"I feel stupid I can't delete...": A Study of Users' Cloud Deletion Practices and Coping Strategies

Kopo Marvin Ramokapane and Awais Rashid, ***Lancaster University;***
Jose Miguel Such, ***King's College London***

https://www.usenix.org/conference/soups2017/technical-sessions/presentation/ramokapane

This paper is included in the Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017).

July 12–14, 2017 • Santa Clara, CA, USA

ISBN 978-1-931971-39-3

Open access to the Proceedings of the Thirteenth Symposium on Usable Privacy and Security is sponsored by USENIX.

"I feel stupid I can't delete...": A Study of Users' Cloud Deletion Practices and Coping Strategies

Kopo M. Ramokapane
Security Lancaster Institute
Lancaster University, UK
k.ramokapane@lancaster.ac.uk

Awais Rashid
Security Lancaster Institute
Lancaster University, UK
a.rashid@lancaster.ac.uk

Jose M. Such
Department of Informatics
King's College London, UK
jose.such@kcl.ac.uk

ABSTRACT

Deletion of data from cloud storage and services is an important aspect of privacy and security. But how easy or simple a task is it for users to complete? Cloud users' deletion practices, challenges and coping strategies have not been well studied to date. We undertook an exploratory study to better understand this issue. Through in-depth semi-structured interviews and use of deletion scenarios with 26 subjects, we explored several key questions: why and when cloud users would like to delete, why cloud users cannot delete, what causes such failures, what users do to work around these problems, and finally what do users want in terms of usable deletion in the cloud. We found that users' failure to delete arises from lack of information about deletion, incomplete mental models of the cloud and deletion within the cloud, and poorly designed user interfaces for deletion functions. Our results also show that users develop different coping strategies such as deleting from certain devices only, seeking help and changing service providers, to overcome such challenges. However, these strategies may not always produce desired results. We also discuss potential ways to improve the usability of deletion in the cloud.

1. INTRODUCTION

Since the advent of cloud computing incomplete deletion of data has been a concern for most organizations and users. Researchers have looked into provision of assured deletion in the cloud [6, 26] and encryption-based solutions to securely dispose of data after use [25, 29]. However, such approaches start from the assumption that users *know* data management in the cloud, have clear mental models of how deletion may operate in the cloud and can accomplish the task of deletion through either the features offered by cloud providers or using more sophisticated assured deletion mechanisms such as encryption-based solutions.

In this paper, we focus on the user's perspective and investigate usability of data deletion from cloud storage and services. We explore several key questions fundamental to usable privacy and security: what are the motivating factors that underpin cloud users' need to delete? Do they find current cloud deletion mechanisms usable and, if not, what are the factors underpinning users' failure to delete? What are the coping strategies that users deploy to work around these problems and what do users want in terms of usable deletion in the cloud?

Recent high profile incidents have highlighted the security and privacy concerns of users with regards to data management and retention in the cloud. For instance, Dropbox users were alarmed when their files and folders deleted as far as 5 years ago mysteriously re-appeared in their accounts [11]. Similar concerns have been raised by iCloud users upon learning that Apple had been retaining their browsing history for more than a year – several months after it was supposed to have been deleted [13].

There has been a substantial body of knowledge and experimental evidence on users' security and privacy behaviors, for instance [1, 30]. The usability issues of encryption mechanisms have also been well-documented, e.g., [10, 33]. Recent research on deletion in the cloud has focused on risks associated with incomplete deletion or retained data in the cloud [26] as well as encryption-based deletion solutions [25, 29]. However, the usability of data deletion in the cloud has not been explored and users' understanding and challenges of deleting from the cloud are still to be studied. For instance, at present, cloud users are allowed to access and delete from the cloud through mobile apps, web interfaces and from their computers. Nonetheless, deleting from these platforms requires different mental models and this can be a challenge for users as most of them assume these platforms work the same way and expect the same results. In this paper, we seek to bridge this knowledge gap.

We conducted an exploratory study using semi-structured interviews [4] to explore users' motivations for deletion, their successes/failures with regards to deletion, their coping strategies upon failures and their wants with regards to deletion in the cloud. We interviewed 26 active cloud users from a wide range of backgrounds and used a grounded theory approach [8] to analyze the insights from the interviews in order to explain why users behave the way they do, or why they make the decisions they make.

