CoPE: Enabling Collaborative Privacy Management in Online Social Networks

Anna C. Squicciarini, Heng Xu, and Xiaolong (Luke) Zhang
College of Information Sciences and Technology, Pennsylvania State University, University Park, PA 16802.
E-mail: {asquicciarini, hxu, lzhang}@ist.psu.edu

Online Social Networks (OSNs) facilitate the creation and maintenance of interpersonal online relationships. Unfortunately, the availability of personal data on social networks may unwittingly expose users to numerous privacy risks. As a result, establishing effective methods to control personal data and maintain privacy within these OSNs have become increasingly important. This research extends the current access control mechanisms employed by OSNs to protect private information shared among users of OSNs. The proposed approach presents a system of collaborative content management that relies on an extended notion of a "content stakeholder." A tool, *Collaborative Privacy Management* (*CoPE*), is implemented as an application within a popular social-networking site, facebook.com, to ensure the protection of shared images generated by users. We present a user study of our CoPE tool through a survey-based study ($n = 80$). The results demonstrate that regardless of whether Facebook users are worried about their privacy, they like the idea of collaborative privacy management and believe that a tool such as CoPE would be useful to manage their personal information shared within a social network.

Introduction

The emergence of Web 2.0 has brought with it the concept of Online Social Networks (OSNs), a major technological phenomenon that has united hundreds of millions of participants around the world (Adamic, Buyukkokten, & Adar, 2003; Gross & Acquisti, 2005; Lenhart & Madden, 2007; McCarthy, 2008). Most OSNs permit members to define personal profiles and customize them as they wish to express themselves, socialize, and interact with others. Through OSNs, users may interact with each other for a variety of purposes, including business, entertainment, and knowledge sharing. Because the commercial success of a social-networking site is highly dependent upon the number of users that it attracts, providers often encourage user behaviors that increase membership numbers and interuser connectivity, potentially at the expense of personal privacy. Users, however, are often unaware of the size or nature of the audience that could potentially access their data. The sense of intimacy generated by being among digital friends often leads to disclosures that may not be appropriate in a public forum.

Users often reveal their true identities on social-networking sites, thus exposing their published personal information (e.g., profiles, photographs, and personal preferences) to potential abuses by online crooks, stalkers, bullies, and commonly, even by their own friends (Gross & Acquisti, 2005). Such open availability of personal data potentially exposes users of OSNs to greater privacy risks (Gross & Acquisti, 2005; Rosenblum, 2007). For example, most social-networking services (e.g., facebook.com) allow users to create content that may connect with their friends' identities (e.g., uploading an image about a friend, tagging a friend in an image, or linking to a friend's personal profile). Such collaborative activities raise a new set of privacy challenges because a person's private information can be easily revealed in content created by others. In other words, in the context of OSNs, private information will not only reside in a single user's own domain but also be co-owned and co-managed by other stakeholders (e.g., friends who upload or comment on an image). Thus, the task of privacy management has to involve other stakeholders in a collaborative fashion. In the context of this research, we use the term *collaborative privacy management* to describe the ways in which users and their social networks collaboratively manage their personal information.

There has been relatively little research examining the notion of collaborative privacy management, particularly how that notion relates to the design of technical and operational means to empower collaborative information control among users (Crescenzo & Lipton, 2009). Several studies have examined the interface design to support user awareness of privacy risks (Lipford, Hull, Latulipe, Besmer, & Watson,

Received September 30, 2010; revised November 2, 2010; accepted November 3, 2010

© 2011 ASIS&T • Published online 25 January 2011 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/asi.21473

2009), and algorithms for relationship-based access-control scheme (Gates, 2007) and collective privacy policy composition protocol (Squicciarini, Shehab, & Paci, 2009). Additionally, a number of studies have examined users' overall general privacy attitudes and behaviors related to OSNs (Gross & Acquisti, 2005; Hoadley, Xu, Lee, & Rosson, 2010). However, we are not aware of any studies to date that have examined privacy-related issues specifically to collaborative content management in OSNs, and the particular privacy problems encountered with content posted by other users. Rather, recent studies have demonstrated how the lack of tools on OSNs (and Facebook in particular) to alter the permanency of others' decisions cause serious privacy concerns in social-network users (see Besmer & Lipford, 2009).

In this article, we seek to add to the growing privacy literature by providing a conceptual understanding of collaborative privacy management and suggesting how to extend access control mechanisms through a collaborative approach to empower users' privacy control over their shared personal information. Specifically, we propose a simple, yet effective, mechanism to support joint management of shared content among users who post content in OSNs and users whose private information is revealed in the posted content. Specifically, we develop a system named *Collaborative Privacy Management* (*CoPE*) to support users' collaborative privacy management. To assess the validity of our proposed access-control model, we implement and evaluate a CoPE system within Facebook.

The article is structured as follows. We first review relevant literature, and then present our collaborative privacy-management approach. Next, we describe the CoPE system designed to support image sharing and privacy protection on Facebook. Then, we present a user study through a survey and report our preliminary findings. The article concludes with a discussion of potential future research.

Literature Review

Privacy in OSNs, and more generally in Web 2.0, are emerging as important and crucial research topics (Adamic et al., 2003). OSNs are currently being studied by scholars in many disciplines, including communication, human–computer interaction (HCI), computer science, information science, information systems, and economics. This section summarizes some of the relevant research, in particular from the perspectives of privacy protection in OSNs, and privacy-related information sharing and protection at the group level.

Protection of Privacy in OSNs

The extensive disclosure of personal information by users of OSNs has made privacy concerns particularly salient. Several studies have investigated users' privacy attitudes (Hoadley et al., 2010; Jagatic, Johnson, Jakobsson, & Menczer, 2007) and the possible risks that users face when they fail to adequately protect their information on OSNs (Gross & Acquisti, 2005). Interestingly, some researchers have highlighted the fact that online friendships can result in a higher level of disclosure due to the lack of real-world contact (Ellison, Steinfield, & Lampe, 2007). Further, social benefits of information sharing such as relationship maintenance and self-presentation may limit the desirability of extensive privacy controls (Ellison et al., 2007).

Gollu et al. (2007) presented a social-networking-based access-control scheme for online information sharing by considering identities as key pairs and identifying social relationship based on social attestations. Under this approach, a simple access-control list is employed to manage user access. A more sophisticated mechanism to manage access controls by Carminati, Ferrari, and Perego (2006) is rule-based and follows complex policies that are expressed as constraints on the type, depth, and trust level of existing relationships. This control mechanism is further extended by making access-control decisions completely decentralized and collaborative (Carminati & Ferrari, 2008). Gates (2007) proposed a relationship-based access-control mechanism as one of the new security paradigms to address the emerging privacy requirements of Web 2.0.

Some research projects have gone beyond the aforementioned approaches based on simple connections among users in OSNs and have explored methods based on the quality measures of connections, such as trust among friends. Golbeck and Hendler (2004) proposed a method in the context of Web-based social networks to rate trust between people and then build a prototype e-mail system to filter messages according to trust ratings. Mannan and van Oorschot (2008) suggested an approach for privacy-enabled Web content sharing by leveraging the existing circle of trust in popular instant messaging networks.

In summary, most of these approaches have focused on a single-user-centered solution. Thus, current literature has focused on *individual* actions and has failed to recognize the need for privacy actions by *groups*. Schwartz (1999) questioned whether individuals are able to exercise meaningful control over their information in all situations, given disparities in knowledge in the process of data collection and transfer. The implication is that privacy management is not just a matter for the exercise of individual actions but also an aspect of collaborative actions through multiple stakeholders who co-own and co-manage data. The only work that has touched issues concerning collaboration on privacy protection among stakeholders is that from Squicciarini et al. (2009), which largely focused on an algorithm for collective policy decisions rather than on designs to support user interactions. Their work proposed a game-theoretical characterization of the problem and provided algorithms to address policy-composition protocol. In this research, we focus on a complementary issue: the design and prototyping of an access-control model for collaborative privacy decision making, focusing on offering a means to empower users' collaborative control over their shared content. To provide a richer conceptual description of privacy management, this research develops the understanding of collaborative privacy

DOI: 10.1002/asi

management that is involved with multiple stakeholders in the context of OSNs.

