Towards improving existing online social networks' privacy policies

Alexandra K. Michota*

Systems Security Laboratory,
Department of Digital Systems,
School of Information and Communication Technologies,
University of Piraeus,
150 Androutsou St. Piraeus 18532, Greece
Email: amichota@unipi.gr
*Corresponding author

Sokratis K. Katsikas

School of Pure and Applied Sciences,
Open University of Cyprus,
33 Giannou Kranidioti Ave. Latsia 2220, Nicosia, Cyprus
Email: sokratis.katsikas@ouc.ac.cy
and
Center for Cyber and Information Security,
Norwegian University of Science and Technology,
P.O. Box 191, Gjøvik N-2802, Norway
Email: sokratis.katsikas@ntnu.no

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

Keywords: privacy policy; standards; social networks; ISO29100:2011; PII lifecycle.

Reference to this paper should be made as follows: Michota, A.K. and Katsikas, S.K. (2018) 'Towards improving existing online social networks' privacy policies', *Int. J. Information Privacy, Security and Integrity*, Vol. 3, No. 3, pp.209–229.

Biographical notes: Alexandra K. Michota is an Officer in Network and Information Security at the European Union Agency for Network and Information Security (ENISA). She is working in the areas of privacy, data protection and fight against cybercrime – computer security incident response teams (CSIRTs) and law enforcement agencies (LEAs) cooperation. She has authored or co-authored journal publications and conference proceedings publications and participated in funded international R&D projects in her areas of interest that include information and communication systems security and privacy.

Sokratis K. Katsikas is the Rector of the Open University of Cyprus, Nicosia, Cyprus. He has authored or co-authored more than 230 journal publications, book chapters and conference proceedings publications and he has participated in more than 60 funded national and international R&D projects in his areas of interest that include information and communication systems security and applications of estimation theory.

This paper is a revised and expanded version of a paper entitled 'Compliance of the Facebook data use policy with the principles of ISO 29100:2011' presented at 6th International Conference on New Technologies, Mobility and Security – NTMS 2014 (Security track), Dubai, United Arab Emirates, 30 March to 2 April 2014; 'Compliance of the LinkedIn privacy policy with the principles of the ISO 29100:2011 standard' presented at 15th International Workshops on Web Information Systems Engineering – WISE 2014 Workshops, IWCSN 2014, Org2 2014, PCS 2014, and QUAT 2014; Org2 Workshop – Towards Organization 2.0: Advancements in Enterprise Social Networks, Thessaloniki, Greece, 12–14 October 2014.

1 Introduction

Surveys on concerns about general privacy, consumer privacy, medical privacy, and other privacy-related areas, as well as indices that allow inferring related trends over time have appeared in the literature since the 1970s (Kumaraguru and Cranor, 2005). In a general online service context, a prototype of an online interactive tool embedding features of the concept of online interactive (OI) privacy in generic online services, was presented and evaluated in Kani-Zabihi and Helmhout (2012). The findings therein suggest that OI privacy features increase users' privacy awareness and encourage users to find out more about the uses of their personal data. Coles-Kemp and Kani-Zabihi (2010) argue that online service providers and service users want to engage in privacy and consent dialogue and explore how a socio-technical approach should ideally form the basis of the design and implementation of any dialogue system.

People use different online social networks (OSNs) depending on their personal needs. The availability of information brings convenience to modern life; however privacy breaches are increasingly getting in the spotlight and have caught people's attention, raising valid privacy concerns (Acquisti and Gross, 2006; Boyd and Hargittai, 2010).

Privacy in the specific world of OSNs has been the subject of extensive research efforts in the past decade. Since 2005, when Gross and Acquisti (2005) published their findings on the potential risks induced by information sharing in Facebook (Acquisti and

Grossklags, 2005), several studies concerning privacy in the online world have appeared in the literature, which shed light on different aspects of privacy in OSNs.

