Toward Understanding Preferences for Sharing and Privacy

Judith S. Olson
University of Michigan
550 E. University
Ann Arbor, MI 48109-1092
+1 734 647-4606
jsolson@umich.edu

Jonathan Grudin
Microsoft Research
One Microsoft Way
Redmond, WA 98052-6399
+1 425 706 0784
jgrudin@microsoft.com

Eric Horvitz
Microsoft Research
One Microsoft Way
Redmond, WA 98052-6399
+1 425 706-2127
horvitz@microsoft.com

ABSTRACT
E-commerce has spawned a growing concern and discussion about privacy. Similar concerns about privacy are emerging with ubiquitous computing applications that sense and report one's location and activity. But sharing is as important as privacy; work and social interaction are more efficient when people share some *information* with some *recipients*. Unfortunately, commonly available tools for specifying who can see what have been too complex and tedious for most computer users. We report on studies of preferences about privacy and sharing aimed at identifying fundamental concerns with privacy and at understanding how people might abstract the details of sharing into higher-level *classes* of recipients and information that people tend to treat in a similar manner. To characterize such classes, we collected information about sharing preferences, recruiting 30 people to specify what information they are willing to share with whom. Although people vary in their overall level of comfort in sharing, we discovered key classes of recipients and information. Such abstractions highlight the promise of developing simpler, more expressive controls for sharing and privacy.

Author Keywords
Information sharing, privacy, perceptions of trust

ACM Classification Keywords
H1.2 User/Machine Systems, *human factors;* H.5.2 User Interfaces, *User-centered design.* H.5.3 Group and organizational interfaces, *collaborative computing.* K.4.1. Public policy issues, *Privacy.*

INTRODUCTION
Numerous advancements in technology have generated concerns about violations of privacy. One of the first calls for privacy legislation came in the late 1800's with the invention of rapid photography. People feared that their pictures would be taken without their permission. [20]. As the telephone was introduced into American homes in the 1920s, concerns were lofted that the ringing phone intruded into the private sanctity of the home [9]. Now, with the ubiquity of networked computers in organizations, electronic commerce on the Internet, and the rise of ubiquitous computing applications that hinge on access to such information as where you are and what you are doing, come similar calls.

People fear that they will not have control over who knows what about them [10]. They want to prevent surveillance, theft of personal identity, intrusion of government, minimize embarrassment, protect their turf, and stay in control of their time [14]. People are quite different in how they think about this issue. Some studies have identified broad clusters of preferences, including people who are "privacy fundamentalists," "privacy unconcerned," and "privacy pragmatists" [19,21].

But, typically, people do not want to keep everything private. People will give away information so they don't have to be bothered answering a question. They are surprisingly willing to give away private information both for small amounts of money or privileges or even when talking with an anthropomorphic softbot on the Web. [7, 16].

Also, willingness to share is likely to vary depending on the kind of information and who will see it [4,13]. Willingness to share is also likely to differ depending on whether the information is tied to a particular person (is not anonymous nor aggregated), the kind of information, and the purpose for which it is collected [3]. Information sharing is of immense value in the workplace because it reduces duplication of effort, and sits at the foundations of collaboration. Indeed, a key motivation for digitized content and networked computing is the enablement of efficient sharing and collaboration.

Attitudes toward privacy and willingness to share also vary significantly across cultures and among individuals within a culture. In some cultures, being photographed or telephoned is considered more intrusive than in others. Social conventions establish limits and regulate behavior in public settings and other situations where privacy is limited.

So we are faced with a dilemma: We want, and we need, to have flexible ways to share information, but our comfort levels and overall preferences are sensitive to situations. And such preferences may change over time.

The goal of efficiency is undercut if we must expend significant scarce attentional resources setting up and maintaining access controls. Several ways to control who sees what have been suggested. It is generally acknowledged that it would be unacceptably time consuming to have everyone specify the matrix of all kinds of information, all people, and all purposes [3]. Settings borrowed from similar people could simplify the specification, much like recommender systems [2]. Privacy parameters could be collected for various types of people with whom the information will be shared; this has been called *faces*, or role based access control systems [8,13]. Privacy 'critics' could alert users when they are about to give away information that they normally don't share [1,3]. Others have suggested more optimistic or interactive approaches in some contexts in which the system logs who is looking at what, and the owner notified or asked for access permission [11, 15]. These and other technologies promise to either lower the tediousness of sharing or raise awareness of potential access violations.

Prior to advancing a technical solution, we seek a better understanding of the patterns of preferences in sharing and privacy across a range of material and people. We need to know who the *faces* are, the comfort people have in sharing different information, and what information and which recipients are treated similarly. Only then can we build simpler systems of access control or automate learning and recommending systems. Are there clusters of information, or clusters of people with whom people share information similarly, that could reduce the complexity or serve as the basis for recommended specifications that are satisfying and suitably expressive for large numbers of people?

Our program of research asks several key questions: What are key concerns with privacy? How do people differ, where are they in agreement, what kinds of people and kinds of information do they treat similarly and differently? Can we identify a set of commonly-encountered profiles? Can we derive a small set of questions that provide an indication of someone's preference pattern? Could we provide people with shrewd guesses as to their access choices, which they could then modify relatively quickly? Could we provide interfaces that allow people to make and maintain access control settings in context, when they best know how they feel?

We are not the first to survey people about their privacy concerns. There are periodic surveys of people's attitudes about privacy online and with ubiquitous computing [13, 16, 21]. Considerable work has been done to help consumers understand the consequences of disclosing information online [2]. But typically these studies have focused on situations in which information is disclosed to online retailers, not on the kinds of sharing and privacy that people typically encounter in workplaces or other settings.

We undertook a pilot study and a more formal survey to address these issues, with the intent of finding clusters of information and clusters of people one might share with, to facilitate the specification of one's personal preferences.

OVERVIEW OF THE STUDY

We engaged in a two-phased study. We started with an exploratory phase: We first asked a set of people to relate various instances of when they shared something that they later regretted sharing. We identified all the pieces of information people regretted sharing and the kinds of people with whom they shared that information. This list informed the design of the survey in the second phase of the study.

In the second phase of the study, we took a more systematic approach. Informed by the items generated in the first phase, we chose 40 kinds of information that were shared or not shared with 19 types of people. We asked 30 people from varied backgrounds to rate *each* kind of information as to how comfortable they were in sharing it with *each* kind of person. We presented them with a 40 x 19 grid of people and information, asking them to fill in each cell with a rating of 1-5, indicating comfort with sharing that piece of information with that person, with 1 being "never" and 5 being "always."

