ON THE LOW DIFFUSION OF PRIVACY ENHANCING TECHNOLOGIES IN SOCIAL NETWORKING: RESULTS OF AN EMPIRICAL INVESTIGATION

Vemou Konstantina. Department of Information and Communication Systems Engineering, University of the Aegean, Greece. kvemou@aegean.gr

Mousa Gavriela. Department of Information and Communication Systems Engineering, University of the Aegean, Greece. icsdm12030@icsd.aegean.gr

Karyda Maria. Department of Information and Communication Systems Engineering, University of the Aegean, Greece. mka@aegean.gr

Abstract

This paper discusses the low adoption of PETs among SNS users, based on the results of an empirical investigation among users of social networking services. 170 members of 5 popular social networks provided information on how they protect their privacy, as well as on the most important factors guiding their decision to use privacy preserving tools or not. Research findings suggest that awareness of PETs is still low among social network users and that quality, effectiveness, cost and ease of use are critical factors influencing PETs adoption. A small number of users was also found not to employ any PETs, despite the fact that they reported being familiar with some of them. This paper enhances our understanding of PETs diffusion from the perspective of users and argues that usability aspects need to guide their design and implementation.

Keywords: Social Network Services, Privacy-Enhancing Technologies, adoption, usability.

1 INTRODUCTION

Social Networking Services (SNS) are constantly gaining popularity, with four of them (Facebook, Twitter, LinkedIn and Pinterest) reaching the top 15 most visited websites, in February 2015 (Ebiz/MbaA 2015). Facebook is estimated to have almost 1.4 billion active registered users, followed by Google+ with 343 million and Twitter with 284 million active users (Statista 2015). While offering a rich networking experience, by allowing users to create a network of friends/followers and communicate by sharing different types of information, such as posts, photos and location data, SNS entail privacy risks, due to the large amount of personal information that is published. These include unauthorized secondary uses of personal information, surveillance, identification theft, bullying and stalking (ENISA 2007). Users are increasingly worried about potential threats (Acquisti and Gross 2006, Boyd and Hargittai 2010), while 59% of teenager users perceive SNS as unsafe (StatisticBrain 2014). SNS users have been reported to follow several strategies to protect themselves, such as self-censorship (Marwick and Boyd 2014). Such an approach, however, cannot eliminate privacy threats, as users are still revealing personal data in an indirect way, as well as secondary data (ENISA 2007). Privacy-enhancing Technologies (PETs) such as access controls and privacy wizards (METAGROUP 2005) provide the means for protecting personal information while online. Relevant research, however, indicates that users of PETs are still far from reaching a critical mass (London Economics 2010, ENISA 2012). This is a complex issue to explain, as a multitude of factors can influence individuals to use privacy tools, including awareness, requirements for special IT skills, their complexity, the diversity of existing tools, costs, inadequate feedback of protection results, partial addressing of users' privacy requirements, responsibility misconceptions, and culture (Vemou and Karyda 2013).

Extant literature on PETs deployment is dominated by studies on their technical characteristics, functionality and constraints (e.g. Yeung et. al (2009) discuss the advantages and disadvantages of decentralized SNS platforms), whereas individual and social aspects are only scarcely tackled (e.g. Balsa et al. 2014, Fahl et al 2012, Wang et al 2014). On the other hand, several studies as well as technical reports claim that specific tools offer user-friendly functionality (e.g. MyPermissions[1]: "…even my mom could manage her permissions now ", Secure.me[2]: "…providing simple and easy actions that you can take to secure yourself", PrivacyFix[3]: "…simple way to manage your online privacy settings through your mobile device. Access… one main dashboard that quickly & easily shows you what and with whom you're sharing stuff…").

This paper explores low PETs adoption in the context of SNS from a user perspective and discusses the findings of an empirical evaluation of PETs deployment. 170 SNS users of different social media provided us with information on their habits concerning their interaction with social networks, which (if any) privacy tools they have used, out of a list of 8 well-known applications (MyPermissions, PrivacyFix, Friendwheel, Bitdefender Safego, ZoneAlarm Privacy Scan, Secure.me, Priveazy lockdown, Safe Secure and Private Facebook messages) and rated the importance of a set of factors that have been identified as important for PETs adoption in relevant literature.

Analysis of survey findings suggests that knowledge of PETs is still limited among SNS users; interestingly, however, 65 out of the 170 respondents replied that that they were familiar with at least one of the tools but had never used them. We also found that users are mostly interested in the effectiveness, quality and cost of a privacy tool. They consider as less important, comparatively, the time needed to get familiar with the tool, user support and requirements for technical expertise or prior knowledge.

This work contributes to the understanding of limited PETs deployment, as it discusses the views of users with regard to these tools. Findings are not to be generalized; they can, however, provide us with insights as to what stimulates or discourages users from adopting privacy enhancing tools and applications, which can inform the design and development of PETs. Research findings also point to several issues that need further investigation, such as the user awareness and training as well as the economics or the cost to use technology.