Contributions. Our analysis reveals that cloud users fail to delete in the cloud because they: (i) lack information on deletion; (ii) have incorrect mental models of deletion; or (iii) because they have to deal with poorly designed cloud interfaces. Users stated that there is not enough informa-

Symposium on Usable Privacy and Security (SOUPS) 2017, July 12–14, 2017, Santa Clara, California.

tion on deletion while information on benefits such as storage size is transparent on advertisements. We discovered that this lack of sufficient information on deletion leads to construction of inaccurate mental models which result in poor decision making and incorrect actions with regards to deletion.

We also learnt that users develop different coping strategies to circumvent their deletion challenges; these strategies are based on their needs and reasons to delete. For example, users with low deletion skills may exclude files they perceive important or confidential from the cloud so that they do not have to deal with deleting them. Surprisingly, we found that none of our participants, including those with privacy concerns, used encryption tools, although literature on cloud deletion proposes the use of encryption [25, 29].

In summary, the novel contributions of our work are as follows:

- We identify four key drivers that motivate users to delete from the cloud.
- We reveal why users fail to delete from the cloud, highlighting what causes and contributes to such failures.
- We uncover different coping strategies adopted by cloud users to address their deletion challenges, discussing the consequences of such strategies with regards to users' motivations to delete.
- We reveal what cloud users want regarding deletion from the cloud, and discuss open challenges and present paths for future research in this area.

This paper is structured as follows: Section 2 gives an overview of related work. Section 3 describes our methodological approach and demographics. Section 4 presents our findings regarding current deletion practices, challenges, coping strategies and what deletion experiences do users want. In Section 5, we discuss how coping strategies relate to users' motivations to delete and their mental models respectively. Section 6 concludes the paper.

2. RELATED WORK

Prior studies have investigated specific areas of security-related behavior like ours, but none have specifically looked at users' perception of deletion in the cloud. In non-cloud contexts such as social media, some aspects of deletion have been explored, for instance, there has been work focusing on understanding users' privacy concerns over social media and their challenges of deleting from such platforms [2, 19, 16, 27]. Some prior studies [19, 31, 21] have found that people use deletion as a coping strategy to handle regrets over posts and in some cases to protect their privacy either by removing a contact (e.g., unfriending) or the post itself. To contextualize our study, we now discuss briefly the most relevant prior work.

2.1 Users' perception of security and privacy in the cloud

Some prior work has investigated users' perception of security and privacy in cloud computing. Ion et al. examined users' attitudes and beliefs regarding the usage of cloud computing comparing them to those of enterprises [18]. They found a significant mismatch between users' security expectations and what was actually being offered. Gashami et al. researched the needs and privacy concerns of individuals adopting Software-as-a-Service (SaaS) [14]. They found that perceived benefits had a more direct effect on users' intention to adopt SaaS while privacy concerns had no direct impact. Daniel et al. investigated users' acceptance of the cloud with regards to trust and risk [5]. Their work focused on understanding how trust and risk perceptions influence users' cloud adoption decisions. Susan et al. found that, while journalists used some cloud tools, a number of them did not perceive any security risks in doing so [23]. These works have explored security as a general concern for users but have not investigated deletion as a specific problem for cloud users.

2.2 Mental models

A number of researchers have adopted the mental models approach to understand how non-expert users perceive privacy and security. Wash has examined how home computer users make their security decisions and how that affects their use of security advice [32]. He identified eight (8) mental models, "folk models", of security threats that users constructed and how these models can be used to justify why home computer users ignore security advice. Camp proposed five (5) possible models that could be used to communicate complex security to normal users [7]. Both Wash and Camp found that users want security but, in different situations, their desire to have security also depends on how they understand and perceive risk. Using a mental model approach, Bravo-Lillo et al. [3] conducted studies to gain an understanding of how users perceive and respond to computer alerts while Ur et al. examined whether users' mental models of password security matched reality [30]. Some studies have also compared how the mental models of experts and non-experts differ, for example, [17]. All these works demonstrate that understanding users' mental models can help to communicate with or educate users on security risks. Our work contributes to this area by trying to understand what deletion mental models cloud users possess.

