ECIS 2010 Proceedings

European Conference on Information Systems (ECIS)

2010

SNS and 3rd Party Applications Privacy Policies and their Construction of Privacy Concerns

Ramzi Rizk
Humboldt University, rizk@wiwi.hu-berlin.de

Seda Gürses
IBBT, seda.guerses@esat.kuleuven.be

Oliver Guenther
Humboldt University, guenther@wiwi.hu-berlin.de

Recommended Citation

Rizk, Ramzi; Gürses, Seda; and Guenther, Oliver, "SNS and 3rd Party Applications Privacy Policies and their Construction of Privacy Concerns" (2010). *ECIS 2010 Proceedings*. 143.
http://aisel.aisnet.org/ecis2010/143

SNS AND 3RD PARTY APPLICATIONS PRIVACY POLICIES AND THEIR CONSTRUCTION OF PRIVACY CONCERNS

Journal:	*18th European Conference on Information Systems*
Manuscript ID:	ECIS2010-0465
Submission Type:	Research Paper
Keyword:	Privacy/information privacy, Online communities, Social issues, Socio-technical approach

SNS AND 3RD PARTY APPLICATION PRIVACY POLICIES AND THEIR CONSTRUCTION OF PRIVACY CONCERNS

Rizk, Ramzi, Institute of Information Systems, Humboldt University, Berlin, Germany, rizk@wiwi.hu-berlin.de

Gürses, Seda, ESAT/COSIC, IBBT and Department of Computer Science, K.U. Leuven, Heverlee, Belgium
seda.guerses@esat.kuleuven.be

Oliver Günther, Institute of Information Systems, Humboldt University, Berlin, Germany, guenther@wiwi.hu-berlin.de

Abstract

In this paper we use template analysis to study the content of privacy policies both of online social networks as well as 3rd party application providers. After analysing and prioritising the topics mentioned in these policies, we discuss potential problems, limitations of privacy policies, and the responsibilities they assign to various stakeholders. These findings will, in future work serve as stakeholder input for aligning social networking sites' privacy definitions, concerns, and practices.

Keywords: Privacy policy, social networks, 3rd party application providers, template analysis.

1 INTRODUCTION

Social networking services (SNS) continue to expand; both in terms of the number of users they have, and the number and scope of integration with other social web applications (Third Party Applications). SNS also remain a very interesting application domain for understanding changing privacy concerns, practices and conflicting definitions from the perspective of different stakeholders.

Most popular SNS and Third Party Applications (TPA) provide privacy policies to address some of these privacy concerns and practices. Privacy policies are legally binding and socially constructed documents (non-human objects) and play an important role in defining the roles and responsibilities of the involved stakeholders. Documents such as privacy policies can be interesting for researchers since they are actively and collectively produced, exchanged and consumed; indicate many decisions by many people; reflect special social circumstances; and, lastly, since their consumption is a social process, governing who will use which documents for what purposes (Miller & Alvarado 2005).

The main objective of this paper is to analyze privacy policies to prioritize the privacy concerns of the SNS and TPA providers and the privacy practices they offer to the different stakeholders. In order to fulfil this objective, we decided to conduct a qualitative study of the privacy policies of social networks. Using a qualitative method, we expect to identify topics of interest, regardless of how, or how often, they are addressed. Our objective is to study the privacy concerns of SNS providers with respect to users and other stakeholders, to understand how these topics are related to each other in the documents, and to study the construction of the different roles, responsibilities and accountabilities assigned to the different stakeholders. Hence, we selected template analysis to study privacy policies. Based on this method we systematically coded the privacy policies and posed the following questions:

- How is privacy defined in the privacy policies of SNS and TPAs? Is it limited to the descriptions in various data protection principles or do the policies extend those principles and/or offer alternatives where data protection has its shortcomings?
- Which issues are relevant and important for the SNS and TPAs with respect to their users' privacy? Which issues do the play down? What kind of accountability and liability do they offer or assign to their users or third parties with respect to the information they manage?
- Which concerns do providers specifically articulate with respect to third parties and users' personal information? Which stakeholders are identified as responsible for addressing these concerns? And, how is the situation framed from the perspective of third parties?

We chose Facebook, Myspace and Orkut as the SNS of interest for a variety of reasons. Facebook is currently the largest SNS and has had its fair share of privacy issues over the years. It also recently adopted a "democratic" approach to updating its Terms of Use and Privacy Policies. Myspace was the largest SNS for a long time and targets a different audience from Facebook, including musicians and artists. Orkut is heavily present in the Brazilian and Indian market and is a Google-owned company. Google itself has been the focus of a series of privacy related critiques. Additionally, we chose two of the largest 3rd party application providers, Zynga and Playfish, whose products include many of the most popular games on SNS. Zynga is based in California, and Playfish in the UK. The different locations are also interesting since they reflect the different data protection laws the companies comply with.

Due to space limitations, we will focus on passages and statements that stand out in the aforementioned policies. We also shortly present an overview of the themes (codes) derived from our analysis. Comprehensive analyses and comparisons of all the policies can be found in a technical report we have produced on this topic (Guerses and Rizk 2010). The same technical report also includes a mapping of a previous study on user privacy concerns with respect to SNS based on another set of documents: news and the blogosphere (Rizk et al. 2009). There we also analyze if the concerns raised by the different stakeholders in these documents are matched or addressed by the privacy policies, or not.

The remainder of this paper is structured as follows. Section 2 presents related work in the areas of SNS and privacy policies and describes template analysis. Section 3 discusses the analysis of the privacy policies of SNS providers and presents the main codes or themes identified therein. Section 4 presents the same analysis for TPA providers. Finally, Section 6 discusses the results and concludes this paper.

2 RELATED WORK, METHODOLOGY AND DOCUMENTATION

SNS and TPA privacy policies are by-products of legislation or national recommendations of data protection principles applied to the collection, processing and distribution of personal information. In the USA, the Federal Trade Commission recommends the Fair Information Practices (2007), which are enforced through self-regulation, private remedies and government enforcement. All data collection processing in continental Europe is subject to the Regulation (EC)No 45/2001 (2000), whereas in the U.K. this is regulated by the Data Protection Act (1998).

In our analysis, we mention the principles and legislation that the privacy policies in our data set explicitly claim to address. Nevertheless, our concern is not to study which information practices or data protection principles are applied or legislation is complied with, as in the recent survey by Reay & Dick & Miller (2009). Instead, we study how these principles are interpreted and communicated in the privacy policies, which ones are emphasized, and which others are left rather nebulous.

