Developing Reliable Measures of Privacy Management Within Social Networking Sites

Catherine Dwyer
Pace University
cdwyer@pace.edu

Starr Roxanne Hiltz
New Jersey Institute of Technology
hiltz@njit.edu

Marshall Scott Poole
University of Illinois, Urbana-Champaign
mspoole@uiuc.edu

Julia Gußner
Paris-Lodron-University of Salzburg
Julia.gussner@sbg.ac.at

Felicitas Hennig
Paris-Lodron-University of Salzburg
fee.hennig@yahoo.de

Sebastian Osswald
Paris-Lodron-University of Salzburg
Sebastian.osswald@gmail.com

Sandra Schließlberger
Paris-Lodron-University of Salzburg
Sandra.Schliesslberger@gmx.de

Birgit Warth
Paris-Lodron-University of Salzburg
birgit.warth@gmx.net

Abstract

*Social networking sites and other examples of online social spaces have greatly expanded their members' opportunities for self expression and social interaction, while creating significant challenges for online privacy management. Within offline social spaces, privacy management is an active part of everyday life, influencing where, when and to whom we decide to reveal private information. Just as technology mediation changes the nature of communication, so will technology mediation of social interaction change the nature of privacy management. This paper describes work done to establish reliable measures of online privacy management based on Adaptive Structuration Theory (AST). AST provides a framework for modeling the use of technology in a social setting, includes a way to measure **appropriation**, the process by which users adapt and adopt technology. These measures have been used to examine appropriation patterns within two US based social networking sites (Facebook and MySpace), and StudiVZ, a site based in Germany. The measures demonstrated an acceptable level of reliability, and the results exposed differences in the privacy management strategies employed by the members of these sites. The result of this research is the establishment of theory based measures that can be used to capture the structure of online privacy management.*

1. The Importance of Reliable Measures for Social Computing

The establishment of valid, reliable measures for social networking sites (SNS) has the following benefits. It allows the comparison of outcomes and results from different examples of SNS. The ability to compare results across sites in a reliable manner is a requirement for the development of standards for the effectiveness or usefulness of differing implementations. Standardized measures are also a necessary component of longitudinal studies. It is very difficult to look at changes in a site over time without dependable, reliable measures.

Besides providing a benefit for future study of SNS, reliable, valid measures are urgently needed due to the unprecedented scale of participation in these sites. SNS have memberships that number in the tens of millions, drawing from countries around the globe [7].

It can be argued SNS are the largest examples of information systems that have ever existed. Some information systems theories, such as the Technology Acceptance Model, have been applied to social computing applications [40], but these efforts show that considerable modification needs to be carried out to traditional information systems theory to yield reliable results. So while information systems theory holds much promise in the analysis of social computing, the differences between systems developed for a commercial enterprise versus one for the general population require a reconsideration and re-validation of both theory and related measures. Given the complexity of social computing, most measures must be focused on particular tools and affordances of the SNS rather than the SNS as a whole. In this study we focus on privacy management tools and the nature of their use.

2. AST-Based Analysis of Online Privacy Management

Privacy management is an essential social skill found in cultures around the world [30]. It is a fundamental component of what the sociologist Erving Goffman called impression management, or the presentation of versions of the self to different audiences [20]. As a result of Goffman's seminal works, we know the strategies people employ for offline privacy management, as well as the critical role it plays in maintaining different levels of social connections [39]. Privacy management consists of

social, relational, cognitive and perceptual components that a person constantly monitors in real time. These components are input into an individual privacy calculus that controls the development of boundaries and the disclosure of confidences [30].

As more and more interaction moves into online social spaces, there has been a rising public debate about the inadequacies of online privacy management tools [23, 24, 27, 32, 33, 36]. While there has been discussion in academic research about the complexities of online privacy management [1, 4, 6, 21], there has been little research on how to develop reliable, repeatable measures of use. The development of these measures would be of great assistance in answering these questions: To what extent are participants in online social spaces aware of the privacy management tools available? To what extent do members of social technologies actually use these privacy management tools?

Adaptive Structuration Theory (AST) provides a framework for examining the social and technical components of use [10-12]. While developed in the 1990s to explain patterns of use in group support systems (GSS), AST has recently been applied to analyses of social software [13, 14, 18, 28]. While this paper specifically focuses on measures of appropriation, a more detailed description of AST and its application to the study of SNS can be found in [14, 18].

AST provides the appropriation construct, which is particularly relevant to measuring online privacy management. Appropriation is defined as the ongoing processes and methods by which people adopt and adapt to technology [11]. Building on structuration theory [19], AST identifies social structures as the rules and resources provided by technologies and institutions, that both enable and constrain human activity.

