LinkedIn removes a user‘s data, their public data may be displayed in search engine results until the search engine refreshes its cache. The 30 days window is also defined as the limit either for the deactivation or for the deletion of an account on Twitter. Instagram‘s policy on termination or deactivation of an account is that the OSNSP may retain information and users' content for a reasonable time for backup, archival, and/or audit purposes. The maintenance of a Google Plus account is not described in its privacy policy; only guidelines about how users can delete their account are provided (Delete your Google+ profile, 2016).

The data subjects should be aware of the changes and revisions of OSN privacy policies. All the OSN privacy policies dedicate one paragraph to the procedure they follow when they update their privacy policy. They describe how they will notify their members and some of them give their registered users the opportunity to review the policy revised versions. Facebook allows its users to comment on the changes they applied in its policy; Twitter may notify its users via email; Instagram urges its users to review its policy periodically for possible changes. Finally, Google Plus asks for the consent of its users to its privacy policy changes; only when these changes are considered to be significant, will the OSNSP provide a prominent notice.

Due to the negative criticism that OSNSPs have received about their privacy policies, references about the regulatory compliance and global services have been added. It is very important for the users to know which privacy legal/regulatory framework for the collection, use and retention of information is followed by each OSNSP. What is more, in order for the "Purpose, legitimacy and specification" principle to be conformed to, a policy part in the examined OSNs exists that describes how the OSNSP responds to legal requests for disclosing users' PII.

Table 5.6 summarizes the results over all the examined OSNs. As seen in the following Table, only the "Accuracy and quality" privacy principle seems to be largely conformed to in all the privacy policies. This is not surprising, as most OSN service providers preserve the accuracy and timeliness of the PII. To the contrary, the principles of "Collection limitation" and "Data minimization" are only partially conformed to by all OSN privacy policy parts. This is because the collection of data is unlimited, even though sensitive data may also be included, and data processing is not minimized as this would defeat the purpose of achieving the OSN service provider's organization goals.

Table 5.6 – Compliance of the Examined OSNs to the ISO 29100:2011 Principles

		ISO 29100:2011 Privacy Principles										
		Consent and Choice	Purpose legitimacy and specification	Collection limitation	Data minimization	Use, retention and disclosure limitation	Accuracy and quality	Openness, transparency and notice	Individual participation and access	Accountability	Information security	Privacy compliance
OSN Privacy Policy	Facebook	O	O	O	O	O	+	O	O	O	O	O
	Linkedin	+	O	O	O	O	+	+	+	O	O	O
	Google Plus	O	O	O	O	O	+	O	O	O	O	O
	Twitter	O	O	O	O	O	+	+	+	+	O	O
	Instagram	+	O	O	O	O	+	O	O	O	O	O

5.5 PII Lifecycle Management

5.5.1 Existing OSN Privacy Policies

The preceding analysis highlighted shortcomings in the privacy policies of the examined OSNs with respect to the ISO 29100:2011 standard. Should these shortcomings be addressed by the respective OSNSPs in redesigning their privacy policies, and should the privacy policy redesign process be informed by appropriate strategies, such as those in (Langheinrich, 2001) or (Hoepman, 2014), as suggested in (Vemou, Karyda, & Kokolakis, 2014), the quality of the content of existing OSN privacy policies would be significantly improved. However, in order to improve their comprehensiveness, readability and simplicity as well, policy restructuring is also required.

By creating a common structure it would be easier for the users to understand the privacy policy of each OSN, as well as to identify differences among such policies, thus allowing them to offer their knowledgeable informed consent to the processing of their PII. It would also be easier to check the privacy policies for compliance to any and all existing or future legal or regulatory frameworks, and to have it certified for conformance against internationally respected, voluntary or mandatory, benchmarks and standards.

In order for the resulting policies to be conformant with the end-to-end lifecycle protection principle of the privacy by design framework (Cavoukian, 2010), it is proposed to re-structure the OSN privacy policies by following the stages of an information lifecycle model that represents the flow of information within the OSN throughout its life cycle, from creation and initial storage to the time when it becomes obsolete and is deleted.

Several information life cycle models have been proposed for different purposes (Ball, 2012). For our purposes herein, as seen in Figure 5.6 a simple model, comprising five stages suffices. The first stage is the collection of users' PII, e.g. the creation of their profile. The next stage, processing, includes possible modifications to the provided information. PII storage is the third stage. PII transfer translates to the internal sharing and to the external dissemination/publication of information. The last stage is the maintenance of the PII that includes PII destruction and retention.

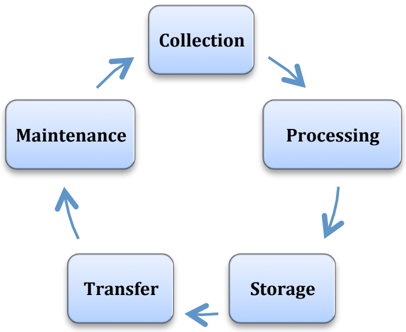


Figure 5.6– PII Lifecycle

Aiming to address the users' concerns, we propose a new OSN model privacy policy, based on the PII lifecycle stages. By designing this model privacy policy, we aim to cover the majority of the users' privacy concerns. This study included Facebook, Google Plus, Twitter, LinkedIn and Instagram and concluded that their privacy policies map only to few of the data lifecycle stages. The mapping of the recently OSN privacy policies onto the PII lifecycle stages are shown in Tables 5.7 - 5.11.

In order to map the examined OSN privacy policies parts to the PII lifecycle stages, we used the methodology introduced in (Michota & Katsikas, 2014a), (Michota & Katsikas, 2014c). The results are shown in Tables 5.7 - 5.11. Two symbols were used for the mapping; the symbol "●" designates that all the necessary information that should be contained to describe in detail a PII lifecycle stage is provided by a policy part, whereas the symbol "○" designates that a PII lifecycle stage is only partially covered by a policy part. Partial coverage may be highlighted in more than one policy parts, as information about a PII lifecycle stage may be addressed in different policy parts. Complete lack of PII lifecycle coverage is also possible. In addition to the PII lifecycle stages that were presented in the previous section, one more part was added, namely "Service Management"; this should be embedded in the proposed model privacy policy and should include guarantees for regulatory compliance as well as change and contact management issues.

As seen in Table 5.7, the Facebook privacy policy fully covers the first stage of the PII lifecycle on its first part. Information for the rest lifecycle stages is included in more than one parts of the policy.

Table 5.7 – Mapping of the Facebook Privacy Policy Parts onto the PII Lifecycle Stages

	Collection	Processing	Storage	Transfer	Maintenance	Service Management
What kind of information we collect?	●					
How do we use this information?		○	○			
How is the information shared				○		
How can I manage or delete information about me?			○		○	
How do we respond to legal request or prevent harm?		○			○	
How our global services operate?				○		○
How will we notify you of changes to this policy?						○
How to contact Facebook with questions?						○

As it can be seen in Table 5.8, the privacy policy of Google Plus follows a structure based on a privacy principle coverage model as presented in the ISO 29100:2011 standard. The information provided about the PII collection is shortly described, vague with several omissions, as it is not specified what PII is provided by others. The “Information we share” policy part includes specifications about the processing, the sharing and the disclosure of the users’ PII.