Privacy in Collaborative Information Sharing and Protection

There has been a movement toward the conceptualization of privacy as the individuals' capabilities to *control* the conditions on how their personal information would be accessed and used (Culnan & Bies, 2003). This concept of *privacy as control,* originated in the theories of privacy by Westin (1967), has since entered the mainstream of privacy research in information systems, marketing, sociology, and HCI. In the privacy literature, "control" has been conceptualized as an individual choice to opt in or opt out (Caudill & Murphy, 2000) or has been operationalized as the technical ability to manage the information flow by users themselves (Zweig & Webster, 2002). Such an understanding of control is narrow because it only considers control by individuals and fails to recognize the need for control by social groups. To date, there has been little research evidence about or insight into the phenomenon of collaborative privacy management.

Note that privacy concerns in collaboration situations have been studied in the area of computer-supported collaborative work (CSCW) (for a review, see Iachello & Hong, 2007); however, privacy research in the context of CSCW has focused largely on the balance of privacy and utility; that is, how to share and use personal information that is critical to collaboration without jeopardizing individual privacy. This balance is achieved through privacy-control policies regarding various aspects of personal information of collaborators. Thus, the privacy issues in CSCW differ from those of collaborative privacy management in ONSs in several ways. First, in collaborative privacy management in OSNs, private information can reside in a user's own domain and also may be co-owned and co-managed by multiple stakeholders. Thus, the task of privacy management has to involve other stakeholders in a collaborative fashion. In CSCW, however, the focus is usually on the users themselves who can control their private information. Second, while in the context of OSNs, privacy control concerns users who are widely distributed in a large social network and may have complicated and heterogeneous social relationships whereas privacy in the context of CSCW often concerns a small group of people who work closely and have more homogeneous social relationships through their tasks. These differences make it difficult to apply CSCW theories on privacy control directly into the OSN domain.

In summary, current research on privacy management cannot fully address the needs for collaborative privacy management in OSNs. While it is increasingly important for people to control online content that concern their privacy, existing tools rarely allow a user to manage content that is owned by others, but directly concern his or her privacy. New designs are needed to help users effectively manage private information by themselves as well as with others.

Collaborative Privacy Management

We chose online image sharing as the application domain to study collaborative privacy management. This context has a number of characteristics that make it particularly suitable for this research. First, online image sharing has become an increasingly popular feature on OSNs. For example, Facebook, one of the most popular social-networking Web sites, hosts over 10-billion user photos, a number that has kept growing at a rate of over 60 million per week (McCarthy, 2008). Consequently, image sharing that increases the opportunities to maintain social relationships to users will become a popular feature globally on OSNs, and its growth trajectory is striking. Second, privacy concerns become particularly salient in this context because online images are often tied to individual profiles either explicitly (through tags on images) or implicitly (through recurrence). As an integral and popular part of personal profiles on OSNs, user-provided digital images constitute a rich data source for those attempting to correlate profiles across multiple services using face recognition. Users are often free to post images regardless of their content, and are usually not required to notify other users prior to publishing their pictures, even if they are explicitly identifiable or tagged.[1] Many privacy concerns may arise from this practice because users may be unaware of the fact that a large and potentially unwanted audience could access their personal data or data related to them. While understudied, we believe that issues related to collaborative privacy management for image sharing will rapidly gain attention due to the growing popularity of social media where collaborative action with rich data exchange is the norm.

Our method is to design tools that allow users to collaboratively manage their shared images in OSNs. This collaborative privacy management approach considers two major factors: content that need to be protected, and stakeholders who are involved in content-sharing and -privacy management. In this section, we first develop a scenario that demands collaborative privacy management in OSNs, and then describe design requirements for tools to support such collaborative privacy management.

A Scenario of Collaborative Privacy Management

We adopted a scenario-based approach in developing user needs and design requirements for collaborative privacy management (Rosson & Carroll, 2002). All authors of this article have extensive experience in the use of OSNs and are familiar with privacy-management tools in various social networks. The scenario presented next was developed based on our firsthand experience.

> Bob and Allen were users of an OSN site, in which they friended each other. They studied in the same university and were roommates. Bob studied engineering, and Allen majored in computer science. Eve, who went to the same high school

[1] Users simply express their consent to publish the image and state that they have the rights to do so; however, there is no mechanism in place to block such publication.

> as did Bob, was a friend of Bob's in both real life and on the OSN site, and was an employee of a Fortune 500 software company. Allen and Eve met each other at a party organized by Bob. During a conversation with Allen, Eve found out that Allen had programming skills her employer may need, so she told Allen that she would be his internal reference if there was any job opening in her company.
>
> After a trip with Allen to New Orleans for spring break, Bob posted some pictures of him on the OSN site and tagged Allen. Soon, Allen received a message from Joe, one of Allen's friends on the OSN, who told Allen that he looked great in those beach pictures. While Allen did not mind sharing such pictures with friends like Joe, he indeed had a concern about Eve's reaction to these pictures from the perceptive of professionalism. Eve, as a friend of Bob's on the OSN site, could view all pictures Bob posted, including those in which Allen appeared. Worried that his beach pictures may jeopardize his opportunity to work in Eve's company, Allen wanted to co-manage those pictures concerning his privacy, but owned by Bob. He needed tools to notify him about any tagging action concerning him, to allow him to specify detailed policies regarding who on the OSN could view any picture in which he appeared, and to provide him information about who viewed the pictures and when. However, the OSN site did not offer such tools to co-manage these pictures. Having no other choice, Allen had to ask Bob to remove those pictures that may hurt his job hunting. Bob was reluctant to do that, but eventually deleted them to help Allen. Allen and Bob then contacted the OSN site and suggested that the site provide users with tools to collaboratively manage this kind of pictures.

This scenario captures stakeholders, concerned parties, and user requirements that should be considered in the design to support collaborative privacy management.

Stakeholders and Concerned Parties of Collaborative Privacy Management

We identified two key concerned parties that should be considered in designs to support collaborative privacy management. The first one is *Bob*, the creator and owner of pictures posted on the OSN site. We call the user who uploads and owns privacy-sensitive online content a *content-owner*. A content-owner is a critical stakeholder in collaborative privacy management because under current designs in most OSN sites, the content-owner is the only person who has full control over the online content. To make collaborative privacy management successful, we must identify and involve the content-owner.

The second key concerned party is *Allen*, the person whose personal information is revealed by Bob's shared content (i.e., online images in our case). We call such a user, whose identity is revealed through the content-owner's tags, a *co-owner* of the shared content. Under current designs in most OSN sites, the tagged-user (i.e., co-owner) has no privacy controls, but can untag herself to remove the explicit reference to the shared image on her profile. In other words, while co-owners (tagged-users) can untag to remove the explicit reference to themselves, they are unable to ever completely prevent disclosure of a particular picture posted by content-owners. Thus, we argue that co-owners (i.e., tagged-users) should be the primary benefactors of collaborative privacy management tools. With our proposed tool, tagged-users can gain control over content that concerns their privacy, but are owned by others.

In addition to the aforementioned two stakeholders, another important concerned party are the *viewers* (e.g., users such as Joe and Eve in our scenario) who can access the shared content. We call such users *content-viewers*. The composition of content-viewers varies and depends on the privacy policies a content-owner has regarding online content. If the content-owner allows sharing his or her content with all users on an OSN, content-viewers include everyone in the OSN. The content-owner can set privacy policies regarding who can view the content.

Note that online content posted by a content-owner but concerning a stakeholder does not have to be an image but can be in any type of format (e.g., image, video, or text) as long as it contains the private information of others and can be identified with methods such as searching or tagging. In this article, we call such online sharing content the *privacy-content*.

User Needs and Requirements of Collaborative Privacy Management

Based on the previous scenario and the analysis of stakeholders and concerned parties, the following user needs and requirements for collaborative privacy management tools can be identified:

- A content-owner should be able to invite tagged-users as a co-owner to co-manage privacy-content.
- A co-owner should be aware of the creation of privacy-content that concerns him or her.
- A co-owner should be able to request the control over the privacy-content from the content-owner who created the privacy-content. The control includes the ability to delete, update, and tag the content.
- A co-owner should be able to specify the accessibility of private-content by content-viewers. Possible access privileges include the ability to view, modify, and comment on given privacy-content.

