Mine, Yours and Ours: Using Shared Folders in Personal Information Management

Hong Zhang
School of Library and
Information Science
University of Kentucky
hong.zhang@uky.edu

Michael Twidale
Graduate School of Library &
Information Science
University of Illinois
twidale@illinois.edu

ABSTRACT

A small pilot study reveals the complexities in the way people think about and use shared folders and how these folders interact with their personal information spaces.

Keywords

Shared folders, personal information management

1. INTRODUCTION

Shared folders are usually seen as separate information storage places for sharing purpose. Different from many group information systems, group information repositories, or "group memory" [1] tools, shared folders are an informal sharing mechanism naturally extended from users' local main folders, with essentially the same metaphor and functionality as local hierarchical folders on personal computers. Minimal rules are built in the system regarding how multiple people access and use the share folders. Because of the simple metaphor, easiness to use, reliability, and less security concern (shared folders are usually on a same computer or a local network drive), shared folders are widely used for personal purposes and work activities.

However, we do not fully understand many issues regarding the use of this deceptively simple tool. For example, are there any hidden "rules" guiding people's behavior in using shared folders? How does the use the shared folder impact personal information management? And how do people coordinate them?

As a preliminary effort in searching for the answers to these questions, this pilot study examines five cases of using shared folders for work and life by five information workers in an academic institution. We observed a close connection and dynamics between the shared folders and the participants' main folders. A unique set of access permissions on shared folders is also identified and discussed.

The data was collected in 2008. Although some of the participants may have updated their computer operating systems, the shared folder mechanism remains almost the same and it is still used in the institution by the time this paper is written. Therefore the results of the study still apply in today's computing environment. Many cloud services such as Dropbox are using similar folder metaphor for sharing documents.

PIM Workshop'12, February 11-12, 2012, Seattle, Washington, U.S.A.
Copyright 2012 ACM 1-58113-000-0/00/0010…$10.00.

2. RELATED STUDIES

Research on sharing practices and mechanisms has mainly focused on the aspects of what to share, with whom to share, and how to share [8]. For example, concerning the privacy issues in sharing information, Olson et al. abstracted several classes of content to share and categorized people with whom to share [4].

"How to share" is a more complicated issue related to system, human, and content. From a human-centered perspective, Voida et al. examined several sharing mechanisms such as emailing, website, concurrent versioning system, and shared folders. They further identified a set of characteristics of sharing practices that play a role in the choice of sharing tools in a corporate environment, e.g., visibility, notifications, location of files during share, specification of access control, access rights, redistribution, among others [8]. Berlin et al. [1] proposed the concept of "group memory" as a "common repository of on-line, minimally structured information of persistent value to a group." They found that individual information management strategies do not map well onto group information. In a group information repository called CTools, Rader [5] observed that the users perceived the content as either yours or mine, instead of "ours," and organized information in different individual ways. She also found that the users "were unwilling to make a decision that might directly prevent another member from accessing the information, especially if they were not the original creator of the file" [5].

More from system design's perspective, Johnson et al. [2] proposed five requirements of "Laissez-faire" file sharing to encourage information workers to use the system. The requirements include: ownership, freedom of delegation, transparency, dependability, and minimization of friction, paralleling the requirements of free market economies.

A large body of research on "how to share" has examined the access control issue in various group information repositories or group information systems. And there is "a long history of work on increasing the usability of interfaces to traditional access control systems" [7]. In exploring for the requirements for access control in CSCW systems, Sikkel clarified several concepts such as authentication, authorization, access rights, and access control. Mazurek et al. investigated the access control for home data sharing and found that users' ideal access control policies tend to be complex. Thus they suggest that system should "allow fine-grained control" [3]. Several other studies, however, suggest that the setting of access control groups and their permissions, which are two key aspects of access control, should be simplified in a group information repository for the ease of understanding and use (e.g., [6], [7]). Smetters & Good state that complex access control "comes at the cost of potentially high user effort, tendency to error and the inability to control" for users [7]. They note that "(w)hile separation of read and write and perhaps execute permissions are clearly valuable to users, it is not clear that others (e.g., separate control of access settings themselves, deletion, or other options) are" [7].

Almost all of the available studies are focused on centralized institutional systems. Few studies examined shared folders use from individual's personal information management perspective.