We then analyzed these 30 grids. We examined them to see what kinds of information were considered sharable in general and which were not. We sought to identify commonality that could inform key distinctions of a language for specifying settings, and also suggest attractive default settings for privacy. We also looked at the variance across participants, noting which items they agreed upon and which were associated with different opinions. Given a particular set of defaults, which items are most likely to be changed based on the nuances of personal preferences?

As a bottom line, in contrast to the overriding attention that privacy has received in the digital arena, we sought to focus on methods to enable *sharing* by reducing the

complexity of specifying privacy preferences. Before we designed a solution, we required basic information about how people really think about this issue.

METHOD

General survey

To begin exploring the general issue of what kinds of items people are sometimes reluctant to share, we conducted a pilot survey asking respondents to provide examples "of a situation in which you or another person did not wish to share information. Include: 1) A description of the information and situation; 2) Why sharing would have been uncomfortable." We were interested in identifying a broad range of situations, without quantifying them, so we allowed multiple submissions that could include personal or second hand experiences. The on-line survey was distributed to a few hundred usability engineers and researchers at a large software company and the students, faculty and staff at a computer-centric department at a major university. Both organizations were based in the United States.

We obtained 170 examples from 83 people altogether. The responses provided a wide range of situations in which people had either bad experiences or simple qualms about sharing information. As examples of responses, people relayed stories about sharing their early work drafts with people who then thought badly of them for sloppy work. Others shared home phone numbers only to be bombarded with telemarketer calls. People named recipients of information to include family members (*e.g.*, sharing a report of an automobile accident with grandparents who then thought badly of their responsibility) and trusted and competitive co-workers as well as the general public, like telemarketers, a company website or one's personal website. They named information types like personal statistics (*e.g.*, age, Social Security number, salary, marital status) as well as more work-related objects (*e.g.*, working drafts, a complete list of finished work products, the history of their performance reviews), and health related information (*e.g.*,. pregnancy status, and general health issues). And they named information that is stable (*e.g.*, Social Security Number) and information that is dynamic (*e.g.* one's location), and some in between (*e.g.*, one's health status) [12].

The two samples were different, suggesting that we have not exhausted all the possibilities. But the degree of overlap in the responses made us confident that we had captured a good core set. These responses served as the basis for the information items and people to share with that formed the basis for the items in the formal survey.

Assessing Detailed Sharing Preferences

From the set of narrative situations in the first phase survey, augmented with some from our own experiences and work we have done with prototyping various policies for sharing, we chose 40 types of information and 19 types of people. The column and row names in Figure 8 list the types of information and the types of people we asked about.

At the beginning of each session, we had participants fill out a questionnaire covering basic demographics and nine questions from a standard scale measuring basic trust of the world [5]. Then, we gave participants an empty table similar to the one shown in Figure 1 to fill in. They were asked to fill in each cell, indicating on a scale of 1 to 5 how comfortable they would be with sharing each particular type of information with each type of person. They were to instantiate each type of person with someone in their current life, putting an "N/A" in the cells that were inappropriate, either because no such person existed (*e.g.*, "adult child"), or because that kind of information was not part of their life (e.g., "desktop video conferencing number").

Given the potentially daunting size of this questionnaire, we asked people to strike out the rows and columns that did not apply, and to concentrate on the remaining cells one by one, either by rows or columns. People filled out the questionnaire with a mixture of going down columns and across rows, following their own strategy. We made this a paper survey in an effort to make it as easy and speedy as possible for the participants, encouraging them to complete the entire grid. We acknowledge that people's filling out a form such as this is not always correlated with their preferences in situ [16]. However, it is difficult to get such ratings in situ, and we were collecting ratings in a setting similar to what a person would be in when setting preferences a priori.

Our own pilot testing showed that the effort required about an hour and 15 minutes to complete the grid. We recruited participants as if for a usability study to come to the lab for two hours, in groups of 1-6, to fill out the grid and then discuss sharing and privacy issues with us. In turn, they were given the standard gratuity for participants in two-hour user studies at our organization. No participant manifested or reported difficulty in filling out the form, and many reported how interesting it was to consider all these situations.

The participants were people who worked at mid-sized companies and used computers as part of their jobs; they were recruited from a participant panel. Thirty participants filled out the grid. Twenty-one of the 30 were males; 9 females. The median age was 35. Companies ranged from 20 to over 150,000 employees. Their occupations ranged from social worker, CIO, materials manager, real estate, project manager—a wide range. This sample was intended to survey people who had some experience with the idea of sharing information with team-mates, managers, family members and others.

Two participants who missed some items (*e.g.*, leaving a row blank) were re-contacted and asked to complete the items. Of the 30 grids of nearly 800 cells each, we ended up with only about 20 blank cells.

Analysis

From the individual grids of ratings, we created several summaries. We computed the mean ratings over all 30 participants as well as the standard deviations of these values. See Figures 7 and 8. Items that were left blank or marked as "N/A" were considered to be blanks. Although this assumption created an imbalance in the number of respondents for some items, this seemed the best way to glean insights from the data.

To facilitate visualization, the columns and rows were ordered left-to-right and top-down from lowest (least likely to be shared) to highest (most likely), and color coded to reveal the bands of opinions (here printed in black and white). Dark gray cells indicate the least likely to be shared; white the most likely to be shared, with light gray indicating the ambiguous middle. We created a visualization for each participant as well as one for the average for the whole group.

As we have been interested in how information items and people with whom to share clustered, we separately performed a hierarchical cluster analysis on the rows and then on the columns. This analysis uses a Euclidean distance metric to asses the similarity of pairs of rows (or columns). The more alike the items are rated across the rows (or columns), the closer they are in the hierarchy. The hierarchy thus shows items that cluster, with those coming together near the leaves of the tree being more similar than those joining the cluster closer to the root [6]. Note that this does not illustrate whether or not items are shared, just how similarly they were treated by the participants.

We did two hierarchical cluster analyses for each of the 30 participants' ratings, one for the information items and one for the people with whom they would or would not share. Then we performed two cluster analyses on the averages, again one for the information and one for the people. Future plans include cluster analyses of the participants themselves, using as a similarity measure the Euclidean distance of all of the items in their matrices.

Our analysis began with a Principal Component Analysis to determine how many clusters were appropriate given the data we had collected. For the *information items*, the first three components covered 94% of the variance. For the *people these items were to be shared with*, the first three components covered 95% of the variance. However, since some of the clusters were large and others small, we expanded the number of clusters of *information items* to be six, and *the people these items were to be shared with* to five. In addition, this clustering was informed by performing the cluster analyses using five methods for joining items to clusters: Average, single, complete, centroid, and Ward. A surprising number of clusters were the same in all solutions. We identified the more fine grained clusters (the three more in the information item hierarchies and two more in the people hierarchy) from the differences in the solutions from the different methods. [Corter,1996] Later, we looked at the average variance within the clusters and found the small standard deviation (0.32) to be consistent with a discovery of stable categories.