By examining appropriations, AST focuses on the exact nature of the relationship between a given technical resource or function, and how it is used, or brought into action. AST argues that appropriations cannot be mandated by technology designs. Instead, human agents independently choose how technology structures are used, resulting in varied adoption practices [11].

AST, by modeling appropriation, can capture in greater detail the means by which users adapt and adopt technology to support a task or objective. Since AST proposes a non-deterministic view of technology use that provides room for social, cognitive, and technical factors [28], it serves as a good foundation for building measures of online privacy management.

Appropriation refers to the dynamic process whereby people integrate technology into processes and tasks. Within AST, the interaction between an information system and a user is seen as a dynamic and complex process with social, cognitive, and technical components. None of these influences are purely deterministic, but all can contribute to how members engage with technology. In addition, appropriation implies that technology leads to changes in behavior, and new behavior or emergent practices lead to re-conceptualization and changes in technology [12].

For example, AST can be applied to describe the changes in the appropriation of cell phone technology, thus illustrating the transformative potential of appropriation. When first introduced, cell phones were used almost exclusively for voice transmissions. As they became more popular, users developed strategies to curb costs. One strategy was to use text messaging or SMS, available in most places for much lower cost. This changed the dominant pattern of cell phone use, so that people turned with increasing frequency to text messaging rather than voice. This led to the adoption of text messages and SMS to communicate for broadcast purposes, such as emergency notifications [29]. So here we see behavior adapting to technology, redefining the affordances of that technology, leading to the re-conceptualization and redesign of the technology. From a socio-technical systems perspective, we see technology influencing social use, leading to new patterns of use that feeds back into a functional re-design and an expanded understanding of the affordances of the technology [11].

3. Applying the Appropriation Construct to Social Computing

Online privacy management presents many levels of complexity to members of SNS. Privacy itself is a complex social concept that has undergone extensive changes over the centuries, and is interpreted differently based on cultural and personal perspectives [25]. Research has found that privacy is a multi-dimensional construct [38].

In addition, privacy management online is even more complex because the disclosure implications of pieces of information must be considered across both time and space [6]. Managing the privacy of online data is done in current SNS by controlling information access by category, not by each piece of information added to a profile. You can set up restrictions for all photos, all videos, all blog entries,

and so forth. This lets you control access to all video entries, but not just one out of your selection. Since limiting everything in a category is usually overkill, members may not bother. Or you may forget that you restricted access to photos, but did not do anything about videos. You may end up posting an embarrassing video thinking it is visible only to your friends, and then find out your school's administrators have seen it.

Research on knowledge contribution within online communities has addressed a construct referred to as perceived identity verification. This is the degree to which a person feels that other members of an online community can identify them. A study found there is a positive correlation between willingness to share knowledge and perceived identity verification. Perceived identity verification is also correlated with overall member satisfaction with an online community [26]. These results should not be surprising, because higher engagement in a community offline is also correlated with greater contributions and greater overall satisfaction [31].

A comparison of the motivation of members who create an online profile versus the nature of privacy management in SNS shows them to be in direct conflict. SNS work hard to create tools that support the ability to express oneself through a profile. This results in more active engagement with the site and its members. However, privacy management tools are designed to share less information with a smaller audience.

The goal of online self presentation within SNS is to create a rich, authentic profile that keeps friends up to date on your activities and presents an interesting personality to potential new friends [5]. Privacy management consists of a collection of settings that either restrict what information is available or restrict the scope of the audience. It does not seem possible to present a rich, authentic digital profile while carrying out an effective appropriation of privacy management. This is because of the following issues:

- Privacy management works by limiting information, especially that which is potentially sensitive. This results in a profile that looks more like a resume than something that would spark the interest of others [6].
- Young consumers value honesty and authenticity, and can easily spot insincerity. They have become jaded by intense marketing and spin doctors, and value something that is "real," [3].
- Privacy management works by limiting the potential audience for your profile. This not only protects privacy, but it also cuts off the

opportunity to develop new relationships, or rekindle distant ones. This is the equivalent of hiding your lamp under a basket[1].

By this analysis, there is a conflict between the goals of creating an interesting profile and practicing faithful privacy management. Insight into the nature of this conflict, as well as how members resolve it, can be addressed by approaching this as an appropriation issue. By studying the process by which members adapt and adopt privacy management, we can gain insight into what methods are employed to resolve this conflict. In this case, unexpected patterns of appropriation may not be symptoms of misuse; instead they may be symptoms of members' grappling with difficulties in protecting their information with tools that have the potential to restrict their ability to present an authentic profile.

There exists a fundamental mismatch between online privacy needs and privacy management functionality that can hopefully be explained more clearly by application of the appropriation perspective. The next section describes scales developed by applying AST to measure appropriation of privacy management in SNS.