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

OSN privacy policies should provide the users with an easy and flexible way to inform and enforce their privacy preferences to other users, to third parties and to the OSN service providers. Unfortunately, in most cases these policies are not clearly and explicitly stated; they are often long and abstruse, thus virtually impossible to understand, even if the user is willing to invest time for reading them (Kayes and Iamnitchi, 2015). Long as they are, these privacy policies tend to be incomplete (Office of the Privacy Commissioner of Canada, 2009), as they often cannot include all the parties to which user's private information will be allowed to flow (such as advertisers). Moreover, since the policies are not documented in a manner easily understandable by the average, non-expert user, the OSN provider can modify them without the users noticing it, thus, putting the users at great risk of privacy violations (Dwyer et al., 2007). The result of all this is that generally people do not read the terms of service and when they do, they do not understand them (Fiesler and Bruckman, 2014), particularly if they are low-level educated (Strater and Lipford, 2008; Cheek and Shehab, 2012; Masoumzadeh and Joshi, 2013). It is also known that individuals are more likely to agree with the privacy policies on familiar social media websites (Yang et al., 2015). Hence, on the users' side, it is apparent that there is a need for OSN privacy policies that will enjoy a number of characteristics, namely appropriate length, high comprehensiveness, low complexity, accessibility, readability, consistency and accuracy; these are equally important factors aside from the actual content of the policy (Capistrano and Chena, 2015).

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

The remainder of this paper is structured as follows: the related work is presented in Section 2. Section 3 briefly discusses the privacy framework proposed by the ISO 29100:2011 standard. In Section 4, we introduce the privacy policies of the five most popular OSNs, namely Facebook; LinkedIn; Google Plus; Twitter; Instagram. Their conformance to the ISO 29100:2011 principles is examined in Section 5. Section 6 describes our proposal for re-designing existing OSN privacy policies and Section 7 summarises our conclusions and outlines directions for future work.

2 Related work

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

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

In this paper, we compare the ISO 29100:2011 standard privacy framework that describes privacy safeguarding considerations that should be observed when a privacy policy is designed, to the privacy policies of the five topmost leading social networks. This is done by building upon, consolidating, re-structuring and expanding earlier works in Michota and Katsikas (2014, 2015b). The results of this examination indicate serious mismatches that need to be addressed if the policies are to be improved. We further propose a restructuring of the existing policies according to a data lifecycle model; this will allow them to enjoy some of the desirable characteristics reported in Capistrano and Chena (2015).

3 The ISO 29100 (2011) privacy framework

The aim of a privacy framework is to guide organisations towards achieving a positive-sum outcome, a win-win solution for the related actors, by ensuring the protection of an individual's privacy without sacrificing functionality or security. Easy-to-use privacy services are keys for enabling users to maintain control of their private data in the online environment. The ISO/IEC 29100:2011 standard (ISO 29100, 2011) provides a privacy framework for handling PII.

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

The design, development and implementation of privacy policies and controls are to be guided by 11 privacy principles as suggested by the standard; these are as follows:

- *Consent and choice*: the PII principal should be presented with the choice whether to allow or not the processing of their PII, such opt-in and informed consent to be given freely, specific and on a knowledgeable basis.
- *Purpose legitimacy and specification*: the purposes of the processing should comply with the law, and they should be communicated to the PII principal before the PII collection, using clear language.
- *Collection limitation*: collected PII should be limited to what is legal and necessary for the specified purposes.
- *Data minimisation*: the PII that is processed should be minimised, as well as the number of entities that have access to it; these entities have to be determined on a 'need-to-know' principle; interactions and transactions which do not involve the identification of PII principals, reduce the observability of their behaviour and limit the linkability of PII should be used; and PII should be deleted and disposed of whenever the purpose for processing it expires.
- *Use, retention and disclosure limitation*: use, retention and disclosure of PII should be limited to what and to when it is necessary for fulfilling the specified purposes.
- *Accuracy and quality*: PII must at all times be accurate, complete, up-to-date, adequate and relevant.
- *Openness, transparency and notice*: PII principals must be, at all times, provided with clear, complete and accessible information on the controller's policies regarding the processing of PII.
- *Individual participation and access*: PII principals should have the ability to simply, quickly and efficiently access and review their PII, to challenge its accuracy and completeness, and to have it modified as appropriate, such modifications to be communicated to any and all recipients of such PII.
- *Accountability*: PII processing must be performed in ways such that duty of care is demonstrated and practical and concrete measures for its protection must be adopted.

- *Information security*: the security of PII must be ensured, with appropriate controls.
- *Privacy compliance*: adherence to privacy safeguarding requirements, laws, and regulations must be verified and demonstrated by means of internal or third party audits and privacy risk assessments.

4 OSN privacy policies

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

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

All OSN privacy policies are structured in parts. The first part explains either in short forms or in detail what kinds of information the OSN service provider collects. The remaining parts are not similarly structured.