RESULTS

Overall ratings

The matrix of the average data is displayed in Figure 7[1]. Of note is the large dark region in the upper left-hand corner and the somewhat smaller white region in the lower right hand corner. From the items and people we asked participants to rate, they were more likely to want to keep information private than to share. The overall average rating was 2.82 (from 1 to 5), with the average standard deviation at 1.46. Not surprisingly, we found that the participants in our study do not want a transgression made public or their email to be widely shared, whereas most participants are comfortable with people seeing their work email address and desk phone number.

Figure 8 shows the same table with the standard deviations, showing which items participants agreed on and which ones not. We found that some of the ratings had very low (even zero) variance across participants, and others were quite variable. The following items had zero variance:

- Always sharing one's work email and work phone number with one's spouse and coworkers
- Always sharing one's home phone number with one's spouse and children (but not always with co-workers)
- Never giving the credit card number to the public.

The highest variance (std>1.5) centered around various personal items being shared with co-workers, including sharing one's age with a competitor, one's pregnancy status with other team members and one's marital status in a company newsletter. Other high-variance items centered on sharing one's credit card number with one's parents or grandparents, and one's pregnancy status with

[1]The matrices of results can be found at the end of the paper.

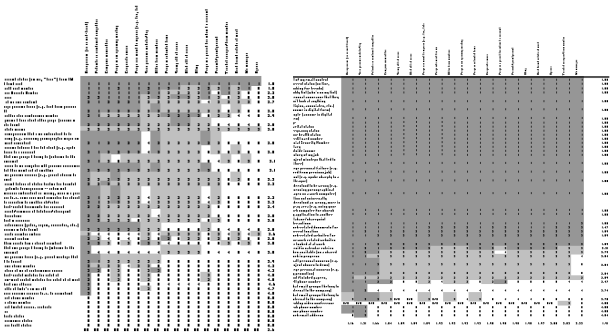

Figure 1. Individual variation among ratings. The preferences of the participant on the left reflects the highest overall willingness to share with others, the one on the right the least willingness.

a sibling. Overall, the most disagreement came in rating one's personal statistics, with more disagreement about sharing them with coworkers than with family members. Similar high variance appeared in the ratings of work-related documents with family members, perhaps reflecting judgments of appropriateness (*i.e.*, they wouldn't care to see them) rather than a desire to exclude.

Figure 1 shows some of the individual variation in thumbnails. On the left is the "privacy unconcerned" [16] participant who prefers to share the most. On the right is the "privacy fundamentalist" who likes to share the least. Figure 2 shows two participants who are in the middle, with the participant on the left having much more certainty than the one on the right—segmenting participants we affectionately call "everything is black and white" people from participants we refer to as "everything is gray." The person on the right is likely a "privacy pragmatist." [19]

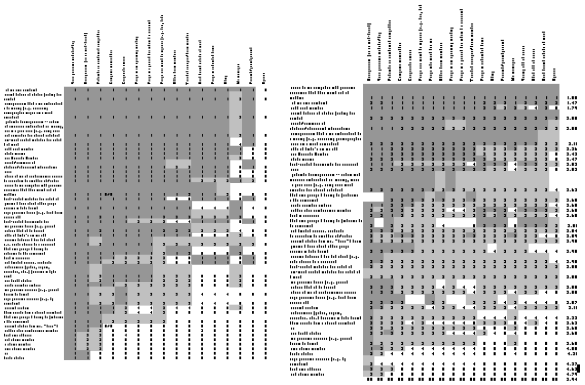

Figure 2. Preferences of the participant on the left have the highest variance, suggesting the most "black and white;" the ones on the right the lowest variance, with many "gray" areas.

Figure 3 shows the distribution of average ratings of the 30 participants, indicating their overall willingness to share. The averages go from 1.89, a "privacy fundamentalist," to 3.69, a "privacy unconcerned," with the majority hovering around the mean rating (3) being "privacy pragmatists" [19,21].

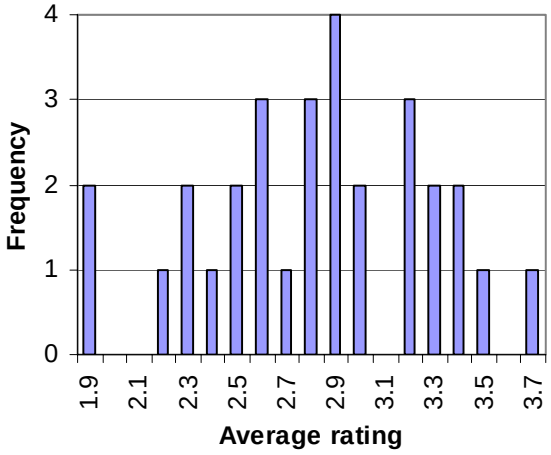

Figure 3. A frequency distribution of people's average willingness to share, from the "privacy fundamentalist" on the left to the "privacy unconcerned" on the right.

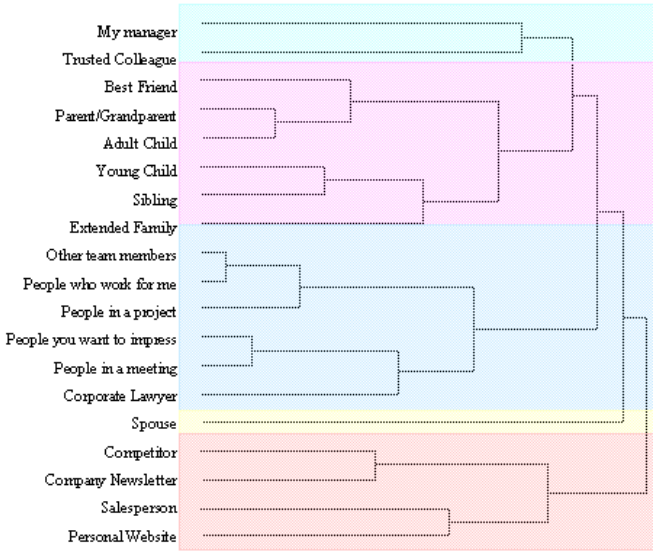

Figure 4. Clusters of people who participants treated similarly

Figures 4 and 5 display the results of the hierarchical cluster analysis of average ratings for people and information items, respectively. These clusters are relatively straightforward to label. People cluster into:

- The public (websites, telemarketers) and a competitor

- Coworkers, including the corporate lawyer
- Your manager and a trusted co-worker
- Your family
- Your spouse

Of interest in this analysis is how far out the manager and trusted coworker join the work-life cluster, and how far out the spouse joins the family cluster, indicating that they are treated unlike the others. However, we found that managers and spouses are not similar to each other. We conjectured that this result may be based in managers having access to some information (*e.g.,* the participants' salary) *ex officio*, whereas a spouse has information based on a trusted partnership.