3. METHODOLOGY

We conducted a qualitative inquiry into how cloud users understand and think about deletion in the cloud. We carried out semi-structured interviews with 26 participants between November and December 2016.

3.1 Ethical considerations

Our study was approved by the relevant Institutional review board (IRB) before any research activities began. We obtained informed written consent from all participants to take part in the study and to have the interviews audio recorded.

3.2 Participants/Sampling methodology

We recruited our participants through our existing professional networks, word of mouth and also advertised the study through posters in the city and around our institution. Interested participants were invited to complete an online form which contained a set of questions designed to screen participants that could be invited for one-to-one interviews.

Other than for balancing demographics, the screener also focused on asking participants about the cloud services they were currently using and the devices they used to connect to

such services. Respondents were also asked about their activities in the cloud, that is, whether they have ever deleted, shared or uploaded and downloaded data from the cloud.

Over a period of 3 weeks, we received a total of 48 responses. From these, 16 were males, 28 were students (3 doing masters degrees while 12 were pursuing a Ph.D.), 18 had some form of employment and 2 were unemployed or retired. The majority (30) were between the ages of 21 and 30 years old.

All 48 of our respondents stated that they used smart phones to connect to the cloud while 43 used their laptops to connect to cloud services. 97% of our respondents stated having shared, uploaded and deleted data from their cloud services. Appendix A.1 summarizes the demographics of all our respondents.

All screener responses were analyzed as we tried to identify a group of about 20 to 25 participants for one-to-one interviews, a number that was enough to reach a saturation point in terms of the emerging codes as discussed in Section 3.4 . For maximum variation, we purposefully selected respondents from a wide variety of backgrounds, ages, education and socio-economic classes. More importantly, we were targeting respondents who use more than one cloud service, preferably a storage service (e.g., Dropbox) and data processing service (e.g., Google Docs). Preference was also given to those participants who had mentioned that they had uploaded, shared and deleted data from these services. Interviewing respondents from a wide range of backgrounds allowed us to capture different perceptions of deletion in the cloud and identify common patterns. In the end, 26 out of the 48 respondents to the preliminary screener were invited by email to participate in the interview. The sample included 14 women and 12 men, between 18 and 50 years old. Appendix A.2 summarizes the demographics of participants invited for interviews. For a 30 to 45 minutes interview, participants were compensated $10 for their time and effort.

3.3 Interviews

Interviews were led and conducted by one researcher in different places to meet participants' needs and requirements (e.g., at a participant workplace because of their work schedule). The vast majority of interviews (25) were conducted in-person, though a single one was conducted via Skype.

We began each interview by first obtaining consent and explaining the purpose of the study. We used a semi-structured interview protocol so that our list of questions could act as a guide throughout the interviews but not restrict us to just those set of questions [24]. Using semi-structured interviews allowed us to probe participants for more information.

We used a reflective questioning technique to interview our participants. This allowed participants to reflect their actions and decisions aloud hence not directing them to a conclusion. Reflective technique also gave us an opportunity to explore a participant's knowledge, skills, experiences, attitudes, beliefs, and values. Our questions focused on the general use of the cloud and deletion of data from the cloud. We asked participants how they use cloud services on a day-to-day basis and their reasons behind using and choosing such services. Regarding deletion, we asked participants about how and why they delete data in the cloud and the situations when they encountered problems when attempting to delete from the cloud. Some of our questions included scenarios (see below) that required participants to use their mental models to make decisions on how to delete data.

All interviews were audio recorded using a secure audio recorder and stored securely. The audio recordings and the transcriptions were not accessible to anyone other than the researchers and the transcribers.