Facebook's privacy policy (*Facebook Data Policy*, 2016) is also known as the 'data policy'. Facebook has split this policy down to eight parts, namely 'what kinds of information do we collect?' (part 1); 'how do we use this information?' (part 2); 'how is this information shared?' (part 3); 'how can I manage or delete information about me?' (part 4); 'how do we respond to legal requests or prevent harm?' (part 5); 'how our global services operate?' (part 6); 'how will we notify you of changes to this policy?' (part 7); and 'how to contact Facebook with questions?' (part 8).

LinkedIn has split its privacy policy (*LinkedIn Privacy Policy*, 2016) down to four parts, namely 'information collected' or 'what information we collect?' (part 1); 'uses and sharing of personal info' or 'how we use your personal information?' (part 2); 'your choices and obligations' (part 3); and the part on 'important information' (part 4).

Google Plus has split its privacy policy (*Google Plus Privacy Policy*, 2016) down to 12 parts, namely 'information we collect' (part 1); 'how we use information we collect' (part 2); 'transparency and choice' (part 3); 'information you share' (part 4); 'accessing and updating your personal information' (part 5); 'information we share' (part 6); 'information security' (part 7); 'when this privacy policy applies' (part 8); 'compliance and cooperation with regulatory authorities' (part 9); 'changes' (part 10); 'specific product practices' (part 11); 'other useful privacy and security related materials' (part 12).

Twitter recently revised its privacy policy (*Twitter Privacy Policy*, 2016) and removed two parts; the current privacy policy of Twitter is split down to five parts, namely 'information collection and use' (part 1); 'information sharing and disclosure' (part 2); 'accessing and modifying your personal information' (part 3); 'our policy towards children' (part 4); 'changes to this policy' (part 5). It is worth pointing out that, in an effort to protect the privacy of the young and to comply with the relevant data protection laws, both Twitter's and Instagram's privacy policies include a part on their specific policies towards the collection of children's PII.

Instagram has split its privacy policy (*Instagram Privacy Policy*, 2016) down to ten parts, namely 'information we collect' (part 1); 'how we use your information' (part 2); 'sharing of your information' (part 3); 'how we store your information' (part 4); 'your choices about your information' (part 5); 'children's privacy' (part 6); 'other websites and services' (part 7); 'how to contact us about a deceased user' (part 8); 'how to contact us' (part 9); 'changes to our privacy policy' (part 10).

5 Conformance of the OSN privacy policies with the ISO 29100:2011 standard privacy principles

5.1 Method

Laws and regulations typically carry with them requirements for assessment of compliance, or conformance in the case of standards. In some cases, these are supplemented by methods for assessing conformance that typically lead to certification of conformance. This is, for example the case with some information security standards, such as the ISO/IEC 27002 (ISO 27002, 2013) standard. Unfortunately, it is not yet the case with the ISO/IEC 29100 standard.

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

For example, adhering to the 'individual participation and access' principle means (ISO 29100, 2011):

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

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

On the other hand, adhering to the 'openness, transparency and notice' principle means (ISO29100, 2011):

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

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

5.2 Results

The results of the evaluation are comprehensively shown in Tables 1–5. Two symbols are used as entries in these tables. The symbol '+' designates that a policy part is largely conformant with a principle, whereas the symbol 'O' designates that a policy part is partially conformant with a principle.

Table 1 Compliance of the Facebook data use policy to the ISO 29100:2011 principles

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

Table 2 Compliance of the LinkedIn privacy policy to the ISO 29100:2011 principles

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

Table 3 Compliance of the Google Plus privacy policy to the ISO 29100:2011 principles

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

Table 4 Compliance of the Twitter privacy policy to the ISO 29100:2011 principles

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

Table 5 Compliance of the Instagram privacy policy to the ISO 29100:2011 principles

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

5.3 Discussions

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

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

Regarding how the OSN service providers use the information they receive from OSN users' profiles, openness, transparency and clear notices about the way the users'

PII is used are provided by the corresponding policy parts of LinkedIn, Google Plus and Twitter, whilst users' participation and access are offered to these OSN users in case they would like to make changes to match their intentions. The 'accountability' privacy principle is largely conformed to only by the corresponding parts of LinkedIn and Twitter.

