IADIS International Journal on WWW/Internet
Vol. 12, No. 2, pp. 16-33
ISSN: 1645-7641

GUIDELINES AND TOOLS FOR INCORPORATING PRIVACY IN SOCIAL NETWORKING PLATFORMS

Konstantina Vemou. *Department of Information and Communication Systems Engineering, University of the Aegean. Samos, GR-83200, Greece.*

Maria Karyda. *Department of Information and Communication Systems Engineering, University of the Aegean. Samos, GR-83200, Greece.*

ABSTRACT

Built-in privacy is important for promoting users' privacy and trust in Social Networking Services (SNS). Up to now, privacy research has its focus on the development and employment of Privacy-Enhancing Technologies as add-on applications and on investigating users' privacy preferences. This paper draws on the principles of privacy-by-design and extends previous literature by identifying privacy requirements for the development of privacy-friendly SNS platforms. The paper also evaluates currently embedded privacy practices in four popular SNS platforms (Facebook, Google+, Twitter and Pinterest) to assess the level of built-in privacy and proposes a list of guidelines and tools SNS platform designers can employ.

KEYWORDS

Privacy by design, privacy requirements, Social Networking Services, Privacy Enhancing Technologies.

1. INTRODUCTION

Social Networking Services (SNS) have gained a place among most visited websites; however privacy breaches are increasingly getting in the spotlight and have caught people's attention, raising privacy concerns (Acquisti and Gross 2006, Boyd and Hargittai 2010).

In SNS information is posted in a continuous, every day flow, as users communicate with friends and share personal information such as photos and location. This provides several entities, including the SNS platform, law enforcement, friends and even non-users of the SNS, access to users' personal information. SNS users are thus exposed to several privacy threats, such as blackmail, secondary use of information or dissemination of misleading information

about the users (ENISA 2007). As a result, users feel discomfort and apply self-censorship (Sleeper et al. 2013), which may lead to quitting the use of the SNS platform, as in the case of excessive commercial exploitation perceptions (Taylor et al. 2011).

Currently, the main focus of privacy research in SNS is on understanding users' privacy attitudes and on designing Privacy-Enhancing Technologies (PETs) for protecting Personal Identifiable Information (PII). PETs that can be applied in SNS include a wide range of applications, such as access controls, privacy signaling tools and social identity management systems. All these approaches, however, focus on privacy as an attribute added to the functionality of SNS, and are not widely adopted by users (ENISA 2012, London Economics 2010). Possible explanations for the low adoption of PETs include low usability, special IT skills requirements, acquisition costs and lack of support by SNS platforms (Vemou and Karyda 2013).

Incorporating privacy mechanisms has since long been identified as a key issue for protecting personal information effectively (Cavoukian 2010, Spiekermann and Cranor 2009), and several approaches have been proposed; however there are still no practical approaches and guidelines for building-in privacy. Lately, the concept of Privacy-by-Design (Cavoukian 2010), aiming at enhancing privacy from the very start of IT design, has emerged as an imperative to privacy protection. Privacy by design principles can guide privacy protection in SNS platforms to enhance users' privacy and bolster trust.

This paper discusses the implementation of Privacy-by-Design principles for providing privacy–friendly services in the context of SNS. We draw on design strategies proposed by Hoepman (Hoepman 2012) and we propose a list of privacy requirements to guide SNS platforms design. Based on the results of the analysis of the scarce privacy practices adopted by popular social media, we provide a list of guidelines and privacy enhancing technologies SNS designers could incorporate to their designs. The rest of the paper is structured as follows: in the following chapter we discuss the concept of privacy by design and proposed approaches to achieve it. In the third section we present a set of privacy requirements to guide privacy-friendly SNS platform design, followed by an evaluation of their embodiment in four popular platforms, to demonstrate only a subset of them is currently incorporated in SNS platforms design. Based on the latter, we propose a set of guidelines and tools for designing privacy friendly platforms, in chapter 5. We conclude with a discussion on open issues and with ideas for further research.

2. INCORPORATING PRIVACY PROTECTION

The idea to build privacy into information systems stems from the argument that when privacy is considered through all phases of systems implementation, it will process PII in a privacy-preserving manner through all its lifecycle (Cavoukian 2010). As basic privacy protection mechanisms will be by default enabled, a minimum level of protection will be provided to all users with limited IT skills that are unable of applying PETs. Also, fundamental privacy issues will be addressed while designing new technology, preventing the need for arduous and costly resolutions at a later stage (Schaar 2010). As the user will be the center of considerations, awareness and transparency options will be provided, to support the needs for providing notice and consent.

The concept of Privacy-by-Design (PbD), introduced by Ann Cavoukian (2010), refers to the introduction of privacy considerations throughout the IT systems implementation cycle and in the process of decision making with regard to business practices (Gürses et al. 2011). It also covers areas, such as business administration and comprises of 7 core principles that drive decisions on how a system will be implemented (Cavoukian 2010):

1. Proactive not Reactive; Preventative not Remedial, meaning that proactive measures to protect privacy are taken, in order to prevent privacy invasive events, instead of trying to resolve and soften consequences from a privacy breach.
2. Privacy as the Default, meaning that privacy is enabled by default in the functionality of a system and it is protected unless the user takes action to change it.
3. Privacy Embedded into Design, meaning that privacy is part of the core functionality of the system, delivered from the beginning without diminishing functionality.
4. Full Functionality—Positive-Sum, not Zero-Sum, meaning that privacy and security can be offered without compromising functionality.
5. End-to-End Lifecycle Protection, meaning that privacy is embedded to the system and is applied to all stages of information processing lifecycle, from its collection to its secure destruction.
6. Visibility and Transparency, meaning that the system will provide insight of the collection and processing processes to all stakeholders, along with ways to verify promised operations.
7. Respect for User Privacy, meaning that the user is considered as the center of the system and is provided with measures to protect his privacy, such as strong privacy defaults, and notice, in a user-friendly manner.