Design of CoPE Access Control System and Policy Composition

We aim to design the CoPE system as an integrated solution that provides users with privacy mechanisms to collaboratively protect and manage accessibility of their published images in OSNs. The advantages of CoPE are twofold. First, it allows users to prevent unauthorized access to their personal data by providing a high-level of control over other users' access rights. Second, all stakeholders are given the ability to jointly manage shared images and mutually benefit from the control features offered by the tool. While we test and design our model focusing on images, our approach can be generalized to deal with other content and identify stakeholders. Further, the general model proposed in this article can be applied to a number of different systems, characterized by different content-sharing features. The overall approach can be tailored for the specific architecture employed by the system in consideration, leaving the fundamental access-control principles unchanged.

In this section, we discuss the design rationale of the CoPE system. We model a social network as a community of users (U), a set of relationship types among users (RT), and a set of data types (S). Each user u in U is uniquely identified and connected to others through at least one type of relationship. Social connections can be of several types and vary according to the specific social networks under consideration. Establishing such relationships requires acceptance by both parties. Some sites may extend privileges to the second (i.e., friends of friends) or third degree of user connections. Usually, it is assumed that all of the relationships are nontransitive and not hierarchically structured. Such relationships are treated as qualitative, in that they are not established based on a computed value but rather reflect the existing social relationships among users. Users can upload and post files of various types. Supported types include multimedia video files, .mp3 files, documents, images, and executables.

In our model, a user also has a profile to describe the relationships between friends and files that concern his or her privacy. The profile of a user u can be considered as a two-dimensional table, in which the columns are files, rows are other users who are in a relationship of a supported type in RT with u, and the intersection cell of a column and a row defines the access privilege of a friend to a file. Then, uploading new files is adding new columns, and deleting existing information is removing columns. Friending other people is adding new rows, and defriending is deleting rows. Changing the access right of a friend to a particular file modifies the value of the corresponding intersection cell.

Users are able to perform several actions within the context of an OSN. In our research, we focus on the actions that are related, directly or indirectly, to posting users' content and the access-control rights to the content. Examples of such actions are adding a picture, removing a picture, adding a friend, removing a friend, tagging a friend on a picture, and so on.

Identifying Stakeholders

The notion of stakeholders in the context of this research is intended to reflect the relationship between users and content. Data instances on a user's profile may pertain to the owner of the profile or may relate to other individuals. Documents, for example, can be authored by multiple users, and pictures and video may show by being tagged with numerous other users. From a data standpoint, a set of users can be connected by the same data instance, and these users are stakeholders of the shared content.

Stakeholders can be identified using several techniques. Tagging is the most common approach. Id-tags consist of applying labels over images to link them with the individuals appearing on the image itself. Therefore, each id-tag essentially corresponds to a unique user-id. Users can add such id-tags as the content is initially posted, starting from the image originator (e.g., the one who first uploads it). Although not error-free (e.g., one could add the wrong tags), using tags offers some benefits to collaborative privacy management. First, tagging makes it easy for a user to be involved in collaborative privacy management. In most OSNs, tagging a picture is a tool available for any user who can see the picture. Thus, if users see themselves in pictures owned by others and want to control access to these picture by their friends, they can simply tag themselves on these pictures and then request co-ownership of them. Second, the tagging mechanism allows owners to automatically identify those users who are stakeholders of a certain image. With facial-recognition algorithms (Lowensohn, 2008), tools can be designed to recognize all people in a picture and then generate tags automatically to specify potential stakeholders, thus minimizing the risk of misplacing or missing stakeholders. Several content-sharing sites (e.g., Picasa, etc.) now offer the opportunity of automatically tagging users based on such automated facial-recognition tools. Finally, id-tags are very popular and well accepted by end users of OSNs. Hence, leveraging this mechanism represents a simple, yet effective, approach to identifying stakeholders of shared objects and does not require end users to perform any additional tasks other than what they normally do when posting images.

With identified stakeholders, a shared profile can be generated based on the profiles of all stakeholders. A shared profile contains those contents that concern all stakeholders. Then, collaborative privacy management is about the control of what content should be included in the shared profile and whether common friends are allowed to access private content. Different privacy policies control what ways the access privilege should be assigned: by a default setting or on a case-by-case basis.

Composing Multiparty Policies

A user's profile is characterized by a set of data items. Since content (specifically, images) can have multiple stakeholders, a particular content is selectively shared with the corresponding stakeholders. To identify stakeholders of a certain uploaded object, we employ id-tagging technologies (discussed earlier). Next, we will further discuss the notion of stakeholders.

Shared profile portions are managed by all stakeholders of the protected content, who also are able to collaboratively determine the scope of sharing. The stakeholders of some data (s) can enforce their privacy preferences with respect to viewers and with respect to additional stakeholders. For each piece of shared data, the preferences of the stakeholders' set are then integrated. For this study, we opted for a simple approach to integrate all users' preferences, although several alternatives are possible. We adopt a simple voting scheme whereby each stakeholder u expresses a vote by indicating a

DOI: 10.1002/asi

set of preferred viewers. Specifically, each stakeholder indicates one of the following: (a) *some-friends*, the users who are in a specific relationship and/or the set of users who they do *not* want them to be granted access u'; (b) *public*, all users U, regardless of the existing relationship and connection path with u; and (c) *co-owner only*, which means that only co-owners are allowed access to the content. Such preferences can be specified in different ways according to the specific OSN platform considered. For example, concerning option (a), users may indicate the specific set of users or provide a succinct description by indicating the relationships that are considered trusted (e.g., all friends) or specifying some profile-specific conditions (e.g., all users in my network). As users input their preferences, the resulting settings for some data s are generated according to the following (simplified) steps:

1. Stakeholders specify their preferences. By default, each stakeholder has no knowledge of the input preferences of others.
2. The number of preferences are counted and grouped by type. If *co-owner only* receives the highest number of votes, then no viewer rights for s will be granted.
3. If *co-owner only* is not the most voted option, for each user's preference such that the preference is either *public* or *some-friends*, the set of corresponding viewers is identified. The final set of viewers is computed exclusively joining the set of users indicated by the corresponding stakeholders and by removing the negative sets, u' (i.e., the users who are requested not to obtain access).
4. Each time a new stakeholder is added to the set of stakeholders, his or her CoPE privacy policies are added. Accordingly, the new overall privacy preferences can be calculated, as described in Steps 2 and 3.

The corresponding access algorithm's pseudocode follows.

```
REQUIRE: User u profile $Profile_{us}$, $Rights_u$, and Stakeholders' preferences $u_1, \ldots, u_n$
  ENSURE: Controlled Access to Profile's Data
  Let $Rights_u$ denote the rights associated to a user u,
  Let Right(u′, s, {list}) denote the access rights in {list} granted to u′ with respect to s.
  Stakeholders = {u|Right(u′, s′, stakeholder, {grant, setprivacy, download, view})∈Rightsu and s = s′}
    Let $Pref_u^s$ be the set users allowed according to u's access preference for s.
    Let |SO_s| = n be the number of stakeholders of s
    IF $\exists Set = \|u', u', \ldots u^{iv}\| = n/2 + 1 \in SO_s$ s.t. $\forall u \in Set$,
        $Pref_u = Stakeholder \wedge ViewersAllowed = \oslash$
    ELSE
        %Intersect the Set of users selected by the stakeholders' preferences
        $ViewersAllowed = Pref_{u1}^s \cap Pref_{u2}^s \ldots \cap Pref_{uk}^s$
        FOR u ∈ViewersAllowed
          $Right_u = Right_u \cup$ Right(u, s, viewer, {view, download})
        END FOR
ENDIF
```

This algorithm enables all stakeholders to input their preferences and ensures that all user preferences are integrated into the shared profile, even if they are restricted by others' preferences. The possibility of indicating excluded users increases individual control by ensuring that even if their option is not selected, these specific preferences are taken into account. To avoid privacy leaks, users are required to express their privacy preferences before being informed of others' preferences. Then, based on the collected results, the set of users who are permitted to view the data can be computed. For example, the content may be available only to the stakeholders themselves if this option is the top choice among stakeholders. Such a restrictive approach ensures that user privacy is paramount. In cases where the overall preference is to share the data with all socially connected users, and users express their preferences in terms of a category of users (e.g., all friends, all colleagues, etc.), then all users' selections will be considered and used to determine the set of users who are granted access to the data.