Furthermore, the OSN PII processing procedure policies do not fully adhere to the privacy safeguarding requirements. For instance, the *LinkedIn Privacy Policy* (2016) states that the OSN service provider may provide, and the users might use, other mechanisms similar to the contacts importer, allowing users to upload individual contacts or their entire address book. The mobile applications may allow the OSN users to synchronise their calendar, email, or contact apps with LinkedIn to show meeting attendees, email correspondents and contacts. As far as the privacy protection and security by using cookies goes, it is claimed that by allowing cookies users help secure Facebook by letting them know if someone tries to access another user's account or engages in activity that violates Facebook's terms of use. However, there is a unique identifying code known as 'pixel' that is assigned to the users by the OSN and that can be matched with behaviour tracked by cookies. This means that third party service providers, such as advertisers, are able to use information gleaned from the OSN to build a profile of a user's life, including linking browsing habits to one's true identity. LinkedIn has clarified that mobile application identifiers are used rather than mobile device identifiers, to help identify the user across their services. The *Google Plus Privacy Policy* (2016) states that although Google Plus may combine personal information from one service with information from other Google services in order to make it easier for its users to share things with people they know, Google Plus will not combine cookie information with PII unless it has its users' opt-in consent. Most of the times, when users do not accept the use of cookies, they cannot take full advantage of the online services; thus, users are pushed to give their consent and to allow the use of cookies. Hence, the 'information security' and 'privacy compliance' principles are only partially conformed to. Fortunately, the 'openness, transparency and notice' principle is largely conformed to in the policy parts that describe how the OSN service providers use their members' PII. This is so because the data subjects are informed about the data controller policies, and the OSN service providers give proper notices that personal data is being processed, and provide their users with information on how to access and review their personal data; for instance, when users' PII is used in advertising campaigns. Only Instagram provides vague information and a poor description of its pertinent policy.

The maintenance of OSN accounts is, justifiable, a source of privacy concerns for the users. According to the *Facebook Data Policy* (2016), accounts are permanently deleted from the Facebook database at the request of a user, but some information may remain in backup copies and logs for up to 90 days, as stated in the 'what's the difference between deactivating and deleting my account?' part of Facebook's Help Center and there is no choice for direct and full deletion even if the user so wished. As stated in the *LinkedIn Privacy Policy* (2016), if a user decides to close her account(s), her information will be removed from the service within 24 hours. LinkedIn deletes closed account information and will de-personalise any logs or other backup information within 30 days of the account closure. It is also specified by its policy that even if LinkedIn removes a user's data, her public data may be displayed in search engine results until the search engine refreshes its cache. The 30 days window is also defined as the limit either for the deactivation or for the deletion of an account on Twitter. Instagram 's policy on

termination or deactivation of an account is that the OSN service provider may retain information and users' content for a reasonable time for backup, archival, and/or audit purposes. The maintenance of a Google Plus account is not described in its privacy policy; only guidelines about how a user can delete her account are provided (*Delete your Google+ Profile*, 2016).

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

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

Table 6 Compliance of the examined OSNs to the ISO 29100:2011 principles

		ISO 29100 2011 privacy principles										
		Consent and choice	*Purpose legitimacy and specification*	*Collection limitation*	*Data minimisation*	*Use, retention and disclosure limitation*	*Accuracy and quality*	*Openness, transparency and notice*	*Individual participation and access*	*Accountability*	*Information security*	*Privacy compliance*
OSN privacy policy	Facebook	O	O	O	O	O	+	O	O	O	O	O
	Linkedin	+	O	O	O	O	+	+	+	O	O	O
	Google Plus	O	O	O	O	O	+	O	O	O	O	O
	Twitter	O	O	O	O	O	+	+	+	+	O	O
	Instagram	+	O	O	O	O	+	O	O	O	O	O

Table 6 summarises the results over all the examined OSNs. As seen in the Table 6, only the 'accuracy and quality' privacy principle seems to be largely conformed to in all the privacy policies. This is not surprising, as most OSN service providers preserve the accuracy and timeliness of the PII. To the contrary, the principles of 'collection limitation' and 'data minimisation' are only partially conformed to by all OSN privacy policy parts. This is because the collection of data is unlimited, even though sensitive data may also be included, and data processing is not minimised as this would defeat the purpose of achieving the OSN service provider's organisation goals.

6 PII lifecycle management

6.1 Existing OSN privacy policies

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

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

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

Several information life cycle models have been proposed for different purposes (Ball, 2012). For our purposes herein, a simple model, comprising six stages suffices. The first stage is the collection of users' PII, e.g. the creation of their profile. The next stage, processing, includes possible modifications to the provided information. PII storage is the third stage. The next stage is the PII transfer that translates to the internal sharing and to the external dissemination/publication of information. The fifth stage is the maintenance of the PII that includes PII destruction and retention. The last stage entitled 'service management' was added to the proposed privacy policy aiming to aggregate all the information related to the interactions between OSN users and OSN providers.