We used template analysis to systematically study the privacy policies. Template analysis is similar to thematic analysis in that it is used to thematically organize and analyse textual data. The essence of template analysis is that the researcher produces a list of codes ('template') representing themes identified in their textual data. The template is most commonly organized in a hierarchical structure, representing the relationships between the themes (King 2004). Template analysis can be used within a range of epistemological positions: anywhere between the positivistic position of quantitative analysis "discovering" underlying causes of human action, to the 'contextual contructivist' position which assumes that there may be many interpretations depending on the researcher and the context of the research (King 2004).

In this study, we subscribe to the second school of thought. Quantitative and experimental studies of privacy policies exist. These studies are concerned with the automation of privacy policies using machine-readable solutions (Reeder & Kelley & McDonald & Cranor 2009), semi-structured language analysis to extract privacy requirements from privacy policies (Breaux and Anton 2005), usability and readability of privacy policies (McDonald & Reeder & Kelley & Cranor 2009), and presentation and visualization of privacy policies (Kelley 2009).

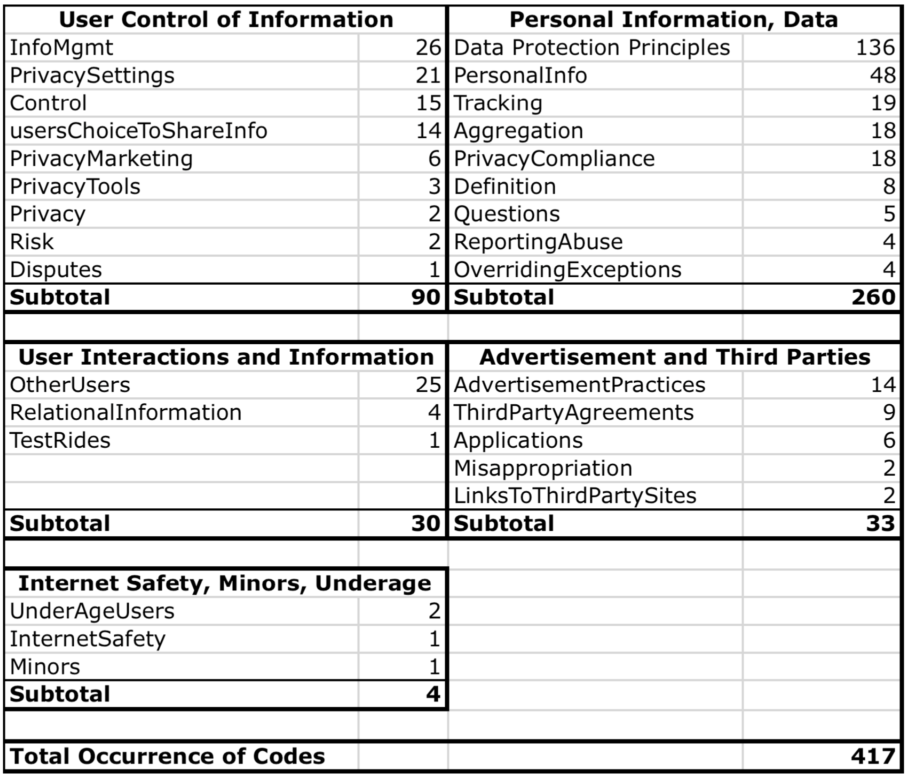
While quantitatively analysing the codes, or even the vocabulary and grammar of the privacy policies, reveals interesting starting points for studies, we assume that the frequency of code may not tell us everything meaningful about the semantics of and relationships between textual data. Sometimes a topic mentioned may make an important difference in the analysis of a privacy policy regardless of the frequency of its mention. As stated on the homepage of the Template Analysis Method: "The fact that a theme is particularly common – or rare – may point to something worth closer attention, but in qualitative analysis it must never be taken as any kind of "evidence" in and of itself. The process of listing themes is about raising questions, not answering them." (Template Analysis 2009)

Further, usability and readability studies focus on the comprehension and transparency of these policies. If privacy policies are to serve any purpose, then the their transparency and usability are central. Yet, making the policies transparent is a different concern then the need for a deeper analysis as to how the policies construct or order the relationship between users and service providers, service providers and third parties, and between users. We are unaware of any studies that move beyond matters of legal compliance and usability that also investigate the construction of roles, responsibilities and accountabilities in privacy policies in a comparable manner.

According to the template analysis method, a first version of the template is either pre-defined or established through some initial coding. A code is a label attached to a section of text, to index it as relating to a theme or issue in the data, which the researcher has identified as important to her interpretation (King 04). The hierarchical organization of codes enables the researcher to analyze the data at varying levels of detail: higher-order codes can give an overview, while lower-order codes allow for fine distinctions to be made both within and among specific cases.

We followed the template analysis process in developing our template (based on an initial first run through the Facebook Privacy Policy, later developed by applying it to the full data set). We expected the main data protection principles to be present, but did not define a priori themes in order to avoid bias. Our data set contained only privacy policies of the subjects, but we did identify helping documents that are explicitly or indirectly linked to the policies, listed here in the form (number of explicit links : number of implicit links): Facebook (11:26), Orkut (8:25), Myspace (3:14), Zynga (3:4), Playfish (4:0). When necessary, we included references to those helping documents. Finally, we used the TAMS Analyzer (Tams 2008) to analyze frequencies of codes, relationships and resulting hierarchies among codes.

3 ANALYSIS OF SNS PRIVACY POLICIES



User Control of Information		**Personal Information, Data**	
InfoMgmt	26	Data Protection Principles	136
PrivacySettings	21	PersonalInfo	48
Control	15	Tracking	19
usersChoiceToShareInfo	14	Aggregation	18
PrivacyMarketing	6	PrivacyCompliance	18
PrivacyTools	3	Definition	8
Privacy	2	Questions	5
Risk	2	ReportingAbuse	4
Disputes	1	OverridingExceptions	4
Subtotal	**90**	**Subtotal**	**260**
User Interactions and Information		**Advertisement and Third Parties**	
OtherUsers	25	AdvertisementPractices	14
RelationalInformation	4	ThirdPartyAgreements	9
TestRides	1	Applications	6
		Misappropriation	2
		LinksToThirdPartySites	2
Subtotal	**30**	**Subtotal**	**33**
Internet Safety, Minors, Underage			
UnderAgeUsers	2		
InternetSafety	1		
Minors	1		
Subtotal	**4**		
Total Occurrence of Codes			**417**

Figure 1 Final Template of high-level codes and the five main topics

Based on the final version of our template, seen in Figure 1, we grouped sets of related codes from all SNS privacy policies into 5 topics. The figure also includes high-level code counts. In the following, we will describe our findings for four of the main topics. We do not discuss minors and underage users as this is a topic in itself that is not only about privacy but also about the relationship between parents and children, children and their peers, children and educational institutions, etc. Much work has been done on the topic of minors by Danah Boyd (Boyd 2007), among others.