4. Scales Derived From the AST Appropriation Construct

AST defines appropriation as the process by which people apply and adapt technology to their tasks. Using the terminology of AST [11, 12], users faithfully appropriate the technology when they use it in compliance with what AST's authors DeSanctis and Poole call the **spirit** of the technology. The spirit is the general values for the technology. If the technology is used in a manner consistent with its spirit, this is referred to as **faithful appropriation**. If the use is not consistent with the spirit, this is referred to as an **unfaithful appropriation** [11]. According to AST, less faithful appropriations are expected to lead to unacceptable or sub-par outcomes [9].

DeSanctis and Poole then further expanded the appropriation construct by examining in detail what they refer to as "**appropriation moves**." These moves describe ways that individuals can appropriate technology. Appropriation moves are organized into four categories, nine types, and 31 sub-types [11]. The four categories are 1) direct use, 2) relating one technical feature to another, 3) constraining a technical feature, and 4) expressing judgment about a

---

[1] "No one lights a lamp and hides it in a jar or puts it under a bed," Luke 8:16

technical feature. Each category is then further divided into types and sub-types. For example, the direct use category is divided into the direct appropriation type, which is then divided into explicit use of the technical feature, implicit use, or a bid (suggestion) for use. This structure of category, type, and sub-type create a taxonomy that has the potential to capture how people directly use or appropriate technology, how they "make sense" out of the technology, how they relate one technology to another example, or how they might misappropriate the technology. For the complete listing of potential appropriation moves see [11].

In order to develop measures for appropriation of online privacy management functions, each category, type, and sub-type was examined for its application to the SNS privacy management context, as well as whether it could be converted into a scale measure format. Some sub-types, such as the explicit use appropriation move, were readily adaptable, while others, such as the composition appropriation move were not. All measures were designed as seven point semantic differential scales, anchored from Strongly Disagree to Strongly Agree. The scales that were developed and tested are now described.

The **Use appropriation move** captures the extent to which members report actual use of privacy settings. It is derived from the Direct Use category, Direct Appropriation type, Explicit use sub-type. Members show evidence of a faithful appropriation by actively and explicitly making use of privacy settings. An example of one of its measures is "I have modified the privacy settings for my profile on [name of SNS]."

The **Familiar appropriation move** measures to what extent members report familiarity, or knowledge of privacy management tools and settings. It is derived from the Direct Use category, Direct Appropriation type, Implicit use sub-type. Familiarity is an indication of implicit appropriation because it involves knowledge, but not necessarily actual use of a privacy management feature. For example, a member of a SNS may know how to restrict access to their profile, but not apply that setting. Members show evidence of a faithful appropriation by demonstrating knowledge of how to use privacy settings. An example of a Familiarity measure is: "I am comfortable with my ability to adjust my privacy settings."

The **Restricted Scope appropriation move** measures to what extent members restrict their contact within the site to those they already know, rather than exploring new relationships and engaging with new people. It is derived from the Relating one technical feature to another category, Substitution

type, Part sub-type. This appropriation move involves using part of the privacy management tools, rather than completely depending on them. In other words, while members do use the site, they apply their own privacy management strategy by restricting who they communicate with. According to AST, this move is an example of faithful appropriation because taking steps to protect your privacy is consistent with the spirit of the privacy settings. An example from this scale is: "I don't use [name of SNS] to make contact with people whom I've never heard of."

The **Rejection appropriation move** measures the extent to which members explicitly state they do not use or bother with privacy settings. It is derived from the Expressing Judgment category, Negation type, Reject sub-type. This appropriation move describes the rejection or negation of privacy management tools. This move measures to what extent members express a negative opinion of privacy management tools, or directly reject appropriation of privacy settings. An example of one of its questions is: "I don't know what my privacy settings are on [name of SNS]."

The **Faithfulness Scale** includes questions adapted from the Scale to Measure Faithfulness of Appropriation [8]. The original scale was developed for electronic meeting systems. It has been rewritten to refer to privacy management within SNS. It includes these questions:

1. I probably use the privacy settings for [name of SNS] improperly.
2. I failed to use the privacy settings of [name of SNS] as it should be used.
3. I did not use the privacy settings in [name of SNS] in the most appropriate fashion.
4. The founders of [name of SNS] would disagree with how I use the privacy settings.
5. The original founders of [name of SNS] would view my use of the privacy settings as inappropriate.

5. Empirical Tests of Privacy Management Scales

In order to test the measures described above, several studies were conducted that collected data from three different SNS. The measures were first tested using subjects from two US based sites, Facebook and MySpace. A detailed report on an earlier version of this study can be found in [17]. The measures were subsequently translated and replicated for StudiVZ, a site popular in Austria and Germany.