A study on the extent to which current OSN policies map upon the information lifecycle was performed in Michota and Katsikas (2015a). This study included Facebook, LinkedIn, Google Plus, and Twitter and concluded that their privacy policies map only to few of the data lifecycle stages. In the following tables, that follows the convention set out for its counterparts in Michota and Katsikas (2015a), the symbol '●' designates that all the necessary information that should be contained to describe in detail a PII lifecycle stage is provided by a policy part, whereas the symbol '○' designates that a PII lifecycle stage is only partially covered by a policy part. Partial coverage may be highlighted in more than one policy parts, as information about a PII lifecycle stage may be addressed in different policy parts.

The mapping of the recently revised Twitter privacy policy onto the PII lifecycle stages is shown in Table 7. According to this mapping, only the PII collection and the PII maintenance among the PII lifecycle stages are fully covered by two Twitter privacy policy parts namely 'information collection and use' and 'modifying your personal

information'. In Twitter's privacy policy, a separate policy part presents the special case of children's PII collection, namely 'our policy towards children'.

Table 7 Mapping of the Twitter privacy policy parts onto the PII lifecycle stages

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

Table 8 Mapping of the Instagram privacy policy parts onto the PII lifecycle stages

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

As can be seen in Table 8, the case of Instagram is not very different. More specifically, in the *Instagram Privacy Policy* (2016), the stage of PII collection is fully covered and is analytically described on its first policy part, namely 'information we collect'; the case of gathering children's PII is also presented. Parts of the remaining PII lifecycle stages are found in more than one policy parts of Instagram.

6.2 An improved privacy policy model

Taking into account the gaps we identified in the mapping of OSN privacy policies to the PII lifecycle stages, we recommend an improved privacy policy model that aggregates all the information that should be included in each policy part aiming concurrently to meet the requirements emerged by the ISO29100:2011 privacy principles. Table 9 summarises the mapping results of all the examined OSN privacy policies onto the PII lifecycle

stages; after having identified the missing information in each OSN policy part, Table 10 presents an improved model that contains all the data we need for creating an effective OSN privacy policy taking into account the principles introduced by the ISO29100:2011.

Table 9 Mapping of the OSN privacy policy parts onto the PII lifecycle stages

	Collection	*Processing*	*Storage*	*Transfer*	*Maintenance*
Facebook data use policy	●				
LinkedIn privacy policy		●		●	
Google Plus privacy policy		○			
Twitter privacy policy	●				●
Instagram privacy policy	●				

Table 10 Improved OSN privacy policy model

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

The first part of an OSN's privacy policy should address the collection of all types of information that the users provide during their membership, regardless of its nature or source or means (i.e., cookies, advertising technologies, web beacons, and anonymous identifiers) of collection. To this end, taxonomy of the OSN data types, such as the one proposed in Richthammer et al. (2014) must be developed. The policy should also specify which types of information are public by default and which are searchable even when privacy restrictions have been applied; thus, the users will be free to decide which PII types they are willing to share with each OSN audience.

The second part should address the processing procedure that includes the use of and the access to the users' PII and its possible modification for proper (or improper) purposes. In existing policies, the reasons why the service provider uses the users' PII are

given, but how this is being done, how PII is modified and who is accountable for all forms of processing and who is allowed to access it are not mentioned. If these issues are sufficiently addressed, the 'data minimisation' and the 'accountability' privacy principles will be fully conformed to.

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

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

The policy part on maintenance should describe what happens when a user decides to delete, deactivate or regain access to her account. Clear notices about these activities should be given to the data subjects and justifications about temporary or permanent PII storage to the OSN servers should be published in the policies when a deletion or a deactivation request has been submitted.

The last part of the proposed policy entitled 'service management' should provide information on regulatory compliance that will cover issues related to legal requests or obligations; policy change management that will explain issues like notifications about policy modifications; and contact management that will provide guidelines on how to contact the corresponding OSN provider.

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

In addition, visualisation as a means for communicating privacy and security measures has been shown to have a positive effect on the trust that the users have in services (Becker et al., 2014). Hence, techniques that allow users to easily grasp the privacy risk associated with the privacy policies and with their own personalised privacy settings, analogous to those proposed in Kang et al. (2015), Yee et al. (2008), Ghazinour et al. (2009) should be also developed and employed in OSNs.