If no users are found to fall within this intersection, only the stakeholders will be permitted to view the content.[2] In addition, cases of ties (i.e., an even number of stakeholders expresses opposite preferences) in the current approach are broken by prioritizing the option expressed by the user who originally posted the content.

Note that this model assumes the honest behavior of end users; that is, it assumes that users correctly enter their privacy preferences and do not attempt to bypass the system's control by not indicating stakeholders or fail to accept the provided policy. While this may be considered as a limitation, we consider it acceptable considering the collaborative and open nature of OSNs, and the possibility of applying more stringent controls as needed by the specific context where such collaborative approach is deployed.

Implementation of CoPE on Facebook

We implemented our prototype referred to as CoPE to support collaborative privacy control of online content in Facebook. We chose Facebook as our implementation platform because it is currently the largest photo-sharing site. Although Facebook provides various privacy control features for end users (see O'Neill, 2009), these existing features have been oriented toward individual privacy responses and behaviors, failing to acknowledge the collective privacy needs for shared content. In a highly connected social network, users' privacy settings would impact other users' information accessibility within the same network, across the boundary of a single user's profile. To address this gap, we implemented CoPE in Facebook as one of the first studies to unpack the conceptual nature of collaborative privacy management. Our proposed approach does not intend to argue for a replacement of the current Facebook privacy settings; rather, we call

[2] This approach may seem restrictive; however, in practice, most users who share content are interconnected by at least one common friend (http://en.wikipedia.org/wiki/Small_world_experiment).

for more research devoted for studying privacy issues at the group level and designing more fine-grained control features for users' collective privacy decisions with their social groups in OSNs.

In what follows, we describe the implementation details of CoPE. In its current form, CoPE is listed among the available applications on Facebook, and users can freely install it as an application. Note that the goals of this prototype are to provide a proof of concept implementation of our model, and to gain a preliminary understanding on the factors motivating users to enact collaborative privacy practices to co-manage their shared data. Several alternative implementation options are possible, such as fully integrating the features of CoPE as part of OSN privacy settings, deploying a remote server to handle the privacy settings of users, and applying the same design principles discussed in this research in other implementation platforms (other than Facebook).

System Architecture of CoPE

Our CoPE tool was implemented under a client–server architecture using an Apache Tomcat application server with PHP, and an MySQL 5.0.22. database server. The Tomcat application server is responsible for the data processing and management of shared content, user profiles, and shared profiles.

The CoPE is implemented as a Facebook application. As each Facebook application, CoPE owns its own unique appkey and secret keys that are used to enable access to the Facebook platform. The application is made to run in an iframe, and support for Facebook Markup Language is enabled. The application settings are customized such that all users can add and use the application.

The application includes several PHP files, which process user authentication, user interface layout, shared content management, co-ownership management, friend management, privacy policy management, and so on. User authentication is integrated with the authentication of Facebook. Once the user installs the application in his or her Facebook profile page, the application file "PrivateBoxAlbum" accesses the user's profile data, and uses such information to complete the application template. In particular, the application imports the user image files and renders them from the CoPE. Image files are locally stored in and managed by the MySQL database server. Upon the user opening the CoPE, photos added by the current user are retrieved from the database. The list of users who have been tagged in the images is retrieved, using Facebook-specific methods [e.g., photo.get.Tags()]. The system is then in charge to remove possible duplicates (i.e., some users may share multiple files) and to create a unique list of stakeholder per each profile. Once the list is identified, the notification process is started by leveraging the notification systems provided by Facebook.

Upon stakeholders entering their privacy preferences (under the settings.php file), the system tracks them and computes the privacy settings resulting from the users' input. Once a common policy is formed, the visibility of the image changes, and the corresponding access policy is enforced. In detail, this is achieved by carrying out the following tasks: First, the values of the settings of the currents users are retrieved (from settings.php). Second, the photo id's images that the current user is sharing are saved. Third, for all such images, the corresponding privacy-setting changes are collected. Fourth, once all these settings are collected, the system composes the policy, including and excluding viewers according to the criteria indicated by users. This policy is added to the settings database for each image so that each time an image is invoked by the application file in charge of rendering the image, the correct settings are applied. If a user fails to provide a preference, the default preference is applied until further modification.

Note that although our application was implemented with the APIs provided by Facebook, it can be easily migrated to other OSN platforms. The APIs our implementation relies on to access the tags of a picture and users are commonly seen in different ONS platforms. For example, the method of photo.get.Tags is required to obtain the tags of a Facebook picture, and a similar function, tags.getListPhoto, is offered by another photo sharing service, flickr.com.

Features of CoPE

Our design of CoPE focuses on supporting the management of the access rights for digital images, and provides the following functions (see the Appendix for the interface design):

- **Potential Co-managed Photos Notification:**

Adding tagged images to the CoPE tool for collaborative privacy management (Tagging can be completed prior to the image being uploaded or as the image is uploaded on CoPE.);

Notifying users when they have been tagged by friends who also are using CoPE.

- **Stakeholder Request:**

Allowing users to request co-ownership on images in which they were tagged;

Notifying users about the requests on co-ownership;

Allowing users to grant co-ownership to others.

- **Photo Access Management:** CoPE allows a stakeholder to control various privacy-related settings that relate to their photos. That is, a user can set the viewable attribute of any photo to "only co-owners," "some friends," or "public" to limit the potential viewers of the photo.
- **Track Viewing History:** CoPE allows a user to keep track of who has viewed their photos.

Note that some functions mentioned earlier, such as notifications of being tagged in a photo, are currently available in Facebook with limiting the access privilege of friends to tagged pictures. However, current tools in Facebook lack the capability to address the issues concerning multiple stakeholders. Facebook allows users to set up a general policy regarding access rights to any pictures in which a user is tagged. For example, a user can specify that any photo of him or her must be viewable only to him or her and the user who uploaded the pictures; however, this policy restricts the image visibility, making it private. Consider the aforementioned scenario: If Allen used such a policy on any picture with him being tagged, then none of Bob's friends would be able to see those pictures. If Bob's policy was to allow his friends to see his pictures, a conflict between Allen's policy and Bob's policy would arise. No tool is available in Facebook to address such policy conflicts. Our collaborative privacy management model can address this issue by composing the policy so that both users' preferences are translated into one privacy setting that strikes a balance between the two users' preferences. In addition, our design offers more tools to manage privacy, including requesting ownership of pictures owned by others and browsing the view history of private content.

A Survey Study

The CoPE tool provides a proof of concept implementation of collaborative privacy management. To gain a preliminary user understanding of such a concept, we conducted a survey study ($n = 80$) to explore the factors motivating users to enact collaborative privacy practices through tools such as our CoPE application. We were particular interested in examining whether users perceive such tools as our CoPE application as being useful, to what extent that they like the idea of collaborative privacy management, and whether they intend to adopt tools such as the CoPE to empower their collaborative privacy control with their social groups.

We analyzed data from the survey using Structural Equation Modeling (SEM) techniques. The statistical technique selected for SEM was the partial least squares (PLS), which is widely accepted as a method for testing theory in early stages (Gefen & Straub, 2005) and has been used in the field of information science (e.g., Zhang & Sun, 2009). Similar to the cases in prior research (Zhang & Sun, 2009), we chose PLS as the statistical technique because of the exploratory nature of this study in the early stage of theoretical development. We used PLS to perform confirmatory factor analysis to assess validity of all multi-item research constructs. The validity of the constructs was assessed in terms of individual item reliability, internal consistency, and discriminant validity. After establishing the validity of the measures, we extracted the statistically significant relationships and tested the causal model (described later).