2 ADOPTION OF PRIVACY ENHANCING TOOLS BY SNS USERS

Following research on rising privacy concerns of SNS users (Acquisti and Gross 2006, Boyd and Hargittai 2010), several Privacy-enhancing Technologies (PETs) have been developed to mitigate privacy risks. Such technologies include a wide range of applications, such as access controls, audience segregation, privacy-signalling tools, third-party tracking tools, social identity management systems, visualization tools and decentralization of Social Network Services (Vemou and Karyda 2013). While some PETs are embedded in SNS platforms (e.g. basic access controls), others adopt a different approach, altering the SNS platform architecture, as in the case of decentralized SNS. However, the majority of PETs concerns tools that can be used as add-ons to the SNS functionality (e.g. browser plug-ins, such as Scrambls[4], MyPermissions[5] and Friend Inspector (Cetto et al 2014)) and users need to initiate their use, in terms of download and installation (Jaatun et al 2011).

Despite the abundance of privacy enhancing tools and applications and the claims of software providers to satisfy users' privacy needs[6][7], users of SNS platforms do not show preference in their use.

[1] http://mypermissions.org/story/
[2] https://www.secure.me/en/about/
[3] https://play.google.com/store/apps/details?id=com.avg.privacyfix
[4] https://scrambls.com
[5] http://mypermissions.org/
[6] http://mypermissions.org/story/

For instance, adolescent SNS users prefer to apply their own strategies on posted data, such as censorship and social steganography (Marwick and Boyd 2014) and show little interest in applying add-on PETs (Balsa et al. 2014). The same applies to embedded PETs in SNS platforms, such as privacy settings, that usually go unnoticed by users (Boyd and Hargittai 2010) or are not used effectively, leading to unintended sharing of personal data (Madejski et al 2011).

Low adoption of PETs among SNS users is credited to different factors, such as lack of users' awareness (Acquisti and Gross 2006, Pötzsch 2009), requirements for special IT skills (Compañó and Lusoli 2010) and diversity of existing tools (Vemou and Karyda 2013). There are also usability issues, such as the time needed to learn a new tool (Vemou and Karyda 2013). Developing user-friendly PETs has been identified as a key requirement for their design (Le Métayer 2010, Jaatun et al 2011) and previous research provides evaluation on several aspects such as non-intrusiveness (Balebako et al. 2011), intuitive interfaces (Kolter et al 2010) and low performance degradation (Saint-Jean and Feigenbaum 2010). Moreover, literature identifies technical issues affecting usability (Madejski et al 2011, Vemou and Karyda 2013) as affecting the adoption of PETs.

Wästlund et al. (2010) developed a questionnaire-based tool for users to assess the usability of PETs, either at a general level, or with regard to specific privacy-critic areas, such as data management and data release. Leon et al. (2012) evaluated a set of available block-tracking tools, based on user experience, leading to conclusions on users' understanding of the interface and configuration capabilities, while Balsa et al. (2014) asked SNS users to evaluate usability of cryptographic access control tools.

Lately, research on privacy tools adoption revealed that user background factors, motivations and social network site experiences influence the use of PETs offered within SNS platforms (Litt 2013).

Conclusively, extant literature identifies a multitude of factors influencing the use of privacy enhancing technologies, emphasizing on awareness and usability issues. This paper adopts a user perspective to explore how SNS users protect their privacy and identify their attitudes towards the use of PETs.

3 PRIVACY ENHANCING TOOLS AND APPLICATIONS FOR SNS

As mentioned above, several types of privacy-enhancing tools, such as access controls, third-party tracking tools, and social identity management systems have been developed to assist SNS users in protecting their privacy. Several types, such as access controls, are now embedded in SNS platforms, however, they only address partial privacy needs and their effectiveness is questionable (Madejski et al 2011). Thus users still need to employ several PETs, add-ons to the SNS platform functionality, to ensure their privacy is protected.

Through research we have identified a set of add-on applications that protect user's privacy. The list was not meant to be exhaustive, but to cover different social media platforms, such as Facebook, Twitter and Google+. We found no official information about the use of these applications, thus our intention was to compile a list of different types of tools and applications available to SNS users for protecting their privacy. Also, as the focus of this research is on SNS users, we excluded general privacy preserving applications such as blockers of third-party tracking entities.

MyPermissions is a browser extension assisting users in managing the access of third-party applications to their profile and is applicable to several SNS platforms, including Facebook, Google+ and Instagram. It reports the applications having access to personally identifiable information, per type of access (e.g. read access, post in the name of user access, location information access) and allows users to directly remove them from their profile, thus offering a single management interface for third-party applications. Another feature, offered as a premium service, is real-time notifications on new applications added and gained access to user's personal data.

[7] https://disconnect.me/help

PrivacyFix[8], developed by AVG, is a browser extension scanning user's privacy settings and proposing changes to apply stricter controls, based on usual privacy risks. The tool then acts as an interface for the user to amend privacy settings. It also presents a list of entities tracking the user's navigation to SNS, along with the choice to block them and an awareness raising feature, presenting the value of the user's data in money.

Friendwheel[9] is a network visualization application for Facebook and Twitter users. Browsing a user's friend list and the respective lists of his or her friends, it creates a radial colourful graph-wheel presenting all user's friends and how they are connected to each other. It also offers the ability to switch data parameters and create a visual wheel for users' networks.

Bitdefender Safego[10] is a free application for Facebook and Twitter scanning each post on the user's profile and informing for malicious links (virus infected links or spam messages). At the same time, it warns the user's friends about findings. Another feature, still in a pre-mature level, is scanning the user's posted information to reveal posts of sensitive data, compromising privacy (e.g. public address information) and directing the user to the respective webpage, in order to amend settings.