Stakeholders in SNS privacy policies: A *stakeholder* can be defined as any individual, group, or organization whose actions can influence or be influenced by the development and use of the system whether directly or indirectly (Pouloudi 1999). According to this definition, parents, privacy initiatives, schools, businesses whose employees use SNS, institutions that offer trust seals, legislators and many others are also stakeholders of SNS.

Parents are mentioned in all three documents as playing an important role for supporting safe internet practices of minors and underage users but are out of the scope of our analysis. The TrustE seal is mentioned as a stakeholder in the Facebook Privacy Policy. The US Safe Harbor Principles as agreed on between the EU and the USA are mentioned in all three policies.

The focus of this study is on privacy policies and hence we limit our stakeholders to those either mentioned or addressed in these documents: the SNS itself, the registered users of an SNS, the readers of the privacy policy, and third parties. Third Parties in SNS are divided into three groups: third party advertisers, third party partners (including partners and affiliates), and TPAs.

3.1 Topic 1: Personal Information, Data Protection and Policy:

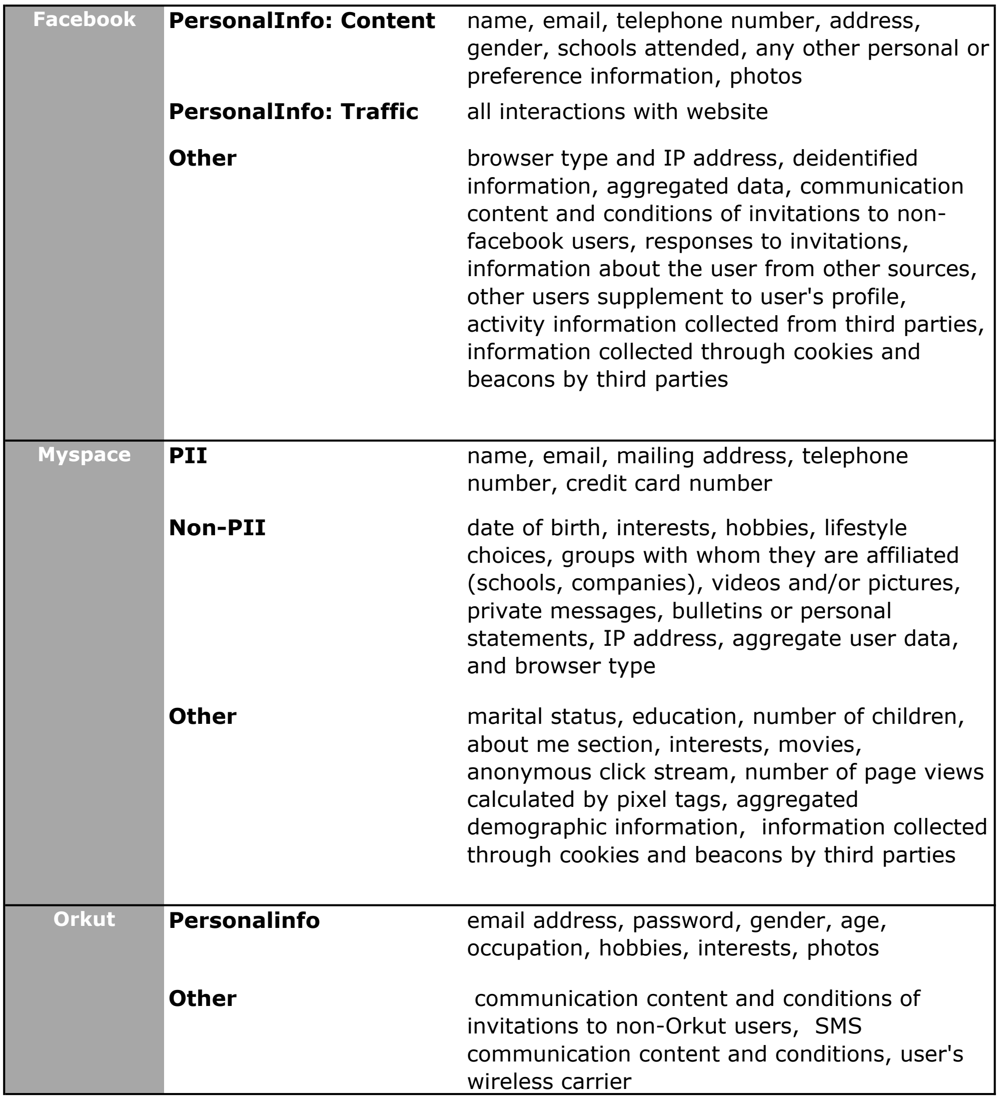
The first topic is concerned with the definition and scope of the policy and explanations of how the policy applies data protection principles to personal information. This topic is closely related to Topic 2 with regards to data collection and processing for advertisement and by third parties.

The main audience of all three privacy policies are registered users, while subtleties in the definitions of the audience exist. Facebook commences the privacy policy by addressing a "you" that is supposedly the user who *voluntarily shares* information with the SNS, both Myspace and Orkut start by defining when the policy start applying to its reader. Moreover, Myspace makes the distinction between *members* and *visitors*, hence suggesting that the policy also applies to the visitors of the site. Although Facebook talks about *test rides* for visitors that can take a peek into the social network, it is not clear if the Facebook Privacy Policy applies to them.

A definition of the "user" is provided only later in the Facebook Privacy Policy after a first section that alludes to a caring relationship between Facebook and its users. This introduction enunciates the importance of sharing information on Facebook and the provider's *helper* role in the process of sharing. Although much of the Facebook policy is about the collection and processing of a wide range of personal information by Facebook and third parties, the privacy problem is defined as something else.

According to the Facebook Privacy Policy, privacy is a matter of controlling personal information that users willingly and knowingly *choose* to put on Facebook. *Control* is defined as the user's ability to control accessibility of personal information to other users. A small number of exceptions apply to controlling information processed by the SNS itself and third parties. Therefore, privacy on Facebook is not about what Facebook itself can do with the information it collects, processes and shares with Third parties.