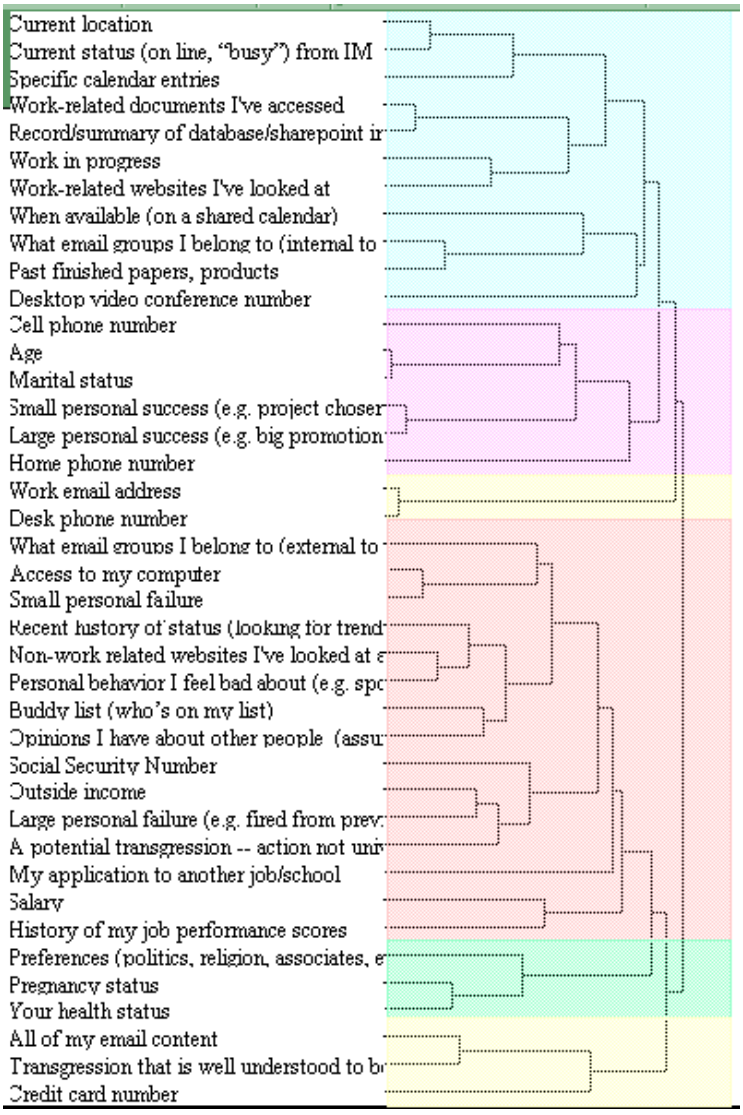

Figure 5. Clusters of the kinds of information people treat similarly when they assess with whom to share it.

The information items also clustered into crisp categories:

- Access to all your email content, your credit card number, and a transgression.
- Failures, opinions, salary and outside income, Social Security Number
- Home and cell number, age and marital status, and successes
- Pregnancy, health and preferences (religious, politics)
- Work related documents, websites, availability.
- Work email and desk phone number

Patterns of Sharing

Figure 6 shows a summary of how participants rated their willingness to share various classes of information with the major classes of people. The items on the x-axis are ordered from the average highest to the lowest willingness to share.

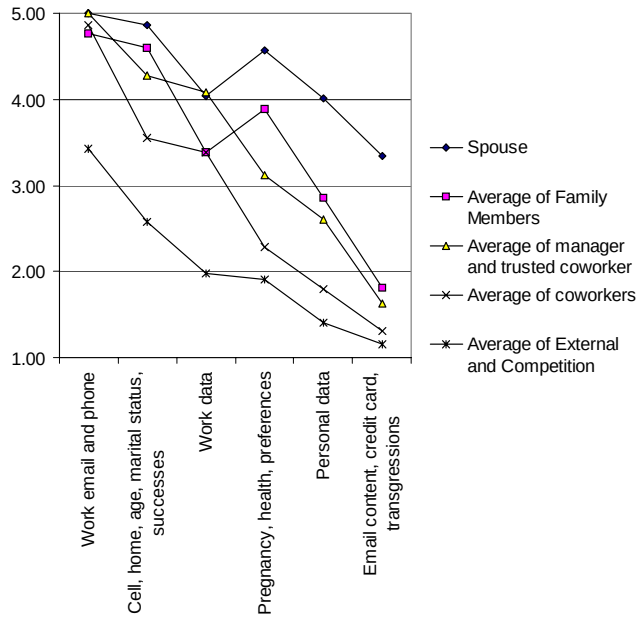

Figure 6. How participants rated willingness to share for various categories of people and information.

Overall, participants in our study were unwilling to share most things with the public (the low line at the bottom). Not everyone is comfortable sharing everything with their spouse. (The top line is not uniformly rated "5"). The pattern of information our participants are willing to share with their managers and trusted co-workers tracks those that they are willing to share with their families, except that work-related items are rated higher.

Our original intent was to relate willingness to share with a number of other demographic variables, such as age,

gender, and overall trust of the world, measured by a standard trust scale. Although interesting patterns emerged, none were statistically significant. We plan to take this data collection out to a much larger, more diverse population. Such a study will be facilitated by our ability to construct a much shorter survey, based on the clusters we have found for information types and types of people with whom to potentially share the items.

DISCUSSION

We believe that the results of the study are significant in several ways. Like Ackerman et al. [2], we find that people differ in their willingness to share. A one-size permissions structure does not fit all. Furthermore, one policy for a piece of information does not fit all. Peoples' willingness to share depends on who they are sharing the information with. However, specifying one's preferences does not have to be as complicated as filling out an 800-item form.

We found that participants' information items clustered into a manageable set of categories, and most peoples' view of others they wish to share this information with is similarly clustered into a manageable set of categories. This finding can provide guidance to the design of access controls and interfaces, that could make specification easier for the end user. If people wish to make finer grained distinctions, there is promise in creating designs for specifying preferences that open up further choices in a hierarchical scheme, to the level of precision that they feel comfortable with in granting information access to others.