Participants and Procedure

We recruited participants to this survey-based study from multiple sessions of the same introduction level of information science course in a public university in the United States. In those class sessions where we recruited participants, we read recruitment materials about the background of researchers and the general purpose of this study without revealing too many design details. We also specified that participants must be active Facebook users. One extra-credit point for the course was awarded for their participations in the study. Students who chose to participate in this study remained in the room after the class. Eighty-nine students agreed to participate in this survey study. Since participation of the study was completely voluntary, some respondents submitted empty or only partially filled questionnaires that were subsequently eliminated. Eighty responses were usable. Among the 80 responses, 24 were female and 56 were male, and they identified their ages as 18 to 23 ($n = 68$) and over 24 ($n = 12$) years. Most reported using the Facebook photos application at least once a week ($n = 62$). Note that the respondents were predominately college-aged students; as a result, some findings may not generalize beyond this group.

In the survey study, participants were first asked to complete a presession questionnaire on their Facebook usage and their general privacy concerns. Next, we presented a usage scenario to illustrate various features of CoPE, followed by the introduction of a fake Facebook account for each participant to which we installed our CoPE tool. Participants then were provided access to these fake Facebook accounts. They were encouraged to explore the functions of CoPE with those photos we uploaded to these accounts. We gave participants no training on the interface and told them that CoPE was listed among the available applications on Facebook and that they can freely install it as an application on their own Facebook profiles. After exploring the various features of the CoPE tool, participants were asked to complete a postsession questionnaire on their attitudes toward this application, to what extent they like the idea of collaborative privacy management, their perceived usefulness and ease of use of this application, and whether they intended to adopt tools such as the CoPE to empower their collaborative privacy control with their social groups.

Measurement Details and Validity

According to Shackel (1991), a system's acceptability is defined as a function of three dimensions—utility (whether the system does what is needed functionally), usability (whether the users can easily work the system), and likeability (whether the users feel the system is favorable)—all balanced against the cost of the system. As an important paradigm in HCI, this framework has been considered as a high-level conceptualization of the acceptability of any system to its intended users. Drawing on Shackel's high-level conceptualization of the system acceptability, we examined the acceptability of the CoPE tool by capturing the respondents' perceptions of utility, usability, and likeability of CoPE in our survey. Specifically, we measured *utility* through the construct of *perceived usefulness* that was defined in the Technology Acceptance Model (TAM; Davis, 1989) as "the degree to which a person believes that using a particular system would enhance his or her job performance" (p. 320). We measured *usability* through the construct of *perceived ease of use* that was defined in TAM as "the degree to which a person believes that using a particular system would be free of

TABLE 1. Psychometric properties of the measurement model.

Measures of constructs[a]	Item loading	Composite reliability	Cronbach's α	Average variance extracted
Intention to Use (INT): ($M = 3.35$, $SD = 0.94$)		0.972	0.821	0.921
• I intend to install this application on my Facebook profile in the near future.	0.956			
• I predict that I will use this application in the near future.	0.966			
• I would like to use this application to share my photos with my friends on Facebook.	0.958			
Perceived Usefulness (PU): ($M = 3.86$, $SD = 0.90$)		0.970	0.954	0.915
• Using the application would better protect my photos.	0.970			
• Using the application would improve my photo privacy.	0.969			
• Using the application would enhance my control over my photos.	0.931			
Perceived Ease of Use (EOU): ($M = 3.64$, $SD = 0.70$)		0.919	0.863	0.792
• My interaction with this application would be clear and understandable.	0.900			
• Interacting with this application would not require a lot of my mental effort.	0.895			
• I would find it easy to get this application to do what I want it to do.	0.874			
Likeability (LIKE): ($M = 3.78$, $SD = 0.91$)		0.814	0.702	0.691
• For CoPE, I like the idea of being in control of the pictures along with others who also appear in the picture.	0.940			
• For CoPE, I like the idea of being able to claim my ownership for those pictures in which I appear.	0.707			
Privacy Concerns (PCON): ($M = 3.55$, $SD = 0.93$)		0.886	0.957	0.798
• There is a high potential for loss involved in sharing personal information (including photos) on Facebook.	0.992			
• I am concerned about providing personal information (including photos) to Facebook because it could be used in a way I did not foresee.	0.782			

[a] Measured on 5-point, Likert-type scale: 1 (*strongly disagree*), 2 (*disagree*), 3 (*neutral*), 4 (*agree*), 5 (*strongly agree*).

effort" (Davis, 1989, p. 320). Based on Shackel's conceptual framework, we developed our own items to measure *likeability,* which we defined as the extent to which a person likes the idea of collaborative privacy management through the CoPE. For the outcome variable, respondents' intention to adopt CoPE was measured by questions that were directly adapted from Davis (1989).

Given that privacy concerns become particularly salient in the context of OSNs, we examined the role of *privacy concerns* in influencing users' perceptions of acceptability of the CoPE application. As shown by prior literature, individual differences in privacy perceptions can be significant (Buchanan, Paine, Joinson, & Reips, 2007; Xu & Gupta, 2009; Yao, Rice, & Wallis, 2007). Thus, we included a set of questions to ask participants about their specific privacy concerns on their information and content sharing on Facebook. Consistent with recent operationalization of privacy concerns in the literature, the construct of *privacy concerns* was measured by questions that were directly adapted from Dinev and Hart (2006).

We evaluated the validity of the survey instrument by examining (a) individual item reliability, (b) internal consistency, and (c) discriminant validity (Barclay, Thompson, & Higgins, 1995). First, individual item reliability was assessed by examining whether the loading of each item on the construct is above 0.6 or, ideally, 0.7 (Barclay et al., 1995). As can been seen from the Table 1, the loadings of all items are above 0.7, thus demonstrating adequate reliability. Second, Cronbach's α and composite reliability scores are used to assess the internal consistency. Nunnally (1978) proposed 0.7 as an indication of adequate Cronbach α. Hair, Anderson, Tatham, and Black (1998) recommended 0.8 as an indication of adequate composite reliability. As shown in Table 1, the internal consistency criteria are met as the Cronbach's α scores are above 0.7, and the composite reliability scores are above 0.8.

The third step to assess the measurement model involves examining its discriminant validity. One criterion for establishing discriminant validity is that no measurement item should load more highly on any construct other than the construct it intends to measure (Chin, 1998). Off-diagonal elements in Table 2 represent correlations of all latent variables whereas the diagonal elements are the square roots of the average variances extracted of the latent variables. For adequate discriminant validity, the square root of the variance shared between a construct and its measures should be greater than the correlations between the construct and any other construct in the model (Barclay et al., 1995). In other words, the diagonal elements should be greater than corresponding

TABLE 2. Discriminant validity of constructs.

Construct	INT	PU	EOU	LIKE	PCON
Intention to Use (INT)	0.960				
Usefulness (PU)	0.665	0.957			
Ease of Use (EOU)	0.546	0.617	0.890		
Likeability (LIKE)	0.596	0.668	0.507	0.831	
Privacy Concerns (PCON)	−0.017	0.118	0.110	0.093	0.893

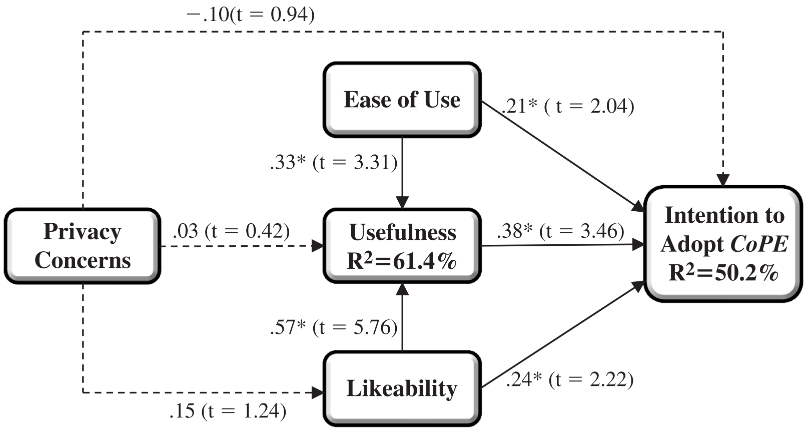


FIG. 1. Causal model and results.

off-diagonal ones. Data shown in Table 2 therefore satisfy this requirement.