The mapping of the recently revised Twitter privacy policy onto the PII lifecycle stages is shown in Table 5.9. According to this mapping, only the PII collection and the PII maintenance among the PII lifecycle stages are fully covered by two Twitter privacy policy parts namely “Information collection and use” and “Modifying your personal information”. In Twitter’s privacy policy, a separate policy part presents the special case of children‘s PII collection, namely “Our policy towards children”.

Table 5.8 – Mapping of the Google Plus Privacy Policy Parts onto the PII Lifecycle Stages

	Collection	Processing	Storage	Transfer	Maintenance	Service Management
Information we collect	○	○	○			
How do we use information we collect	○	○	○			
Transparency and choice	○			○		
Information you share				○		
Accessing and updating your personal information		○			○	
Information we share		○		○		
Information security	○	○	○			
When this privacy policy applies						
Compliance and cooperation with regulatory authorities						○
Changes						○
Specific product practices						○
Other useful privacy and security related materials				○		○

As seen in Table 5.10, not only the first part of the LinkedIn privacy policy but also its second part describes partially the stage of PII collection. Polls and surveys, groups, testimonials, talent recruiting, marketing, sales solutions and pages are some of the PII that is collected by the SPs, according to the second part of the policy. In the same part, the issue of who is authorized to have access to the PII is fully covered. Specifications about the processing stage are given in the last paragraph of the same part but only the data processing within the users' country is presented. "Your choices and obligations" is the title of the third part of the LinkedIn privacy policy that seems not to match to its content, as in this paragraph, deletion, retention and correction of users' accounts are described.

Table 5.9 – Mapping of the Twitter Privacy Policy Parts onto the PII Lifecycle Stages

	Collection	Processing	Storage	Transfer	Maintenance	Service Management
Information collection and use	●	○	○	○		
Information sharing and disclosure		○		○		
Modifying your personal information		○	○		●	
Our policy towards children	○					○
Changes to this policy						○

Table 5.10 – Mapping of the LinkedIn Privacy Policy Parts onto the PII Lifecycle Stages

	Collection	Processing	Storage	Transfer	Maintenance	Service Management
What information we collect?	○		○		○	
How we use your personal information?	○	●	○	●		○
Your choices & obligations					○	
Important information						○

As seen in Table 5.11, in the Instagram privacy policy, the stage of PII collection is fully covered and is analytically described on its first policy part, namely “Information we collect”; the case of gathering children’s PII is also presented. Parts of the remaining PII lifecycle stages are found in more than one policy parts of Instagram.

Table 5.11 – Mapping of the Instagram Privacy Policy Parts onto the PII Lifecycle Stages

	Collection	Processing	Storage	Transfer	Maintenance	Service Management
Information we collect	●	○	○	○		
How we use your information		○	○			
Sharing your information		○	○	○		
How we store your information		○	○	○		
Your choices about your information			○		○	
Children’s privacy	○					
Other websites and services		○		○		
How to contact us about a deceased user					○	
How to contact us						○
Changes to our privacy policy						○

5.5.2 An Improved Privacy Policy Model

Taking into account the gaps we identified in the mapping of OSN privacy policies to the PII lifecycle stages, we recommend an improved privacy policy model that aggregates all the information that should be included in each policy part aiming concurrently to meet the requirements emerged by the ISO29100:2011 privacy principles. Table 5.12 summarizes the mapping results of all the examined OSN privacy policies onto the PII lifecycle stages; after having identified the missing information in each OSN policy part, Table 5.13 presents an improved model that contains all the data we need for creating an effective OSN privacy policy taking into account the principles introduced by the ISO29100:2011.

Table 5.12 – Mapping of the OSN Privacy Policy Parts onto the PII Lifecycle Stages

	Collection	**Processing**	**Storage**	**Transfer**	**Maintenance**
Facebook Data Use Policy	●				
LinkedIn Privacy Policy		●		●	
Google Plus Privacy Policy		○			
Twitter Privacy Policy	●				●
Instagram Privacy Policy	●				

Table 5.13 – Improved OSN Privacy Policy Model

Collection	***Processing***	***Storage***	***Transfer***	***Maintenance***	***Service Management***
Information OSN users provide	Who are processing users' PII	Where the PII is stored	Sharing and disclosure activities	Deletion	Regulatory compliance
Information provided by others	Which are the processing procedures	How the PII is used: • whether it is modified or not; • accountability roles	Proper notices for: • timing • sender • receiver • reference of PII	Deactivation	Policy change management
Connections and networks				Regain access	Contact management
Third parties and affiliates					
Payment information that include users' transaction data					
Log files, addresses and device information					

The first part of an OSN's privacy policy should address the collection of all types of information that the users provide during their membership, regardless of its nature or source or means (i.e. cookies, advertising technologies, web beacons, anonymous identifiers) of collection. To this end, a taxonomy of the OSN data types, such as the one proposed in (Richthammer, Netter, Riesner, Sänger, & Pernul, 2014) must be developed. The policy should also specify which types of information are public by default and which are searchable even when privacy restrictions have been applied; thus, the users will be free to decide which PII types they are willing to share with each OSN audience. This is considered to be one of the users' great concerns, thus, this information should be positioned with an easy view on the OSN platform. This could be done, for instance, by using a symbol that will designate the default visibility level of the PII. When the OSN users' information contains public data, the "earth" symbol could be placed on the left side of the corresponding category, aiming to help the users understand with whom they are going to share their information. When the same category also includes private information or information that the OSN users can customize their content's visibility settings, a symbol such as the "Friends" symbol that is currently used by Facebook or the symbol of the gear could be added next to it. These symbols are recommended, as the majority of the OSN users are familiar with them.

The second part should address the processing procedure that includes the use of and the access to the users' PII and its possible modification for proper (or improper) purposes. In existing policies, the reasons why the SPs use the users' PII are given, but how this is being done, how PII is modified and who is accountable for all forms of processing and who is allowed to access it are not mentioned. If these issues are sufficiently addressed, the "Data minimization" and "Accountability" privacy principles will be fully conformed to.

The third part of the proposed policy, that addresses PII storage, should provide information on where the PII is stored; whether the storage space conforms to the safeguarding requirements; whether access to it is restricted to authorized personnel and whether the data subjects have also access to it. Users should be aware of their PII repository and play also the role of PII administrators when they desire, as stipulated by the "Individual participation and access" principle.

The fourth part of the proposed policy pertains to the transfer of the users' PII. According to the "Purpose, legitimacy and specification" privacy principle, proper notices should be given to the users about the occurrences of PII transfers, such as the timing, the sender, the receiver and reference of the PII involved.

The policy part on maintenance should describe what happens when a user decides to delete, deactivate or regain access to her account. Clear notices about these activities should be given to the data subjects and justifications about temporary or permanent PII storage to the OSN servers should be published in the policies when deletion or deactivation requests have been submitted. Furthermore, information on how legal and regulatory requirements are met should be also provided.

An additional part to the proposed model policy that could cover issues related to the interactions between OSN users and OSN providers would be very useful. This part, entitled “Service Management” should provide information about: a. Regulatory compliance that will cover legal issues, b. Policy change management that will explain issues like notifications about policy modifications, and c. Contact management that will provide guidelines for the communication with the corresponding OSN.

It is important to note that the analysis herein is limited to the stated OSN policies. However, key privacy management gaps exist between privacy policies and privacy controls; hence the policy design guidelines proposed herein should be complemented by a full assessment of the effectiveness of the privacy measures, as suggested in (Anthonysamy, Greenwood, & Rashid, 2013).