7 Conclusions

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

The European general data protection regulation (GDPR) establishes the 'privacy by design' principle as a legal obligation for privacy protection. However, the abstractness of the legal obligation calls for systematic guidance for adhering to it, such as the

guidance provided by international standards. Even though such high-level guidance is provided by existing standards, the need for establishing methodologies and mechanisms for auditing the conformance of information communication technology (ICT) systems, including OSNs, with the requirements set out in the standards becomes apparent. The imminent enforcement of the GDPR calls for standardisation bodies to move swiftly in this direction.

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

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

Future work includes the development of a structured methodology for assessing conformance of a privacy policy with the ISO 29100 standard that may pave the way towards certification. It also includes the empirical assessment of the validity of the assumption that an OSN privacy policy re-structured according to the model proposed herein leads to improved user comprehension, accessibility, acceptance and usability. It further includes developing and validating an OSN-specific data lifecycle model; and designing, developing and evaluating privacy policy visualisation techniques and tools for OSNs.

References

Acquisti, A. and Gross, R. (2006) 'Imagined communities: awareness, information sharing, and privacy on Facebook', in Danezis, G. and Golle, P. (Eds.): *Privacy Enhancing Technologies*, pp.36–58, Springer, Berlin Heidelberg, DOI 10.1007/11957454_3.

Acquisti, A. and Grossklags, J. (2005) 'Privacy and rationality in individual decision making', *IEEE Security and Privacy*, Vol. 3, No. 1, pp.26–33.

American National Standards Institute (ANSI) (2004) *Privacy Impact Assessment Standard*, ANSI X9.99-2004 [online] https://www.ansi.org (accessed 17 January 2018).

Anthonysamy, P., Greenwood, P. and Rashid, A. (2013) 'Social networking privacy: understanding the disconnect from policy to controls', *IEEE Computer*, Vol. 46, No. 6, pp.60–67.

Ball, A. (2012) *Review of Data Management Lifecycle Models (Version 1.0)*, REDm-MED Project Document redm1rep120110ab10, University of Bath, Bath, UK.

Becker, J., Heddier, M. and Öksüz, A. (2014) 'The effect of providing visualizations in privacy policies on trust in data privacy and security', in *Proceedings of 2014 47th Hawaii International Conference on System Science*, IEEE Computer Society Press, pp.3224–3232, DOI 10.1109/HICSS.2014.399.

Boyd, D. and Hargittai, E. (2010) 'Facebook privacy settings: who cares?', *First Monday*, Vol. 15, No. 8 [online] http://firstmonday.org/article/view/3086/2589 (accessed 22 February 2016).

Canadian Standards Association (1996) *Model Code for Protection of Personal Information*, CAN-CSA-Q830-96 [online] https://simson.net/ref/RSA/1996.CanadianStandardsAssociation.ModelCodeForProtectionOfPersonalInfo.pdf (accessed 17 January 2018).

Capistrano, E.P.S. and Chena, J.V. (2015) 'Information privacy policies: the effects of policy characteristics and online experience', *Computer Standards & Interfaces*, Vol. 42 pp.24–31.

Castelluccia, C. and Narayanan, A. (2012), *Privacy Considerations of Online Behavioural Tracking*, Report 2012, Enisa [online] https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking/at_download/fullReport (accessed 22 February 2016).

Cavoukian, A. (2010) 'Privacy by design: the definitive workshop', A foreword by Ann Cavoukian, *Identity in the Information Society*, Vol. 3, No. 2, pp.247–251.

Cheek, G.P. and Shehab, M. (2012) 'Policy-by-example for online social networks', in *Proceedings of the 17th ACM Symposium on Access Control Models and Technologies (SACMAT'12)*, ACM Press, pp.23–32, DOI 10.1145/2295136.2295142.

Chen, S. and Williams, M-A. (2009) 'Privacy in social networks: a comparative study', in *Proceedings, Pacific Area Conference on Information Systems (PACIS 2009)*, Paper 81, Association for Information Systems.

Coles-Kemp, L. and Kani-Zabihi, E. (2010) 'Online privacy and consent: a dialogue, not a monologue', in *Proceedings of NSPW'10*, ACM Press, Concord, Massachusetts, USA, 21–23 September, pp.95–105.

Delete your Google+ Profile (2016) [online] https://support.google.com/plus/answer/1044503?hl=en (accessed 7 October 2016).