These high-level principles aim to drive practices for PII collection by entities processing personal data, as well as the implementation of their IT systems. They can be interpreted and implemented in different ways, allowing for a wide range of privacy decisions, thus making the PbD concept applicable to all types of business process or IT systems. For instance, PbD application can range from electronic toll pricing systems (Gürses et al. 2011) to health care systems (Cavoukian et al. 2010) and Social Networking Services (Hoepman 2012).

The main element among different approaches to embedding privacy practices to systems' design is data minimization (Shapiro 2010; Gürses et al. 2011). Gürses et al. (2011) introduced a methodology for applying PbD, which includes 5 basic activities: Strict functional requirements analysis; Data minimization; Modeling attackers and threats, in order to foresee privacy issues; Multilateral security requirements analysis, to understand the correct behavior of the system, as all stakeholders may understand it, and Implementation/testing of the design.

Hoepman (2012) distinguishes 8 privacy design strategies that address different aspects of privacy, by analysis of different violating activities. The first strategy is to *minimize*, meaning that the system will collect the minimum amount of personal data. In case of PII collection, these data need to be hidden from plain view, so the second strategy is to *hide.* Distribution in processing and storage of PII (*separation strategy*) should be used wherever is possible, to eliminate chances of users being completely profiled. Also, processing data in the highest data of aggregation, and least detail forms the forth strategy, *aggregate*. The following two strategies, *inform* and *control*, aim at addressing the need for users transparency, in terms of knowledge of which data about them is processed and how, and having control over the processing procedure. The last two strategies *enforce* and *demonstrate* assure that a privacy policy will be present and compatible with legal requirements, along with a mechanism to prove compliance to this policy.

Privacy patterns have been proposed by Shapiro (2010) and Chen (Chen and Williams 2010), who modeled privacy requirements for SNS recommendation systems, based on three axes: i) choice options, ii) consent mechanisms and iii) control devices. In the same context, but specifically addressed to IT implementation, Hong proposed a software suite specialized for building privacy sensitive systems (Hong and Landay 2004). The use of PETs in terms of design patterns, such as attribute access controls or decentralization architectures, is also considered as steps towards Privacy-by-Design application (Hoepman 2012); however this refers to consideration of such technologies from the beginning of the design, and not as a late add-on.

Finally, drawing on security assessment principles, Oetzel and Spiekermann (2013), suggested to pursuit PbD via Privacy Impact Assessments (PIAs) throughout the development lifecycle. Their seven steps to conducting PIAs are driven by privacy requirements mandated or not by laws, and include system documentation, defining privacy targets, assess impact degree of each target, define privacy threats and controls to prevent them from realizing, assessment of residual risks and detailed reporting of the findings.

Concluding, despite the importance of built-in privacy, current strategies are high-level and fail to provide designers with explicit guidance on specific privacy practices and/or tools to implement. The absence of practical guidance to Pbd is important in the context of SNS, which base their operations on large amounts of personal data and could specially benefit from the PbD approach.

3. PRIVACY REQUIREMENTS FOR SNS

Hoepman's strategies (Hoepman 2012) can be used for informing the design of privacy preserving SNS platforms. In the following, we specify privacy practices that can be embedded to SNS platforms, covering a wide range of topics, such as privacy policies, privacy settings and privacy awareness techniques (Table 1). We emphasize on the usability and performance of the embedded practices, because applying privacy enhancing technologies (PETs), even in the notion of embedded practices, may not always be embraced by users because of performance issues (Vemou and Karyda 2013). For instance, encryption of personal information with each friend's key may cause delays, especially in case of large lists of recipients. Also, establishing a complex process for publishing information, e.g. by requiring many steps to define the post's audience, may discourage users from using the SNS platform. ***Usability*** of privacy settings adds to this notion. Although SNS platforms typically offer privacy settings, users do not take advantage of them (Madejskiy et al. 2011), partly due to the not obvious location of these settings, in the SNS interface. Also, the amount of time users need to invest to manage their privacy settings may be a preventing factor for their deployment. For these reasons, the SNS platforms need to organize privacy settings under one, easily accessible, simple management board and apply assisting technology to explain the privacy risks related to each setting or guide users through the setting process.

Table 1. Requirements for privacy-friendly SNS services

STRATEGY	REQ#	REQUIREMENT DESCRIPTION
MINIMIZE	1.1	Allow use of pseudonyms and support anonymity
	1.2	Require minimum information for identification
	1.3	Provide identifiability tests
	1.4	Control which third-party applications have access to information
HIDE	2.1	Provide access control in parts of information
	2.2	Make information inaccessible to public (non-users)
	2.3	Deactivate internal search
	2.4	Organize around the concept of audience segregation
	2.5	Provide functionality for private communication
	2.6	Conceal information from the platform
SEPARATE	3.1	Distribute profile storage
	3.2	Allow different data type access to different third-party companies
INFORM	4.1	Provide Privacy Mirroring functionality
	4.2	Provide users with access to activity logs
	4.3	Inform users about entities prohibited to access information
	4.4	Notify of changes on privacy policy or Terms of Service (TOS)
	4.5	Provide users with access to stored information
	4.6	Notify of other users' actions (e.g. tags)
CONTROL	5.1	Provide functionality to report abusive behavior
	5.2	Provide functionality to report identity theft
	5.3	Eliminate transitive access controls
	5.4	Provide third-party applications management board
	5.5	Allow complete deletion of account
	5.6	Prohibit automated extraction of information
	5.7	Provide functionality for context declaration
AGGREGATION	6.1	Aggregate information before handing to third-parties
ENFORCE	7.1	Explicitly mention collected PII and purpose in the privacy policy and ask for user consent
	7.2	Prohibit secondary use of user's information
DEMONSTRATE	8.1	Be certified under Privacy Seals / Publish internal security audit results
USABILITY	9.1	Organize privacy settings under a single, easily accessible board
	9.2	Require minimum user effort and IT skills to manage privacy
	9.3	Configuration of privacy settings with minimum number of steps