In comparison, Myspace and Orkut's privacy policies are more functional and are concentrated on making transparent their data practices. Both policies do not provide users with definitions of privacy; the word privacy is never mentioned in the main text of the Orkut Privacy Policy. Rather, they describe if and how the providers apply subsets of the data protection principles. In that sense, these two policies are predominantly about defining the conditions with respect to personal information between a single user and the provider of the SNS. Both, Myspace and Orkut mention functionality to control sharing among users, but this is not the dominant theme in their privacy policies.



Facebook	**PersonalInfo: Content**	name, email, telephone number, address, gender, schools attended, any other personal or preference information, photos
	PersonalInfo: Traffic	all interactions with website
	Other	browser type and IP address, deidentified information, aggregated data, communication content and conditions of invitations to non-facebook users, responses to invitations, information about the user from other sources, other users supplement to user's profile, activity information collected from third parties, information collected through cookies and beacons by third parties
Myspace	**PII**	name, email, mailing address, telephone number, credit card number
	Non-PII	date of birth, interests, hobbies, lifestyle choices, groups with whom they are affiliated (schools, companies), videos and/or pictures, private messages, bulletins or personal statements, IP address, aggregate user data, and browser type
	Other	marital status, education, number of children, about me section, interests, movies, anonymous click stream, number of page views calculated by pixel tags, aggregated demographic information, information collected through cookies and beacons by third parties
Orkut	**Personalinfo**	email address, password, gender, age, occupation, hobbies, interests, photos
	Other	communication content and conditions of invitations to non-Orkut users, SMS communication content and conditions, user's wireless carrier

Figure 2 Categorization of the policies of the data collected in each SNS.

The definition of personal information plays an important role in articulating the scope of the privacy policies. Figure 2 shows the different categories of personal information used by the privacy policies, the data that is explicitly classified under each category, and the data that is mentioned in the policies but is not explicitly classified under a given category. We listed such data in the rows labeled "other" for each privacy policy.

We note here a difference between the US definition of *personally identifiable information* (PII) (Office of Management and Budget 2007), and the EU's broader definition of *personal data.* While PII covers data that directly identifies an individual e.g., name, social security number, the EU Directive 95/46/EC provides a much broader and vague definition of personal data. For computer scientists, this includes de-identified personal information through which individuals can be identified probabilistically:

Myspace's privacy policy refers to the US definition of PII whereas Google and Facebook define a larger set of data as personal information, more close to the EU Directive’s definition. Any options Myspace offer to users are mainly about the protection of the PII. Given the limited scope of PII as defined above, Myspace can share almost all other profile information uploaded by the users with to third parties without apprehension.

In Orkut, personal information includes all the profile content but traffic data is not explicitly classified as personal information. Orkut does document their extensive collection of their users' traffic data which includes the content and conditions of all communications with non-Orkut users.

Facebook has an even broader definition of personal information. It is the only privacy policy that explicitly makes a distinction between the personal information provided by the user, which we coded as *PersonalInfo:Content*, and "Web Site use information collected by us as you interact with our Web Site" which we coded as *PersonalInfo*:*Traffic*. Facebook offers users privacy controls only with respect to their PersonalInfo:Content and not with respect to their traffic data. Hence, traffic data is rendered as being outside of the privacy concerns and control of users.

Further, Facebook explicitly states that it collects information about its users from other sites in order to offer users a personalized experience. Users are able to opt-out of the collection of data from other sources. But, there are no statements about the users' ability to access, edit or delete information previously collected.

In all three privacy policies, anonymized or de-identified data is described as being data that cannot be linked back to the original users. It is not described how far the SNS go with de-identification, whether they make use of state of the art privacy preserving data mining techniques, whether they update these techniques as proofs of their vulnerability are made public, and whether they deal with the anonymization of network structures that have proven to be difficult (Narayanan and Shmatikov 2009).

“Accessing and editing personal data” is mentioned by all three privacy policies, however, only Myspace (ironically, the site which least requires users to input the “real” information) makes guarantees with respect to accuracy of personal information.

The policies mention a number of possibilities to opt out of a subset of the data collection and processing activities indicated in the policies. These possibilities are always coupled with third party applications and data collection practices, the only exceptions being email notifications and Facebook Beacon.

All three sites state that they may not be able to secure the users’ data, that data may become public, and that they are not accountable for such leakages. Facebook states that they may constrain the use of personal information by Third parties through agreements but they are not responsible for resulting breaches.

Such statements can be interpreted in two ways. Either as a sign of honesty, given digital systems, the nature of the Internet and the security problems therein, any security or privacy mechanisms are subject to threats due to conditions that the providers themselves do not always control. Or as a means of freeing all three data collectors from accountability for the massive databases that they are running.

Facebook explicitly makes no guarantees with respect to TPA providers’ privacy compliance, while Myspace and Google state that the agreements include agreements with respect to necessary security measures for the shared information.

Both peer-to-peer add-ons and encryption could offer more secure alternatives with the same functionalities to SNS, none of the three SNS offer such mechanisms to secure sensitive or other information belonging to their users. Facebook and Orkut do mention the use of SSL for some of their communication, whereas we found no mention of such technologies in Myspace.

Description of data retention practices in all three policies does not contain time limitations. Facebook and Orkut state that the retention of data is necessary to provide the SNS services. It is also not clear if this unspecified "reasonable period of time" also applies to the traffic data.

Deletion should terminate data retention, but all of the policies make a distinction between deletion and deactivation, state that traces may be left on back up devices or mirror servers, and make it costly to delete the profile. The policies again do not state if deletion also applies to traffic data. Myspace does not explicitly state what happens to non-PII when a user deletes her account. Further, it states that PII necessary for federal, state or local law will also be retained. It is unclear how much of the small set of PII needs to be retained according to federal, state or local law. All policies state something similar. None of the policies offer to notify the users with respect to breach of data, delivery of data for legal purposes, or sharing with third parties.

Orkut provides a two-step explanation of profile deletion that leaves the reader perplexed. According to these descriptions, logging in after deletion may re-activate the user's account. Further complete deletion is only possible if the user deletes all Google related accounts. This is a high price to pay to achieve the complete deletion of a profile on one of the Google services.

3.2 Topic 2: Advertisement and Third Parties

All privacy policies describe the SNS' sharing practices with third parties. There are four types of data sharing statements that are mentioned: (1) sharing profile information with third parties, (2) collecting information from Third Parties, (3) SNS providers blocking access to certain information with Third Parties, and (4) users revealing information to third parties directly. Third parties are either advertisers, search engines, subcontractors for the services offered by the SNS, third party sites that are linked through the SNS, or legally defined third parties (government agencies, law enforcement, or any subjects with a legitimate legal request for data).