In addition, visualization as a means for communicating privacy and security measures has been shown to have a positive effect on the trust that the users have in services (Becker, Heddier, & Öksüz, 2014). Hence, techniques that allow users to easily grasp the privacy risks associated with the privacy policies and with their own personalized privacy settings, analogous to those proposed in (Kang J. , Kim, Cheong, & Huh, 2015), (Yee, Korba, & Song, 2008), (Ghazinour, Majedi, & Barker, 2009) should be also developed and employed in OSNs.

5.6 Results and Discussion

User concerns about the privacy of their personal information that they willingly provide to OSNs in exchange for receiving their services are justified, as manifested by the lack of conformance of the OSNs' privacy policies with the privacy principles established by the ISO 29100:2011 standard. Such policies can be significantly improved by satisfying the requirements set out therein.

The European General Data Protection Directive (GDPR) (European Parliament and Council of the European Union, 2016) establishes the Privacy by Design principle as a legal obligation for privacy protection. However, the abstractness of the legal obligation calls for systematic guidance for adhering to it, such as the guidance provided by international standards. Even though such high-level guidance is provided by existing standards, the need for establishing methodologies and mechanisms for auditing the conformance of Information Communication Technology (ICT) systems, including OSNs, with the requirements set out in the standards becomes apparent. The imminent enforcement of the GDPR calls for standardization bodies to move swiftly in this direction.

The mandatory standards regime is the most effective way of enhancing consumer trust; hence, market designers and government regulators should consider complementing existing or emerging privacy legislation with a requirement to conform, initially perhaps on a voluntary basis, with international privacy standards.

An additional deficiency of existing OSN privacy policies is that users find them difficult to read and understand. One of the reasons for this problem, which leads to reduced privacy protection of PII is the structure of these policies. A common and well-understood model for systematically managing data is to follow an appropriate data lifecycle model. Existing OSN privacy policies do not conform to any such model. We propose that a new model structure for OSN privacy policies, based on the data lifecycle model, could prove useful in alleviating user privacy concerns by making privacy policies more comprehensible and conformant with the ISO 29100:2011 standard.

Chapter 6 Conclusions

This chapter summarizes the findings and contributions of the thesis; identifies its limitations; and outlines directions for future research.

6.1 Summary of Findings and Contributions

We demonstrated that not only the privacy offered by design in OSNs is inappropriate, as privacy management seems to be a challenging and complex procedure for the data subjects, but also the privacy offered by default in OSNs seems to be insufficient for protecting even at a minimum level the users' PII. On the one hand, OSN users seem to have low insight into how to use the safeguarding mechanisms in order to properly manage their PII privacy. On the other, these challenges make the users keep the default privacy setting as recommended by the OSNSPs, although by doing so they grant excessive access to their PII.

We identified significant problems with the privacy of tagged data when examining all the visibility combinations over sharing content with multi-ownership functionality. Improper and inaccurate implementation of the visibility permission levels results in privacy violations.

We identified serious privacy risks in association with popular user interactions with OSNs, when the users retain the default privacy controls. We proposed ways of visualizing and managing these risks.

Legal and regulatory frameworks focus on establishing and maintaining privacy by design and by default in OSN services, as well as on the data subjects' rights enshrined in them. However, laws and regulations seem not to have fully brought upon the desired effects, partly because it takes time for their implementation and much more time until they become fully enforced. Furthermore, although the growing demand for privacy in OSNs is highlighted in several research studies, this comes into conflict with the commercial use of personal data uploaded in online communities. This explains why privacy invasive services seem to be more popular than services developed in line with privacy principles.

Finally, serious mismatches of the OSN privacy policies with the stipulations of the ISO 29100:2011 principles have been identified.

6.2 Limitations

Although this research has reached its aims, it has some unavoidable limitations.

The questionnaire used in our first survey, designed to measure the users' attitude towards the use of privacy settings of Facebook and LinkedIn, might give useful information about the usability of their privacy management interfaces; nevertheless, it seems not to provide enough evidence of the users' actual performance as the population of the experimental group is small compared to the popularity of both OSNs and the total number of their registered users. In particular, only 100 Greek young adults in Facebook and 45 in LinkedIn participated in this user survey; this limits the representativeness of the sample.

Although an exhaustive analysis was performed by examining all the information visibility combinations that may be applied between tagged content owners and heirs against privacy threats, the analysis was limited to cover only a two-level scale of the social relationships created through the OSNs. For instance, we did not examine how the privacy restrictions of users who belong in other social circles and whose profiles may be linked in common tagged content items influence the visibility of this data.

Since the assessment of the privacy risks comes, as all risk assessments do, unavoidably with a certain extent of subjectivity. Furthermore, additional risks may be identified if more user activities are considered.

Last, the compliance gap analysis presented in chapter 5 included a mapping between the OSN privacy policies and the privacy principles proposed in the ISO 29100:2011 standard. The provisions of this standard are not mandatory; thus, it would be of great interest to examine the case of the requirements set by the relevant legislation.

6.3 Future Work

In order to generalize the results of this study, work needs to be done; extended research including more OSNs should be conducted for all the cases we examined. By acknowledging the limitations of this study and by evaluating our findings, we see the need for future research in the field of OSN privacy. In particular:

The weaknesses we identified in current privacy options increase the need for more flexible mechanisms in privacy architectures that will be stable, independent from the social relationship management and adequate to restrict unauthorised users from accessing their data.

In order to fully understand the workings of conflicts of privacy preferences over tagged multimedia content and the privacy problems thereof, a comprehensive model needs to be constructed. To this end, more case studies in other OSNs need to be undertaken, and their results need to be jointly considered; this is one area on which our future work will focus. Additional items for future work are an in depth study of possible technical and procedural measures that can be applied to thwart the consequences of privacy preference conflicts within the existing architectural framework of current OSNs; and the development of data governance models that could be used towards the same purpose.

Although many efforts for raising OSN users' privacy awareness have been made, users seem to repeat the same mistakes over their PII privacy management either because of the challenges they face with the interfaces of privacy controls or because their maturity level against the emerging privacy risks is still low-levelled as wrong privacy risk perception dominates. The need for enhancements in the current default privacy controls was evident by taking into consideration the results of privacy risk assessment we performed. The method proposed in this chapter can be applied to other OSNs as well. It is our intention to pursue this direction of research in the future, so as to develop a comprehensive understanding of the privacy risks of default privacy settings in all popular OSNs, to be subsequently used for recommending appropriate mitigation action to their users. Furthermore, a privacy self-assessment tool will be included in our future work; this will be shared with PII stakeholders in order to receive feedback from the target audience. Moreover, we also intend to focus on providing a fuller picture of the emerging privacy risks in OSNs, by extending our analysis to more interactions.

Stricter laws, standards and regulations increase the levels of the PII privacy that should be provided in online interactions. Effective privacy governance and risk management solutions should be embedded in PII controllers' program, i.e. the OSN providers' privacy programs in order to provide PII privacy assurance as requested. In the course of regulatory implementation, the most important aspect is the data protection obligations to be properly applied and monitored. The compliance gap analysis findings need to be addressed if the policies are to be enhanced. Future work includes the development of a structured methodology for assessing conformance of a privacy policy with the ISO 29100 standard that may pave the way towards certification. It also includes the empirical assessment of the validity of the assumption that an OSN privacy policy restructured according to the model proposed herein leads to improved user comprehension, accessibility, acceptance and usability. It further includes developing and validating an OSN-specific data lifecycle model; and designing, developing and evaluating privacy policy visualization techniques and tools for OSNs.