	9.4	Eliminate contradicting privacy settings
	9.5	Apply assisting technology for privacy settings
PERFORMANCE	10.1	Apply privacy enhancing technology with minimum overhead

The first requirement we have identified relates to the ***minimization*** of the PII amount processed by the SNS platform. Practices of this category focus on the information collection process and necessitate collection of a limited set of information or the users' choice to deny collection of several information types. SNS platforms can enhance privacy by allowing use of pseudonyms and by requesting the minimum amount of information during sign-up, avoiding data types that could lead to user identification, such as birth date. For the latter, users should be provided with awareness functionality to test their identifiability. In case of third-party applications requesting access to users' PII, the SNS platform needs to apply controls to ensure they are requesting the minimal amount of information, instead of just asking them to declare it prior of installation.

The second requirement is related to ***hiding*** personal information. If the users were provided with capability to prevent access to certain types of posted information and could declare explicitly whether their profiles should be public or searchable via search engines outside the SNS platform, this would contribute to protecting their privacy against user profiling or unwished audiences. In terms of access control functionality, the platform should provide the capability to apply different access controls on each piece of posted information, e.g. in different photo albums, or define custom user groups, which will be granted access to parts of the profile. To gain users' trust, special access controls, with default value "private" can be applied to sensitive data, such as political or religious preferences. Another option for providing access controls is to organize the platform around the concept of audience segregation, such as in Google+, to allow users create distinct views of their profiles, based on scope, e.g. family, work, friends. In addition, as communication needs between users overcome public posts on one's profile, the platform may provide functionality for private communication between users (e.g. private messaging box, chat). Furthermore, as the platform itself can pose a threat to users' privacy by exploiting PII, encryption may be applied to obscure users' information and demonstrate company integrity.

Most widely-used SNS platforms provide services under a centralized architecture leading to centralized storage and processing of users' personal data. However, to fulfill ***separation*** requirements SNS platforms can apply distribution techniques, in terms of de-centralized or peer-2-peer architectures, as for example Diaspora (Diaspora 2013).

SNS platforms should also apply ***aggregation*** methods during data mining to extract knowledge for new services or marketing, to ensure personal data are processed at the highest level of aggregation and with the least possible detail in which it is (still) useful. For instance, by processing information at the group level, with information being aggregated, and the size of the group over which it is aggregated being sufficiently large, little information can be attributed to a single person, thus protecting user privacy. Extra care should be given to deliver unidentifiable information, in case of data processing outsourcing. This could be achieved by providing different third-parties with different parts of the users' stored data.

SNS platforms are required to enhance transparency and visibility by ***informing*** users whenever their personal information is collected or accessed and why, and by offering relative reports if requested. More specifically, users need to be provided with functionality to test which of their information is available to other entities (privacy mirroring functionality).

"View as", applied in Facebook and Google+ is a good example of such practices, because users can test viewable information by groups, strangers or even by applying specific friend name, however the same functionality is not offered for testing PII access by third-party applications. Also, SNS platforms need to provide users with activity logs to understand which of their actions lead to revelation of their personal data, as well as history reviews of which data were accessed or shared by others. SNS platforms could additionally provide feedback on proper operation of access controls, namely reporting which entities were restricted accesses to personal information, through the use of access control systems. Furthermore, notification of users on other users' actions affecting their data (e.g. photo tags), prior to publishing, as well as on changes in the privacy policy can be provided by the platform, by e-mail, sms or pop-up messages.

Users should also be able to ***control*** their information and even be able to request their complete deletion. SNS platforms are required to provide easily accessible reporting functionality, for users to report abusive behavior or identity theft. Also, to implement the *hiding* strategy, SNS can take actions to prevent transitive access controls and grant users exclusive access control on their information, meaning, for example, that friends' privacy settings will not lead to unwished publishing of information. This also applies to access of information by third-party applications, which can be organized under a single management board. In addition, since context information is as important as data itself, the SNS platform may embrace technology to attach integral context information and notify about acceptable use (e.g. privacy signaling technology). Furthermore, SNS platforms should disable automated information extraction to prevent user profiling by third-parties.

Although it is a common practice to provide a privacy policy, SNS platforms need to explicitly mention which types of personal information they store and for which purposes. Explicit mention may also take place for accessibility by third parties, such as advertising networks; in conjunction with asking for the user's consent, prior to sharing. Furthermore, SNS platforms should enhance privacy by avoiding users' commitment to future changes of the privacy policy, with no direct notice and also ***demonstrate*** privacy preserving practices, through certifications, privacy seals or through establishing transparent internal audit processes, to avoid misuse of PII by malicious or unconcerned employees.

4. IDENTIFYING CURRENT PRIVACY PRACTICES

In the following we provide an analysis of the privacy practices currently incorporated in four of the most populated general purpose social networks, according to EBiz/MBA(EBiz/MBA 2014): Facebook, Google+, Twitter and Pinterest. The choice of the above platforms was based mainly on the number of monthly unique visitors, however it was interesting to identify and compare privacy practices incorporated in the first two platforms, Facebook and Google+, being competitors. Also, Pinterest was chosen because of the amount of personal data exposed indirectly via "pins", implying users' demographics and interests. This analysis was based on the set of requirements described previously (see Table 1) and was conducted during October 2014.