3.3.1 Scenarios

As part of understanding users' perception of deletion, we used two scenarios and asked participants to describe what would happen when deleting under each scenario. By doing this, we gave our interviewees the opportunity to apply their mental models of the cloud and deletion. We chose these scenarios as they represent typical deletion tasks associated with cloud storage services. Each scenario was contextualized based on the information the interviewee provided and then narrated to the participant. For example, if the interviewee mentioned that they regularly used Dropbox to share photos, then the scenario would involve Dropbox and sharing of photos. We wanted to create a scenario that appeared real to the interviewee. The two scenarios are as follows:

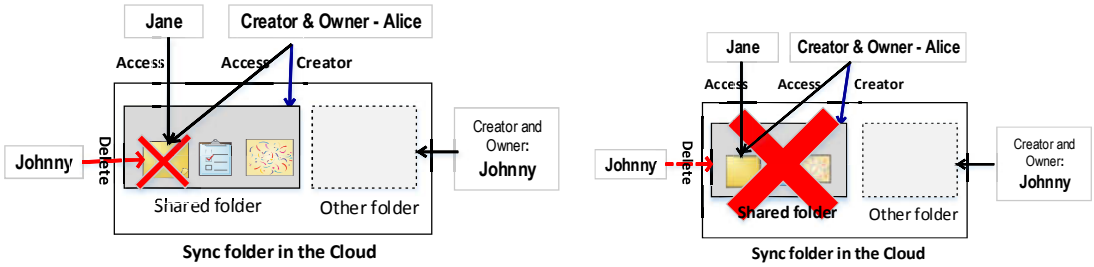
Deleting from a shared folder. This scenario (shown in Fig. 1a) asked participants what would happen if they deleted a file from a shared folder created by their colleague or friend. In this scenario, Alice has created and shared a folder with both Jane and Johnny. Johnny is running out of space but decides that the only file he can delete is the one in this shared folder because he has finished using it. However, without first contacting Jane and Alice, Johnny has to make the decision whether to delete the file or not. Would Johnny be able to delete this file? If he deletes this file, what would happen?

Deleting a shared folder. The second scenario (shown in Fig. 1b) asked users what would happen if they tried to delete a shared folder created by their colleague or friend. In this scenario, Alice has created a project folder and shared it with both Jane and Johnny. After the project has been completed, Johnny thinks he has no use for all the files in the shared folder. Johnny goes to his laptop and deletes the shared folder from his sync folder. Would Johnny be able to delete the folder? If he deletes it, what would happen? Will Jane and Alice still have access to the files in the shared folder or the folder will disappear from both of their accounts? Or will it only disappear from Johnny's sync folder?

3.4 Grounded Theory

After the first five interviews, we transcribed the audio files and began coding. Beginning coding as soon as we received data was important because it allowed us to identify interesting categories and themes which needed further exploration [8, 15] during subsequent interviews. Data was analyzed through several iterative stages of open, axial and selective coding and constant comparisons of codes [8, 15]. Using NVIVO[1], we went through each transcript line-by-line and developed our first descriptive open codes. Several codes about how cloud users use the cloud and how they delete began to emerge. This process resulted in 120 unique codes. To verify the codes, after the main coder had coded the first two scripts, the second researcher independently coded two

[1] http://www.qsrinternational.com/what-is-nvivo



(a) Deleting a shared file

(b) Deleting a shared folder

Figure 1: Deletion scenarios: (a) We asked a user "Johnny" what would happen if he deleted a file shared between him and his friends "Jane and Alice" created by "Alice", and (b) we asked what would happen if Johnny attempted to delete a shared folder instead of the file.

other scripts resulting in a subset of codes from the main coder and the codebook was modified accordingly [20].

Our second phase of coding involved identifying patterns, connections, and relationships between the codes we initially developed. By doing this, we grouped similar or related codes to form categories (concepts) and in some cases expand the codes themselves to make categories. As different groups continued to emerge, we began to compare the groups against each other looking for connections between them. While additional interviews were performed, we continued with coding and memo writing until no more new codes were emerging. New codes stopped emerging after analyzing 13 interviews,that is, we reached saturation in grounded theory terms. In this phase, memos were used to describe codes, events, behaviors, and record emerging questions during the study. Following this, we ordered and further grouped our categories into more broad and abstract groupings. In the last round of data collection, we added a few more questions to the interview based on our groupings and the questions that emerged from our memos. For example, in our second phase of data analysis, two participant mentioned they would want their photos to be completely deleted, so we began to ask our next set of participants what kind of information would they want to see completely deleted.