For example, a preference-specification tool could allow users to specify in general their permissions per category of person (*e.g.*, the public, high level people in your organization, co-workers, your family, your manager, your spouse, etc.), but make an exception for one particular person or a particular information type.

Similar to the idea of an agent with such specifications, with some content analysis, a system might be able to detect your email address, SSN, or personal facts in the document, setting automatically the appropriate permissions. When people ask to access a file, the permission scheme could assess who they are, and then either grant or deny access.

Others [5, 8] have explored less extreme schemes for access that could be set with these abstractions of people and information. For example, rather than simply granting or denying access, additional sharing actions could be provided. Such additional actions could, for example, include a policy of informing the person requesting access, at the time of an attempted access, that there is an audit trail of accesses—and then logging the accesses for the owner's later review.

Another potential policy, giving users moment-by-moment control, is to provide selected groups of people with a mechanism for easily requesting permission to access information of specified types. This would accommodate changes in willingness to share without requiring changes to global settings.

Beyond direct specification, there is opportunity to leverage the type of data we collected in our study within statistical recommender systems. Such systems can be viewed as performing dynamic cluster analysis of users based on a partial specification of preferences. Such systems could be deployed with the goal of providing guesses about sets of preferences with regards to sharing on a people and items bases, and then allow users to refine the guesses.

SUMMARY

Our intent has been to broaden the discussion of personal information sharing by balancing the very real privacy concerns engendered by the growing ease of recording and distributing status information with the equally real benefits of controlled sharing of such information. The benefits of sharing led to the embrace of digital technologies. Concerns for security and privacy are a understandable, but can limit valuable sharing and collaboration. If we do not make the benefits as explicit as the drawbacks, the pendulum could swing too far. We have reported on studies aimed at identifying attitudes about privacy and sharing. We believe that this research and follow-on studies will serve to inform designs for efficient languages and tools that allow users to specify, and refine over time, what they wish to share with whom.

ACKNOWLEDGMENTS

This research was conducted while the first author was a Visiting Researcher at and supported by Microsoft Research. We thank Ed Cutrell and Cory Knobel for assisting with data analysis. This research was partly supported by the National Science Foundation grant IIS 0308009.

REFERENCES

1. Ackerman, M. S. (2000). Developing for privacy: Civility frameworks and technical design. *Proc. ACM Conference for Computers, Freedom, and Privacy*, 19-23.
2. Ackerman, M. S. and Cranor, L. F. (1999). Privacy Critics: UI components to safeguard users' privacy. *CHI'99 Extended Abstracts*, 258-259.
3. Ackerman, M. S., Cranor, L. F., and Reagle, J. (1999). Privacy in e-commerce: Examining user scenarios and privacy preferences. *Proc. ACM Conference on Electronic Commerce*, 1-8.
4. Bellotti, V., and Sellen, A. (1993). Design for privacy in ubiquitous computing environments. *ECSCW.*
5. Butler, J. K. (1991).. Toward understanding and measuring conditions of trust: Evolution of a

conditions of trust inventory. *Journal of Management, 17,* 643-663.

6. Corter, J. E. (1996) *Tree models of similarity and association.* Thousand Oaks, CA: Sage University Paper.
7. Hann, I-H., Hui, K.-L., Lee, T.S. & Png, I.P.L. (2002). Online information privacy: Measuring the cost-benefit tradeoff. Proc. 23rd International Conference on Information Systems.
8. Ferraiolo, D., Duginin, J. A., and Kuhn, D. R. (1995). Role based access control (RBAC): Features and motivation. *11th Annual Computer Security Applications Conference.*
9. Fischer, C. (1992). America Calling: A Social History of the Telephone to 1940. Berkeley: University of California Press.
10. Fox, S. Rainie, L., Horrigan, J., Lenhart, A., Spooner, T., and Carter, C. (2000). Trust and privacy online: Why Americans want to rewrite the rules. *The Pew Internet and American Life Project.*

    http://www.pewinternet.org/pdfs/PIP_Trust_Privacy_Report.pdf
11. Jiang, X., Hong, J. I., and Landy, J. A. (2002). Approximate information flows: Socially based modeling of privacy in ubiquitous computing. *Ubicomp.*
12. Lederer, S., Beckmann, C., Dey, A., and Mankoff, J. (2003). Managing personal information disclosure in ubiquitous computing environments. *Intel Research Berkeley Technical Report 03-015.*
13. Lederer, S., Dey, A. K., Mankoff, J. (2003). Who wants to know what when? Privacy preference determinants in ubiquitous computing *CY* 2003 Shortpapers.* 724-725.
14. Palen, L., and Dourish, P. (2003). Unpacking privacy for a networked world. *CHI 03.*
15. Povey, D. (1999). Optimistic security: A new access control paradigm. *Proc. ACM New Security Paradigms Workshop,* 40-45.
16. Spiekermann, S., Grossklags, J., and Berendt, B. (2001). E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behavior. *ACM Conference on Electronic Commerce (EC-01).* ACM Press, NY.
17. Stevens, G.and Wulf, V. (2002). A new dimension in access control: Studying maintenance engineering across organizational boundaries. *Proc. CSCW 2002,* 196-205.
18. Stiemerling. O., and Wulf, V. (2000) Beyond 'yes or no'—Extending access control in groupware with awareness and negotiation. *Group Decision and Negotiation, 9,* 221=235.
19. Taylor, H. (2003). Most people are 'privacy pragmatists' who, while concerned about privacy, will sometimes trade it off for other benefits. *Harris Interactive.* http://www.harrisinteractive.com/harris_poll/index.asp?PID=365.
20. Warren, and Brandeis. (1890). The Right to Privacy. *Harvard Law Review, IV(5).*
21. Westin, A. F. (1998). *E-commerce & Privacy: What Net Users Want.* Hackensack, NJ: Privacy & American Business.