ZoneAlarm Privacy Scan[11](renamed to**SocialGuard Privacy Scan**) is a free Facebook application accessing recent activities in the user's profile (posts, tags, likes) and the respective audience settings, to identify posts that could be privacy compromising, e.g. posts that are visible to friends of friends. It then presents the results to the user, along with a grade for user's privacy during the past month. It also provides recommendations to change privacy settings, in the form of a Frequently Asked Questions tutorial.

Secure.me[12], developed by Avast, is a free Facebook application scanning users' profiles and settings to find potential privacy risks by publicly available personal information. It then provides recommendations on audience access control settings. The tool also provides warnings about questionable posts on the user's profile, posted by him or third-party applications. It also provides parents with the capability to observe their children' profiles and be notified for privacy risks.

Priveazy lockdown is a deprecated free web browser extension providing user notifications on privacy and security configurations related to several privacy risks. It could be used with Facebook, LinkedIn, Twitter and several other platforms. Priveazy lockdown provided privacy wizards with detailed information, helping the user change his privacy settings and even notified when changes in the platforms' setting boards had been applied, to revisit them.

Safe secure and private Facebook messages[13](renamed to **Secret Wall**) is a free browser extension encrypting the user's Facebook private messages and timeline posts. The user creates an audience group and invites friends, who receive the necessary decryption key to see posted content. It is available for Firefox, Chrome and Internet Explorer 8+ browsers.

4 Theoretical Background: Adopting Privacy Protection Technology

According to the Diffusion of Innovations theory (Rogers 2010), four main elements influence the spread of a new idea or technology: the innovation/technology per se, the communication channels, time, and the characteristics of the social system. Rogers (2010) defines an innovation as "an idea, practice, or object that is perceived as new by an individual or other unit of adoption'. Despite the fact that PETs have been developed since more than two decades now, when cryptographic applications became widely available (Danezis and Gurses 2010), for most users they are still a novelty.

[8] https://privacyfix.com/

[9] https://friend-wheel.com/

[10] http://www.bitdefender.com/solutions/bitdefender-safego.html [11] https://www.facebook.com/games/sgprivacy/

[12] https://www.secure.me/en/

[13] www.secretwall.me

Drawing on innovation theory, use of PETs can be considered as an individual decision-making process, comprising the following steps: i) individuals become aware of the innovation and have some idea of how it functions (knowledge stage), ii) they form a favourable or unfavourable attitude toward the innovation (persuasion stage), iii) they choose to adopt or reject the innovation (decision stage), iv) they employ the innovation (implementation stage) and v) finally users evaluate the results of the innovation and finalize their decision to continue using it (confirmation stage). Consequently, to understand the diffusion of PETs we need to take into consideration not only their technical characteristics, but also social and communication issues (e.g. the role of technology opinion leaders and the nature of communication between SNS users), as well as aspects of individual decision-making.

To investigate how users' shape their decisions with regard to employing privacy enhancing technologies we derived a set of factors from relevant literature and we composed a questionnaire, based on these factors.

- **Quality of the tool/application**: Quality refers to the tool properties and characteristics that contribute to meeting users' privacy needs.
- **Cost:** The cost required to acquire a tool, in terms of direct buy or subscription costs, has been found to influence user behavior towards or away from using a tool (Acquisti 2010, Vemou and Karyda 2013). Providing a free tool (or free features of it) encourage users to try and, in a later stage, to adopt it. However, as a percentage of users are willing to pay a certain cost for privacy tools (Acquisti 2010), trial versions, similar to those of various antivirus software packages (e.g. ESET 30-days trial), may convince them to overcome cost barriers.
- **Time to learn the tool:** The amount of time that is required for a typical (non-expert) user to become familiar with a tool affects its adoption (Vemou and Karyda 2013). It refers to whether the interface is intuitive (Kolter et al 2010), whether the user is required to perform simple, easily-remembered steps to accomplish a task, but also to wizards or other helping features guiding the user through his first experience of using the tool. Considering the diversity of tools offering similar functionality, e.g. access controls, time to learn differentiates tools.
- **Ease of use:** Ease of use (also described as perceived complexity) has been identified as a major factor influencing the adoption of an innovation (Davis 1986, Rogers 2010). Users prefer applications which are easy to use, both during installation/configuration and every day operation (Leon et al 2012). In terms of installation, steps need to be few and easily understood (London Economics 2010), or even to be provided with a wizard, a demo or a presentation that guide the user to understand and apply without fear of severe mistakes. In terms of operation, users require few and easy steps in order to remember application. This is very important considering the diversity of existing PETs, fulfilling partial privacy requirements, thus requiring the user to apply several tools for protection (Vemou and Karyda 2013). Also, impact on performance of everyday SNS operations is important, as users wish to protect privacy without experiencing low latency of the service (Balsa et al. 2014).
- **Requirement for technical expertise:** Several privacy-enhancing tools involve tasks which require advanced technical skills, beyond that of an average user (Vemou and Karyda 2013). For instance, users of Safe secure and private Facebook messages need to manage encryption keys, whereas to use MyPermissions one needs to be familiar with managing browser extensions. As requirements for technical expertise can discourage users from employing PETs, Balsa et. al. (2014) stress the need to further research how to securely automate some tasks on cryptographic tools and has been one of the main reasons mandating promotion of built-in privacy in SNS platforms (Vemou and Karyda 2014).
- **Technical support:** Assistance could be provided through the tools' website, by phone, email or even live chat. In addition, demos may guide users through installation and configuration, thus achieving satisfaction.
- **Effectiveness Feedback:** Users' perceptions on the effectiveness of PETs influence their adoption. This can be attributed to the way PETs communicate, or rather fail to do so, their results, and to the way they give feedback for actions they have performed to protect the user (Balsa at al. 2014). Also, as the way privacy related dangers are presented relates to perceived effectiveness of a tool (Vemou and Karyda 2013), offering the user transparency of successful

operations on personal data protection and adequate risk presentation is one of the factors influencing towards the adoption of a tool. In addition, brief awareness features, such as warnings for third-party applications access rights, prior to installation (e.g. my permissions cleaner) or scores of achieved privacy level (e.g. Bitdefender Safego) are features that directly and non-intrusively catch the user's attention and can positively influence PETs adoption.