3. METHOD

A small pilot study was developed to help us identify and understand some of the issues around personal information organization, access and sharing on personal computers in an academic institution. A group of 5 information workers, including 3 Ph.D. students (P1-P3) and 2 administrative employees (A1-A2), were interviewed and walked through the files and email folders on their computers with the investigator and talked about the use of shared folders. The selection of these two groups of participants is for opportunities to obtain more varied data, not for comparison purpose.

Four of the five participants used a PC with Windows XP operating system and the other one used a Mac. By the interview time, P3 and A1 had been in the institution for less than one year.

In the following description, all personal or organizations' names are anonymized for privacy concerns.

4. RESULTS

The five participants used the shared folders in different ways. P1 and P2 shared a home computer with their family members for files related to personal lives. P3, A1 and A2 used the institution's local network drives to share work-related files with their colleagues. The following list describes the details about how the 5 participants used the shared folders:

1. P1 and her husband were on the job market at the time, and had several "common" folders on their home desktop PC: "Some (folders) are common, like 'interview question' is a common one". They also have several other common shared folders about their daughter and parents.

2. P2 shared a folder with his son on his Mac OS laptop, for "the stuff he's created, or he likes". His son used the folder when he visited. He would also put some files for his son in that folder. At the same time, he saved duplicate copies of certain files such as pictures in his own directories "in case he (his son) wants to delete something." The folder is shared between P2 and his son.

3. P3 worked on an institutional Windows shared drive for her research assistantship work. She "worked at several of the folders, 'recruiting' is one of the folders, 'summer institute' is another folder, 'PR materials', 'needs assessment', 'curriculum' is another one." After clicking in one of the folders, she explained: "this is stuff Mary and I work on together. So it's not just my stuff. It's both of our stuff. … she'll ask me to do something, and we store it on the shared folder". In addition to P3 and Mary, the two PIs of the project also have the access to these shared folders.

4. A1 used an institutional Windows shared drive in the institution with several other colleagues and student workers for various events and tasks, in addition to the main folders on her local drives. On the shared drive, she had her own folders, named with her name, and several common folders. For example, there is a common folder "event" for all the events A1 and other colleagues have been working on.

5. A2 used the same shared drive as the one A1 was using. Similarly, she had her own personal shared folder, and used the common folders with several other colleagues and student workers.

4.1 Is the Shared Folder Mine?

In the five cases, P1 and P2 both had shared folders together with their main folders on their personal computers. P2 clearly sees the shared folder as belonging to his son and realized his son's full control over the shared folder. Consequently he saved duplicate copies of some files in his own folders under his full control. P1, on the other hand, sees the shared folders a part of her information space and at the same time a part of her husband's information space. Although these folders are shared between the two people, they usually have a single role and same perspective in using these folders. To P2 and her husband, these folders are "ours."

A1 and A2 had their personal shared folders separate from other shared folders, and they see their personal shared folders as a part of their information spaces, but not for the other common ones. Perhaps related to the different senses of ownership, A1 can tolerate the common folders' organization structure imposed by other people even though the structure does not look right for her: "…this one, (and) this one…should all be under here. I decided the initial structure, but someone can change it."

Unlike A1 and A2, P3 had her own files and subfolders mixed with other project members' items, without a separate personal shared folder. She was not sure if she sees the shared folders a part of her information space. She was clear that some of the items are not hers. "I can just tell the way the files are labeled, what's mine and what's not mine." "…this looks like Mary, because I don't write things that way. These are all Mary's." In addition to that, she cannot decide the organization structure of the shared folders. She described that she once created a subfolder for a set of files based on her understanding, but then found that the other project members actually put the similar files at a different place. "It's very confusing, because there are two different folders." "Because both of these (parent) folders were already here, and I added in the (sub)folder within the folders, so I don't know where the best place would be to put stuff." As a result, she has no clear sense of ownership for the shared folders she had been working on.

4.2 Incorporating Shared Folders into Personal Information Management

For A1 and A2, they need to put files outside of their main folders' organization structures to share with others. Although they see their personal shared folders are a part of their information spaces, they still need to figure out a way to incorporate the shared folder into their personal information management schemes.

Participant A2 had implicit but clear rules in working with her shared folders and main folders. She claimed that she sees her personal shared folder a part of her file system and thus does not intentionally keep a duplicate copy in her main folders if she has the file in her personal shared folder. When she had a student worker to work on a file (in the student's personal shared folder), "then frequently, when it's done, I'll put it back on my local folder," "or ask her to move it out of her folder into my folder, and I'll put in a different place, in my local folder." "Try to keep all information from all places for one event in one place. That's the goal."