Facebook states that it shares de-identified information with advertisers and offers customized ads based on user behaviour. Facebook does not offer any option for users to opt-out of such a customized advertisement program, while both Myspace and Orkut do. Myspace depends on the veritability of the Network Advertising Initiative's Opt-Out program. Orkut lists only Predicta and Double Click as advertisement partners with the ability to opt-out. For the Predicta site we were unable to find an opt-out option. Orkut offers no opt-out from the collection of communication content of SMS.

Facebook explicitly states that it collects information about its users from third party sites. Although by now it is common to get access to users web based address books, none of the policies mentioned this sensitive aspect in their privacy policies.

Further, the address book imports and collection (or scraping) of data from third party sites, practices that SNS admit to themselves, have led to a series of yet unresolved lawsuits about data portability and user lock-in. It is interesting that these lawsuits are being challenged as a matter of "Terms of Use" and not as a matter of privacy and related policies (Techcrunch a, 2009). Facebook states that it will discard data collected from third party sites if the users opts out, meaning that the information is collected even if the user opts-out, to be discarded afterwards.

All three SNS mention that users may share information with third parties directly, if they install TPAs, follow links to other sites, or receive advertisements. All SNS do not take responsibility for information collected by the TPAs and instead, advise the users to read their privacy policies. Orkut explains that TPAs receive all public profile information, which is defined to include all content that is not set to a limited circle of friends. The application also receives information about other pages that the user visits (given the application is also installed there). The user's information becomes visible to users of the application on other sites.

TPAs do not contain privacy policies on their SNS-based information pages. Therefore, users are left to their own device for locating these privacy policies, discovering which terms apply to their use of the application in the specific SNS and making an informed decision about their privacy.

3.3 Topic 3: User Control of Information:

Sharing in SNS includes the right to own one's own information and control with whom to share information. Hence, Facebook provides users with privacy settings in order to control their sharing. But what control, ownership and sharing means are constrained by all SNS providers.

The *controls* that users are given for their profile information applies at a maximum to: limiting search and access to profile information by other users; limiting access to third parties, and disabling indexing of profiles by third party search engines. With the exception of email notifications and Beacon, all three sites offer no controls with respect to data that is uploaded to the SNS itself. No mechanisms are provided to the users to keep any of their information confidential from the SNS.

In that sense, in their privacy policies the SNS flaunt themselves as trusted. Users should be concerned about controlling their information with respect to other users and third parties. With the SNS themselves such controls are not necessary and are not provided. This contrasts with the accountability guarantees that the SNS provide their users: all SNS state in their privacy policies that they are not responsible for any security breaches and public leakages of data.

By limiting the scope of the controls, not only do the SNS not step up to being accountable for the data they hold in their databases, they also construct the user as the figure responsible for making the right privacy decisions and controlling access to their own profile information. The users are the ones that *choose* to provide their information, they use the site *at their own risk* and they have to *decide* set their controls towards others.

And yet this choice and control ends already with traffic data: revelation of traffic data is not information that a user ``knowingly chooses" to provide the SNS, nevertheless, they have no controls over it.

In comparison, the "choices" made by the SNS and Third Parties are depicted in privacy policies as a matter of fact, a necessity for better services, and a description of practice. The SNS determine the boundaries of the choices that users make and may even override these. Even further, the underlying design is set up such that users may override other user’s choices with respect to controlling their profile information, if it conflicts with their desire to share information. The fact that one user's decision to share information with TPAs determines what happens with their friends' data further exacerbates the problem of addressing data sharing and control decisions as a matter of individual choice.

3.4 Topic 4: User Interactions and Information

SNS are designed to enhance sharing based on relationships between users and a number of features that broadcast information to (subsets of) these relationships. SNS work with transitive access control models where related users may be granted access rights and control rights i.e., the ability to dynamically extend the access list for one piece of information. For example, if a piece of information is accessible to friends-of-friends, then that means that friends of the user co-determine who is allowed on the access control list by virtue of defining their own set of friends. When a relationship is established between two users, both have control permissions on the relationship information itself: they can both delete the relationship and make its presence accessible to their choice of friends. We call any information in an SNS that can be *controlled* by more than one user *relational information*.

Relational information is not an exception in SNS but rather the rule: photos are commented by others, walls are written on by many, discussions have many participants. “Other users may supplement your profile”, states Facebook. Hence, if a user wants to share their information, it is possible that supplements to that user's profile by others will also be shared. Hence, the concept of individually controlling data towards other users is intrinsically bound to fail.

Depending on the underlying design, those friends may then make that information accessible to a greater public. This points to an unresolved contradiction between the fact that the SNS are platforms for sharing; the design is optimized for sharing collectively, and the fact that privacy related controls are designed for individual users. The controls set by individual users may become meaningless and provide no more guarantees as soon as information is shared with or controlled by one or more users. None of the SNS take responsibility for information that becomes public as a result of their underlying design or give a reasonable description of how it works.

The ability to only individually control a limited amount of personal information coupled with the hands-off attitude of SNS providers with respect to information belonging to many suggests that the privacy policies and controls they offer only effectively apply to data that is not shared and is related to a single user. This is in most cases is limited to the persons contact information and personal attributes. Any other settings to control information may be overridden by the underlying design and this is not the responsibility of the SNS.

Being able to control private attributes has recently been questioned. Studies have shown that attributes revealed by friends in a profile's vicinity might be used to infer confidential attributes (Zheleva & Getoor 2009) cautioning about revelations of networks. Against this type of thinking, Stalder (2002) argues that in a networked world the intrinsic attributes of individuals are less valuable than being able to prove that a user is well networked. It is the connectedness and being able to prove their “existence” that allows individuals access to communities and organizations.

Hence, although the revelation of hidden personal attributes is a problem, we conclude that the privacy policies attention to individual control of private attributes and not much more does disservice to the importance of relational information and collective sharing in a networked world.