- **Reputation/popularity of the tool:** It is common for users to avoid being the first to try a tool or a technology, fearing side-effects of technology immaturity (Wu and Wang 2005). However, positive reputation of a tool and popularity motivates users to try it (Rogers 2010). Thus, users base their choice of tools on assessments from other users and even seek for comments in social media or forums. Positive assessments and trust by other users, as well as adoption by other users in the same SNS platform positively influence users to adopt a tool, and so does popularity of the tool provider, being well known from other applications.

5 Empirical Research and Data Collection

5.1 Research design and data collection

To explore users' preferences with regard to PETs adoption, we conducted a survey involving SNS members, using an online questionnaire created with Google Drive Forms. Online questionnaires allow anonymous answers and provide sufficient time for respondents to answer, while they support the collection of large amounts of information in a short time (Henerson et al. 1987). After a pilot test involving ten SNS users, who helped identifying and correcting ambiguous wording, the questionnaire was disseminated via public profiles in Facebook and Google+, created by the authors for the purposes of the research.

Overall, we received a total of 170 completed questionnaires.61% of the respondents were female, 82% were between 22 and 45 years old, 12% between 16 and 21, and 6% were over 46 years old. The great majority of users (89%) have finished college. 48% of the respondents work in the private or public sector and 30% were students.

5.2 The questionnaire

The questionnaire (provided in appendix A) included 17 multiple-choice questions arranged in 4 sections and began with an introductory paragraph explaining the purpose of the survey, which was followed by 4 questions on personal status (age, sex, education and occupation). Respondents were then asked to provide information on the social networking platforms they use, out of a list of the five most popular ones (Facebook, Pinterest, Twitter, Google + and LinkedIn) according to eBiz/MBA (Ebiz/MbaB 2014) and how frequently they use them. The first four platforms are general purpose SNS offering the user a wide range of networking services, from sharing comments and photos to adding third-party applications (except from Pinterest that does support third-party applications). LinkedIn belongs to niche SNS platforms (ENISA 2010), offering special purpose networking services, related to one's professional sphere. While we expect users to be more cautious on posts in LinkedIn (Martensen et al 2011), we included this platform in the questionnaire because of the high impact a social network can have on professional life (Black and Johnson 2012).

Respondents where then asked on the types of personal data they provide, whether they provide real or false data and if they communicate with persons they do not know. They were also asked whether they use applications provided by third parties, if they control their privacy settings and whether they maintain private or public profiles.

In the following section respondents were asked to indicate which privacy preserving applications they were familiar with and which of these they had actually used (out of a list of 8 tools). Finally, respondents evaluated a set of factors (elicited by relevant literature as described in Section 4) with regard to their importance for using a privacy tool, on a 5-point Likert scale.

6 Results Analysis: SNS Users Experience with PETs

6.1 Users' privacy behavior

All users reported that they are members of at least one of the social networks in the questionnaire, namely Facebook, Google+, Pinterest, Twitter and LinkedIn. Very few respondents used the option "other" provided and specified additional SNS: Tumblr, Delicious, Foursquare, Instagram, StumbleUpon, We heart it, Favim and ask.fm. Interestingly, 79% of the respondents replied that they are members in more than one social networking service and 57% are very frequent users.

Most respondents (85%) post their real name and personal data, and half of them (51%) replied that their social networks include individuals not previously known to them. Most users publish their personal photos (81%) and date of birth (67%), their education background (67%) and many indicate their occupation (48%). However, most users refrain from posting information about their sexual, religious and political preferences (only 18%, 11% and 6% respectively, provide this information). 40% provide their email address, 6% their home address and only 2% publish the number of their mobile phone. Several users publish their marital status (19%), the name of their partner (11%) and names of members of their family (26%). 23% of users publish photos very frequently. It is also worth noting that publishing false information is not an exception: 21% replied that they use fake names, 15% that they do not publish the real date of their birth, 10% provide fake email addresses, 10% provide false information about their family and personal status and 15% deliberately provide false information with regard to their occupation.

37% of the respondents use third-party applications, such as games and contests, and 36% replied that they are aware of the fact that such applications access their personal data. 19% of them consider this an unimportant issue, whereas 31% check privacy settings when they use these applications. Few users (13%) have never used third-party applications. Most users (64%) chose to maintain a private profile, 57% control who has access to their personal information and 2% replied that they do not know if their profile is public or private. About half of the respondents (53%) use the privacy settings provided by the SNS platform very often or often, while the rest use them seldom or occasionally (44%) and only 2% have never used them. However, fewer users (33%) consider privacy settings easy to use, whereas more than half (55%) find them difficult or relatively difficult to use.