    Economics of privacy resource page: http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm

	Salesperson (live or web-based)	Your personal website/blog	Potential or confirmed competitor	Company newsletter	People in an upcoming meeting	People you want to impress (e.g. hire, date)	Corporate lawyer	People in a project for whom it is relevant	People who work for me	Other team members	People in extended family	Young child of yours	Trusted colleague/team member	Sibling	My manager	Adult child of yours	Parent/grandparent	Best friend outside of work	Spouse	Average	Standard Deviation
Transgression that is well understood to be wrong (e.g. accessing pornographical images on a work computer)	1.07	1.50	1.04	1.16	1.17	1.10	1.32	1.23	1.26	1.20	1.34	1.63	1.57	1.61	1.60	1.79	1.82	2.17	2.55	1.48	0.40
All of my email content	1.07	1.17	1.11	1.20	1.30	1.24	1.64	1.50	1.47	1.43	1.66	1.94	1.73	1.68	2.00	1.57	1.89	2.00	3.10	1.62	0.47
Credit card number	1.57	1.06	1.00	1.00	1.10	1.10	1.40	1.17	1.40	1.27	1.59	1.59	1.43	1.75	1.47	2.43	2.32	1.83	4.38	1.62	0.78
Social Security Number	1.30	1.06	1.14	1.08	1.17	1.38	1.80	1.31	1.60	1.47	2.07	2.18	1.80	2.61	2.67	3.14	3.41	2.17	4.45	1.99	0.92
A potential transgression -- action not universally understood as wrong, more in a gray area (e.g. using your work computer for church activities)	1.10	1.61	1.14	1.36	1.33	1.41	1.68	1.67	1.65	1.80	1.97	2.12	2.30	2.46	2.40	2.93	2.68	2.90	3.69	2.01	0.70
Outside income	1.48	1.37	1.19	1.21	1.34	1.46	1.79	1.43	1.63	1.52	2.25	2.25	1.76	2.59	1.83	3.14	3.26	2.97	4.36	2.04	0.86
Salary	1.41	1.28	1.18	1.16	1.17	1.46	2.16	1.17	1.39	1.48	2.07	2.06	2.14	2.52	4.00	2.62	3.11	2.66	4.39	2.08	0.96
Large personal failure (e.g. fired from previous job)	1.30	1.50	1.25	1.24	1.48	1.46	1.88	1.62	1.58	1.80	2.21	2.59	2.33	2.79	2.47	3.00	3.29	3.33	4.21	2.17	0.85
Personal behavior I feel bad about (e.g. spoke sharply to a colleague)	1.17	1.56	1.36	1.56	1.70	1.62	2.00	2.00	2.05	2.27	2.28	2.35	2.73	2.68	2.77	2.79	2.89	3.13	3.79	2.25	0.68
Buddy list (who's on my list)	1.32	1.25	1.55	1.61	1.62	1.70	1.72	1.67	1.93	2.05	2.57	3.21	2.19	3.05	2.33	3.22	3.19	3.10	3.50	2.25	0.75
Non-work related websites I've looked at at work	1.24	1.67	1.57	1.56	1.80	1.83	1.92	1.93	1.79	2.20	2.64	2.76	2.60	2.70	2.60	3.08	2.74	3.17	3.71	2.29	0.66
Recent history of status (looking for trends)	1.57	1.41	1.62	1.85	2.05	2.05	1.90	2.14	2.13	2.27	2.32	2.87	2.59	2.60	2.73	2.80	2.62	2.68	3.38	2.29	0.51
History of my job performance scores	1.17	1.29	1.39	1.68	1.53	2.03	2.24	1.80	1.74	1.83	2.28	2.59	2.40	2.96	4.17	3.00	3.07	2.97	4.10	2.33	0.87
Opinions I have about other people (assume in digital form)	1.43	1.67	1.46	1.56	1.73	1.79	1.56	1.90	1.89	2.03	2.79	2.53	2.50	3.11	2.37	3.43	3.29	3.50	3.97	2.34	0.79
My application to another job/school	1.33	1.61	1.25	1.44	1.43	1.76	1.52	1.63	1.58	1.67	2.93	2.71	2.30	3.50	1.97	3.71	3.79	3.80	4.62	2.34	1.06
Access to my computer with personal assurance that they won't look at anything	1.20	1.19	1.29	1.32	1.57	1.69	1.88	1.93	2.53	2.40	2.54	2.71	3.23	2.81	3.37	3.15	3.22	3.14	3.82	2.37	0.84
Small personal failure (e.g. project missteps that led to failure)	1.30	1.50	1.29	1.48	1.73	2.00	2.08	2.07	2.47	2.43	2.59	2.76	3.03	3.07	3.33	3.21	3.36	3.47	4.03	2.48	0.82