The development of these scales is derived from four years of research beginning in 2006, on a subject

that has only recently received a significant amount of academic attention. Few if any measures for items regarding the use of these sites were available, and so these had to be developed and validated. More detailed descriptions of prior studies can be found in [15-18].

The scales were tested in three different studies that are summarized below. The first test was a pilot study conducted to capture preliminary data on the measures and gauge their validity and reliability. The second study was conducted to further establish these scales by testing them in randomly selected populations. The third study was conducted to test the reliability and validity of the scales in another language and cultural setting.

5.1 Pilot Test of Appropriation Measures

The first version of the appropriation measures were tested in a pilot study administered using an online survey in August 2007, with subjects from Facebook and MySpace. One version of the survey was created for Facebook, and another was customized for MySpace. Subjects were recruited by posting messages in public forums in Facebook and MySpace offering $5 for completion of the survey.

The survey was available for eight days. The goal was to obtain about 50 subjects in order to carry out reliability tests on the appropriation measures. Ideally, this translates into 25 Facebook subjects and 25 MySpace subjects. During the administration, it turned out to be much harder to recruit MySpace subjects than Facebook subjects. The responses included 35 subjects from Facebook and 16 subjects from MySpace, for a total of 51.

Reliability analysis (Cronbach's alpha) was administered to the appropriation measures. Feedback from the reliability analysis was used to eliminate 16 questions from the survey.

Factor analysis was also administered. A rotated solution found that the measures loaded independently on each appropriation measure.

5.2 US Based Facebook/MySpace Study

The next test of the appropriation measures was conducted from November 2007 through January 2008. Using the measures revised based on results from the pilot study, new versions were created for MySpace and Facebook.

The target population for the US based study consisted of members of a Northeastern U.S. technological university (henceforth, NEIT) community who participate in Facebook or MySpace, including students, faculty, and alumni. A random sample of NEIT Facebook and MySpace members were invited to complete the survey. The survey was

fully completed by 115 MySpace subjects from a sample of 927 members, resulting in a response rate of 11.9%. The survey was completed by 107 Facebook subjects from a sample of 778 members, for a response rate of 14.2%.

The responses from the MySpace subjects and the Facebook subjects were combined for a total of 222 subjects. These results were used to evaluate the reliability and validity of the appropriation measures. Reliability is the extent to which a measure yields the same result even if administered at different times in different circumstances. It is an indication of a measure's stability or consistency [34].

The validity of a measure is a determination of whether the measure accurately captures what is claimed, and that it is logical to draw conclusions from the results of those measures [34]. Problems with validity usually take the form of biases or specific events that call into question whether results are meaningful. By using a random sample for this study, the risk of selection bias from using a convenience sample is reduced.

The data collected for this study were examined using a process for multi-variate data analysis as recommended in [22]. These authors recommend the following steps be taken for a multivariate data analysis:

- Examine the data set for missing data and assess its potential impact
- Examine the data for outliers and assess their impact
- Test for reliability (this was done using Cronbach's alpha and factor analysis)

A factor analysis was conducted to confirm that the measures load as expected on the appropriation construct. When conducting a factor analysis, important issues to consider are the number of factors extracted, and the percentage of variance explained. These are usually apparent in an initial, unrotated solution. Factor loadings of $\pm.30$ to $\pm.90$ are considered for initial analysis. Factor loadings should be .50 or above for practical significance, and the goal is factor loadings of $\pm.70$.

Following this process as described in [22], the measures were examined using Principal Component Analysis. In this step five factors were identified, explaining 66.98% of the variance.

The next step was to further clarify the factors by creating a rotated solution. Following the factor rotation method described in [22], several rotation methods were tested. The rotation method found to return the best results is the Equamax method. The Equamax attempts to both simplify the rows and the columns of the solution matrix.

When conducting factor rotation, the goal is to simplify the loadings so that each measure loads only on one factor. When a measure does load on more than one factor, it is said to be cross loading and is a candidate for deletion. When looking at factor loadings, another goal is to identify factor loadings that are statistically significant. With a sample size of about 200 subjects (222), the level for significant factor loadings for this analysis is .40 [22].

Table 1: Factor loadings for Facebook MySpace study (rotated solution).