6.2 Deployment of privacy tools

Overall, the majority of respondents were not familiar with the PETs indicated in the survey (see Table 1). 18 users have used Safe secure and private Facebook messages and 9 used Secure.me. MyPermissions, PrivacyFix and ZoneAlarm Privacy Scan have been used by 7 users (each), while 5 users have used Bitdefender Safego. Last but not least, Friendwheel and Priveazy lockdown have been used by 1 user each.

Tools	**Have used it (%)**	**Aware but have not used it (%)**	**Not aware (%)**
MyPermissions	4	13	83
PrivacyFix	4	12	84
Friendwheel	1	8	91
Bitdefender Safego	3	9	88
ZoneAlarm Privacy Scan	4	18	78
Secure. me	5	21	74
Priveazy lockdown	1	11	88
Safe secure and private Facebook messages	11	19	70

Table 1. Use of privacy tools.

Interestingly 65 users (out of 170) replied that they have never used any of these tools, despite the fact that these users had previously replied that they are aware of at least one of them. For instance, 21% replied that they are familiar with Secure.me but had not used it. This finding suggests that limited awareness should not be solely accredited for low PETs adoption.

When asked to evaluate the importance of the factors that would influence their decision in deploying a privacy preserving application, respondents identified the following factors as important: **quality** (84% reported it is important or very important, 14% not so important or little important and 2% not important at all), **effectiveness feedback** (79% reported it is important or very important, 17% not so important or little important and 4% not important at all), **cost** (77% reported it is important or very important, 19% not so important or little important and 4% not important at all), **ease of use** (65% reported it is important or very important, 31% not so important or little important and 4% not important at all) and **time needed to learn how to use the tool** (59% reported it is important or very important, 36% not so important or little important and 5% not important at all). Users were divided with regard to the importance of **requirements for technical expertise**: 51% consider it important or very important, 43% not so important or little important and 6% not important at all. Half the respondents consider that it is important or very important that other SNS users use the same privacy tool (**popularity**), 45% consider it of not so important or little important, of and only 5% consider it of no importance at all. Finally, **technical support** is identified as important or very important by 60% of the users, while 34% consider that it is of moderate or low importance.

7 DISCUSSION: THE USER PERSPECTIVE

The findings of the survey presented in this paper provide an insight to the privacy behavior of SNS users and the deployment of Privacy-enhancing Technologies from the user perspective. These findings are not to be generalized, as the sample was relatively small and self-selected; the set of privacy tools included in the questionnaire was also small and not exhaustive, in order not to drive away respondents. The results of the survey are in line with relative research and move the discussion on the diffusion of PETs one step further by a) providing the user's perspective; b) indicating that lack of awareness is not the only obstacle to the diffusion of privacy enhancing technologies and c) providing feedback on which factors users consider more influential in adopting a privacy preserving application.

Overall, survey results provide us with interesting findings with regard to the privacy behavior of the average SNS user: most are quite active on publishing their personal information and share this with strangers, however, they often provide false data and avoid providing information of sensitive information, such as religion and sexual preferences. Very few did not know the difference between private and public profiles and many (more than half) regularly or some times change their privacy settings. It seems, thus, that SNS users are familiar with privacy issues and take some actions to protect their personal information. On the other hand, we found that most SNS users experience difficulties in managing the privacy settings offered by the SNS platforms or consider them as relatively difficult, aligning with findings of Madejski et al. (2011). Thus, users do not see SNS platforms as allies in their effort to protect their privacy.

Another interesting finding is that SNS users seem to ignore, or underestimate, privacy implications by third party applications. These applications are quite popular among SNS users, but it seems that users do not realize the extent of secondary uses of information. This is an area indicating that privacy awareness needs to be enhanced.

Most respondents were not familiar with any of the privacy enhancing tools included in the questionnaire. We believe that this result would not have been dramatically different even if we had selected a different set of tools. This finding has been cited elsewhere as well (Flash Eurobarometer 2008). The fact, however, that some users (not very few) chose not to use privacy enhancing tools, despite the fact that they are familiar with at least one of them, needs further investigation.

In terms of the Diffusion of Innovation theory (Rogers 2010), this means that users are still not aware of the innovation (PETs). Moreover, findings suggest that informed users may form an unfavourable attitude toward privacy tools. Due to the nature of this research, we were not able to further investigate this issue. Future research needs to focus on how we can influence this stage towards a favourable decision.

In general, people are more likely to adopt an innovation if they believe that it will enhance their utility. This means they need to have an idea for the benefits they will get from using it. People also consider related costs and the degree to which the innovation would disrupt or change their ordinary actions. They evaluate how compatible the innovation is with their existing habits and values, if it is hard to use, and evidently, its effectiveness (Davis 1986). Some also take into account how socially acceptable the innovation is and what will other people think of them using it (reputation / popularity).

Survey results also suggest that SNS users consider quality, effectiveness feedback and low cost as the most important factors, in order to adopt a privacy tool. Obviously, we need to investigate further, the factors that can influence the decision of SNS users to deploy privacy tools, based not only on self-reported attitudes of users, but also on hands-on experimenting of such tools. Furthermore, as some factors may have different involvement in some types of PETs (e.g. in cryptographic PETs use of the tool by the user's friends is a prerequisite) research should be conducted separately for different categories of PETs.