Bibliography

Årnes, A., Skorstad, J., & Michelsen, L. (2011). *Social network services and privacy*. Technical Report, Datatilsynet. Retrieved May 5, 2015, from: https://www.personuvernd.is/media/frettir/Microsoft-Word---11-00643-5-Part-I---Rapport_Facebook_2011-_april-2011_.pdf

Acquisti, A., & Fong, C. M. (2015). *An Experiment in Hiring Discrimination Via Online Social Networks*. Retrieved March 1, 2016, from SSRN: https://ssrn.com/abstract=2031979

Acquisti, A., & Grossklags, J. (2005). Privacy and Rationality in Individual Decision Making. *Journal of IEEE Security and Privacy, 3* (1), pp. 26-33.

Acquisti, A., Gross, R., & Stutzman, F. (2014). Face Recognition and Privacy in the Age of Augmented Reality. *Journal of Privacy and Confidentiality, 6* (2), pp. 1-20.

Ahern, S., Eckles, D., Good, N. S., King, S., Naaman, M., & Nair, R. (2007). Over-exposed?: privacy patterns and considerations in online and mobile photo sharing. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '07*. ACM, New York, USA, pp. 357-366.

Al-Badi, A., Michelle, O. O., Al Roobaea, R., & Mayhew, P. (2013). Improving Usability of Social Networking Systems: A Case Study of LinkedIn. *Journal of Internet Social Networking & Virtual Communities (JISNVC), 2013. doi: 10.5171/2013.889433*.

American National Standards Institute (ANSI). (2004). *Privacy Impact Assessment Standard*, ANSI X9.99-2004. Retrieved September 20, 2017, from: https://www.ansi.org

Ananthula, S., Abuzaghleh, O., Alla, N. B., Chaganti, S. P., Kaja, P. c., & Mogilineedi, D. (2015). Measuring Privacy in Online Social Networks. *International Journal of Security, Privacy and Trust Management (IJSPTM), 4* (2), pp. 1-9.

Anthonysamy, P., Greenwood, P., & Rashid, A. (2013). Social networking Privacy: Understanding the Disconnect from Policy to Controls. *Journal of Computer Society*, *46* (4), pp. 60-67. doi:10.1109/MC.2012.326

Ball, A. (2012). *Review of Data Management Lifecycle Models*. Retrieved October 20, 2013, from University of Bath: http://opus.bath.ac.uk/28587/1/redm1rep120110ab10.pdf

Barnes, S. (2006). A privacy paradox: Social networking in the United States. *First Monday, Peer-Review Journal on the Internet, 11* (9). Retrieved October 20, 2013, from: http://firstmonday.org/issues/issue11_9/barnes/index.html.

Barth, S., & de Jong, M. D. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Journal of Telematics and Informatics, 34* (7), pp. 1038-1058.

Becker, J., & Chen, H. (2009). *Measuring Privacy Risk in Online Social Networks*. Retrieved July 11, 2017, from http://web.cs.ucdavis.edu/~hchen/paper/w2sp2009.pdf

Becker, J., Heddier, M., & Öksüz, A. (2014). The Effect of Providing Visualizations in Privacy Policies on Trust in Data Privacy and Security". *Proceedings of 2014 47th Hawaii International Conference on System Science*. IEEE Computer Society, Washington, DC, USA, pp. 3224-3232. doi: 10.1109/HICSS.2014.399

Besmer, A., & Lipford, H. R. (2010). Moving beyond untagging: photo privacy in a tagged world. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '10*. ACM, New York, USA, pp. 1563-1572.

Besmer, A., & Lipford, H. R. (2008). Privacy Perceptions of Photo Sharing in Facebook. *Proceedings of the 4th Symposium on Usable Privacy and Security, SOUPS '08*. ACM, Pittsburgh, PA.

Betterley, R. S. (2014). *Cyber/privacy insurance market survey –2014: "Maybe Next Year" Turns Into "I Need It Now"*. Technical Report, International Risk Management Institute, Inc. (IRMI). Retrieved September 10, 2015, from: https://www.irmi.com/online/betterley-report-free/cyber-privacy-media-liability-summary.pdf

Bevan, N., Spinhof, L. (2007) Are Guidelines and Standards for Web Usability Comprehensive?. *Jacko, J.A. (eds) Proceedings of the International Conference on Human-Computer Interaction, HCI 2007*. Springer, Berlin, Heidelberg Lecture Notes in Computer Science, vol 4550, pp. 407–419.

Beye, M., Jeckmans, A., Erkin, Z., Hartel, P., Lagendijk, R., & Tang, Q. (2012). Privacy in online social networks. *Abraham, A. (eds) Computational Social Networks: Security and Privacy, Springer, London*, pp. 87-113. doi: 10.1007/978-1-4471-4051-1_4

Bilge, L., Strufe, T., Balzarotti, D., & Kirda, E. (2009). All your contacts are belong to us: automated identity theft attacks on social networks. *Proceedings of the 18th international conference on World wide web, WWW '09*. ACM, New York, USA, pp. 551-560.

Birge, C. (2009). Enhancing research into usable privacy and security. *Proceedings of the 27th ACM international conference on Design of communication, SIGDOC '09*. ACM, New York, USA, pp. 221-226.

Bonneau, J., Anderson, J., & Danezis, G. (2009). Prying Data out of a Social Network, Social Network Analysis and Mining. *International Conference on Advances in Social Network Analysis and Mining (ASONAM)*. IEEE, pp. 249–254.

Bort, J. (2013). *Business Insider*. Retrieved July 20, 2016, from A High School Coach Was Fired For This Facebook Photo: http://www.businessinsider.com.au/laraine-cook-high-school-coach-fired-over-facebook-photo-2013-11

Botezatu, B. (2015). *Facebook Tag Scams are Back with Malicious Payload*. Retrieved May 14, 2016, from Hot for Security: https://www.hotforsecurity.com/blog/facebook-tag-scams-are-back-with-malicious-payload-11238.html

Boyd, D., & Hargittai, E. (2010). *Facebook privacy settings: Who cares?* Retrieved February 20, 2016, from First Monday: http://firstmonday.org/article/view/3086/2589

Brooks, S., Garcia, M., Lefkovitz, N., Lightman, S., & Nadeau, E. (2017). *NISTIR 8062: An Introduction to Privacy Engineering and Risk Management in Federal Systems*. National Institute of Standards and Technology. Retrieved from: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf

Burr, W., Dodson, D., Newton, E., Perlner, R., Polk, T., Gupta, S., & Nabbus, E. (2011). *NIST SP 800-63-1: Electronic authentication guidelines*. National Institute of Standards and Technology. Retrieved February 13, 2014, from https://www.nist.gov/publications/electronic-authentication-guideline-2.