Meas.	1	2	3	4	5
Use 3	**.866**	-.130	.174	.040	-.087
Use 2	**.827**	-.215	.238	.039	-.043
Rej3	**-.805**	.214	-.093	-.042	-.024
Use 4	**.708**	-.364	.198	.052	.090
Fth2	-.237	**.799**	-.210	-.001	.167
Fth1	-.155	**.737**	-.371	.128	.107
Fam2	.189	-.083	**.798**	.097	-.030
Fam4	.078	-.283	**.722**	-.103	-.094
Fam1	.153	-.177	**.678**	-.135	-.138
Sco4	-.017	.002	.048	**.865**	.065
Sco3	.036	.127	-.026	**.837**	-.008
Sco2	.075	-.060	-.129	**.776**	-.096
Fth5	.004	.087	-.041	.049	**.887**
Fth4	.006	.093	-.113	-.085	**.868**

The five factors and their loadings are presented in Table 1. In the rotated solution shown in Table 1, the Faithfulness measure divided into two factors. The third Faithfulness measure was dropped because it did not load high enough with the other measures. The retained questions that correspond to each of the final factors are shown in Table 3 below.

The results of the rotated factor analysis led to a reconstruction of some of the constructs under measurement. The Rejection appropriation move was dropped, because its measures loaded strongly on other constructs. For the Use appropriation move, one initial measure was dropped (Use1) and replaced with Rejection3. The Familiarity move and the Restricted Scope move now have three measures each.

5.3 StudiVZ Study in Austria
The Austrian study was conducted using measures that remained from the factor analysis in the Facebook/MySpace study, and applying them to a very different setting. This study was conducted in another cultural area (Austria and Germany). It was conducted during November and December of 2008 using subjects from StudiVZ. For the StudiVZ survey, the questions were translated into German and a few additional questions were added to that version to reflect some of its unique privacy management features, as described below.

Table 2: Factor loadings from all three sites.

Meas.	1	2	3	4	5
Fam3	**.885**	.195	.009	-.047	.127
Rej1	**-.833**	-.186	.020	.095	-.033
Fam4	**.809**	.071	.037	-.073	.285
Use3	.215	**.848**	.076	.079	.033
Use1	.053	**.844**	.080	.113	.152
Rej3	-.181	**-.832**	.010	.002	-.049
Sco3	-.002	.039	**.868**	.044	.026
Sco4	-.068	.095	**.857**	.058	.028
Sco2	.081	-.003	**.720**	-.027	-.138
Fth5	-.055	.065	.034	**.899**	-.064
Fth4	-.084	.059	.014	**.896**	-.052
Fam2	.133	.179	-.003	.067	**.825**
Fam1	.127	-.026	-.073	-.196	**.818**

StudiVZ, which does not have an English interface, is very popular among European university students. Its users are primarily from Austria and Germany, but there is also a Spanish, Italian, and Polish language version. Although Facebook has filed suit against StudiVZ for appropriating its design without permission [2], there are some important differences between the systems in regard to privacy management, especially familiarity with the options.

For example, StudiVZ sets the privacy management defaults at the minimum privacy protection levels, meaning that anyone, including advertisers, can see one's profile or be notified of things like additions to your profile. The default in Facebook, to give one contrast, is that only friends or group members can see such information. (However, many groups are very large; for instance, the "group" of Harvard users numbers about 55,000). The default for MySpace members is to make their profile content visible to anyone on the Internet.

Table 3: Final measures and their factor loadings.

Measure	Factor 1 - Familiarity
Fam3	I am familiar with my privacy settings on [name of SNS]
Reject1	I don't know what my privacy settings are on [name of SNS]
Fam4	When I need to modify my privacy settings for [name of SNS], I am able to do it
	Factor 2 - Actual Use
Use3	I have adapted the privacy settings to control who can view my profile on [name of SNS]
Use1	In order to control who can contact me using [name of SNS] I have adjusted my privacy settings.
Reject3	I don't use the privacy settings to control who can access my profile
	Factor 3 - Restricted Scope
Scope3	I never accept invitations of people I never met before.
Scope4	When I use [name of SNS] I ignore people whom I never heard of and who try to contact me
Scope2	I don't use [name of SNS] to make contact with people whom I've never heard of.
	Factor 4 – Faithfulness
Faith5	The original founders of [name of SNS] would view my use of the privacy settings as inappropriate
Faith4	The founders of [name of SNS] would disagree with how I use the privacy settings
	Factor 5 – Confidence
Fam2	I am confident that I know how to control who is able to see my profile on [name of SNS]
Fam1	I am comfortable with my ability to adjust my privacy settings
All questions were measured as semantic differential measures, from 1 (Strongly Disagree) to 7 (Strongly Agree)	

One important difference between the sites, in terms of member familiarity with the tools, is that StudiVZ leads every new user who is registering through the privacy settings. It is an explicit part of setting up a new membership. This is not part of the member activation process for either Facebook or MySpace.