Causal Model

To explore the factors motivating users to enact collaborative privacy practices through tools such as our CoPE application, we developed a causal model to describe how privacy concerns may influence a user's acceptability of the CoPE. Depicted in Figure 1, the causal model is developed based on Shackel's (1991) conceptualization of system acceptability and the TAM (Davis, 1989). The relationships among research variables in the causal model are explained in detail in this section.

With adequacy in the measurement model affirmed, the PLS structural model was next examined to assess the explanatory power and the significance of the paths in the causal model. Bootstrapping techniques in PLS were used to obtain the corresponding t values to assess the significances of the path coefficients. The explanatory power of the structural model was determined based on the amount of variance in the endogenous construct (i.e., adoption intention in our study) for which the model could account. The structural model explained 50.2% of the variance in adoption intention. This greatly exceeded 10%, which was suggested by Falk and Miller (1992) as an indication of substantive explanatory power. In other words, the casual model we constructed (in Figure 1) possesses enough explanatory power to make the interpretations of path coefficients meaningful.

Role of privacy concerns. To further understand why Facebook users would be motivated to adopt the CoPE tool, the survey explored the role of privacy concern in predicting the user's perceived usefulness, likeability, and intention to use CoPE. Results show that the relationship between users' privacy concerns and their perceived usefulness of CoPE was not significant ($b = 0.03$, $t = 0.42$). Similarly, the relationship between users' privacy concerns and their usage intentions ($b = -0.10$, $t = 0.94$) and the relationship between users' privacy concerns and the likeability of CoPE ($b = 0.15$, $t = 1.24$) also were not significant. Given that respondents' ratings for perceived usefulness ($M = 3.86$, $SD = 0.90$), likability ($M = 3.78$, $SD = 0.91$), and usage intention ($M = 3.35$, $SD = 0.94$) were high, these results suggest that regardless of whether Facebook users are worried about their privacy, a majority of them like the idea of collaborative privacy management and believe that a tool such as CoPE would be useful to protect their photo privacy. A plausible explanation for such a result pattern may be related to the impact of the media's extensive coverage of Facebook privacy. Prompted by a chain of privacy-related scandals associated with services offered by *Facebook* (e.g., *News Feed* in late 2006, *Beacon* in early 2008), many users have become more aware of their personal privacy on Facebook. As a result, it is not surprising to find that Facebook users are more aware of privacy issues and thus more likely to perceive privacy-enhancing features useful and adopt these features as a part of their daily usage of Facebook.

Factors predicting usefulness of CoPE. Results show that perceived ease of use ($b = 0.33$, $t = 3.31$) and likability ($b = 0.57$, $t = 5.76$) were positively related with perceived usefulness of CoPE. These two factors alone can explain as high as 61.4% of the variance in perceived usefulness. Among the two factors that can significantly enhance users' perceived usefulness of CoPE, likability had a stronger positive effect ($b = 0.57$) compared to ease of use ($b = 0.33$). This suggests that users placed high importance on both aspects, but could more likely regard CoPE as valuable if it is perceived to be fun and favorable.

Factors predicting use intention of CoPE. Our results confirm the positive effects of ease of use, usefulness, and likability on intention to adopt CoPE. These three factors can explain as high as 50.2% of the variance in adoption intention, which reinforces Shackel's (1991) three-dimension conceptualization of the system acceptability. Among the three dimensions that can determine a system's acceptability

TABLE 3. Usefulness rankings of the four features by participants.

	Co-ownership notification (%)	Stakeholder request (%)	Manage photo access (%)	Track viewing history (%)
First choice	10.9	12.7	50.9	21.8
Second choice	21.8	23.6	30.9	29.1
Third choice	32.7	40.0	12.7	14.5
Fourth choice	34.5	23.6	5.5	34.5

by users, perceived usefulness ($b = 0.38$, $t = 3.46$) appears to have a greater impact compared to ease of use ($b = 0.21$, $t = 2.04$) and likability ($b = 0.24$, $t = 2.22$). This suggests that the dimension of *utility* (as reflected by the construct of *perceived usefulness*) is considered as the fundamental value in terms of adopting CoPE by our survey respondents.

Further Analyses of the CoPE Features

Participants also were asked to compare the different features offered by our CoPE tool and rank them according to the usefulness of each feature. As shown in Table 3, more than 50% of participants ranked the feature that allows them to manage photo access as being the most useful. This was followed by the feature for viewing history tracking (Note that 21.8% ranked this feature as their first choice, and 29.1% as their second choice.) These results indicate that users desire a high level of control regarding the management of photo access, as well as the ability to know the history of content access.

Discussion and Conclusions

This article presents an approach of collaborative privacy management to improve private-data management and protection within OSNs. An extended notion of collaborative privacy management among stakeholders is introduced, along with a simple and practical approach for defining and establishing access rights across users. In addition, this research demonstrates an initial application that supports such new collaborative privacy-control mechanisms. This application, known as CoPE, is implemented within the context of Facebook. Through a survey-based study, we have further explored the notion of collaborative privacy management from an end-user perspective by surveying individuals' attitudes and perceptions toward the proposed design concept. The primary empirical evidence obtained from this study shows that users of OSNs value the notion of collaborative privacy management and are likely to adopt privacy-enhancing features offered by our application to co-manage their shared contents on OSNs.

This research is one of the first attempts to model collaborative privacy management. Although the CoPE tool targets collaborative management of image-related privacy, our approach can be generalized and used to manage privacy in other types of contents within the context of Web 2.0, such as videos and documents, if appropriated techniques are applied to identify stakeholders.

This research has some limitations. First, the simple mechanism to determine stakeholders may raise an issue of trust. Under the current design model, stakeholders are not necessarily related to each other. A user can become a co-owner as long as the user is tagged. This approach may create opportunities for abnormal behaviors (e.g., malicious tags). To avoid sharing data with users who are not trusted, a stakeholder can specify the conditions that must be met before a new stakeholder can be accepted. For example, stakeholders can be assessed in a collaborative way by asking users to indicate how many degrees of separation they believe are reasonable between them and potential stakeholders. A resolution algorithm then can factor these constraints when calculating the conditions that must be met for someone to become a stakeholder.

Second, the way to control viewers in our design may not be as comprehensive as what users need. Currently, a stakeholder specifies who among their friends list can view the images without consulting other stakeholders. To ensure privacy and trust, designs may need to consider more sophisticated approaches such as selecting preferences as an online voting system, or an auction, as suggested by Squicciarini et al. (2009). Of course, these approaches require more involvement from other stakeholders and may discourage the use of collaborative privacy management. Further, our approach may not return the most appropriate collective policy in certain scenarios. For example, if a common agreement cannot be reached, the stakeholders could negotiate the image's privacy in multiple rounds.

Through a number of iterations, parties may reach an agreement and decide to alter the image content (by clipping or cropping some parts of it) prior to its disclosure on the OSN. We choose not to adopt this approach since, as shown by prior research (Hoadley et al., 2010), users tend to spend little effort on configuring their privacy settings, and a multiround protocol for a single image that requires image modification may be too cumbersome and thus not enabled by mass users.

In conclusion, we have observed that the problems related to collaborative privacy management present long-term challenges. These challenges concern modeling relationships in social networks, user profiles, stakeholders, and privacy control for all possible cases of collaborative sharing that could arise rather than technical design and implementation. The CoPE system represents a first step toward a comprehensive solution for collaborative privacy management and offers a technical platform on which we can explore and test other advanced models and algorithms. Using the groundwork developed by this study, we hope to extend our research by improving the theoretical model of collaborative privacy management, investigating the user adoption of the CoPE tool through field studies, and applying this approach in other different types of online contents.

References

Adamic, L., Buyukkokten, O., & Adar, E. (2003). A social network caught in the Web. First Monday, 8(6).

Barclay, D., Thompson, R., & Higgins, C. (1995). The partial least squares (PLS) approach to causal modeling: Personal computer adoption and use an illustration. Technology Studies, 2(2), 285–309.

Besmer, A., & Lipford, H. (2009). Tagged photos: Concerns, perceptions, and protections. Proceedings of the 27th International Conference Extended Abstracts on Human Factors in Computing Systems (pp. 4585–4590). New York: ACM Press.