Diaz, I. and Ralescu, A. (2012) 'Privacy issues in social networks: a brief survey', in Greco, S., Bouchon-Meunier, B., Coletti, G., Fedrizzi, M., Matarazzo, M. and Yager R.R. (Eds.): *Advances in Computational Intelligence*, pp.509–518, Springer, Berlin, Heidelberg.

Dwyer, C., Hiltz, S.R. and Passerini, K. (2007) 'Trust and privacy concern within social networking sites: a comparison of Facebook and Myspace', in *Proceedings of the Thirteenth Americas Conference on Information Systems (AMCIS 2007)*, Paper 339, AIS.

Facebook Data Policy (2016) [online] https://www.facebook.com/about/privacy (accessed 5 October 2016).

Fiesler, C. and Bruckman, A. (2014) 'Copyright terms in online creative communities', in *CHI'14 Extended Abstracts on Human Factors in Computing Systems*, ACM Press, pp.2551–2556.

Gerlach, J., Widjaja, T. and Buxmann, P. (2015) 'Handle with care: how online social network providers' privacy policies impact users' information sharing behavior', *Journal of Strategic Information Systems*, Vol. 24, No. 1, pp.33–43.

Ghazinour, K., Majedi, M. and Barker, K. (2009) 'A model for privacy policy visualization', in *Proceedings of 2009 33rd Annual IEEE International Computer Software and Applications Conference*, pp.335–340, DOI 10.1109/COMPSAC.2009.156.

Google Plus Privacy Policy (2016) [online] https://www.google.com/policies/privacy (accessed 28 October 2016).

Gross, R. and Acquisti, A. (2005) 'Information revelation and privacy in online social networks', in *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society (WPES '05)*, ACM Press, pp.71–80.

Han, P. and Maclaurin, A. (2002) 'Do consumers really care about online privacy?', *Marketing Manage*, Vol. 11, No. 1, pp.35–38.

Hoepman, J-H. (2014) 'Privacy design strategies', in Cuppens-Boulahia, N. et al. (Eds.): *ICT Systems Security and Privacy Protection, Proceedings of the 29th IFIP TC 11 International Conference (SEC 2014)*, Springer, Marrakech, Morocco, 2–4 June, pp.446–459.

Instagram Privacy Policy (2016) [online] https://www.instagram.com/about/legal/privacy (accessed 6 September 2016).

ISO 27001 (2013) *ISO/IEC 27001:2013-Information Technology – Security Techniques – Information Security Management Systems – Requirements* [online] https://www.iso.org/standard/54534.html.

ISO 27002 (2013) *ISO/IEC 27002:2013 Information Technology – Security Techniques – Code of Practice for Information Security Controls* [online] https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en.

ISO 27007 (2011) *ISO/IEC 27007:2011-Information Technology – Security Techniques – Guidelines for Information Security Management Systems Auditing* [online] https://www.iso.org/obp/ui/#iso:std:iso-iec:27007:ed-1:v1:en.

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

ISO 29100 (2011) *ISO/IEC 29100:2011-Information Technology – Security Techniques– Privacy Framework* [online] https://www.iso.org/standard/45123.html.

Kang, J., Kim, H., Cheong, Y.G. and Huh, J.H. (2015) 'Visualizing privacy risks of mobile applications through a privacy meter', in Lopez, J. and Wu, Y. (Eds.): *Information Security Practice and Experience, Proceedings of the 11th International Conference ISPEC 2015*, Springer, Beijing, China, 5–8 May, pp.548–558.

Kani-Zabihi, E. and Helmhout, M. (2012) 'Increasing service users' privacy awareness by introducing online interactive privacy features', in Laud, P. (Ed.): *NordSec 2011*, LNCS 7161, pp.131–148.

Kayes, I. and Iamnitchi, A. (2015) *A Survey on Privacy and Security in Online Social Networks*, Cornell University Library [online] http://arxiv.org/abs/1504.03342v1 (accessed 22 February 2016).

Kumaraguru, P. and Cranor, L. (2005) *Privacy Indexes: A Survey of Westin's Studies*, Technical Report, Institute for Software Research, Carnegie Mellon University [online] http://www.cs.cmu.edu/~ponguru/CMU-ISRI-05-138.pdf (accessed 03 June 2016).

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

LinkedIn Privacy Policy (2016) [online] https://www.linkedin.com/legal/privacy-policy (accessed 28 October 2016).

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* [online] http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf (accessed 22 February 2016).