What email groups I belong to (external to the company)	1.50	1.71	1.59	1.92	2.21	2.21	2.08	2.32	2.29	2.28	2.70	3.00	2.62	3.11	2.62	3.27	3.42	3.59	4.11	2.56	0.71
Record/summary of database/sharepoint interactions	1.29	1.29	1.76	1.91	2.73	2.60	2.59	3.00	3.17	3.31	2.59	2.87	3.85	2.90	3.96	2.90	2.95	2.91	3.77	2.76	0.76
Preferences (politics, religion, associates, etc.) (assume in digital form)	1.70	2.33	1.79	1.72	1.77	2.38	1.84	2.10	2.32	2.33	3.66	3.65	2.90	4.00	2.57	4.07	4.11	4.27	4.52	2.84	1.00
Work-related documents I've accessed	1.29	1.18	1.79	2.04	2.83	2.76	2.92	3.03	3.42	3.53	2.56	2.94	4.20	2.71	4.23	2.91	3.00	3.08	3.76	2.85	0.84
Your health status	1.50	1.78	1.96	2.12	2.17	2.24	2.36	2.30	2.50	2.57	3.41	3.47	3.23	3.57	3.10	3.93	3.93	4.03	4.55	2.88	0.88
Specific calendar entries	1.52	1.78	2.00	2.17	3.07	2.59	2.54	3.17	3.16	3.17	3.08	3.40	3.48	3.36	3.62	3.38	3.40	3.56	4.18	2.98	0.70
Pregnancy status	1.87	2.11	2.00	2.07	2.27	2.29	2.40	2.33	2.22	2.73	3.73	4.13	3.53	3.79	3.40	3.83	4.00	4.20	4.64	3.03	0.92
Work in progress	1.32	1.67	1.67	2.16	3.21	3.07	2.96	3.76	3.67	3.72	2.89	3.50	4.21	2.92	4.31	3.17	3.08	3.14	3.78	3.06	0.84
Desktop video conference number	1.29	1.83	2.50	3.17	3.83	3.20	3.50	4.33	3.33	3.83	3.00	2.75	3.71	3.20	4.29	2.00	3.33	3.17	3.83	3.16	0.81
Work-related websites I've looked at	1.41	1.72	2.00	2.52	3.20	3.03	3.16	3.60	3.26	3.70	3.39	3.53	4.13	3.33	4.23	3.62	3.37	3.48	4.00	3.19	0.77
Current location	1.63	1.94	2.11	2.25	3.07	3.07	2.76	3.73	3.26	3.37	3.41	4.06	3.77	3.75	3.70	3.64	3.79	3.83	4.31	3.23	0.76
Current status (on line, "busy") from IM	1.78	1.82	2.33	2.24	3.18	3.05	2.58	3.45	3.47	3.45	3.77	4.07	3.55	4.05	3.50	3.78	3.86	3.91	4.19	3.27	0.76
Past finished papers, products	1.55	2.61	2.43	3.24	3.63	3.59	3.64	3.93	3.79	4.13	3.25	3.47	4.43	3.26	4.60	3.31	3.48	3.48	4.00	3.46	0.71
What email groups I belong to (internal to the company)	1.45	1.81	2.43	3.32	3.69	3.52	3.76	3.97	4.11	4.33	3.19	3.38	4.63	3.52	4.63	3.58	3.64	3.78	4.08	3.52	0.84
Small personal success (e.g. project chosen to demo)	1.87	2.50	2.89	3.16	3.23	3.45	3.24	3.47	3.65	3.53	3.72	4.12	4.00	4.07	4.30	4.29	4.25	4.30	4.76	3.62	0.71
When available (on a shared calendar)	1.67	2.00	2.30	2.61	4.10	3.39	3.29	4.24	4.21	4.07	3.69	4.13	4.38	4.12	4.38	4.00	4.04	4.22	4.59	3.65	0.88
Home phone number	1.55	1.47	2.07	2.25	2.76	3.32	3.17	3.31	3.44	3.59	4.75	5.00	4.45	4.96	4.59	5.00	4.96	4.93	5.00	3.71	1.25
Large personal success (e.g. big promotion)	1.90	2.67	2.96	3.24	3.40	3.62	3.36	3.60	3.85	3.73	3.90	4.24	4.17	4.29	4.43	4.50	4.50	4.43	4.83	3.77	0.74
Age	2.57	2.89	3.00	3.20	3.30	3.24	3.60	3.47	3.95	3.90	4.76	4.65	4.00	4.82	4.07	4.71	4.68	4.63	4.83	3.91	0.75
Marital status	2.60	2.83	3.11	3.12	3.37	3.41	3.48	3.67	3.85	3.97	4.72	4.76	4.17	4.79	4.13	4.71	4.82	4.83	4.83	3.96	0.76
Cell phone number	1.78	2.00	3.00	3.22	3.77	3.84	3.86	3.92	3.50	4.15	4.44	4.80	4.48	4.79	4.41	4.83	4.75	4.81	4.92	3.96	0.93
Desk phone number	2.57	2.28	4.26	4.67	4.76	4.50	4.92	4.90	5.00	4.97	4.32	4.81	5.00	4.74	5.00	5.00	4.93	4.83	5.00	4.55	0.78
Work email address	2.37	2.56	4.21	4.56	4.87	4.62	4.96	4.87	5.00	5.00	4.66	4.65	5.00	4.79	5.00	4.79	4.81	4.97	5.00	4.56	0.77
Average	1.55	1.76	1.95	2.16	2.49	2.50	2.59	2.72	2.76	2.86	3.04	3.25	3.26	3.33	3.43	3.46	3.53	3.53	4.19	2.86	0.79
Standard Deviation	0.42	0.45	0.72	0.79	0.67	0.55	0.73	0.58	0.61	0.59	0.63	0.57	0.50	0.60	0.49	0.61	0.55	0.53	0.37	0.47	0.14