For A1, however, it was a challenge, probably because she had been in the job for only 9 months and was less experienced. “There are two sets of files. There are my personal files, and my files in the shared drive, which is my greatest challenge. On the shared drive, I have access to all of these documents, and all of these individuals have access to my documents. So here is my added challenge: did I put in the shared file or did I put it in my own personal protected file (folder)? And therein lies my struggle because I should probably be filing them in both but then I’m not sure if I update one.”

The files in shared folders are closely connected with main folders. While the current or final version file is in the shared folder, many related files or old version ones may locate in the main folders. To make it more complicated, some related files may also exist in the shared folder. All these impose challenges for the user’s personal information management.

4.3 Access Permissions: Technical vs. Social

The five cases especially P1 and P2 show that whether or not the participant sees the shared folders a part of her/his own personal information space is independent of *where* the shared folders are located or *who* created the files or folders -- it is consistent with the access permissions the participant and the other members have over the target files or folders.

Although Unix provides read, write, and execute permissions for different groups, and Windows shared folders have read, change, and full control permission options, the access permissions in the five cases in this study are all at the system level; that is, all the people having access to a folder have full control over the folder and its content.

However, although each team member technically has full control, the participants had a sense of what actions they and the other group members *should* do. This type of social “rules” or norms about access permissions were never made explicit, but when one member breaks the “rules,” the others can have problems. The implicit assumptions identified in the five cases are based on three types of access permissions on the shared folders:

A. Read, copy (out), create (a file or a subfolder), and save;

B. Move (out), delete, rename, edit, re-organize (i.e., change folder structure);

C. “Sticky bit” permission, i.e., group A actions on all items, and group B actions on personal items.

In Type A, “copy (out)” means to copy file(s) to a place outside of the target shared folder. Similarly, the “move (out)” in Type B means to move file(s) to a place outside of the shared folder. Type A and B together are full control. The “sticky bit” permission in Type C refers to the one usually set on a temporary folder in Unix system that different users can use for temporary files. With this permission set on a folder, only the file owner can delete his/her file, which prevents other users from deleting temporary files created by others and harming their work. In a shared folders, the “sticky bit” permission allows group A actions on all files and subfolders, and group B actions on the user’s own files and subfolders. The identified implicit access permissions and how the participants see the shared folders are outlined in Table 1.

These access permission categories are a little different from the common read and write permission setting in Unix or Windows. In Type A, “read” and “copy” are the same as the “read” permission defined in Unix and Windows shared folders. However, “create” and “save”, which belong to the “write” permission in Unix and the “change” permission in Windows shared folders, are together with “read” and “copy” as a group of allowed actions. For example, P2 put something that he would like his son to look at in the shared folder. A1 and A2 also described occasions when another colleague put files in their personal shared folders, although they do not expect other people to delete or modify files in their personal shared folders. In this sense, A and B can be seen as constructive actions and destructive actions, respectively.

Table 1: Access Permissions in the Five Cases

Cases		The Participant	Other member(s)	Part of PIS
1 (P1)		A+B	A + B	Yes
2 (P2)		A	A + B	No
3 (P3)		C	C	Not sure
4 (A1), 5 (A2)	Personal shared folder	A + B	A	Yes
	Common shared folders	A + B	A + B	No

It is worth noting that “copy (out)” and “move (out)” are in different groups and participants had clearly different tolerances to these two actions conducted by others. In case 4, participant A1 talked about a problem she experienced when she could not find a file in her own shared folder and finally found that her supervisor took the file and moved it to her own shared folder. “It was unnerving, I wish there were a way where if someone did something like that, a, I wish they would tell me so that I wouldn’t have been going through such angst, or b, a note that said ‘moved to such and such’, some automatic indicator, so I could find it there.” Although the A1, A2, and the other related colleagues “talked about it” in terms of how to use the folders on the shared drive, according to A2, apparently they did not make everything explicit. Because participant A1 assumed full control over her personal shared folder and Type A permission from her colleagues, she was upset when the other people conducted a Type B action.

Table 1 implies a connection between the access permissions the team members have and their senses of ownership. If a user has the full control (A+B) and the other members have only group A permission, the user may have a clear sense of “mine.” All members having “sticky bit” permission may result in unclear sense of “mine or not.” All members having full control may see the folder as “ours.”

5. DISCUSSION

This is a preliminary study based on a small sample, and the results are by no means conclusive even within a single work context. But the study identified some of the issues that merit further investigation to deepen our understanding and improve system design.