Canadian Standards Association. (1996). *Model Code for Protection of Personal Information*, CAN-CSA-Q830-96. Retrieved September 20, 2017, from: https://simson.net/ref/RSA/1996.CanadianStandardsAssociation.ModelCodeForProtectionOfPersonalInfo.pdf

Capistrano, E., & Chena, J. (2015). Information privacy policies: The effects of policy characteristics and online experience. *International Journal of Computer Standards & Interfaces , 42*, pp. 24–31. doi: 10.1016/j.csi.2015.04.001

Castelluccia, C., & Narayanan, A. (2012). *Privacy considerations of online behavioural tracking*. Technical Report, ENISA. Retrieved September 5, 2013, from: https://www.enisa.europa.eu/publications/privacy-considerations-of-online-behavioural-tracking

Cavoukian, A. (2010). Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph. D, *International Journal of Identity in the Information Societ*y, *3* (2), pp. 247-251.

Chen, S., & Williams, M.-A. (2009). Privacy in social networks: a comparative study. *Proceedings of Pacific Area Conference on Information Systems, PACIS 2009*. Retrieved September 10, 2013, from: http://aisel.aisnet.org/pacis2009/81.

Coles-Kemp, L., & Kani-Zabihi, E. (2010). On-line Privacy and Consent: A Dialogue, Not a Monologue. *Proceedings of New Security Paradigms Workshop, NSPW'10.* ACM, Massachusetts, USA, pp. 95-105.

Cross-Tab Marketing Services. (2010). Online Reputation in a Connected World. Retrieved Janyary 10, 2013 from: https://www.job-hunt.org/guides/DPD_Online-Reputation-Research_overview.pdf

Cutillo, L. A., Manulis, M., & Strufe, T. (2010). Security and privacy in online social networks. *Furht, B. (Ed.)*, *Handbook of Social Network Technologies and Applications* Springer US, Boston, MA, pp. 497-522. doi: 10.1007/978-1-4419-7142-5_23

Cutillo, L. A., Molva, R., & Onen, M. (2011). Analysis of Privacy in Online Social Networks from the Graph Theory Perspective. *Proceedings of the Global Telecommunications Conference (GLOBECOM 2011).* IEEE. doi: 10.1109/GLOCOM.2011.6133517

Delete your Google+ profile. (2016). Retrieved May 20, 2016, from Google Plus: https://support.google.com/plus/answer/1044503?hl=en

Díaz, I., & Ralescu, A. (2012). Privacy Issues in Social Networks: A Brief Survey. *Greco, S., Bouchon-Meunier, B., Coletti, G., Fedrizzi, M., Matarazzo, B., Yager, R.R. (eds) Advances in Computational Intelligence, IPMU 2012.* 300 of the series Communications in Computer and Information Science, Springer Berlin Heidelberg, pp. 509-518.

Did the Internet Kill Privacy? (2011). Retrieved July 19, 2016, from CBS News : http://www.cbsnews.com/news/did-the-internet-kill-privacy/

Dwyer, C., Hiltz, S. R., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of facebook and myspace. *Proceedings of the Thirteenth Americas Conference on Information Systems (AMCIS 2007).* Retrieved May 5, 2014, from: http://aisel.aisnet.org/amcis2007/339

European Parliament and Council of the European Union. (1995), *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals* *with regard to the processing of personal data and on the free movement of such data*. Retrieved June 10, 2015, from: https://eur-lex.europa.eu/legal-content/en/ALL/?uri= CELEX%3A31995L0046

European Parliament and Council of the European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. Retrieved October 20, 2016, from EUR- Lex: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri= CELEX%3A32016R0679

Facebook Data Policy. (2017). Retrieved July 11, 2017, from https://www.facebook.com/ policy.php

Facebook. (2015). *What's the Privacy Checkup and how can I find it?* Retrieved May 20, 2015, from Facebook: https://www.facebook.com/help/443357099140264

Featherman, M., & Pavlou, P. (2003). Predicting e-services adoption: a perceived risk facets perspective. *International Journal of Human Computing Studies, 59* (4), pp. 451-474.

Feldman, A. J., Blankstein, A., Freedman, M. J., & Felten, E. W. (2012). Social networking with frientegrity: privacy and integrity with an untrusted provider. *Proceedings of the 21st USENIX conference on Security symposium*, Bellevue, WA. USENIX Association Berkeley, CA, USA, pp. 31-31.

Fiesler, C., & Bruckman, A. (2014). Copyright terms in online creative communities. *Proceedings of CHI Conference on Human Factors in Computing Systems, CHI'14, Extended Abstracts on Human Factors in Computing Systems*. ACM, pp. 2551–2556. doi: 10.1145/2559206.2581294

Furnell, S., & Botha, R. A. (2011). Social networks – access all areas?". *Journal of Computer Fraud & Security, 2011* (5), pp. 14-19.

Gerlach, J., Widjaja, T., & Buxmann, P. (2015). Handle with care: How online social network providers' privacy policies impact users' information sharing behavior. *Journal of Strategic Information Systems, 24*, pp. 33–43.

Ghazinour, K., Majedi, M., & Barker, K. (2009). A model for privacy policy visualization. *Proceedings of 33rd Annual IEEE International Computer Software and Applications Conference (COMPSAC '09)*, Seattle, WA, USA. IEEE, pp. 335-340. doi: 10.1109/ COMPSAC.2009.156

Google Plus Privacy Policy. (2016). Retrieved October 7, 2016, from Google Plus: https://www.google.com/policies/privacy

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. *Proceedings of the 2005 ACM workshop on Privacy in the electronic society, WPES '05*. ACM, New York, USA, pp. 71-80.

Han, P., & Maclaurin, A. (2002). Do consumers really care about online privacy? *Journal of Marketing Manage, 11* (1), pp. 35–38.

Henne, B., & Smith, M. (2013). Awareness about Photos on the Web and How Privacy-Privacy-Tradeoffs Could Help. *Proceedings of Financial Cryptography 2013*. Springer Verlag, pp. 131–148.

Hicks, M. (2009). *New Tools to Control Your Experience*. Retrieved September 20, 2013, from Facebook: https://www.facebook.com/notes/facebook/new-tools-to-control-your-experience/196629387130/

Ho, A., Maiga, A. I., & Aïmeur, E. (2009). Privacy Protection Issues in Social Networking Sites. *Proceedings of 7th IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*. Rabat, Morocco. doi: 10.1109/AICCSA.2009.5069336

Hoepman, J.-H. (2014). Privacy Design Strategies. *Cuppens-Boulahia, N., Cuppens, F., Jajodia, S., Abou El Kalam, A., Sans T. (eds) Proceedings of the 29th IFIP TC 11 International Conference, SEC 2014, ICT Systems Security and Privacy Protection*. 428 of the IFIP Advances in Information and Communication Technology book series. Springer, Berlin, Heidelberg, pp 446-459

Holzinger, A. (2005). Usability Engineering Methods for Software Developers. *Magazine of Communications of the ACM - Interaction design and children, 48* (1), pp. 71-74. doi: 10.1145/1039539.1039541

Hom, J. (2002). *The Usability Methods Toolbox Handbook.* Retrieved October 24, 2013, from http://usability.jameshom.com

Hu, H., Ahn, G.-J., & Jorgensen, J. (2013). Multiparty Access Control for Online Social Networks: Model and Mechanisms. *Journal of IEEE Transactions on Knowledge and Data Engineering, 25* (7), pp. 1614 - 1627. doi:10.1109/TKDE.2012.97

Ilia, P., Polakis, I., Athanasopoulos, E., Maggi, F., & Ioannidis, S. (2015). Face/Off: Preventing Privacy Leakage From Photos in Social Networks. *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, CCS '15*. ACM, New York, USA, pp. 781-792.