Overall, we found that SNS platforms currently incorporate a small subset of the proposed privacy requirements, by offering functionality such as access controls (*hide*) and mirroring functionality (*inform*). For instance, no platform was found to provide identifiability tests

(*minimize*), single/simple settings operation boards (*usability*) or privacy signaling technology (*control*). In terms of *performance*, we experienced no significant delay in the use of the platforms, mainly because no complex protecting technology, such as encryption, was applied.

In terms of minimizing collected data we found that out of four platforms, only Facebook has an explicit policy for real name declaration on user profiles. At the same time, Twitter and Pinterest request the minimum amount of information during sign-up, while Facebook and Google+ request a set of extra data, including birth date that could lead to user identification. However, no platform provides users with awareness functionality to test their identifiability. In case of third-party applications requesting access to user PII, Facebook obligates third-parties to declare which data types will be accessed, prior to acceptance and installation, but no actual control is declared for minimization of such access requests.

In terms of restricting access to posted information (*hide*), we identified several privacy settings in all four platforms to restrict access to user profiles. Despite the fact that the privacy panel location is not always obvious to the users, SNS provide a vast amount of privacy settings related to access controls. However, while in Facebook and Google+ users are able to differentiate access controls for several types of information (e.g. photos, timeline posts), Twitter only offers access limitation of the whole profile to "followers". In a similar manner, Pinterest provides users with the choice to upload only six private boards (raised from three during November 2013) in which they can set explicit access controls. Also, although Facebook incorporated functionality to allow users define groups of friends and use them on access controls and Google+ organized its interface around the concept of audience segregation, Twitter and Pinterest offer only the "followers vs. public" choice. This means that when users decide to declare their profiles as private, all of their friends (followers, pinners) will be entitled to access the same amount of posted information.

In case of sensitive data, such as political or religious preferences, we found no difference on applied access controls. Facebook is the exception, with default access controls for sensitive data set to "Friends of Friends" instead of "Public" and preventing third-party applications to access it, as a result of transitive access controls. However Facebook still prompts users to enter sensitive information, such as sexual, religious and political preferences in their profiles and this is information viewable by default. Furthermore, this default value has changed during the past year, with the past default value being accessible only to "Friends". On the other hand, Twitter and Pinterest share less interest in such information and users are not explicitly prompted to add it on their profiles.

In addition, while Google+ is organized around audience segregation for posted information, the other three platforms do not offer such functionality. Facebook has made few steps towards this direction offering users functionality to create custom groups of friends and apply group-based access controls. A recent addition, functionality to explicitly declare users or groups that should not gain access to certain pieces of information, also works towards this direction. However, none of the platforms offers by default inaccessibility of information to public. For instance, Pinterest and Twitter have options to prevent search engines and search by e-mail respectively, but these options are off by default. What is more, in Facebook the users can select their profile to be private, but cannot limit publicity of profile names and profile photos. We also found that explicit functionality for private communication between users is offered only in Facebook and Twitter and none of the researched platforms applies technology, such as encryption, to hide user information from the platform itself.

Table 2. Privacy practices currently embedded in SNS platforms (✔: supported, -: not supported, comments: partially supported)

REQ #	REQUIREMENT DESCRIPTION	FACEBOOK	GOOGLE+	TWITTER	PINTEREST
1.1	Allow use of pseudonyms and support anonymity	Explicit policy for use of real names (-)	✔	✔	✔
1.2	Require minimum information for identification	Requests extra data, including birth date, during sign-up (-)	Requests extra data, including birth date, during sign-up (-)	✔	✔
1.3	Provide identifiability tests	-	-	-	-
1.4	Control which third-party applications have access to information	-	-	-	-
2.1	Provide access control in parts of information	✔	✔	Access limitation of the whole profile to "followers"	Ability to have only six private boards with explicit access controls
2.2	Make information inaccessible to public (non-users)	Profile name and profile photo cannot be set to private	-	Option to prevent search by e-mail is off by default.	Option to prevent search engines is off by default.
2.3	Deactivate internal search	-	-	✔	-
2.4	Organize around the concept of audience segregation	Functionality to create custom groups of friends and apply group-based access controls	✔	-	-
2.5	Provide functionality for private communication	✔	-	✔	-
2.6	Conceal information from the platform	-	-	-	-
3.1	Distribute profile storage	-	-	-	-
3.2	Allow different data type access to different third-party companies	-	-	-	-
4.1	Provide Privacy Mirroring functionality	✔	✔	-	-

4.2	Provide users with access to activity logs	✔	✔	✔	✔
4.3	Inform users about entities prohibited to access information	-	-	-	-
4.4	Notify of changes on privacy policy or Terms of Service (TOS)	-	-	-	-
4.5	Provide users with access to stored information	✔	-	✔	-
4.6	Notify of other users' actions	Off by default	-	-	✔
5.1	Provide functionality to report abusive behavior	✔	✔	✔	✔
5.2	Provide functionality to report identity theft	✔	✔	✔	✔
5.3	Eliminate transitive access controls	-	-	✔	✔
5.4	Provide third-party applications management board	✔	✔	-	-
5.5	Allow complete deletion of account	-	-	✔	-
5.6	Prohibit automated extraction of information	-	Only for saving of published photos	-	-
5.7	Provide functionality for context declaration	-	-	-	-
6.1	Aggregate information before handing to third-parties	-	-	-	-
7.1	Explicitly mention collected PII and purpose in the privacy policy and ask for user consent	-	-	-	-
7.2	Prohibit secondary use of user's information	-	-	-	-
8.1	Be certified under Privacy Seals /	-	-	-	-

	Publish internal security audit results				
9.1	Organize privacy settings under a single, easily accessible board	-	-	-	-
9.2	Require minimum user effort and IT skills to manage privacy	-	-	-	-
9.3	Configuration of privacy settings with minimum number of steps	-	-	-	-
9.4	Eliminate contradicting privacy settings	-	-	-	-
9.5	Apply assisting technology for privacy settings	Pop-ups on the upper right of its interface (focused on new users). No explanation of the privacy threats they prevent.	-	-	-
10.1	Apply privacy enhancing technology with minimum overhead	-	-	-	-

With regard to awareness raising privacy practices (*inform*), we found that two of the researched platforms, Facebook and Google+ offer privacy mirroring functionality (called "View as"), in which the users can test which information is available to others. The users can test viewable information by groups, strangers or even by applying specific friend names, however the same functionality is not offered for testing profile information access by third-party applications. On the other hand, the absence of such functionality in Pinterest and Twitter was no surprise, because of the inability to apply different access controls to specific posts ("tweets" or "pins").