Unlike centralized group information repositories where people usually do not have a sense of ownership of the information items, people may have a clear sense of “mine or not” on shared folders. Shared folders can be closely connected with main folders as a part of workspaces and personal information spaces, far from being separate, static storage and organization places. Therefore people have good reasons to have control and ownership clearly acknowledged on shared folders. Although technically everyone can modify, delete, and move other people’s files in shared folders, there are implicit rules and assumptions guiding their behaviors. These norms affect how each team member organizes his/her personal information space. The participants A1 and A2 had a “transition” layer – personal shared folder -- between their main folders and the common shared folders, different from how P3 and her team members used the shared folders. In P3’s model of using shared folders, no ownership is clearly acknowledged, files and folders of “mine” are mixed with “yours,” and the different perspectives and organization structures conflict directly, similar to what Rader observed in her study (see above RELATED STUDIES). Rader raised the question of how to make people perceive as “ours” the content of a group information repository [5]. The model A1 and A2 used indicates that, after what is mine and what is yours are clearly specified, what is “ours” becomes clear.

Consistent with how people see the shared folders in relation to their main folders, access permissions affect how people incorporate shared folders into their personal information management schemes. Different from the setting on available computer systems, the identified permissions in this study suggest that the access control on shared folders is not only for sharing, but also for personal information management. System designers of sharing mechanisms have to take into account each user’s personal information management.

In this study, several cases involved sharing between just two people. Ignoring the issue of ‘ours’, that means that other ownerships are very easy to determine – if it isn’t mine then it must be yours. With larger groups, certain distinctions become a bit harder to manage (but certainly not impossible). How do people manage? Is there a move to simple distinctions of mine, ours and not-mine? Where are the borders between personal and shared? Are there any transitions between these spaces?

Trouble can occur if different people have different senses of ownership; of mine, yours and ours. Problems can become more acute if those differences are unacknowledged, or you think everyone else has the same sense as you. This is just as true of shared folders as it is of shared refrigerators.

6. REFERENCES

[1] Berlin, L.M., Jeffries, R., O’Day, V.L., Paepcke, A., and Wharton, C. 1993. Where did you put it? Issues in the design and use of a group memory. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Amsterdam, The Netherlands). CHI’93. ACM Press. New York, NY, 23-30. DOI=http://doi.acm.org/10.1145/169059.169063.

[2] Johnson, M.L., Bellovin, S.M., Reeder, R.W., and Schechter, S.E. 2010. Laissez-faire file sharing: Access control designed for individuals at the endpoints. In *NSPW’09 Proceedings of the 2009 Workshop on New Security Paradigms*. New York NY: ACM Press.

[3] Mazurek, M.L., Arsenault, J.P., Bresee, J., Gupta, N., Ion, I., et al. 2010. Access control for home data sharing: Attitudes, needs, and practices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Atlanta, Georgia, April 10 – 15, 2010). CHI '10. ACM, New York, NY. 62-71. DOI=http://doi.acm.org/10.1145/1753326.1753421

[4] Olson, J.S., Grudin, J., and Horvitz, E. 2005. A study of preferences for sharing and privacy. In *CHI’05: CHI’05 extended abstracts on Human Factors in Computing Systems*(Portland, Oregon, April 02-07, 2005). CHI’05. ACM. New York, NY, 1985-1988. DOI=http://doi.acm.org/10.1145/1056808.1057073

[5] Rader, E. 2010. The effect of audience design on labeling, organizing, and finding shared files. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Atlanta, Georgia, April 10 – 15, 2010). CHI’10. ACM Press, New York, NY, 23-30. DOI=http://doi.acm.org/10.1145/1753326.1753440

[6] Sikkel, K. 1997. A group-based authorization model for cooperative systems. In *Proceedings of the 5th conference on European Conference on Computer-Supported Cooperative Work* (Lancaster, UK, September 07 – 11, 1997), 345-360.

[7] Smetters, D.K. and Good, N. 2009. How users use access control. In *Proceedings of the 5th symposium on Usable Privacy and Security* (SOUPS) (Mountain View, California, July 15 - 17, 2009). ACM, New York, NY. DOI=http://doi.acm.org/10.1145/1572532.1572552

[8] Voida, S., Edwards, W.K., Newman, M.W., Grinter, R.E., and Ducheneaut, N. 2006. Share and share alike: Exploring the user interface affordances of file sharing. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Montréal, Québec, April 22 – 27, 2006). CHI’06. ACM Press, New York, NY, 221-230. DOI=http://doi.acm.org/10.1145/1124772.1124806