In addition, StudiVZ has more privacy settings that the two U.S. systems, including choices on how or whether advertisers can mine data about them to send them "appropriate" advertisements and special offers. StudiVZ has been using its users' data for advertisement since 2007. The collection of user data for use in targeted advertising was the subject of a public debate, and received a lot of coverage in the Austrian press. Therefore almost everyone knows about that and has become sensitized. Another

difference is that within StudiVZ warning messages about the implications of various privacy settings are visible within the users' profile settings. Additional questions were added to the StudiVZ version of the study to cover familiarity with and use of several of StudiVZ's unique privacy choices, including the choice on whether members allow their profile to be released for targeted marketing ads.

An important difference in the StudiVZ study design was that a type of "snowball" sample was used. Five students in a course taught by the second author at the University of Salzburg worked on both the translation and the dissemination. They sent an invitation to students and administrators they knew within universities in primarily Austria, but also a few in Germany. This invitation asked the contact not only to answer the survey, but also to pass it on to other student users of StudiVZ whom they knew or could reach by mailing lists. It promised a 50 euro gift certificate (about $65 at the exchange rate at the time) for one randomly drawn respondent for every 100 respondents or portion thereof. It was planned to shut off the survey just before 300 subjects completed. The first few days, less than 100 responses were received. Then suddenly the snowball picked up momentum, and we had 388 respondents.

The results from the StudiVZ study were added to data previously collected and used to conduct a factor analysis on the measures. The results of this combined analysis is presented in Table 2. From the three site data set, there were 14 measures remaining, divided between five factors. Each of these factors was shown to have a Cronbach's alpha value of .7 or above. The final factors and their measures are listed in Table 3.

6. Discussion

After developing measures derived from the analysis of appropriation moves in AST, and subjecting them to several efforts to establish validity and reliability, we are left with five factors made up of 14 measures (see Table 3). These measures can now be used to describe differences between SNS. While these findings are the result of three exploratory studies, the results and consistent factor loadings add more credibility to comparisons between the sites, and support the use of these measures to the study of additional examples of SNS.

In comparing these five remaining factors to the taxonomy of appropriation moves from AST, there are four factors that have persisted from the first analysis on online privacy management, as listed in Table 3. They are Factor 1 – Familiarity, Factor 2 –

Actual Use, Factor 3 – Restricted Scope, and Factor 4 – Faithfulness.

There is one new factor that was not initially identified in the beginning analysis. This is Factor 5, which we are calling Confidence. The two measures that make up this factor were originally created for the Familiarity scale, but have loaded on another factor. Comparing this factor with the AST appropriation moves taxonomy, this factor is related to the Expressing Judgment category, Affirmation type, Agreement sub-type.

The fact that four original appropriation moves map to factors extracted from empirical data, plus a fifth factor that can be interpreted using AST, provides evidence that AST can serve as a theoretical foundation for the study of social computing sites. This is important to note, because there is a clear need to ground the study of social computing in a theoretical foundation [37].

In addition, the taxonomy of appropriation moves within AST is flexible enough to be applied to other examples of social computing. Since the use of social computing platforms is expanding so much, this helps establish AST as an important tool for explaining the complexity of interaction within online social spaces.

After establishing 14 reliable measures, the results were compared across the three SNS. The results of that comparison are shown in Table 4. All measures indicated statistically significant results with the exception of Faith5 and Fam1.

These results demonstrate differences between the sites that are of interest. The measure showing the widest range of difference is Use 3, with Facebook the highest, followed by StudiVZ then MySpace. In contrast, Fam 4 has the highest result for StudiVZ, and the lowest for Facebook. This result at first is confusing, suggesting Facebook members use these tools frequently but don't feel familiar with them. However, this can be explained by commentary about the privacy management tools within Facebook, which have been criticized as being complex and confusing [14, 35].

Another interesting result from these findings is the differences between the sites in the Restricted Scope measures. StudiVZ members have the highest result for Scope 2 and the lowest result for Scope 4. So StudiVZ members are the least likely to use the site to contact people they have never heard of (Scope 2), followed by Facebook and then MySpace. In contrast, Facebook members are the most likely to ignore contact from strangers (Scope 4), followed by MySpace and then StudiVZ. This suggests that the nature of the sites can influence the initiating of contact versus the acceptance of new contacts in different ways.

Table 4: Comparison of results: Facebook, MySpace and StudiVZ.