Masoumzadeh, A. and Joshi, J. (2013) 'Privacy settings in social networking systems: what you cannot control', in *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security (ASIA CCS'13)*, ACM Press, pp.149–154, DOI: 10.1145/2484313.2484331.

Michota, A. and Katsikas, S. (2014) 'Compliance of the Facebook data use policy with the principles of ISO 29100:2011', in *Proceedings, NTMS 2014 (Security Track)*, Dubai, UAE, pp.96–100.

Michota, A. and Katsikas, S. (2015a) 'Designing a seamless privacy policy for social networks', in *Proceedings, 19th Panhellenic Conference on Informatics (PCI 2015)*, DOI: 10.1145/2801948.2801998.

Michota, A. and Katsikas, S. (2015b) 'Compliance of the LinkedIn privacy policy with the principles of the ISO 29100:2011 standard', in Boualem, B. et al. (Eds.): *Web Information Systems Engineering – WISE 2014 Workshops, 15th International Workshops IWCSN 2014, Org2 2014, PCS 2014, and QUAT 2014*, *Revised Selected Papers Org2 Workshop – Towards Organization 2.0: Advancements in Enterprise Social Networks*, Thessaloniki, Greece, 12–14 October 2014, pp.1–12.

NIST SP 800-53 (2013) *Security and Privacy Controls for Federal Information* [online] http://dx.doi.org/10.6028/NIST.SP.800-53r4 (accessed 13 February 2014).

Office of the Privacy Commissioner of Canada (2009) *Privacy Commissioner Recommends Steps to Ensure Social Networking Site Better Protects the Privacy of Users and Meets the Requirements of Canadian Privacy Legislation*, Office of the Privacy Commissioner of Canada [online] https://www.priv.gc.ca/media/nr-c/2009/nr-c_090716_e.asp (accessed February 2016).

Richthammer, C., Netter, M., Riesner, M., Sänger, J. and Pernul, G. (2014) 'Taxonomy of social network data types', *EURASIP Journal on Information Security*, Vol. 2014, p.11, DOI: 10.1186/s13635-014-0011-7.

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

Tang, Z., Hu, Y. and Smith, M.D. (2008) 'Gaining trust through online privacy protection: self-regulation, mandatory standards, or caveat emptor', *Journal of Management Information Systems*, Vol. 24, No. 4, pp.153–173.

Twitter Privacy Policy (2016) [online] https://twitter.com/privacy (accessed 2016).

Vemou, K. and Karyda, M. (2014) 'Embedding privacy practices in social networking services', in Powell, P., Nunes, M.B. and Isaías, P. (Eds.): *Proceedings of the 7th IADIS International Conference Information Systems 2014*, IADIS Press, Madrid, Spain, March, pp.201–208.

Vemou, K., Karyda, M. and Kokolakis, S. (2014) 'Directions for raising privacy awareness in SNS platforms', in *Proceedings of the 18th Panhellenic Conference on Informatics (PCI '14)*, ACM Press, New York, NY, pp.1–6, DOI: http://dx.doi.org/10.1145/2645791.2645794.

Vu, K-PL., Chambers, V., Garcia, F.P., Creekmur, B., Sulaitis, J., Nelson, D., Pierce, R. and Proctor, R.W. (2007) 'How users read and comprehend privacy policies', in Smith, M.J. and Salvendy, G. (Eds.): *Human Interface and the Management of Information. Interacting in Information Environments, Symposium on Human Interface 2007, Held as Part of HCI International 2007*, Proceedings, Part II, Springer Verlag, Beijing, China, 22–27 July, pp.802–811.

Yang, R., Ng, Y.J. and Vishwanath, A. (2015) 'Do social media privacy policies matter? Evaluating the effects of familiarity and privacy seals on cognitive processing', in *Proceedings of 2015 48th Hawaii International Conference on System Sciences*, IEEE Computer Society Press, pp.3463–3472, DOI: 10.1109/HICSS.2015.417.

Yee, G.O.M., Korba, L. and Song, R. (2008) 'Cooperative visualization of privacy risks', in Luo, Y. (Ed.): *Cooperative Design, Visualization, and Engineering, Proceedings of the 5th International Conference CDVE 2008*, Springer, Calvià, Mallorca, Spain, 21–25 September, pp.45–53.

Zheleva, E. and Getoor, L. (2011) 'Privacy in social networks: a survey', in Aggarwal, C.C. (Ed.): *Social Network Data Analytics*, pp.277–306, Springer, Boston, MA.