Figure 7. Overall mean ratings of comfort in sharing various kinds of information with various kinds of people. 1=Never, 5=Always. Dark gray are low ratings, white are high.

	Salesperson (live or web-based)	Other team members	Your personal website/blog	Potential or confirmed competitor	People in an upcoming meeting	People who work for me	People you want to impress (e.g. hire, date)	People in a project for whom it is relevant	Trusted colleague/team member	Company newsletter	Spouse	Adult child of yours	My manager	Best friend outside of work	Sibling	People in extended family	Parent/grandparent	Young child of yours	Corporate lawyer	Average standard deviation
Work email address	1.16	0.00	1.38	1.20	0.43	0.00	0.78	0.43	0.00	1.00	0.00	0.58	0.00	0.18	0.50	0.72	0.56	0.86	0.20	0.53
Desk phone number	1.48	0.19	1.53	1.02	0.79	0.00	0.84	0.41	0.00	0.96	0.00	0.00	0.00	0.54	0.53	0.94	0.27	0.75	0.41	0.56
Transgression that is well understood to be wrong (e.g. accessing pornographical images on a work computer)	0.25	0.48	0.92	0.19	0.46	0.56	0.31	0.57	0.97	0.47	1.45	0.80	1.10	1.21	0.79	0.61	0.86	0.72	0.75	0.71
Credit card number	0.97	0.64	0.24	0.00	0.31	0.75	0.31	0.46	1.01	0.00	1.32	1.34	1.01	1.23	1.04	0.91	1.56	1.00	1.04	0.80
Home phone number	0.91	1.12	0.80	1.21	1.24	1.20	1.47	1.34	0.99	1.42	0.00	0.00	0.91	0.26	0.19	0.84	0.19	0.00	1.55	0.82
Large personal failure (e.g. fired from previous job)	0.53	0.66	0.79	0.44	0.63	0.61	0.58	0.78	1.06	0.44	1.08	0.96	1.14	1.03	0.99	0.90	1.21	1.33	1.15	0.86
A potential transgression -- action not universally understood as wrong, more in a gray area (e.g. using your work computer for church activities)	0.31	0.76	0.98	0.36	0.55	0.67	0.57	0.96	1.06	0.81	1.31	1.14	1.19	1.27	0.96	0.87	1.19	1.11	0.95	0.89
All of my email content	0.25	0.77	0.51	0.31	0.70	0.70	0.64	0.94	1.08	0.50	1.72	1.02	1.26	1.11	1.16	1.04	1.20	1.03	1.11	0.90
Salary	0.68	0.78	0.57	0.39	0.47	0.78	0.69	0.47	1.19	0.37	1.23	1.04	1.49	1.17	1.12	0.98	1.37	1.25	1.49	0.92
When available (on a shared calendar)	1.00	0.80	1.03	1.27	0.82	0.71	0.92	0.74	0.82	1.31	0.69	0.91	0.78	0.80	1.01	1.01	1.06	0.83	1.27	0.94
Outside income	0.78	0.78	0.68	0.48	0.61	0.83	0.79	0.74	0.87	0.51	1.16	0.95	1.23	1.30	1.25	1.14	1.35	1.13	1.38	0.95
Small personal failure (e.g. project missteps that led to failure)	0.53	0.86	0.79	0.53	0.87	0.84	0.89	1.17	1.03	0.71	1.05	1.19	1.15	0.97	0.98	1.15	1.13	1.39	1.22	0.97
Personal behavior I feel bad about (e.g. spoke sharply to a colleague)	0.38	0.87	0.98	0.68	0.75	0.91	0.82	1.05	1.14	0.82	1.21	0.89	1.19	1.07	1.16	1.10	1.13	1.27	1.12	0.98
Opinions I have about other people (assume in digital form)	0.73	0.93	0.91	0.64	0.83	0.94	0.82	0.92	1.17	0.77	1.32	1.09	1.13	1.22	1.23	1.18	1.44	1.18	0.87	1.02
My application to another job/school	0.66	0.84	0.98	0.59	0.73	0.96	1.02	1.07	1.21	0.77	0.94	1.27	1.30	1.30	1.17	1.19	1.17	1.36	0.87	1.02
Current location	0.76	1.00	1.00	1.13	1.07	0.99	0.92	0.98	1.04	1.22	0.97	0.93	0.99	0.99	1.08	1.18	0.99	1.09	1.39	1.04
Social Security Number	0.70	0.86	0.24	0.45	0.54	0.94	0.82	0.76	1.21	0.28	1.27	1.35	1.69	1.42	1.52	1.25	1.70	1.42	1.35	1.04
Cell phone number	1.12	1.16	1.22	1.38	1.37	1.46	1.34	1.35	0.94	1.59	0.40	0.58	1.12	0.49	0.51	1.00	0.74	0.77	1.46	1.05
Preferences (politics, religion, associates, etc.) (assume in digital form)	0.88	1.03	1.28	0.83	0.90	1.25	1.24	1.03	0.99	1.02	0.91	1.14	1.17	0.94	1.15	1.23	1.03	1.46	1.14	1.09
Work in progress	0.48	0.88	0.84	0.92	0.77	0.84	0.94	0.74	0.77	1.07	1.42	1.40	0.71	1.46	1.49	1.45	1.57	1.59	1.33	1.09
Specific calendar entries	0.94	0.93	1.11	1.04	1.22	1.12	1.05	1.23	1.06	1.34	1.02	0.96	0.98	1.01	1.08	0.93	1.15	1.24	1.32	1.09
History of my job performance scores	0.38	0.83	0.59	0.79	0.86	0.87	1.24	1.10	1.22	1.14	1.35	1.36	1.09	1.25	1.32	1.07	1.30	1.42	1.59	1.09
Non-work related websites I've lookec	0.58	1.10	0.91	1.00	1.03	0.79	0.97	1.01	1.19	1.00	1.21	1.19	1.28	1.17	1.23	1.22	1.26	1.30	1.32	1.09
Large personal success (e.g. big promotion)	1.24	1.08	1.57	1.26	1.38	1.14	1.18	1.28	0.91	1.48	0.47	0.76	0.82	0.82	0.85	1.29	0.84	0.97	1.58	1.10
Small personal success (e.g. project chosen to demo)	1.20	0.97	1.38	1.31	1.33	1.23	1.24	1.22	0.95	1.43	0.51	0.83	0.88	0.84	0.94	1.25	1.04	0.99	1.56	1.11
What email groups I belong to (internal	0.87	0.92	1.22	1.53	1.17	1.10	1.27	1.21	0.61	1.57	1.02	1.31	0.72	1.28	1.45	1.36	1.29	1.41	1.16	1.18
What email groups I belong to (externa	0.96	1.10	0.85	0.93	1.35	1.31	1.03	1.36	1.29	1.26	1.07	1.42	1.21	1.21	1.28	1.23	1.27	1.11	1.50	1.20
Past finished papers, products	0.95	0.82	1.33	1.40	0.81	0.92	1.18	0.87	0.82	1.30	1.28	1.38	0.72	1.40	1.58	1.53	1.53	1.59	1.38	1.20
Desktop video conference number	0.49	1.33	0.98	1.52	1.17	1.53	1.10	1.21	1.25	1.47	1.33	0.00	1.11	1.17	1.64	1.55	1.37	1.50	1.22	1.21
Your health status	0.94	1.19	1.26	1.26	1.18	1.32	1.24	1.15	1.14	1.27	0.95	1.07	1.30	1.03	1.23	1.24	1.15	1.46	1.58	1.21
Access to my computer with personal assurance that they won't look at anything	0.48	1.33	0.54	0.60	0.86	1.58	0.89	0.96	1.57	0.78	1.61	1.52	1.56	1.51	1.30	1.32	1.60	1.61	1.39	1.21
Work-related documents I've accessed	0.46	1.11	0.53	1.13	1.14	1.35	1.21	1.25	1.10	1.27	1.45	1.58	1.10	1.52	1.57	1.42	1.67	1.57	1.47	1.26
Buddy list (who's on my list)	0.89	1.16	0.68	1.10	1.12	1.00	1.17	1.15	1.25	1.20	1.67	1.48	1.24	1.48	1.54	1.47	1.66	1.53	1.18	1.26
Record/summary of database/sharepoir	0.46	1.23	0.59	1.13	1.19	1.25	1.22	1.30	1.32	1.16	1.48	1.45	1.28	1.50	1.55	1.44	1.62	1.60	1.37	1.27
Age	1.57	1.27	1.53	1.74	1.51	1.39	1.53	1.46	1.29	1.63	0.76	1.07	1.31	0.93	0.77	0.83	0.90	1.06	1.58	1.27
Marital status	1.67	1.19	1.65	1.66	1.65	1.42	1.55	1.49	1.21	1.79	0.76	1.07	1.25	0.75	0.79	0.84	0.77	0.97	1.69	1.27
Work-related websites I've looked at	0.68	1.12	0.89	1.36	1.24	1.28	1.40	1.19	1.17	1.39	1.36	1.33	1.14	1.43	1.47	1.47	1.60	1.62	1.60	1.30
Current status (on line, "busy") from IM	1.28	1.26	1.13	1.43	1.40	1.06	1.32	1.30	1.41	1.35	1.25	1.72	1.47	1.23	1.28	1.23	1.28	1.44	1.57	1.34
Recent history of status (looking for tre	1.16	1.24	0.71	1.16	1.21	1.09	1.24	1.36	1.53	1.18	1.63	1.62	1.58	1.49	1.50	1.46	1.47	1.68	1.37	1.35
Pregnancy status	1.46	1.71	1.54	1.47	1.44	1.86	1.54	1.50	1.68	1.59	1.08	1.60	1.68	1.32	1.72	1.62	1.41	1.64	1.76	1.56
	0.83	0.96	0.97	0.97	0.98	1.01	1.03	1.04	1.06	1.07	1.07	1.08	1.11	1.11	1.15	1.16	1.20	1.23	1.28	1.07

Figure 8. The standard deviations of the items in Figure 7, columns and rows ranked from low to high standard deviations. Gray cells indicate that the standard deviations are high.