Meas.	FB	MY	SVZ	F	Sig.
Fam3	4.71	5.23	5.92	2.982	.051
Reject1	3.00	2.63	2.02	3.292	.038
Fam4	5.49	5.83	6.10	19.299	.000
Use3	4.26	3.76	4.16	28.765	.000
Use1	4.11	3.70	3.08	23.128	.000
Reject3	3.13	4.03	3.85	7.251	.001
Scope3	4.57	4.72	4.39	14.328	.000
Scope4	4.63	4.42	3.90	5.452	.005
Scope2	5.42	4.71	5.53	7.207	.001
Faith5	2.94	2.43	2.52	1.103	.332
Faith4	2.78	2.51	2.35	6.182	.002
Fam2	4.79	5.17	3.74	9.311	.000
Fam1	5.19	5.82	4.75	1.391	.250

6.1 Relationships between Familiarity and Use Measures

Although relatively few StudiVZ users have adjusted privacy settings to control who can contact them (Use 1), its users have a much higher result for Use 3, which measures whether they have adjusted their privacy settings in general. This seems to be related to two other items on which StudiVZ users are significantly different from the two U.S. based systems. StudiVZ users are the most familiar with their privacy settings (Fam 3). StudiVZ users also generally feel confidence in their ability to modify their privacy settings (Fam 4). This higher degree of confidence in their awareness of their privacy settings is confirmed by differences in Reject 1: relatively few StudiVZ users don't know the settings for their profiles (see Table 4).

6.2 Possible Cultural Differences

Cultural differences between U.S. and Austria/Germany are perceived by the Austrian authors of this paper: U.S. users express less anxiety about their own management of privacy settings compared to the European subjects.

Consider the results for Factor 1 (measures Fam 3, Fam 4, and Reject 1), versus Factor 5 (measures Fam 2 and Fam 1). Members of StudiVZ express a higher level of familiarity (Fam 3) and facility (Fam 4) with their privacy settings, but express less comfort (Fam 1) with their abilities. The combination

of higher use but lower comfort level for the StudiVZ subjects is an indirect measure of levels of anxiety about privacy management.

7. Conclusions and Future Research

This paper describes the development of theory based measures of appropriation of privacy management within SNS. The results of a series of empirical studies provide support for the establishment of these measures as reliable mechanisms for examining patterns of use within social mediating technologies.

The limitations of this study are that the target population of the U.S. sample may not be representative of either site as a whole, since it came from only one university. On the other hand, the Austrian and German participants in the StudiVZ survey came from many universities, but were a self-selected sample rather than a random sample from a list of users (which is not obtainable). In addition, these are new measures that have not been extensively tested in other settings. While these results are promising, they must be considered to be preliminary.

In addition, we found many differences between the U.S. users of Facebook and MySpace, and the Austrian and German users of StudiVZ. We have no way of disentangling cultural differences from system privacy features design in explaining these differences.

More analysis is planned to further establish the validity and reliability of these measures. Specifically this will involve conducting confirmatory factor analysis using structural equation modeling.

In addition, future research is planned to apply these scales to other SNS in other countries, such as Orkut in Brazil and India, CyWorld in South Korea, or the heavily used Chinese social networking systems. More work is planned to conduct qualitative studies of individual privacy management strategies, and then use AST to adapt new measures for these strategies. Given the promising results of this study, there is support for the further application of AST to modeling the complex interactions that take place within SNS.

8. References

[1] Acquisti, A. and Gross, R., "Imagined Communities: Awareness, Information Sharing and Privacy on The Facebook." in *6th Workshop on Privacy Enhancing Technologies*, (Cambridge, UK, 2006).

[2] Allison, K. "Facebook Sues 'Knock off' Site." Financial Times, 2008, Accessed on December 13, 2008, http://www.ft.com.

[3] Atal, M. and Wilson, C., "Feeling Trashed on the Web? How to avoid having your brand message hijacked.," in *Business Week*, August 30, 2007.

[4] Barnes, S.B. "A privacy paradox: Social networking in the United States." *First Monday*, *11* (9).

[5] Boyd, D. "Identity Production in a Networked Culture: Why Youth Heart MySpace." American Association for the Advancement of Science, St. Louis, MO. February 19., 2006, Accessed on November 24, 2006, http://www.danah.org/papers/AAAS2006.html.

[6] Boyd, D. "Social Network Sites: Public, Private, or What?" 2007, Accessed on July 25, 2007, http://kt.flexiblelearning.net.au/tkt2007/?page_id =28.

[7] Boyd, D. and Ellison, N.B. "Social network sites: Definition, history, and scholarship." *Journal of Computer-Mediated Communication*, *13* (1).

[8] Chin, W.W., Gopal, A. and Salisbury, W.D. "Advancing the Theory of Adaptive Structuration: The Development of a Scale to Measure Faithfulness of Appropriation." *Information Systems Research*, *8* (4). 342.

[9] Dennis, A., Wixom, B. and Vandenberg, R. "Understanding Fit and Appropriation Effects in Group Support Systems via Meta-Analysis." *MIS Quarterly*, *25* (2). 167-193.

[10] DeSanctis, G. and Gallupe, B. "A Foundation for the Study of Group Decision Support Systems." *Management Science*, *33* (5). 589-609.

[11] DeSanctis, G. and Poole, M.S. "Capturing the Complexity in Advanced Technology Use: Adaptive Structuration Theory." *Organization Science*, *5* (2). 121-147.