Buchanan, T., Paine, C., Joinson, A.N., & Reips, U. (2007). Development of measures of online privacy concern and protection for use on the Internet. Journal of the American Society for Information Science and Technology, 58(2), 157–165.

Carminati, B., & Ferrari, E. (2008, October). Privacy-aware collaborative access control in Web-based social networks. Paper presented at the 22nd annual IFIP Working Group 11.3 Working Conference on Data and Applications Security, London, UK.

Carminati, B., Ferrari, E., & Perego, A. (2006, October). Rule-based access control for social networks. Paper presented at the On the Move to Meaningful Internet Systems Workshops.

Caudill, E.M., & Murphy, P.E. (2000). Consumer online privacy: Legal and ethical issues. Journal of Public Policy & Marketing, 19(1), 7–19.

Chin, W.W. (1998). The partial least squares approach to structural equation modeling. In G.A. Marcoulides (Ed.), Modern methods for business research (pp. 295–336). Mahwah, NJ: Erlbaum.

Crescenzo, G., & Lipton, R.J. (2009). Social network privacy via evolving access control. Proceedings of the Fourth International Conference on Wireless Algorithms, Systems, and Applications (pp. 551–560). Boston: Springer-Verlag.

Culnan, M.J., & Bies, J.R. (2003). Consumer privacy: Balancing economic and justice considerations. Journal of Social Issues, 59(2), 323–342.

Davis, F.D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–339.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. Information Systems Research, 17(1), 61–80.

Ellison, N.B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "Friends:" Social capital and college students' use of online social network sites. Journal of Computer-Mediated Communication, 12(4), 1143–1168.

Falk, R.F., & Miller, N.B. (1992). A primer for soft modeling. Akron, OH: University of Akron Press.

Gates, C.E. (2007, May). Access control requirements for Web 2.0 security and privacy. Paper presented at the Institute of Electrical and Electronics Engineers Web 2.0 Privacy and Security Workshop, Oakland, CA.

Gefen, D., & Straub, D. (2005). A practical guide to factorial validity using PLS-graph: Tutorial and annotated example. Communications of the Association for Information Systems, 16, 91–109.

Golbeck, J., & Hendler, J. (2004, July). Reputation network analysis for email filtering. Paper presented at the Conference on Email and Anti-Spam, Mountain View, CA.

Gross, R., & Acquisti, A. (2005, June). Information revelation and privacy in online social networks. Paper presented at the Workshop on Privacy in the Electronic Society.

Hair, J.F., Anderson, R.E., Tatham, R.L., & Black, W.C. (1998). Multivariate data analysis with readings (5th Ed.). New York: Macmillan.

Hoadley, C.M., Xu, H., Lee, J.J., & Rosson, M.B. (2010). Privacy as information access and illusory control: The case of the Facebook news feed privacy outcry. Electronic Commerce Research and Applications, 9(1), 50–60.

Iachello, G., & Hong, J. (2007). End-user privacy in human–computer interaction. Foundation and Trends in Human–Computer Interaction, 1(1), 1–137.

Jagatic, T.N., Johnson, N.A., Jakobsson, M., & Menczer, F. (2007). Social phishing. Communications of the ACM, 50(10), 94–100.

Kiran K. Gollu, Stefan Saroiu, & Alec Wolman. (2007, October). A Social Networking-Based Access Control Scheme for Personal Content Proc. 21st ACM Symposium on Operating Systems Principles (SOSP '07), Stevenson, Washington. (WIP)

Lenhart, A., & Madden, M. (2007, April 18). Teens, privacy & online social networks. Pew Internet & American Life Project. Retrieved November 29, 2010, from http://www.pewinternet.org/Reports/2007/Teens-Privacy-and-Online-Social-Networks.aspx

Lipford, R.H., Hull, G., Latulipe, C., Besmer, A., & Watson, J. (2009, August). Visible flows: Contextual integrity and the design of privacy mechanisms in online social networking. Paper presented at the Workshop on Security & Privacy in Online Social Networking, Vancouver, Canada.

Lowensohn, J. (2008, August 1). Facebook's auto-tagging feature could be tip of tagging iceberg. Retrieved November 29, 2010, from http://news.cnet.com/8301-17939_109-10004835-2.html

Mannan, M., & van Oorschot, P.C. (2008, April). Privacy-enhanced sharing of personal content on the web. Paper presented at the Proceedings of the 16th International World Wide Web Conference, Hong Kong, China.

McCarthy, C. (2008, October 15). Facebook hosts 10 billion photos. Retrieved November 29, 2010, from http://news.cnet.com/8301-13577_3-10066650-36.html

Nunnally, J.C. (1978). Psychometric theory (2nd Ed.). New York: McGraw-Hill.

O'Neill, N. (2009). 10 privacy settings every Facebook user should know. Retrieved November 29, 2010, from http://www.allfacebook.com/facebook-privacy-2009-02

Rosenblum, D. (2007). What anyone can know: The privacy risks of social networking sites. IEEE Security and Privacy, 5(3), 40–49.

Rosson, M.B., & Carroll, M.J. (2002). Usability engineering: Scenario-based development of human–computer interaction. San Francisco: Academic Press.

Schwartz, M.P. (1999). Privacy and democracy in cyberspace. Vanderbilt Law Review, 52, 1610–1701.

Shackel, B. (1991). Usability—Context, framework, definition, design, and evaluation. In B. Shackel & S. Richardson (Eds.), Human factors for informatics usability (pp. 21–38). New York: Cambridge University Press.

Squicciarini, A., Shehab, M., & Paci, F. (2009). Collective privacy management in social networks. Proceedings of the 17th International World Wide Web Conference (pp. 461–484). New York: ACM Press.

Westin, A.F. (1967). Privacy and freedom. New York: Atheneum.

Xu, H., & Gupta, S. (2009). The effects of privacy concerns and personal innovativeness on potential and experienced customers' adoption of location-based services electronic markets. International Journal on Networked Business, 19(2), 137–140.

Yao, M.Z., Rice, R.E., & Wallis, K. (2007). Predicting user concerns about online privacy. Journal of the American Society for Information Science and Technology, 58(5), 710–722.

Zhang, P., & Sun, H. (2009). The complexity of different types of attitudes in initial and continued ICT use. Journal of the American Society for Information Science and Technology, 60(10), 2048–2063.

Zweig, D., & Webster, J. (2002). Where is the line between benign and invasive? An examination of psychological barriers to the acceptance of awareness monitoring systems. Journal of Organizational Behavior, 23, 605–633.

Appendix

CoPE Interface Design Details

Default privacy policy setting for all pictures in CoPE. Setting privacy policies for individual pictures could be time-consuming and inconvenient to co-owners. Thus, we designed a tool that allows a user to set up default privacy policies on all pictures that concern a user's privacy. The CoPE offers four options: only open to co-owner, open to some friends, open to the public, and different policies for different pictures (see Figure A1).

The first three policy options set a universal policy on all pictures. Under either of these policies, whenever a user is tagged in a picture, the picture is added to CoPE under a given universal policy. The user is notified by the system about the addition of the picture and the setting of the private policy. When the case-by-case policy is used, the user must specify the policy for each picture.

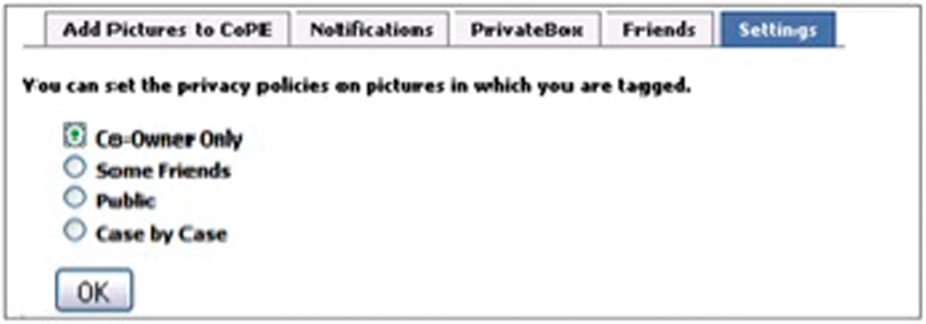
Adding tagged images to CoPE. After a picture is added into CoPE, the owner of the picture can decide whether to invite the person who was tagged as a co-owner of the picture. Figure A2 shows the user interface the owner sees after a tagged picture is added into CoPE.