Instagram Privacy Policy (2016). Retrieved October 7, 2016, from Instagram: https://www.instagram.com/about/legal/privacy

Iofciu, T., Fankhauser, P., Abel, F., & Bischoff, K. (2011). Identifying Users Across Social Tagging Systems. *Proceedings of the 5th International AAAI Conference on Weblogs and Social Media, ICWSM*. Barcelona, Spain. Association for the Advancement of Artificial Intelligence, pp. 522-525

Irani, D., Balduzzi, M., Balzarotti, D., Kirda, E., & Pu, C. (2011). Reverse Social Engineering Attacks in Online Social Networks. *Proceedings of the 8th International Conference on Detection of Intrusions and Malware & Vulnerability Assessment, DIMVA 2011. 6739 of the series Lecture Notes in Computer Science*, Springer Berlin Heidelberg, pp. 55-74.

ISO27001. (2013). *ISO/IEC 27001:2013-Information technology - Security techniques - Information security management systems – Requirements*. Retrieved May 1, 2016, from: https://www.iso.org/standard/54534.html

ISO 27002. (2013). *ISO/IEC 27002:2013 Information Technology – Security Techniques – Code of Practice for Information Security Controls*. Retrieved May 2, 2016, from: https://www.iso.org/standard/54533.html

ISO27007. (2011). *ISO/IEC 27007:2011-Information technology - Security techniques - Guidelines for information security management systems auditing*. Retrieved May 1, 2016, from: https://www.iso.org/standard/42506.html

ISO 27018. (2014). *ISO/IEC 27018:2014, Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors*. Retrieved May 3, 2016, from: https://www.iso.org/standard/61498.html.

ISO29100. (2011). *ISO/IEC 29100:2011-Information technology – Security techniques– Privacy framework*. Retrieved May 5, 2013,from: https://www.iso.org/standard/45123.html

ISO31000. (2009). *ISO 31000:2009 Risk Management - Principles and guidelines*. Retrieved September 5, 2015, from: https://www.iso.org/standard/43170.html

Ivory, M. Y., & Hearst, M. A. (2001). The State of the Art in Automating Usability Evaluation of User Interfaces. *Journal of ACM Computing Surveys (CSUR), 33* (4), pp. 470-516.

Johnson, C. Y. (2009). *At MIT, an experiment identifies which students are gay, raising new questions about online privacy*. Retrieved September 12, 2016, from http://www.utdallas.edu/~muratk/news/globe-version.pdf

Johnson, M., Egelman, S., & Bellovin, S. M. (2012). Facebook and privacy: it's complicated. *Proceedings of the 8th Symposium on Usable Privacy and Security, SOUPS '12*. ACM, New York, USA. doi: 10.1145/2335356.2335369

Joinson, A. (2008). Looking at, looking up or keeping up with people?: motives and use of Facebook”. *Proceedings of ACM CHI 2008 Conference on Human Factors in Computing Systems*, pp. 1027-1036.

Joint Task Force Transformation Initiative (JTF). (2013). *NIST SP 800-53: Security and Privacy Controls for Federal Information*. National Institute of Standards and Technology. Retrieved February 13, 2014, from http://dx.doi.org/10.6028/NIST.SP.800-53r4

Kaiser, T. (2010). *DailyTech*. Retrieved May 23, 2016, from Germany Sues Facebook For Violating Users' Privacy: http://www.dailytech.com/Germany+Sues+Facebook+For+Violating+Users+Privacy/article18976.htm

Kang, J., Kim, H., Cheong, Y. G., & Huh, J. (2015). Visualizing Privacy Risks of Mobile Applications through a Privacy Meter. *Lopez, J. & Wu, Y. (ed.), Proceedings of the 11th International Conference ISPEC 2015, Beijing, China*. Springer, pp. 548–558.

Kani-Zabihi, E., & Helmhout, M. (2012). Increasing Service Users’ Privacy Awareness by Introducing On-Line Interactive Privacy Features. *Proceedings of the 16th Nordic conference on Information Security Technology for Applications, NordSec 2011,* Tallinn, Estonia. Springer-Verlag Berlin, Heidelberg, pp. 131–148.

Kayes, I., & Iamnitchi, A. (2015). *A Survey on Privacy and Security in Online Social Networks*. Retrieved February 20, 2016, from Cornell University Library: http://arxiv.org/abs/1504.03342v1

Kirkpatrick, D. (2010). *The Facebook Effect: The Inside Story of the Company That Is Connecting the World*. Simon and Schuster, New York.

Klemperer, P., Liang, Y., Mazurek, M., Sleeper, M., Ur, B., Bauer, L., et al. (2012). Tag, you can see it!: using tags for access control in photo sharing. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '12*. ACM, New York, USA, pp. 377-386.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Journal of Computers & Security, 64*, pp. 122-134. doi: 10.1016/j.cose.2015.07.002

Koops, B.-J. (2014). The trouble with European data protection law. *Journal of International Data Privacy Law, 4* (4), pp. 250-261. doi: 10.1093/idpl/ipu023

Kosta, E., Kalloniatis , C., Mitrou, L., & Gritzalis, S. (2010). Data protection issues pertaining to social networking under EU law. *Journal of Transforming Government: People, Process and Policy , 4* (2), pp. 193 - 201. doi: 10.1108/17506161011047406

Krishnamurthy, B. (2010). I know what you will do next summer. *ACM SIGCOMM Computer Communication Review, 40* (5), pp. 65-70. Retrieved May 2, 2014, from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.450.2480&rep=rep1&type=pdf

Krishnamurthy, B., & Wills, C. E. (2008). Characterizing privacy in online social networks. *Proceedings of the first workshop on Online social networks, WOSN '08*. ACM, New York, USA, pp. 37-42.

Kumaraguru, P., & Cranor, L. F. (2005). *Privacy Indexes: A Survey of Westin's Studies*. Retrieved May 1, 2011 from Carnegie Mellon University: http://www.cs.cmu.edu/~ponguru/CMU-ISRI-05-138.pdf

Langheinrich, M. (2001). Privacy by design - principles of privacy-aware ubiquitous systems. *Proceedings of the 3rd international conference on Ubiquitous Computing*. Springer-Verlag, London, UK, pp. 273–291.

Levine, D. (1971). *On Individuality and Social Forms*. University of Chicago Press, Chicago.

LinkedIn Privacy Policy (2016). Retrieved October 7, 2016, from LinkedIn: https://www.linkedin.com/legal/privacy-policy

Lipford, H. R., Besmer, A., & Watson, J. Understanding privacy settings in Facebook with an audience view. *1st Conference on Usability, Psychology and Security, UPSEC' 08*, San

Francisco, California. USENIX Association Berkeley, CA, USA, p. 2008.

Liu, K., & Terzi, E. (2009). A framework for computing the privacy scores of users in online social networks. *Proceedings of the 2009 ninth IEEE Intrnational Conference on Data Mining (ICDM09).* IEEE Computer Society, Washington, DC, USA, pp. 288-297. doi: 10.1109/ICDM.2009.21

Liu, Y., Gummadi, K. P., Krishnamurthy, B., & Mislove, A. (2011). Analyzing facebook privacy settings: user expectations vs. reality. *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference, IMC '11.* ACM, New York, USA pp. 61-70.