The last phase of coding involved selective coding, where further transcripts were analyzed and we attempted to identify a linking core category that describes the underlying phenomenon in the observed and interpreted behavior. This iteration gave us the chance to engage more with the study, understanding what the users were saying and doing with regards to deletion.

4. KEY FINDINGS

Fig. 2 presents an overview of our key findings which we summarize below:

(1) What makes them delete? Our analysis suggests that users' motivation to delete falls into four major categories: privacy-driven, policy-driven, expertise-driven and storage-driven.

(2) What causes deletion failures? Not everyone can delete when they want to. Failure to delete in the cloud is not merely caused by poorly designed user interfaces but rather this can be attributed to a lot of other factors which may include inaccurate mental models and lack of sufficient information on deletion.

(3) How do users cope with deletion failures? Users develop and choose a coping strategy based on their motivation to delete or the cause of their failure to delete. For example, users whose intention to delete is privacy-driven will always choose a strategy that will remove the file from the cloud or will stop uploading the files they perceive to be important or confidential. Whereas, users whose reason to delete is to gain more storage space, will not mind cloud hopping to gain additional storage.

(4) What do users want? Users desire four key characteristics with respect to deletion in the cloud: transparency in deletion, deletion to be complete, control over deletion, and help service to support deletion tasks.

We next detail each of these findings:

4.1 What motivates users to delete?

Before we could try to understand why users could not delete, it was important to first understand what motivates users to delete or the situations in which people want to delete. Users' motivations to delete were: privacy-, expertise-, policy- or storage-driven.

4.1.1 *Privacy-driven Motivations.*

Users' concerns about online information, the level of trust the user has towards the provider, or the perceived negative consequences of not deleting a file from the cloud are often driving factors for deletion.

Lack of trust in provider. Users with high privacy concerns towards cloud providers are always motivated to delete. Participants revealed that they delete because they fear that their data may fall into the wrong hands. For instance, P4 said,

"*It's just me being cautious that this, from my understanding and it's not that good, Dropbox is something like an online database like or a storage space, so I prefer just to be on the safe side to delete everything so that nobody else can access to these files apart from me.*"

P4 later on continued,

"*. . . I don't want anything bad to happen or Dropbox being hacked. . . I have interviews with children, so I send recordings of interviews with children so just to be on the safe side*