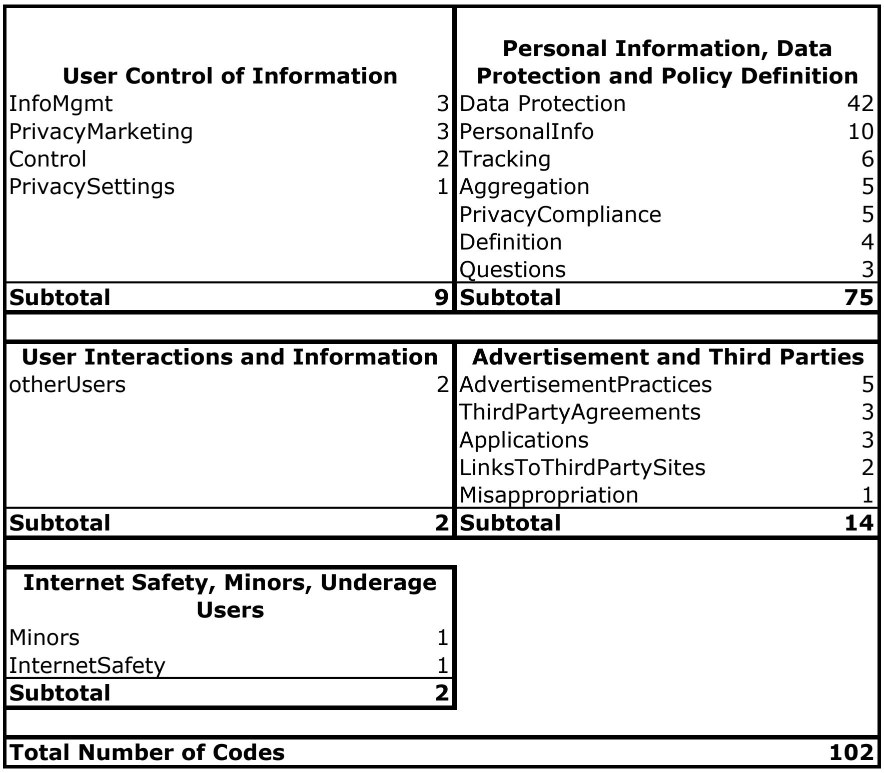
Myspace's privacy policy is less concerned with justification of the sharing practices, although they also explain that making profiles accessible through search engines and browsing is important to connecting members. Orkut uses a similar language, states that privacy controls may be overridden by the decisions of other users, and takes no responsibility.

Relational information also causes problems with the deletion of data. It is not clear which information will be deleted when users terminate their accounts. In Orkut there are dozens of help pages for the different deletion options. None of these are mentioned or linked on the page for deleting profiles. In some cases, users may also delete contributions made by others: community owners are able to delete all comments from single users; a photo owner is able to delete comments to her photos and on her wall or comments she left on other users' walls. Deletion of relational information can be about both the privacy of a user or the integrity of a user's profile or a community's discussion forum.

The differences in opinion as to which of privacy and integrity is of higher priority may lead to conflicts. Neither the design nor the privacy policies address potential conflicts arising out of relational information removal. They also do not offer the possibility to negotiate or notify users when deletion is desired or unwanted deletion occurs. Only Facebook addresses that disputes may arise, but what kind of disputes, if they also include disputes among users is unclear.

4 PRIVACY POLICIES OF 3RD PARTY APP PROVIDER

In addition to analyzing the privacy policies of SNS, we decided to study two of the largest providers of TPAs, Zynga (a San Francisco based company) and Playfish (London based). Between the two of them, these providers are responsible for more than 10 of the top (mostly games) third party applications on Facebook and other SNS (Gamasutra, 2009).



User Control of Information		Personal Information, Data Protection and Policy Definition	
InfoMgmt	3	Data Protection	42
PrivacyMarketing	3	PersonalInfo	10
Control	2	Tracking	6
PrivacySettings	1	Aggregation	5
		PrivacyCompliance	5
		Definition	4
		Questions	3
Subtotal	**9**	**Subtotal**	**75**

User Interactions and Information		Advertisement and Third Parties	
otherUsers	2	AdvertisementPractices	5
		ThirdPartyAgreements	3
		Applications	3
		LinksToThirdPartySites	2
		Misappropriation	1
Subtotal	**2**	**Subtotal**	**14**

Internet Safety, Minors, Underage Users	
Minors	1
InternetSafety	1
Subtotal	**2**

Total Number of Codes	**102**

Figure 3 Final Template of high-level codes and the five main topics

We will again describe our findings for the main template topics. The policies of Zynga and Playfish are brief, however they do offer a different angle from which to study privacy policies.

The privacy policies here also list the user and the provider as clear stakeholders. In addition to SNS, advertising partners, 3rd party content providers, partners, affiliates and the users' contacts on the SNS themselves.

Parents of minors and legal bodies are also mentioned, as are certain legislations. As these are not discussed in detail, they do not play a large role in our analysis here.

Stakeholders in TPA privacy policies: The stakeholders mentioned in TPA privacy policies are as follows: the TPA itself, the registered users of a TPA, the readers of the privacy policy, and third parties. Third Parties in TPA are third party advertisers, third party partners (including partners and affiliates), other TPAs, and additional third parties called content providers.

4.1 Topic 1: Personal Information, Data Protection and Policy:

Both providers start by identifying their sites and the documents. Playfish continues by immediately mentioning their compliance with data protection legislation (Data Protection Act, 1998) this is later somewhat negated by the fact that user information might be transferred outside of Europe where similar legislation might not exist (section 4). Zynga, on the other hand, starts by assuring the user that their information privacy is important, and that the service is designed to protect that information from misappropriation. They explicitly mention Californian law’s protection of opt-out right from disclosing information to third parties. Furthermore, Zynga confirms that they use SSL (Secure Socket Layer) technology for processing sensitive information. Playfish states that they have *“implemented reasonable technical and organisational measures dedicated to secure your personal [...]”*. Those measures are not explicitly discussed, and this statement is immediately followed by a disclaimer that the internet is an open system, and that they cannot guarantee that unauthorised third parties will not be able to defeat those measures and misappropriate users' personal information. Playfish uses an unidentified third party for payment processing. We will discuss third parties in section 5.2.

Both providers dedicate sections to the collection and processing of personal information. Users are told that they consent to the collection of their personal information by using the service on Zynga, and that they reserve the right to retain all that information, *"in anonymous form"* for as long as they see fit. Playfish makes no mention of consent on a global level, they do however mention consent with regards to transfer of personal information outside of Europe.

In addition to basic personal data that both services collect on registration, SNS accounts (such as Facebook IDs) are gathered when users use applications on those SNS. Remarkably, Zynga states that the IDs are also collected if a user uses the app on a contact's SNS page. No further information is given at this point, particularly, there is no mention made of what exactly constitutes "usage" in this case. This confirms, to a certain extent, the privacy breach identified by Guerses et. Al (2008), that TPAs have access not only to their users' accounts, but also to those of the users' friends. At this point, Zynga points users towards the ToS and PPs of SNS providers for more information.