London School of Economics. (2010). *Study on the economic benefits of privacy-enhancing technologies (PETs).* Retrieved March 8, 2013, from https://londoneconomics.co.uk/blog/publication/study-on-the-economic-benefits-of-privacy-enhancing-technologies-pets/

Mackay, J. (1991). Triggers and barriers to customizing software. *Proceedings of the ACM CHI 91 Human Factors in Computing Systems Conference.* ACM, New York, US, pp. 153–160. doi: 10.1145/108844.108867

Madejski, M., Johnson, M., & Bellovin, S. M. (2011). The Failure of Online Social Network Privacy Settings. Columbia University Academic Commons, *CUCS-010-11.* doi: 10.7916/D8NG4ZJ1

Masoumzadeh, A., & Joshi, J. (2013). Privacy settings in social networking systems: What you cannot control. *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security, ASIA CCS'13.* ACM, New York, USA, pp. 149-154.

Michota, A., & Katsikas, S. (2017b). Default OSN Privacy Settings: Privacy Risks. *Proceedings of the 7th International Conference on e-Democracy (e-Democracy 2017). Katsikas, S., Zorkadis, V. (eds) E-Democracy – Privacy-Preserving, Secure, Intelligent E-Government Services.* 792 of the Communications in Computer and Information Science book series. Springer, Cham. doi: 10.1007/978-3-319-71117-1_5

Michota, A., & Katsikas, S. (2015a). Designing a seamless privacy policy for social networks. *Proceedings of the 19th Panhellenic Conference on Informatics, PCI15, Athens, Greece*. ACM, New York, USA, *pp. 139-143*. doi: 10.1145/2801948.2801998

Michota, A., & Katsikas, S. (2017a). Privacy Protection of Tagged Multimedia Content in Online Social Networks. *International Journal of Electronic Governance, 9* (3/4). doi: 10.1504/IJEG.2017.088222

Michota, A., & Katsikas, S. (2015b). Tagged Data Breaches in Online Social Networks. *Proceedings of 6th International Conference on e-Democracy (e-Democracy 2015). Katsikas, S.K., Sideridis, A.B. (eds.) E-Democracy – Citizen Rights in the World of the New Computing Paradigms*. 570 of the Communications in Computer and Information Science book series, pp. 95–106. Sp*ringer, Cham*. doi: 10.1007/978-3-319-27164-4_7

Michota, A., & Katsikas, S. (2014a). The Compliance of the Facebook Data Use Policy with the Principles of the ISO 29100:2011. *6th International Conference on New Technologies, Mobility & Security, NTMS2014 (Security Track),* Dubai, UAE. Springer-Verlag New York, Inc., pp. 96 - 100. doi: 10.1007/978-3-319-20370-6_6

Michota, A., & Katsikas, S. (2014c). The Compliance of the LinkedIn Privacy Policy with the principles of the ISO 29100:2011. *Revised Selected Papers of the 15th International Workshops on Web Information Systems Engineering - WISE 2014 Workshops - IWCSN 2014, Org2 2014, PCS 2014, and QUAT 2014. Benatallah, B., et al. (eds.) Org2 Workshop - Towards Organization 2.0: Advancements in Enterprise Social Networks*. 9051 of the series Lecture Notes in Computer Science, Springer-Verlag New York, Inc., pp. 72-83. doi: 10.1007/978-3-319-20370-6_6

Michota, A., & Katsikas, S. (2014b). The evolution of privacy-by-default in Social Networks. *Proceedings of the 18th Panhellenic Conference in Informatics, PCI14, Athens, Greece*. ACM, New York, USA, pp. 1-6. doi: 0.1145/2645791.2645823

Mont, M. C., Pearson, S., & Bramhall, P. (2003). Towards accountable management of identity and privacy: Sticky policies and enforceable tracing services. *Snekkenes, E.,* *Gollmann, D. (eds) Computer Security – ESORICS 2003. European Symposium on Research in Computer Security, ESORICS 2003*. 2808 of the series Lecture Notes in Computer Science. Springer, Berlin, Heidelberg.

Most popular activities of Facebook users worldwide as of 1st quarter 2016. (2016). Retrieved July 7, 2017, from Statista, The Statistics Portal: http://www.statista.com/statistics/420714/top-facebook-activities-worldwide/

Nepali, R. K., & Wang, Y. (2015). Privacy impact assessment for online social networks. *Proceedings of the International Conference on Collaboration Technologies and Systems (CTS 2015), Atlanta, GA, USA*. doi: 10.1109/CTS.2015.7210451

Nielsen, J. (2003). *Usability 101: Introduction to Usability*. Retrieved February 10, 2012, from Nielsen Norman Group: https://www.nngroup.com/articles/usability-101-introduction-to-usability/

Nielsen, J. (1993). Usability Engineering. *Morgan Kaufmann Publishers Inc. San Francisco, CA, USA*

Office of the Privacy Commissioner of Canada. (2009). *Privacy Commissioner recommends steps to ensure social networking site better protects the privacy of users and meets the requirements of Canadian privacy legislation*. Retrieved February 20, 2016, from Office of the Privacy Commissioner of Canada: ttps://www.priv.gc.ca/media/nr-c/2009/nr-c_090716_e.asp

Open Web Application Security Project (OWASP). (2017). Retrieved July 11, 2017, from https://www.owasp.org/index.php/Main_Page

Otaiza, R., Rusu, C., & Roncagliolo, S. (2010). Evaluating the Usability of Transactional Websites. *Proceedings of the Third International Conference on Advances in Computer-Human Interactions, ACHI'10*. IEEE, Computer Society Press, pp. 32-37.

Paul, T., Puscher, D., & Strufe, T. (2011). Improving the Usability of Privacy Settings in Facebook. *Journal of Computing Research Repository, abs/1109.6046*

Pesce, J. P., Las Casas, D., Rauber, G., & Almeida, V. (2012). Privacy Attacks in Social Media Using Photo Tagging Networks: A Case Study with Facebook. *Proceedings of the 1st Workshop on Privacy and Security in Online Social Media, PSOSM '12*. ACM, New York, USA. doi: 10.1145/2185354.2185358

Pulse (2014). Retrieved May 20, 2014, from Pulse: www.pulse.me

Racz, N., Weippl, E., & Seufert, A. (2010). A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC). *Chapter Communications and Multimedia Security*. 6109 of the series Lecture Notes in Computer Science, Springer Berlin Heidelberg pp. 106-117.

Richthammer, C., Netter, M., Riesner, M., Sänger, J., & Pernul, G. (2014). Taxonomy of social network data types. *EURASIP Journal on Information Security, 2014* (11).

Rubin, J., & Chisnell, D. (2008). *Handbook of Usability Testing: How to Plan, Design and Conduct Effective Tests*. I. Wiley Publishing. Retrieved September 10, 2013, from http://ccftp.scu.edu.cn:8090/Download/efa2417b-08ba-438a-b814-92db3dde0eb6.pdf

Sanghvi, R. (2009). *Facebook blog: New tools to control your experience*. From Facebook newsroom: https://blog.facebook.com/blog.php?post=196629387130

Schneier, B. (2010). A Taxonomy of Social Networking Data. *International Journal IEEE Security and Privacy, 8* (4), pp. 88-88.