In addition, all four SNS platforms provide users with activity or history logs to view their latest activities, but no activity on processed information by third-party applications, functioning through the users' profiles, is reported. Another awareness issue that is not addressed is the need to provide the users with feedback about proper operation of access controls, namely reporting which entities requested access on some information and were restricted grace to access controls. Also, existing SNS platforms offer some functionality to notify users about other users' actions that may affect them, such as comments and photo tags, prior to publish of these actions; however this functionality is off by default, such as in Facebook. Also, SNS platforms do not explicitly notify the users on all changes applied in privacy policy or terms of service (TOS). Terms of use usually contain a term that the users are responsible for revisiting the terms and privacy policy to be informed of any changes and

the platform may notify them on any changes are believed to introduce major changes. Finally, only Facebook and Twitter provide users with the ability to request access to information the platform has stored about them.

To *control* their information, users are provided with easily accessible report functionality, to report abusive behavior or identity theft in all four researched platforms, but they are not provided with technology to provide integral context information to their data or notify about acceptable use (e.g. privacy signaling technology). Also, users are not provided with exclusive access control about their information, as friends' privacy settings may lead to unwished publishing of information, such as the case of transitive access controls applied on Facebook profiles in relation to third-party applications. As for automated information extraction, only Google+ offers settings to disable saving of published photos, which is by default turned off, and applies only to this type of posted information. It is not transparent to the users which information is deleted and when from the SNS platform archives, in case of deletion or deactivation of the account and no link to request correction of stored data from the privacy settings interface was found.

All four SNS platforms provide services under a centralized architecture. No decentralization to avoid concentration of PII is mentioned in their privacy policies, while the platforms retain the right to provide personal information to any cooperating third-party complying to their privacy policies, with no mentioned efforts to prevent aggregation of information to third-parties (*separate*). Moreover, we found no mention to the use of aggregation technology to deliver unidentifiable information to third-parties (*aggregate*).

All four SNS platforms evaluated provide a privacy policy and terms of service (*enforce*), to inform the users of their function principles. However, these privacy policies include vague descriptions of collected information and processing procedures, as well as commit users to future changes, with no direct and explicit notice. Application of this privacy policy is not controlled by third-parties, to assure collected data is processed per declared methods and no up-to-date privacy seal or other type of audit outcome was found (*demonstrate*). Facebook reported as aTRUSTe licensee in 2010, but many changes have been applied to its privacy policy since then.

Concluding, SNS users are provided with functionality to control, up to an extent, access of other users to their posted information and view their activity history. However, functionality to report on access controls results or directly raise awareness on users' activities exposing their own privacy is not yet provided. Also, audience segregation and anonymity is still in a pre-mature level while control and secondary use of information by the SNS platforms and third parties, is far from being abandoned. Our analysis revealed that although some steps have been taken to offer the user with hiding or awareness functionality, SNS platforms lack privacy preserving practices concerning information segregation and aggregation and enforcing strategies that would prevent direct exploitation of PII for secondary use.

5. GUIDELINES AND TOOLS FOR DESIGNING PRIVACY FRIENDLY SNS PLATFORMS

Our analysis shows that popular SNS platforms do not support most of the privacy requirements identified, and few support a subset of them. In the following, we provide

guidelines and suggestions as to how social media design can benefit from current privacy preserving methods and tools.

5.1 Providing Users with access Control to their Information

To allow the users share parts of their information to different audiences (requirement no 2.1), there are several types of access controls. Attribute-based access control applies certain conditions about the users' attributes wishing to obtain this information, for instance allows access only to users over 18 years old. Lockr (Tootoonchian et al. 2009), Persona (Baden at al. 2009) and EASiER (Jahid et al. 2011) are examples of attribute-based access control application. While in Lockr relationship type is the attribute used to apply access control, in Persona attributes and keys are applied to friends of a user. In this way they are divided in groups and keys are used to get access to data. In EASiER, attribute-based access control included a third party adding to the attributes, to ensure efficient revocation of access to some users.

In role-based access control, users can access data according to the relationship paths that connect them with the user whose data they are willing to access. Apart from the existence of a relationship path, access controls may take into account the depth of the relationship, in other words how close friends the two users are, as well as the trust level between them, as in work of Carminatti and Ferrari (Carminati and Ferrari. 2010), Ali et al. (Ali et al. 2007), and Kruk et al. (D-FOAF) (Kruk et al. 2006). Other examples of access control based on the users' roles are Scramble! (Beato et al. 2011) and Stegoweb (Besenyei et al. 2011). When users' friends are grouped into categories according to their relationship with the user and user data are grouped in categories based on their context, then access control may be defined based on the mapping between users and data classes, such as in the Clique and Beato et al. prototype (Beato et al. 2009). This is the basic idea of audience segregation, actually implemented by Google+. Also, more generic solutions for role-based access control such as BlogCrypt (Paulik et al. 2010) and Flybynight (Lucas and Borisov. 2008) that apply cryptography may have application in SNS, as by having the set of necessary encryption keys the users can demonstrate they have the rights to access data. However, the choice of encryption should be taken into account along with usability (no 9.2) and performance (no 10.1) requirements.