We can also derive a set of directions for designers and developers of privacy enhancing applications: a) privacy tools need to enhance their functionality to let the user know which actions were performed by the tool to protect user privacy (e.g. which entities were restricted access to personal data from his profile), and which were the possible privacy threats; b) privacy tools need to fulfil multiple privacy requirements (for instance, while a user may be in need of assistance to set audiences of his posts, he is at the same time in need to protect his personal information from the SNS platform itself). Thus a tool proposing groups of friends for access controls or only encrypting messages could not be derived of high quality by the user, because it would address only a part of his privacy requirements. Organization of several privacy enhancing technologies under a single, simple tool would be more attractive to users; c) Last but not least, as high costs can be an inhibitor of privacy tools use, providers should study users' perceptions over PETs costs prior to setting a tool's price or consider offering some of its functionality for free, to convince users into trying the tool.

8 CONCLUSIONS AND FURTHER RESEARCH

This paper provides insights on the privacy behavior of SNS users and corroborates similar research on showing that adoption of PETs among them is still limited. This is mainly attributed to low awareness of privacy enhancing tools and applications among SNS users. It also argues that awareness is not the only factor strongly influencing PETs adoption and user weighting of several adoption factors, such as effectiveness feedback, costs and requirements for technical expertise should be further explored.

We were able to identify a number of factors that, according to the users, would significantly influence their decision in adopting a privacy tool. This also needs to be validated through future qualitative research, minding the different role each factor could have in different types of PETs (e.g. use of the tool by other users would be a prerequisite for its use). The outcome of such a research could provide more accurate directions for PETs developers, in order to focus on SNS users' needs. For instance, as effectiveness was stated to influence users' adoption attitude, providing transparency of threats the tool protected the user from, should be a leading consideration during its design and development.

Online questionnaires give respondents the opportunity to provide their views anonymously and without the pressure of time that would be present in an interview; however there is always the possibility of inaccurate responses, lack of spontaneity and the restriction to specific answers. Survey findings presented in this paper are not to be used for generalizing and do not serve as the only basis for the design and implementation of privacy preserving applications for social network users.

They can be used to understand the low diffusion of PETs in terms of limited user awareness, and indicate that user-centred factors need to be considered for designing and developing privacy tools.

References

Acquisti A. 2010. 'The Economics of Personal Data and the Economics of Privacy', DRAFT, November 24, 2010, http://www.heinz.cmu.edu/~acquisti/papers/acquisti-privacy-oecd-22-11-10.pdf

Acquisti A. and Gross R. 2006.'Imagined communities: awareness, information sharing, and privacy on Facebook'. PET 2006. LNCS (4258):36–58. Berlin: Springer Heidelberg.

Balebako R., Leon P.G., Almuhimedi H., Kelley P.G., Mugan J., Acquisti A. and Sadeh, N. 2011. 'Nudging users towards privacy on mobile devices'.CHI 2011 workshop article. Balsa E., Brandimarte L., Acquisti, A., Diaz, C., Gürses, S. 2014. 'Spiny CACTOS: OSN users attitudes and perceptions towards cryptographic access control tools', http://www.cosic.esat.kuleuven.be/publications/article-2400.pdf

Black S.L. and Johnson A.F. 2012. 'Employers' Use of Social Networking Sites in the Selection Process'. The Journal of Social Media in Society, 1(1): 7-28.

Boyd D. and Hargittai E. 2010. 'Facebook privacy settings: Who cares?'.First Monday, 15(8).

Cetto A., Netter M., Pernul G., Richthammer C., Riesner M., Roth C. and Sänger, J. 2014. 'Friend Inspector: A Serious Game to Enhance Privacy Awareness in Social Networks'. Proceedings of the 2nd International Workshop on Intelligent Digital Games for Empowerment and Inclusion (IDGEI), Haifa, Israel.

Compañó R. and Lusoli W. 2010. "The Policy Maker's Anguish: Regulating Personal Data BehaviorBetween Paradoxes and Dilemmas". Economics of Information Security and Privacy: 169-185, Springer Science+Business Media, LLC.

Danezis G. and Gurses S. 2010. 'A critical review of 10 years of Privacy Technology'. Proceedings of Surveillance Cultures: A Global Surveillance Society?.

Davis Jr F.D. 1986. 'A technology acceptance model for empirically testing new end-user information systems: Theory and results'. Doctoral dissertation, Massachusetts Institute of Technology.

Ebiz/MbaA 2015, 'Top 15 Most Popular Websites | February 2015', http://www.ebizmba.com/articles/most-popular-websites

Ebiz/MbaB 2015. 'Top 15 Most Popular Social Networking Sites | February 2015', http://www.ebizmba.com/articles/social-networking-websites

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

ENISA 2010. 'Online as soon as it happens'. Report 2010

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

Fahl S., Harbach M., Muders T., Smith M. and Sander U. 2012.'Helping Johnny 2.0 to encrypt his Facebook conversations'.Proceedings of the Eighth Symposium on Usable Privacy and Security.ACM.

Flash Eurobarometer 2008. 'Flash Eurobarometer 225: Data Protection in EU: Citizens' Perception'.European Commission.

Henerson M., Morris T. and Fitz-Gibbon A. 1987.'How to measure attitudes'. California: Shape Publishers.

Jaatun, M. G., Tøndel, I. A., Bernsmed, K., & Nyre, Å. A. (2011). Privacy Enhancing Technologies for Information Control. Privacy Protection Measures and Technologies in Business Organizations, 1-31, IGI Global.