Shneiderman, B. (1991). A Taxonomy and Rule Base for the Selection of Interaction Styles. *Shackel, B., and Richardson, S. (eds.), Human Factors for Informatics Usability. Cambridge University Press*, pp. 325-342.

Slideshare (2014). Retrieved May 20, 2014, from Slideshare: www.slideshare.net

Smith, C. (2013). *Business Insider*. Retrieved May 10, 2014, from Facebook Users Are Uploading 350 Million New Photos Each Day: http://www.businessinsider.com/facebook-350-million-photos-each-day-2013-9

Sophos Security Threat Report. (2012). Retrieved March 1, 2013, from Sophos Security Threat Report: http://www.sophos.com/medialibrary/PDFs/other/ SophosSecurityThreatReport2012.pdf

Squicciarini , A., Xu , H., & Zhang, X. (2011). CoPE: Enabling collaborative privacy management in online social networks. *Journal of the American Society for Information Science and Technol-ogy, 62* (3), pp. 521-534.

Squicciarini, A., Shehab, M., & Paci, F. (2009). Collective privacy management in social networks. *Proceedings of the 18th international conference on World Wide Web*. ACM, New York, USA, pp. 521–530. doi: 10.1145/1526709.1526780

Strano, M. M., & Queen, J. W. (2012). Covering Your Face on Facebook. *Journal of Media Psychology, 24* (4), pp. 166-180.

Strater, K., & Lipford, H. R. (2008). Strategies and struggles with privacy in an online social networking community. *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction, BCS-HCI '08 - Volume 1 Liverpool, United Kingdom*. BCS Learning & Development Ltd. Swindon, UK, pp. 111-119.

Symeonids, I., Beato, F., Tsormpatzoudi, P., & Preneel, B. (2015). Collateral damage of Facebook Apps: an enhanced privacy scoring model. *Journal of IACR Cryptology ePrint Archive, 2015:456*. IACR.

Tang., H. Y., & Smith, M. (2008). Gaining Trust Through Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor. *Journal of Management Information Systems, 24* (4), pp. 153-173.

Thomas, K., Grier, C., & Nicol, D. (2010). unFriendly: multi-party privacy risks in social networks. *Proceedings of 10th International Symposium, PETS 2010*, Berlin, Germany. 6205 of the series Lecture Notes in Computer Science, pp. 236–252. doi: 10.1007/978-3-642-14527-8_14

Thompson, H. H. (2010, August 18). *Scientific American*. Retrieved May 18, 2016, from How I Stole Someone's Identity: https://www.scientificamerican.com/article/anatomy-of-a-social-hack/

Twitter Privacy Policy. (2016). Retrieved September 20, 2016, from Twitter: https://twitter.com/privacy

Vemou, K., Karyda, M., & Kokolakis, S. (2014). Directions for Raising Privacy Awareness in SNS Platforms. *Proceedings of the 18th Panhellenic Conference on Informatics, PCI14, Athens, Greece*. ACM New York, USA, pp. 1-6. doi: 10.1145/2645791.2645794

Vermeeren, A. P., van Kesteren, I. E., & Bekker, M. M. (2003). Managing the Evaluator Effect in User Testing. *Proceedings of the IFIP 9th International Conference on Human Computer Interaction*. IOS Press, pp. 647-654.

Wuёst, C. (2010). *The Risks of Social Networking*. Symantec Report. Retrieved September 5, 2015, from: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_risks_of_social_networking.pdf

Yang, R., Ng, Y. J., & Vishwanath, A. (2015). Do Social Media Privacy Policies Matter? Evaluating the Effects of Familiarity and Privacy Seals on Cognitive Processing. *Proceedings of 2015 48th Hawaii International Conference on System Sciences*. IEEE Computer Society Press, pp. 3463-3472.

Yee, G. M., Korba, L., & Song, R. (2008). Cooperative Visualization of Privacy Risks. *Y. Luo (ed.), 5th International Conference, CDVE 2008*. 5220 of the series Lecture Notes in Computer Science, Springer Berlin Heidelberg, pp. 45-53.

Yin, R. (2009). Case Study Research: Design and Methods. *Volume 5 of Applied Social Research Method*s. SAGE, CA.

Zephoria. (2015). *The Top 20 Valuable Facebook Statistics – Updated September 2016*. Retrieved May 5, 2016, from Zephoria Digital Marketing: https://zephoria.com/top-15-valuable-facebook-statistics/

Zheleva, E., & Getoor, L. (2011). Privacy in Social Networks: A Survey. *Aggarwal, C. (eds) Social Network Data Analytics*. Springer Boston, MA, US, pp. 277-306.

Appendix A: Publications

Michota, A., & Katsikas, S. (2014a). The Compliance of the Facebook Data Use Policy with the Principles of the ISO 29100:2011. *6th International Conference on New Technologies, Mobility & Security, NTMS2014 (Security Track),* Dubai, UAE. Springer-Verlag New York, Inc., pp. 96 - 100. doi: 10.1007/978-3-319-20370-6_6

Michota, A., & Katsikas, S. (2014b). The evolution of privacy-by-default in Social Networks. *Proceedings of the 18th Panhellenic Conference in Informatics, PCI14, Athens, Greece*. ACM, New York, USA, pp. 1-6. doi: 0.1145/2645791.2645823

Michota, A., & Katsikas, S. (2014c). The Compliance of the LinkedIn Privacy Policy with the principles of the ISO 29100:2011. *Revised Selected Papers of the 15th International Workshops on Web Information Systems Engineering - WISE 2014 Workshops - IWCSN 2014, Org2 2014, PCS 2014, and QUAT 2014. Benatallah, B., et al. (eds.) Org2 Workshop - Towards Organization 2.0: Advancements in Enterprise Social Networks*. 9051 of the series Lecture Notes in Computer Science, Springer-Verlag New York, Inc., pp. 72-83. doi: 10.1007/978-3-319-20370-6_6

Michota, A., & Katsikas, S. (2015a). Designing a seamless privacy policy for social networks. *Proceedings of the 19th Panhellenic Conference on Informatics, PCI15, Athens, Greece*. ACM, New York, USA, *pp. 139-143*. doi: 10.1145/2801948.2801998

Michota, A., & Katsikas, S. (2015b). Tagged Data Breaches in Online Social Networks. *Proceedings of 6th International Conference on e-Democracy (e-Democracy 2015). Katsikas, S.K., Sideridis, A.B. (eds.) E-Democracy – Citizen Rights in the World of the New Computing*

Paradigms. 570 of the Communications in Computer and Information Science book series, pp. 95–106. Springer, Cham. doi: 10.1007/978-3-319-27164-4_7

Michota, A., & Katsikas, S. (2017a). Privacy Protection of Tagged Multimedia Content in Online Social Networks. *International Journal of Electronic Governance, 9* (3/4). doi: 10.1504/IJEG.2017.088222

Michota, A., & Katsikas, S. (2017b). Default OSN Privacy Settings: Privacy Risks. *Proceedings of the 7th International Conference on e-Democracy (e-Democracy 2017). Katsikas, S., Zorkadis, V. (eds) E-Democracy – Privacy-Preserving, Secure, Intelligent E-Government Services*. 792 of the Communications in Computer and Information Science book series. Springer, Cham. doi: 10.1007/978-3-319-71117-1_5