[12] DeSanctis, G. and Poole, M.S., "Understanding the differences in collaborative system use through appropriation analysis." in *Twenty-Fourth Annual Hawaii International Conference on System Sciences*, (Kauai, HI, USA, 1991).

[13] Donner, J. "The rules of beeping: Exchanging messages via intentional 'missed calls' on mobile phones." *Journal of Computer-Mediated Communication*, *13* (1).

[14] Dwyer, C. "Appropriation of Privacy Management Within Social Networking Sites." Information Systems Department, Ph.D. Dissertation, New Jersey Institute of Technology, Newark, NJ, 2008.

[15] Dwyer, C., "Digital Relationships in the 'MySpace' Generation: Results From a

Qualitative Study." in *40th Annual Hawaii International Conference on System Sciences (HICSS)*, (Hawaii, 2007).

[16] Dwyer, C., Hiltz, S.R. and Jones, Q., "Discovering Boundaries for Mobile Awareness: An Analysis of Relevant Design Factors." in *Americas Conference on Information Systems*, (Acapulco, Mexico, 2006).

[17] Dwyer, C., Hiltz, S.R. and Passerini, K., "Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace." in *Thirteenth Americas Conference on Information Systems*, (Keystone, Colorado, 2007).

[18] Dwyer, C., Hiltz, S.R. and Widmeyer, G., "Understanding Development and Usage of Social Networking Sites: The Social Software Performance Model." in *41st Annual Hawaii International Conference on System Sciences (HICSS)*, (Hawaii, 2008).

[19] Giddens, A. *The Constitution of Society*. University of California Press, Berkeley, CA, 1984.

[20] Goffman, E. *The Presentation of Self in Everyday Life*. Doubleday and Co., Garden City, NY, 1959.

[21] Gross, R. and Acquisti, A., "Information revelation and privacy in online social networks." in *2005 ACM Workshop on Privacy in the Electronic Society*, (2005), ACM, 71-80.

[22] Hair, J., Black, W., Babin, B., Anderson, R. and Tathman, R. *Multivariate Data Analysis*. Prentice Hall, Upper Saddle River, New Jersey, 2006.

[23] Hass, N., "In Your Facebook.com," in *The New York Times*, January 8, 2006.

[24] Hempel, J., "The MySpace Generation," in *Business Week*, December 12, 2005.

[25] Lessig, L. "The Architecture of Privacy." 1998.

[26] Ma, M. and Agarwal, R. "Through a Glass Darkly: Information Technology Design, Identity Verification, and Knowledge Contribution in Online Communities." *Information Systems Research*, *18* (1). 42-67.

[27] Maag, C., "When the Bullies Turned Faceless," in *The New York Times*, December 16, 2007.

[28] Markus, M.L. and Silver, M.S. "A Foundation for the Study of IT Effects: A New Look at DeSanctis and Poole's Concepts of Structural Features and Spirit." *Journal of the Association for Information Systems*, *9* (10).

[29] Mendonca, D., Jefferson, T. and Harrald, J. "Collaboration Adhocracies and Mix-and-Match Technologies in Emergency Management." *Communications of the ACM*, *50* (3). 45-49.

[30] Petronio, S. *Boundaries of Privacy: Dialectics of Disclosure*. State University of New York Press, Albany, 2002.

[31] Putnam, R.D. *Bowling Alone: The Collapse and Revival of American Community*. Simon and Schuster, New York, 2000.

[32] Read, B., "Think Before You Share: Students' online socializing can have unintended consequences," in *Chronicle of Higher Education*, January 20.

[33] Richel, M., "MySpace.com Moves to Keep Sex Offenders Off of Its Site," in *The New York Times*, December 6, 2006.

[34] Rosenthal, R. and Rosnow, R. *Essentials of Behavioral Research: Methods and Data Analysis*. McGraw Hill, New York, 1991.

[35] Schneier, B. "Facebook and Data Control." 2006, Accessed on May 6, 2007, http://www.schneier.com/blog/archives/2006/09/facebook_and_da.html.

[36] Schrobsdorff, S., "Predators Playground?," in *Newsweek*, January 27, 2006.

[37] Shneiderman, B. "Web Science: A Provocative Invitation to Computer Science." *Communications of the ACM*, *50* (6). 25-27.

[38] Smith, H.J., Milberg, S. and Burke, S. "Information Privacy: Measuring Individuals' Concerns About Organizational Practices." *MIS Quarterly*, *20* (2). 167-196.

[39] Solove, D.J. "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy." *San Diego Law Review*, *44*. 745.

[40] Van der Heijden, H. "User Acceptance of Hedonic Information Systems." *MIS Quarterly*, *28* (4).