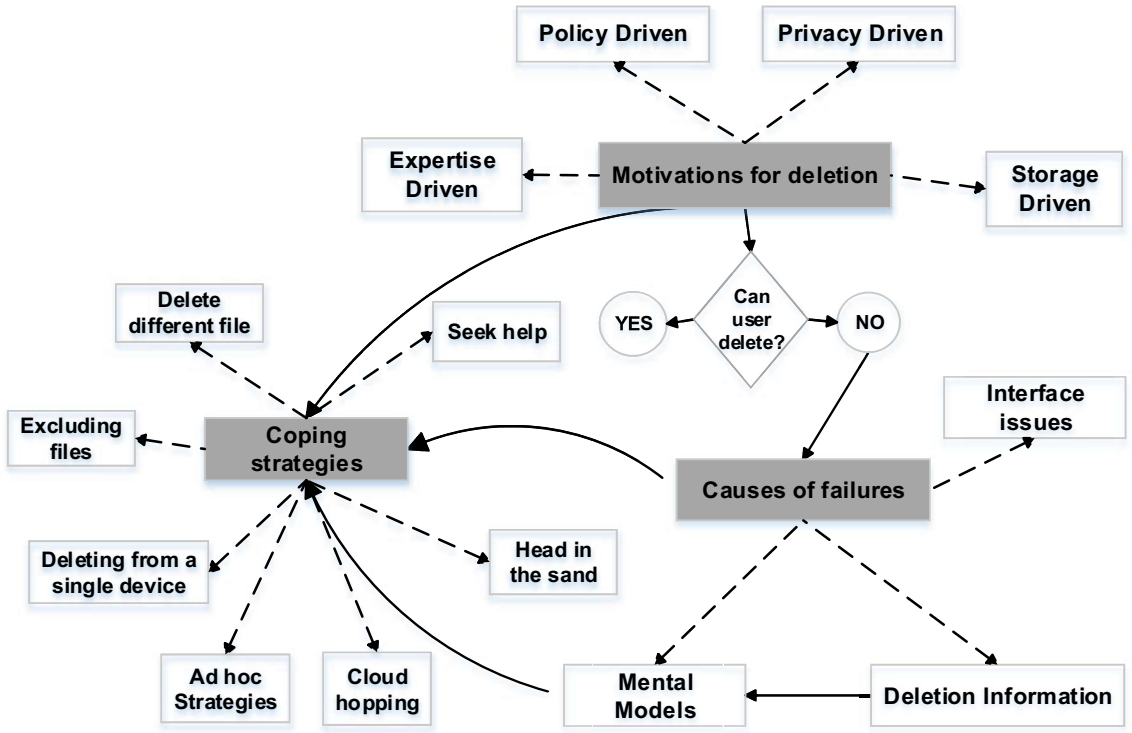


Figure 2: Key Findings

once she receives everything, I delete everything."

To avoid future conflicts. Participants deleted to avoid future conflicts which may be unearthed by the data they have in the cloud.

"*. . . I no longer want the pictures of my lover to be accessible to anybody else I'd want them gone from the servers forever, because my next future [partner] might discover them . . .*" P11

"*I get rid of things that could come back to haunt me. . .*" P10

To forget. Some users delete in order to forget. Most participants who automatically save their photos in the cloud revealed to us that they commonly delete photos from the cloud in order to forget about them, e.g., photos which are perceived to be embarrassing or contain an unpleasant memory.

"*. . . I'm always deleting pictures and stuff that I don't need to remember.*" P20

"*Some unhappy memories maybe, I would want them [to] disappear forever and I don't want to see them again.*" P17

4.1.2 Expertise-driven Motivations.

These are factors that are motivated by the level of understanding a user has or their ability to delete successfully.

Self-efficacy. Users' desire to delete is heavily influenced by their confidence in their ability to complete the desired task. Participants who had enough knowledge or skill to delete tended to make the decision to delete whenever they wanted and execute it immediately. However, those who struggled to delete showed less interest in wanting to do so.

Deleting after unintentional use. As highlighted in other cloud studies [9], our early coding resulted in the category of "unintentional use". Several of our participants deleted from the cloud because they first used it without knowing. Nowadays, it is common to find cloud-based applications already installed in smart devices and computers. However, at first, most users are not aware that some of these cloud applications will automatically log them into these services and start saving data to the cloud. Upon realization, most users' response was to delete the data as soon as possible. Participants *rushed* to delete because they were not sure how their data got there in the first place and, because they were not sure whether their data was public and, hence, visible to everyone. One participant who did not realize she was using OneDrive for 2 years noted:

"*When I first found out I had it I tried to delete all the photos because I got scared and I managed to. . . , I deleted the files and I got really confused when I first opened it because I was like well how did these files end up here? I never put them there but obviously, I'd whacked them in my phone and that's where it'd automatically saved to. So I deleted them.*" P18

4.1.3 Policy-driven Motivations.

Users are driven to delete due to *extrinsic* policies, e.g., organizational security policies to which they must adhere, as well as *intrinsic* ones, e.g., perceived value of information held in a file.

Organizational policy compliance. Compliance with organizational security and information sharing policies is often a driving factor for deletion. Participants mentioned that their work policies required them to manage data securely which included deletion. However, interviewees also revealed that they continued to use public clouds – despite this being in violation of organizational policies – because they were convenient and easy to use.

"*. . . I use [Box] because it was recommended and we were told that we couldn't store research work on Dropbox . . . Sometimes I use Dropbox . . . most people use it, but if I use Dropbox I delete...*" P9

Perceived value. Users' decision to delete was also influenced by the usefulness, sensitivity and value of a file. When users perceived a file to be confidential or more sensitive or valuable, they would want to delete it immediately after using it. Also, if users considered a file to be no longer useful or needed, they would consider it a good candidate for deletion.

"*. . . It's just normal deleting. I read the paper and if it's no use for me, then I delete it, that's it. . . There was document we had, it was not good for our job, we just deleted [it].*" P8

4.1.4 Storage-driven Motivations.

Users are also driven by storage size and the need to organize their data systematically.