Designers of SNS platforms should also pay attention to special types of information, often omitted in the privacy decisions, such as applying access controls to viewing a users' friends list. Users' friends lists have been identified as valuable and sensitive information that can be exploited during mutual-friends attacks (Lei et al. 2013).

In the same way, but focusing on obscuring personal information from the platform itself, SNS designers could allow submission of perturbated profile information. Perturbation, may involve a second, trusted server to hold the real values of data, in order to display to users granted access by the profile owner, as in Facecloak (Luo et al. 2009), or just store relevant data to the users' browser, as in the case of NOYB (Guha et al. 2008) and FaceVPSN (Conti et al. 2011). In the context of avoiding secondary use, application of purpose based access controls (Byun et al. 2005) could also be applied, for the users to define allowed use of their data and embed this limitation to access controls, however there are still some limitations to blocking secondary use.

5.2 Prohibiting Personal Data use by Third Parties

Expiration technologies, although yet being in a pre-mature level, could be incorporated in user data shared through the SNS platforms, to avoid out of context and out of time use. This can work towards safeguarding SNS users from secondary use (7.2). Encryption could serve data expiration, by making the decryption key unavailable, such as in the case of Xpire a Firefox extension that stores the decryption key in a public server (Backes et al. 2011) and the case of Vanish, an application storing parts of the key in a distributed hash table (Geambasu et al. 2009). This is also the case in Scrambls (Scrambls 2014), where users can set an expiration date for encrypted posts. However, the above technologies could raise some usability issues (no 9.2), such as access to the profile from different devices, especially in the case of stored information (encryption keys, hash tables) within the users' browser.

In case of outsourcing data mining of user data, SNS designers could incorporate aggregation techniques, to achieve handing over anonymized/aggregated data to third-parties collaborating with the SNS platform. SNS designers could take advantage of relative research in the field of data mining (Aggarwal and Philip, 2008) and apply algorithms for horizontal (records are distributed across multiple entities) or vertical partitioning (attributes distributed across multiple entities) of data to be handed to third-parties, e.g. based on Naive Bayes Classifier, SVM classification and k-means clustering.

5.3 Enhancing user Control on Personal Data

Focusing more on enhancing the privacy awareness of SNS users and offering another means of controlling personal information, SNS platform designers could adopt privacy signaling practices for the users to declare preferences on scope and context of their data use (no 5.7). Although a standard has not been established for SNS platforms, designers could take advantage of proposed applications, such as Respect my privacy-RMP, an application that allows users to declare their data usage restrictions, e.g. no-commercial, no-depiction (Kang and Kagal. 2010). Also Privicons (Holtz et al. 2011), a set of icons defined during the PRIMElife project to depict how data can be handled in a website, e.g. who is able to see them, according to respective privacy policies could be used. Last but not least, or Iannella et al. have proposed a set of icons, applicable to SNS platforms, to depict privacy preferences, especially visibility of private information, including cases such as viewable by Everyone, Only Friends, Some Friends, All my Networks/Groups, Some of my Networks/Groups and Friends of Friends (Iannella et al. 2010).

5.4 Enhancing the Usability of Privacy Settings

To enhance usability of privacy embedded practices, SNS platforms could be enhanced with functionality to assist the users while deciding and applying their privacy settings (no 9.5). SNS platform designers could embed privacy wizard functionality to walk the users through basic setting categories and propose changes to better conceal their privacy, such as in the case of PrivacyFix (PrivacyFix 2014), Priveazy Lockdown (Priveazy 2014) or even select privacy settings in their name, as in the work of Baatarjav et al. (Baatarjav et al. 2008). Furthermore, the users can be assisted by presentation of statistical information on settings their friends have applied (Lipford and Zurko. 2012). Technology to assist the users in segregating the

audience of their posted information or even automatically setting access controls could be used. Netter's prototype (Netter et al. 2011) and Fang's proposed privacy wizard (Fang and LeFevre. 2010) are just examples of such technology.

In the same direction, SNS designers could also provide assistance to the users wishing to manage third-party applications' access to their profile information. This can be achieved by presenting them with an analytic management board which explains privileges each installed third-party application has to their accounts. Such information may be categorized by types of profile access and could be enhanced by offering recommendations, as in the case of MyPermissions Cleaner application (Mypermissions 2014).

Adding to privacy wizard technology (no 9.5) and in collaboration with users' informing on other users' actions affecting their privacy (no 4.6), SNS platforms designers could introduce functionality to inform the users on any tags or mentions of their profile and even blocking or removing them if they pose a threat to privacy (personal containers technology). Privacy Butler (Wishart et al. 2010) can be identified as a simple application of this category, but SNS designers could also take advantage of content-based filtering technology to identify threats to users' reputation, such as in the proposed work of Vanetti et al (Vanetti et al. 2013).

6. CONCLUSIONS AND FURTHER RESEARCH

This paper describes both at the privacy requirements level, as well as at the technological level, how SNS platforms can enhance user privacy by embedding privacy technologies and adopting privacy practices. It extends previous literature on privacy requirements in the context of building and designing privacy friendly SNS platforms. It provides guidelines that are based on Hoepman's designing strategies, and address the characteristics of SNS, emphasizing on the performance and usability of embedded privacy practices.

The paper also analyzes the findings of four popular SNS platforms evaluation that aimed to identify currently embedded privacy practices and tools. We show that popular SNS support few privacy requirements; however, they have taken some steps towards users' hiding or controlling their information, along with some awareness functionality to understand applied settings. To offer privacy-friendly services platforms can additionally simplify privacy settings and prevent transitive access controls, which may lead to access rules contradicting to users' settings. SNS platforms can also apply audience segregation techniques, as well as data aggregation technology to prevent direct exploitation of PII for secondary use. Especially with regard to user friendliness, existing literature shows that the SNS platforms' privacy settings need to be reformed to adequately reflect principles presented in SNS privacy policies (Anthonysamy et. al 2011).