Kolter J., Netter M. andPernul, G. 2010.'Visualizing past personal data disclosures'. Proceedings of ARES'10 International Conference on In Availability, Reliability, and Security, 131-139. IEEE.

Leon P., Ur B., Shay R., Wang Y., Balebako R. and Cranor, L. 2012. 'Why Johnny can't opt out: A usability evaluation of tools to limit online behavioral advertising'. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 589-598, ACM.

Le Métayer D. 2010. 'Privacy by design: a matter of choice'. S. Gutwirth, Y. Poullet and P. De Hert (Eds.) Data protection in a profiled world:323-334. Springer, Heidelberg.

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

Litt E. 2013. ‘Understanding social network site users’ privacy tool use’. Computers in Human Behavior, 29(4): 1649-1656 .

Madejski M., Johnson M., Bellovin S.M. 2011.‘The Failure of Online Social Network Privacy Settings’. In: CUCS-010-11, 2011, http://academiccommons.columbia.edu/catalog/ac:135406

Martensen M., BorgmannL.and Bick M. 2011. ‘The Impact of Social Networking Sites on the Employer-Employee Relationship’. Proceedings of 24th Bled eConferenceeFuture: Creating Solutions for the Individual, Organizations and Society, Bled, Slovenia, (2011) Marwick A.E. and Boyd D. 2014. ‘Networked privacy: How teenagers negotiate context in social media’. New Media & Society: 1461444814543995.

METAGROUP 2005. ‘Privacy Enhancing technologies. META Group Report v1.1’. Denmark: Danish Ministry of Science Technology and Innovation’.

Pötzsch S. 2009. ‘Privacy Awareness: A Means to Solve the Privacy Paradox?’ In: Matyáš, V., Fischer-Hübner, S., Cvrček, D., Švenda, P. (eds.) The Future of Identity. IFIP AICT, vol. 298, pp. 226–236. Springer, Heidelberg.

Rogers E.M. 2010 ‘Diffusion of Innovations’. New York: Simon and Schuster. Saint-Jean F.andFeigenbaum, J. 2010. ‘Usability of browser-based tools for web-search privacy’.(No.YALEU/DCS/TR-1424). YALE UNIV NEW HAVEN CT DEPT OF COMPUTER SCIENCE.

Statista 2015, ‘Leading social networks worldwide as of January 2015, ranked by number of active users (in millions)’, http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

StatisticBrain 2014, Social Networking Statistics - Statistic Brain, http://www.statisticbrain.com/social-networking-statistics/

Vemou K. and Karyda M. 2013.‘A classification of factors influencing low adoption of PETs among SNS users’.Trustbus 2013. LCNS (8058): 74–84. Berlin: Springer, Heidelberg.

Vemou K. and Karyda, M. 2014.‘Guidelines and tools for incorporating privacy in Social Networking Platforms’.IADIS International Journal on WWW/Internet , 12(2): 16-33.

Wang Y., Leon P.G., Acquisti A., Cranor L.F., Forget A. and Sadeh, N. 2014. ‘A Field Trial of Privacy Nudges for Facebook’. CHI 2014 workshop article.

Wästlund E., Wolkerstorfer P. and Köffel C. 2010.‘PET-USES: Privacy-Enhancing Technology–Users’ Self-Estimation Scale’. In: M. Bezzi ae al. (Eds.) Privacy and Identity Management for Life, IFIP AICT 320, pp. 266-274), IFIP International Federation for Information Processing.

Wu J.H. and Wang S.C. 2005. ‘What drives mobile commerce?: An empirical evaluation of the revised technology acceptance model’. Information & management, 42(5):719-729.

Yeung C.M.A., Liccardi I., Lu K., Seneviratne O. and Berners-Lee T. 2009. ‘Decentralization: The future of online social networking’. W3C Workshop on the Future of Social Networking Position Papers (Vol. 2).

Appendix A – Survey questionnaire (translated in english)

User profile (personal status) 1. Sex

○ Male

○ Female

2. Age

○ 16-21

○ 22-28

○ 29-35

○ 36-45

○ 46-50

○ 51+

3. Education

○ Primary

○ Secondary

○ Higher (e.g. college)

4. Occupation

○ Private sector

○ Public sector

○ Freelancer

○ Unemployed

○ Student

○ Retired

○ Other:

Use of social networking services
1. Are you a member of social networking services?
(More than one answer is allowed)

□ Facebook

□ Google+

□ Linkedin

□ Pinterest

□ Twitter

□ None

□ Other:

2. How often do you use them?

	1	2	3	4	5	
Very often Select a value from a range of 1,Very difficult , to 5,Very easy.	○	○	○	○	○	Never

3. As a name of your profile you use:

○ Real

○ Alias

○ Fake

○ Other:

4. In social networks your contacts consist of:

○ Only those who I know

○ Mostly known and less strangers

○ Acquaintances and strangers

○ Mostly strangers and less known

Privacy attitudes

1. What information do you provide as a member of the social network you belong to?

	I do not provide this information	I provide this information, but deliberately not complete and accurate	I provide this information and it is complete and accurate
Name	○	○	○
Profile photo	○	○	○
Name day	○	○	○
Sex	○	○	○
Sexual preferences	○	○	○
Languages	○	○	○
Religious preferences	○	○	○
Political preferences	○	○	○
E-mail	○	○	○
Mobile phone	○	○	○
Telephone (home phone)	○	○	○
Alias	○	○	○
Home address	○	○	○
Website	○	○	○

	I do not provide this information	I provide this information, but deliberately not complete and accurate	I provide this information and it is complete and accurate
Marital status	○	○	○
Name partner	○	○	○
Family relatives	○	○	○
Profession	○	○	○
Education	○	○	○

2. Which of the following activities do you perform?

	Very often	Seldom	Little - not at all
Post photos	○	○	○
Submit a video	○	○	○
Post a comment	○	○	○
Participation in games	○	○	○
Participation in competitions	○	○	○
Check in	○	○	○

3. Do you know which of your personal data you allow access to by third-party applications (apps), such as contests, games, etc, in order to use them?