Both providers, as in most other PPs that we have studied, discuss the user's responsibility to read changes to the policies, inform the user about their information moving to new owners in case of a change of ownership, and about the fact that they may gather information about the user from various sources.

With regards to legal bodies, Zynga states that they may access, preserve and disclose information as they see fit in order to avoid liability or when required to do so by law. Playfish does not mention this particular topic. Zynga additionally states that they may maintain and/or delete information as they see fit, particularly if such content constitutes an infringing or prohibited posting.

Activity tracking, and particularly the usage of cookies, is given major coverage on Playfish. Almost a third of the policy is dedicated to explaining what cookies are, and how playfish uses them. The provider identifies two types of cookies, those issued by Playfish itself, and those issued by third party advertisers. For the latter, Playfish clearly states that they have neither access to, nor control of the cookies. Furthermore, the provider informs users about their ability to disable cookies, with the notice that not all features of the service may be available in the case of disabled cookies. Zynga also mentions both cookies placed by other content providers since *"most content delivered through Zynga games originates with another content provider"*. No further mention of how and what information is gathered here, who those "content providers" are, and how users can get to the bottom of this chain of responsibility can be discerned from the policy.

Both providers discuss newsletters and other forms of notifications sent to users. Playfish mentions an opt-in system whereby users request certain newsletters, whereas Zynga says that they offer an unsubscribe link in the case of emails. They however state that they may use *"your name, email address and other information on our system to notify you of [...]"*. What that "other information" is, and how users can opt-out of receiving notifications through those channels is not made clear.

4.2 Topic 2: Advertisement and Third Parties:

After data collection, retention and processing, advertisements and third parties make up the second largest data body in both policies. Sharing information with third party content providers, advertisers and others is mentioned regularly throughout, and the line between data anonymization, aggregation, mining, as well as PII and non-PII is very blurred. In this section we will dissect that information and try to clarify what type of information is shared with whom, according to the privacy policies.

Playfish informs users that they may use targeted/behavioral advertising, but issues an assurance that the advertisers will not receive information regarding who views those advertisements. They do, however, mention passing along activity information to third parties in order to improve the service.

That information is, however, aggregated data and statistics which can not be used to identify individual users.

In both policies, a differentiation is made regarding third party advertising companies. Those may place cookies and use pixel tags (or beacons) in the advertisements. The providers do not claim any responsibility for information gathered through these cookies or tags. Additionally, Zynga mentions that, even though they do not provide any PII to these advertisers, information is sent when a user views a targeted add, and the advertiser may then conclude that the user has the characteristics (age, gender, etc) which that ad was targeting.

This information conflicts with the statements made in another section, that Zynga DOES provide non-PII and certain technical information (including IP and activity information) to its partners (including advertisers). However, the partners have no independent right to further share that information. Zynga also states that users may not opt-out of sharing that information *"whether personally identifiable information or other information"*. Suddenly, there is mention of PII, which wasn't the case before. Particularly since, only a few paragraphs before that statement, Zynga clearly states *"We do not sell or rent your "Personally Identifiable Information to any third party. We may, however, use certain information about you that is not personally"*. This whole section starts to contradict itself, and does not offer a coherent statement to the user, with all the conflicting statements regarding sharing, renting and selling, as well as PII, non-PII and activity information. Someone who studies the section in detail, let alone a casual reader, is left confused and not really aware of what their rights are.

Both providers do not explicitly mention security practices, rather, Playfish issues an assurance to the user: *"In some cases, the third party may receive your information. However, at all times, we will control and be responsible for the use of your information."* This claim of responsibility is quite unusual, and does not appear in any of the other policies we analysed. However, Playfish does not really explain what that "responsibility" really entails in terms of accountability. Zynga simply claims that certain of its partners, their contractors and employees may view user information and perform the various tasks (as set forth in the Privacy Policy).

4.3 Topic 3: User Control of Information:

There are interesting points to be made regarding control of information on both services. Playfish offers users the chance to request to see the information available about them (for a fee of 10 GBP). There is no specification regarding what that information exactly is, whether it includes relational information, or information gathered from other sources. One caveat is the providers' right to withhold access to that information where that right is provided under data protection legislation. Users may review, correct, update or change their personal information by directly contacting Playfish. There is no mention of allowing users to complete delete their information. Zynga, on the other hand, makes no mention of allowing users to view or change their information. They do state that any interactions and content sent through the service may be collected and used by unspecified "others"! Account termination is explicitly mentioned here, but again with the caveat that information available on users may be retained even after said termination.

4.4 Topic 4: User Interactions and Information:

Users of Zynga may invite other people to join the service, or to deliver information to users through SNS apps offered by Zynga. Zynga reserves the right to retain and disclose that information to legal bodies, as well as to send invitations and reminders to those users. Recipients have the right to opt-out of receiving further invitations. There is no mention of this in Playfish's privacy policy.

In conclusion, Zynga's Privacy Policy is much more detailed and comprehensive than that of Playfish, however, they tend to offer fewer rights to the users, and make more use of data mining and information aggregation and sharing for various purposes. Playfish assumes a more reassuring, user-friendly tone, but on the downside, offers a more vague document that leaves many topics (ex: account termination) untouched. Both providers share information with numerous unspecified partners, associates and content providers. The extent of the information shared, and who the recipients of that information are must be made available to users, at the least.

5 DISCUSSION AND CONCLUSION

The objectives that these privacy policies fulfil are unclear. Based on the section titles, the policies read as attempts to document how the data is collected and processed according to principles of data protection. But the policies don't provide proper guarantees on data security or on the privacy controls offered through the privacy tools, share data extensively with third parties and offer few possibilities for users to negotiate what data is collected and disseminated.

The way privacy related information is not concentrated in one central document or location but are spread over several related documents across websites of SNS and TPA provider's, their partners, and unidentified others makes it nearly impossible for users to have a comprehensive overview of their privacy information. Users are left with the grand responsibility of controlling their "personal information", while the rules of the game are determined by those who collect information and can juggle data protection compliant privacy policies in such a way that they offer no accountability for their actions.

SNS and TPA providers tend to play a game of ping-pong, volleying user data to each other and trying to absolve themselves of responsibility. 3rd party providers state that they gather information from their users' SNS accounts. Neither stakeholder specifies the extent of that information. The SNS providers state that users are agreeing to the 3rd party's policies when they add an application while the 3rd parties state that user information on SNS is governed by the SNS' policies. Users can easily get lost in a maze of privacy policies.