This paper also provides SNS platform designers with a list of guidelines and privacy enhancing technologies they can employ. While there is an abundance of tools and methods to achieve several privacy requirements, e.g. several access control types, our research resulted in identifying several technologies that are still in a premature level, such as data expiration and awareness methods (identifiability tests), and need to be further researched.

Our research also underlines the fact that privacy protection cannot be based only on technical measures. Several privacy requirements may be fulfilled by taking strategic decisions while designing or operating an SNS platform. For instance minimization of requested and stored data may be achieved through strategic decisions not to require their

filling during the sign-up process and by increasing users' awareness in relation to the privacy risks they are exposed to as a result of sharing them. Also, by setting default values to private, in existing privacy settings, a limited increase of SNS users' privacy can be achieved, with no extra technological measures from the SNS platforms. Concluding, although SNS platforms seem to be aware of the privacy awakening of their users, most platforms still do not embrace abandoning personal data exploitation and allow secondary uses of personal information. It would be interesting to explore the features of an SNS business model that would balance SNS platform profits and functionality with user privacy.

In this paper, we have introduced a list of privacy requirements and guidelines SNS platforms, opting for offering privacy-friendly services, can use. We also highlighted the need for further research in personal data control techniques, such as data expiration technologies, to ensure that users and SNS platforms are in control of information even when they are in the hands of third-parties. Our research was limited by the number of SNS platforms analyzed and the general-purpose of selected platforms. For instance, in the above mentioned platforms no encryption techniques, usually criticized for causing overhead to social experience, were embedded to protect users' privacy. This limited our research relating to performance requirements. Also, although general-purpose SNS require users' attention to protect their privacy in many aspects of their social browsing, researching special-purpose SNS, such as those concerning professional life, could offer different insight in SNS users' privacy needs and practices.

Further research is needed to investigate whether SNS platforms can profit from inscribing privacy practices, and whether further privacy requirements are required to fully implement the right of SNS users to privacy. Finally, this research identified that there is a need to develop PETS for enhancing identifiability testing and for sharing expirable data, which, however, will not impede usability and performance of the platform.

REFERENCES

Acquisti, A. and Gross, R., 2006. Imagined communities: awareness, information sharing, and privacy on Facebook. *Privacy enhancing technologies*, Springer Berlin Heidelberg, pp. 36-58.

Aggarwal, C. and Philip, S., 2008. *A general survey of privacy-preserving data mining models and algorithms*. Springer US, pp. 11-52.

Ali, B. et al, 2007. A trust based approach for protecting user data in social networks. *Proceedings of the 2007 conference of the center for advanced studies on Collaborative research*, pp. 288-293.

Anthonysamy, P. et al, 2011. Do the Privacy Policies Reflect the Privacy Controls on Social Networks*?".Proceedings of 2011 IEEE International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing*, Boston, MA, USA, pp. 1155-1158.

Baatarjav, E. et al, 2008. Privacy management for facebook. *Proceedings of the International Conference on Information Systems Security*, Hyderabad, India, pp. 273–286.

Backes, J. et al, 2011. X-pire!-a digital expiration date for images in social networks. *arXiv preprint arXiv:1112.2649*.

Baden, R. et al, 2009. Persona: An online social network with user-defined privacy. *Proceedings of the ACM SIGCOMM 2009 conference on Data communication*, Barcelona, Spain, pp.135-146.

Beato, F. et al, 2009. Enforcing access control in social networks. *Proceedings of Hot Topics in Privacy Enhancing Technologies*, Seattle, USA.

Beato, F. et al, 2011. Scramble! your social network data, *Proceedings of the 11th international conference in Privacy enhancing technologies*, Waterloo, Canada, pp. 211-225.

Besenyei, T. et al, 2011. StegoWeb: Towards the Ideal Private Web Content Publishing Tool, *Proceedings of the Fifth International Conference on Emerging Security Information, Systems and Technologies*, Nice/Saint Laurent du Var, France, pp. 109-114.

Boyd, D. and Hargittai, E., 2010. Facebook privacy settings: Who cares?.*First Monday*, Vol. 15, No. 8.

Byun, J. et al, 2005. Purpose based access control of complex data for privacy protection. *Proceedings of the tenth ACM symposium on Access control models and technologies*, Stockholm, Sweden, pp. 102-110.

Carminati, B. and Ferrari, E., 2010. Privacy-Aware Access Control in Social Networks: Issues and Solutions. *Privacy and Anonymity in Information Management Systems, Advanced Information and Knowledge Processing*, Springer London, pp. 181-195.

Cavoukian, A., 2010. Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph. D..*Identity in the Information Society*, Vol. 3, No. 2, pp. 247-251.

Chen, S. and Williams, M.A., 2010.Towards a comprehensive requirements architecture for privacy-aware social recommender systems.*Proceedings of the Seventh Asia-Pacific Conference on Conceptual Modelling*, Brisbane, Australia, pp. 33-42.

Conti, M. et al, 2011. Virtual private social networks. *Proceedings of the first ACM conference on Data and application security and privacy*, San Antonio, Texas, *USA*, pp. 39-50.

Diaspora, 2013. *Diaspora**. https://joindiaspora.com/

EBiz/MBA, 2014.*Top 15 Most Popular Social Networking Sites. October2014*, http://www.ebizmba.com/articles/social-networking-websites.

ENISA, 2007.Security Issues and Recommendations for Online Social Networks, Position Paper No.1.