○ Yes

○ Whenever I download an application, I check the privacy settings

○ I do not pay attention

○ I do not know what applications are

○ I have never used such an application

4. You've set your profile as:

○ Private so that only my contacts can see

○ Partly private so that contacts of my contacts can see

○ Public, which is open to
everyone ○ I do not know

5. If you have private or partially private profile:

○ Limit which contacts can have access to information I provide

○ Everyone can see the
same ○ I do not know

6. How often do you check the settings of your personal data?

	1	2	3	4	5	
Very often Select a value from a range of 1,Very difficult , to 5,Very easy,.	○	○	○	○	○	Never

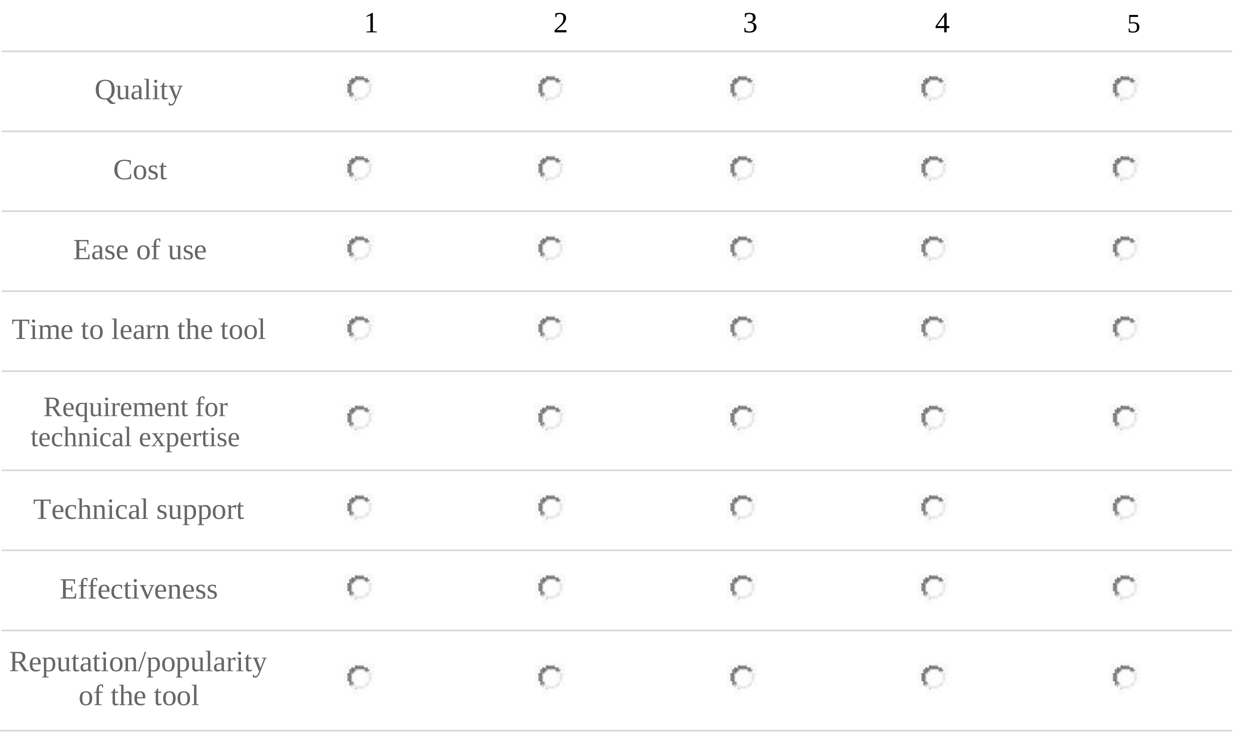
7. In social networks, the management of your personal data appears:
Select a value from the range 1 very difficult to 5 very easy

	1	2	3	4	5	
Very difficult Select a value from a range of 1,Very difficult , to 5,Very easy,.	○	○	○	○	○	Very easy

Tools to protect privacy
1. Do you know and / or use any of the following tools?

	I've used	I know but I have not used	I do not know
myPermissions	○	○	○
PrivacyFix	○	○	○
Friendwheel	○	○	○
Bitdefender Safego	○	○	○
ZoneAlarm Privacy Scan	○	○	○
Secure. me	○	○	○
Priveazy lockdown	○	○	○
Safe secure and private Facebook messages	○	○	○

2. How important do you consider the following factors for the use of protection tools? (rating from very important to not at all important)



	1	2	3	4	5
Quality	○	○	○	○	○
Cost	○	○	○	○	○
Ease of use	○	○	○	○	○
Time to learn the tool	○	○	○	○	○
Requirement for technical expertise	○	○	○	○	○
Technical support	○	○	○	○	○
Effectiveness	○	○	○	○	○
Reputation/popularity of the tool	○	○	○	○	○