Further, in none of the SNS do users have access to their traffic data, this also holds for Zynga. Playfish offers users access to all the information held about them, although it is not clear if that includes traffic data. None of the policies offer users a means of finding out when their personal information has been subpoenaed or forwarded to other parties. How relational information behaves often remains a mystery, since it does not easily fit into the personal information cast. Under these conditions, access rights prove to be a weakness of SNS and TPA. This is a surprising result given that SNS are about users feeding and accessing profile information.

Based on our previous studies, we know that when it comes to privacy concerns users do not use the same vocabulary or make the same distinctions as the data protection principles. Facebook was the only provider that tried to address user concerns with their language, but they also managed to maximize and legitimize their interests in their privacy policy. It is important to study if and how user concerns can be addressed by data protection, and which issues remain untouched by privacy legislation and recommendations.

Paradoxically, in the case of the SNS policies that we studied, data protection leads towards reducing privacy, rather than protecting it. This paradox is mainly attributed to these principles reflecting a procedural approach to maximizing individual control over data thus placing the burden of protection to the individual rather than society and its institutions (Cate, 2006). SNS and TPA providers have successfully taken advantage of this weakness.

At the same time, it seems that social networks inherent structure of sharing has provided alternative approaches to privacy concerns: the ability to collectively respond to privacy breaches as an SNS community. This was best observed through user reactions to Beacon and Facebook's Terms of Use (Rizk et al. 2009). This could be a cue that instead of focusing on individualized and proceduralized solutions to privacy concerns, we should think about collective forms which increase users awareness of existing information practices and allow them to determine or negotiate how their information is collected, retained, distributed or deleted. This may lead to other concerns like ownership of relational information, indeterminate visibility, and community accountability that the privacy debate and policies have so far rarely addressed.

Acknowledgements

This work was supported in part by the Concerted Research Action (GOA) Ambiorics 2005/11 of the Flemish Government, by the IAP Programme P6/26 BCRYPT of the Belgian State (Belgian Science Policy), and by the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n 216287 (TAS3 -Trusted Architecture for Securely Shared Services).

References

Breaux, T., Antón A.(2005). Deriving Semantic Models from Privacy Policies. In Proceedings of the 6th IEEE International Workshop on Policies for Distributed Systems and Networks, 67-76.

boyd, d. (2007). **"Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life."** *MacArthur Foundation Series on Digital Learning - Youth, Identity, and Digital Media Volume* (ed. David Buckingham). Cambridge, MA: MIT Press, pp. 119-142.

Cate, F. (2006). The Failure of Fair Information Practice Principles. In Consumer Protection in the Age of the Information Economy.

European Parliament (2001). Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000. Official Journal of the European Communities. http://www.europarl.europa.eu/tools/disclaimer/documents/l_00820010112en00010022.pdf

Facebook (2009). Privacy Policy. Effective as of 26 November 2008. http://www.facebook.com/policy.php. Last checked on 31 August 2009.

Federal Trade Commission (2007). Fair Information Practice Principles. http://www.ftc.gov/reports/privacy3/fairinfo.shtm

Gamasutra (2009). http://www.gamasutra.com/php-bin/news_index.php?story=25132

Gurses, S., Rizk, R., and Gunther, O. (2008). "Privacy Design in Online Social Networks: Learning from Privacy Breaches and Community Feedback". ICIS 2008 Proceedings. Paper 90. http://aisel.aisnet.org/icis2008/90

Gurses, S. and Rizk, R. (2010). Privacy policies of Social Networking Sites and Third Party Application providers and their implications, a template analysis. Technical Report.

Kelley, P. (2009). Designing a privacy label: assisting consumer understanding of online privacy practices. In Proceedings of the International Conference Extended Abstracts on Human Factors in Computing Systems, 3347-3352.

King, N. (2004). Using Templates in the Thematic Analysis of Text. In Cassell, C. & G. Symon (Eds.), Essential Guide to Qualitative Methods in Organizational Research, Sage: London.

Miller, F. and Alvarado, K. (2005). Incorporating Documents Into Qualitative Nursing Research. In Journal of Nursing Scholarship, 37 (4), 348-353.

McDonald A., Reeder R., Kelley P., Cranor L. (2009). A Comparative Study of Online Privacy Policies and Formats. In Proceedings of Privacy Enhancing Technologies (PETS), 9th International Symposium. 37-55

Myspace (2008). Privacy Policy. Effective as of 28 February 2008. http://www.myspace.com/index.cfm?fuseaction=misc.privacy Last checkd on 31 August 2009.

Narayanan, A. and V. Shmatikov (2009). De-anonymizing social networks. In Proceedings of the 30th IEEE Symposium on Security and Privacy, 173-187.

Office of Data Protection Commissioner (1998). Data Protection Act. http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

Office of Management and Budget (2007). Memorandum for the Heads of Executive Departments and Agencies, Clay Johnson III.

Orkut (2009). Privacy Policy. Effective as of 25 June 2009. http://www.orkut.com/html/en-US/privacy.orkut.html?rev=6 Last checked on 31 August 2009.

Playfish.com (2009). Privacy Policy. http://playfish.com/?page=privacy retrieved on August 13th 2009.

Pouloudi, A. (1999). Aspects of the stakeholder concept and their implications for information systems development. In Proceedings of the 32nd Hawaii Conference on System Sciences.

Reay, I, Dick S, and Miller J.,(2009). A large-scale empirical study of P3P policies: Stated actions vs. legal obligations. In ACM Transactions on the Web 3 (6), 1-34.

Rizk, R, Marx, D, Schrepfer, M, Zimmerman, J, and Guenther, O. (2009). "Media Coverage of Online Social Network Privacy Issues in Germany: A Thematic Analysis" AMCIS 2009 Proceedings. Paper 342. http://aisel.aisnet.org/amcis2009/342

Stalder, F. (2002). The Voiding of Privacy. Sociological Research Online. 7(2).

TAMS Analyzer (2008) http://tamsys.sourceforge.net/

Techcrunch a, (2009). http://www.techcrunch.com/2009/07/09/powercom-countersues-facebook-over-data-portability

Template Analysis http://www.hud.ac.uk/hhs/research/template_analysis/technique/technique.htm (retrieved September 4th, 2009).

Zheleva, E. and L. Getoor. (2009). To Join or Not to Join: the illusion of privacy in social networks with mixed public and private user profiles. WWW'09.

Zynga.com (2009). Privacy Policy. As of January 7, 2009. http://www.zynga.com/privacyPolicy/