ENISA, 2012.Privacy considerations of online behavioural tracking. Report 2012

Fang, L. and LeFevre, K., 2010. Privacy wizards for social networking sites. *Proceedings of the 19th international conference on World wide web*, Raleigh, NC, USA, pp. 351-360.

Geambasu, R. et al, 2009. Vanish: Increasing Data Privacy with Self-Destructing Data. *Proceedings of USENIX Security Symposium*, pp. 299-316.

Guha, S. et al, 2008. NOYB: privacy in online social networks. *Proceedings of the first workshop on Online social networks*, Seattle, WA, USA, pp. 49-54.

Gürses, S. et al, 2011.Engineering Privacy by Design.*Conference on Computers, Privacy & Data Protection (CPDP 2011)*.

Hoepman, J.H., 2012. Privacy Design Strategies, draft version, http://arxiv.org/abs/1210.6621.

Holtz, L. et al, 2011. Privacy Policy Icons, *Privacy and Identity Management for Life*, Springer Berlin Heidelberg, pp. 279-285.

Hong, J.I. and Landay, J.A., 2004. An architecture for privacy-sensitive ubiquitous computing, *Proceedings of the 2nd international conference on Mobile systems, applications, and services*, Boston, MA, USA, pp. 177-189.

Iannella, R. et al, 2010. Privacy awareness: Icons and expression for social networks. *Proceedings of the 8th Virtual Goods Workshop and the 6th ODRL Workshop*, Namur, Belgium, pp. 1-15.

Jahid, S. et al, 2011. EASiER: Encryption-based Access Control in Social Networks with Efficient Revocation. *Proceedings of 6th ACM Symposium on Information, Computer and Communications Security*, Hong Kong, China, pp. 411-415.

Kang, T. and Kagal, L., 2010. Enabling privacy-awareness in social networks, *Proceedings of the Intelligent Information Privacy Management Symposium at the AAAI Spring Symposium 2010*, pp. 1-6.

Kruk, S. et al, 2006. D-FOAF: Distributed Identity Management with Access Rights Delegation, *Proceedings of the Asian Semantic Web Conference*, Beijing, China, pp. 140-154.

Lei, J. et al, 2013. Mutual-friend based attacks in social network systems. *Computers & security*, Vol. 37, pp. 15-30.

Lipford, H. and Zurko, M., 2012. Someone to watch over me. *Proceedings of the 2012 workshop on New security paradigms*, Bertinoro, Italy, pp. 67-76.

London Economics, 2010. London Economics: Study on the economic benefits of privacy-enhancing technologies (PETs). Final Report to The European Commission DG Justice, Freedom and Security

Lucas, M. and Borisov, N., 2008. FlyByNight: mitigating the privacy risks of social networking. *Proceedings of the 7th ACM workshop on Privacy in the electronic society*, Alexandria, Virginia, USA, pp. 1-8.

Luo, W. et al, 2009. FaceCloak: An Architecture for User Privacy on Social Networking Sites. *Proceedings of the 2009 International Conference on Computational Science and Engineering*, Vancouver, Canada, pp. 26 – 33.

Madejskiy, M. et al, 2011.The Failure of Online Social Network Privacy Settings.*CUCS-010-11*, http://academiccommons.columbia.edu/catalog/ac:135406 .

Mypermissions, 2014. Mypermissions, https://mypermissions.com/

Netter, M. et al, 2011. Assisted Social Identity Management – Enhancing Privacy in the SocialWeb, *Proceedings of the 10th International Conference on Wirtschaftsinformatik*, Zurich, Switzerland.

Oetzel, M. C., Spiekermann, S., 2013. A systematic methodology for privacy impact assessments: a design science approach. *European Journal of Information System*, vol. 2013, pp.1-25.

Paulik, T. et al, 2010. BlogCrypt: Private Content Publishing on the Web. *Proceedings of the 2010 Fourth International Conference on Emerging Security Information, Systems and Technologies*, Venice, Italy, pp. 123–128.

PrivacyFix, 2014. PrivacyFix, https://privacyfix.com/start

Priveazy, 2014. Priveazy, https://www.priveazy.com/

Schaar, P, 2010. Privacy by design, *Identity in the Information Society*, Vol. 3, No. 2 , pp. 267-274.

Scrambls, 2014. Scrambls, https://scrambls.com

Shapiro, S. S., 2010. Privacy by design: moving from art to practice, *Communications of the ACM*, Vol. 53, No. 6, pp.27-29.

Sleeper, M. et al, 2013. The post that wasn't: exploring self-censorship on facebook. *Proceedings of the 2013 conference on Computer supported cooperative work*, San Antonio, TX, USA, pp. 793-802.

Spiekermann, S., Cranor, L. F., 2009. Engineering privacy. *Software Engineering, IEEE Transactions on*, Vol. *35*, No.1, pp. 67-82.

Taylor, D. et al, 2011. Friends, fans, and followers: do ads work on social networks?.*Journal of Advertising Research* Vol. 51, No. 1, pp. 258-275.

Tootoonchian, A. et al, 2009. Lockr: better privacy for social networks. *Proceedings of the 5th international conference on Emerging networking experiments and technologies*, Rome, Italy, pp 169-180.

Vanetti, M. et al, 2013. A System to Filter Unwanted Messages from OSN User Walls. *IEEE Transactions on Knowledge and Data Engineering*, Vol. 25, No. 2, pp. 285-297.

Vemou, K., Karyda, M., 2013.A framework for understanding low adoption of PETs among SNS users.*Proceedings of the 10th International Conference on Trust, Privacy & Security in Digital Business*, Prague, Chech Republic, pp. 74-84.

Wishart, R. et al, 2010. Privacy Butler: A Personal Privacy Rights Manager for Online Presence, *Proceedings of the 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), 2010*, pp. 672 – 677.