Accepting co-ownership invitation. A user will be notified when he or she was invited to be a co-owner of a picture. The user can immediately accept the invitation.

Co-ownership request. An invitation of co-ownership is not guaranteed, however. It is possible that a content-owner uploads a picture, tags a co-owner, but does not check the invitation option. Then, the picture would be out of the control of the tagged co-owner, and the privacy of the co-owner may be harmed. To prevent this situation, we designed a feature to allow the tagged co-owner to request the co-ownership of a picture in which he or she was tagged. If the tagged user does not receive an invitation to be a co-owner of the private-content, she will be notified by the system of the tagging event. Figure A3 is a screenshot showing the pictures a user tagged, the content-owners of these pictures, and the decision to request the co-ownership for one picture. Co-ownership requests will be sent to the corresponding content-owners. After seeing a notification of a request, a content-owner must grant the co-ownership to the requester.

Browsing private picture. The CoPE allows a user to see all pictures that concern his or her privacy (Figure A4). The user can browse and change the privacy policies for individual pictures.

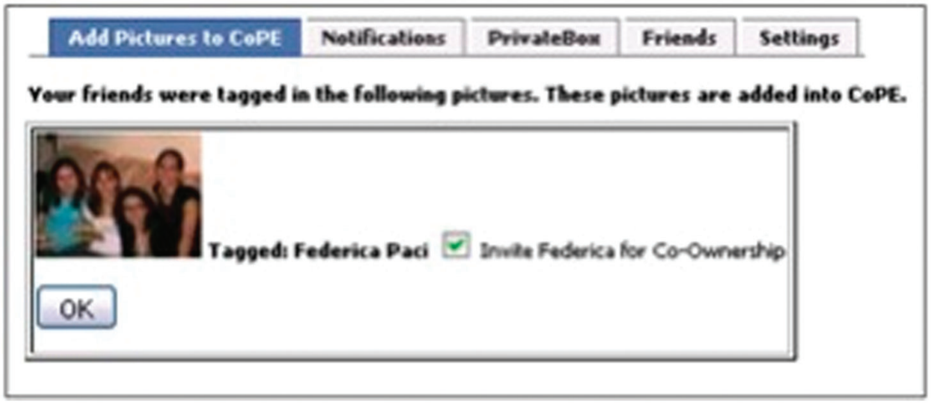
Browsing visit history. To further help users protect their privacy, the CoPE allows users to keep track of the browsing histories of the pictures that concern them. The user can see who has visited the pictures and when (Figure A5).



You can set the privacy policies on pictures in which you are tagged.

● Co-Owner Only
○ Some Friends
○ Public
○ Case by Case

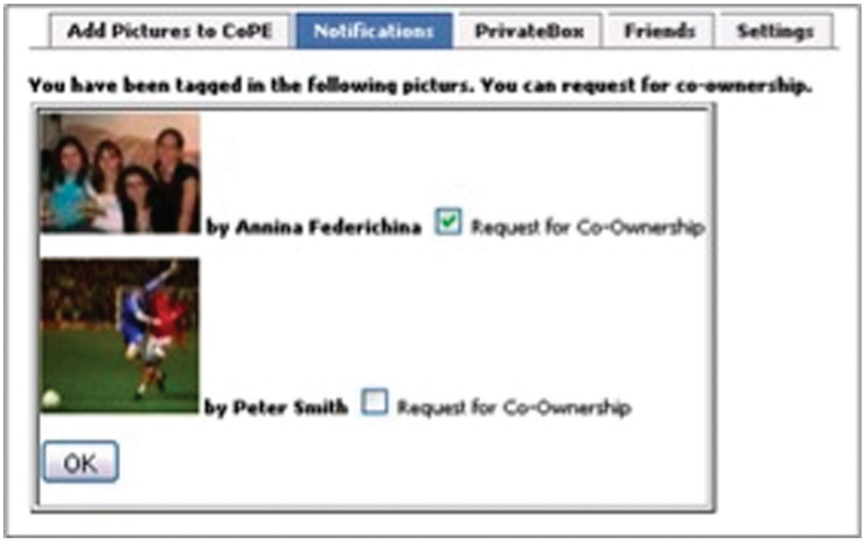
FIG. A1. General privacy settings.



Your friends were tagged in the following pictures. These pictures are added into CoPE.

Tagged: Federica Paci ☑ Invite Federica for Co-Ownership

FIG. A2. Adding a picture to CoPE and inviting a co-owner.

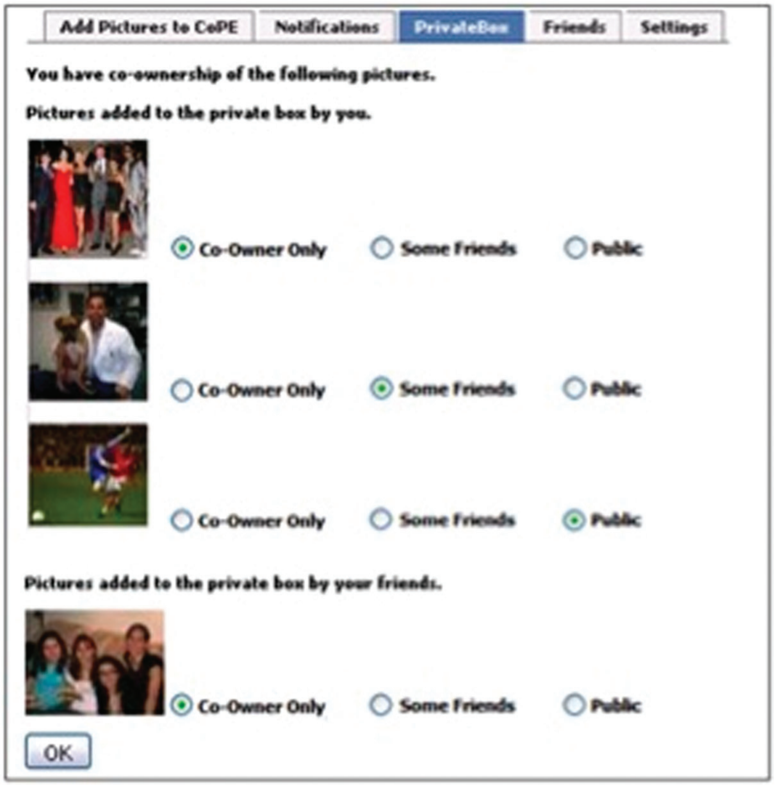


You have been tagged in the following pictures. You can request for co-ownership.

by Annina Federichina ☑ Request for Co-Ownership

by Peter Smith □ Request for Co-Ownership

FIG. A3. Notification of being tagged and request for co-ownership.



You have co-ownership of the following pictures.

Pictures added to the private box by you.

● Co-Owner Only ○ Some Friends ○ Public

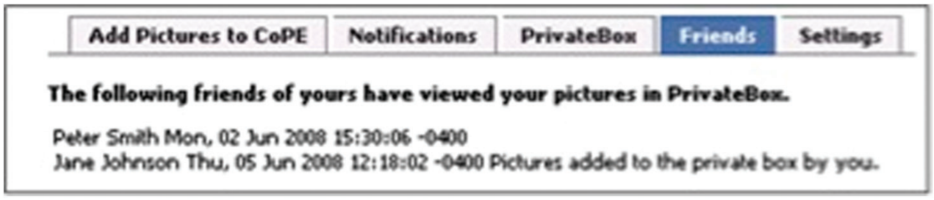
○ Co-Owner Only ● Some Friends ○ Public

○ Co-Owner Only ○ Some Friends ● Public

Pictures added to the private box by your friends.

● Co-Owner Only ○ Some Friends ○ Public

FIG. A4. All pictures added into CoPE and their collaborative privacy policies.



The following friends of yours have viewed your pictures in PrivateBox.

Peter Smith Mon, 02 Jun 2008 15:30:06 -0400
Jane Johnson Thu, 05 Jun 2008 12:18:02 -0400 Pictures added to the private box by you.

FIG. A5. History of picture browsing by friends.