Storage size. The most prominent repertoire was deleting in order to free some space. Instead of buying more storage some cloud users use deletion to reclaim used space. The less space a user has, the more motivated they will be to delete.

"*I didn't have a lot of space so I had to take out some pictures and videos so I deleted them from iCloud.*" P16

"*[When my] space was limited I would actually go through and prune out what's important what's not.*" P11

Tidying up. Sometimes cloud users delete to keep things tidy. We discovered that when users have the skill and the knowledge to delete, they will sometimes take time out just to tidy things up from their cloud accounts.

4.2 Why do users fail to delete?

Although the exact details of users' failure to delete varied, our data suggests a range of common factors that lead to deletion failure. These factors include insufficient deletion information, mental models, and user interface designs.

4.2.1 Insufficient information

Insufficient information on deletion contributed to lack of understanding on deletion. Although we did not ask our participants about information on deletion, participants notified us that such information is hardly available. It also emerged that service provider advertisements had information on the benefits of using the cloud (e.g., storage size) but none on deletion.

"*Nothing like that is made very clear when you sign up. Maybe if you read through the gazillion terms and conditions you would find out, but there's nothing obvious that I've come across anyway that says, 'After this amount of period of time this will actually be deleted.' So, surely that should be one of the first things that they tell people.*" P19

Users sometimes find deletion messages difficult to understand and not providing them information that is pertinent to the deletion task.

"*Sometimes on iCloud it does not allow you to delete, like if you are trying to delete something it says that if you delete it will mess up everything else, but on Google Drive and on Dropbox, I've never found anything like that. On ICloud sometimes it does not allow you to delete some stuff.*" P24

Although such information is sometimes made available in the terms and conditions of services, our interviews show that users do not read the terms and conditions, therefore, they do not have a full understanding of how their data will be handled by the provider. Concepts such as retention period are unknown among users. Previous research on privacy policies and terms and conditions states that users perceive terms and conditions as being long and unreadable[12, 22]. Some of our participants noted that, while they did not have problems with deleting, there was insufficient information on whether their deletion is permanent or not.

4.2.2 Mental Models

Users have been known to construct their own mental models when they are insufficiently educated on an issue but have to complete a task [32]. However, most of these models are inaccurate and in most cases lead to wrong results. Unsurprisingly, most cloud users with incomplete mental models of data management in the cloud reported not being able to delete. Users' inaccurate mental models did not just lead to deletion failure but also to wrong expectations.

Our data shows that most cloud users have less or minimal understanding of the cloud and of deletion. For example, some users presented limited knowledge on how the synchronization folder works or that they can access the cloud independent of apps that consumed or used the cloud. In terms of deletion, they did not understand the concept of *Deleted folder* (i.e, where deleted data goes), retention period, and different levels of deletion. Using these themes, we identified several mental models that existed among our participants concerning deletion and the cloud. In table 1 we show which models were common among our participants and which one were not. Also, since some of our participants owned more than one model, we do not report how many participants owned each model.

Table 1: Common mental models

Popular Models	Uncommon Models
- Sync folders are not the cloud - Saving and deleting work the same way - The cloud within an app - Borrowed deletion models - Shared folder: Deletion is one sided	- Shared folder: Deletion affects all members - Providers don't delete

Sync folders are not the cloud. To automatically save data in the cloud, cloud users have to install synchronization software or applications in their devices. During installation, a synchronization application will create a local folder in the user's computer which will be linked with the cloud service.

The purpose of the synchronization application is to detect all the changes (e.g., adding or removing files) in the folder and update user's contents in the cloud. This ensures that user's files in the cloud and the local device are up to date. For this to work, a user is required to be logged in to their cloud account through the application. Although, this is popular amongst users, our data suggests that most of them do not understand how this works. Some users deleted from the sync folder while their computers were offline but expected the files to be deleted instantly from the cloud. Also, another group did not understand that deleting from this folder would also mean deletion from the cloud.

"*So once I put [my] files in Box sync folder and it uploaded automatically but I wondering if deleting my files in that folder would also delete from the cloud as well... but then I just deleted those files from my folder and then logged into my box [account] and found [that the] files in the cloud were deleted as well. I was not happy to see that.*" P24

Saving and deleting work the same way. Some users wrongly concluded that deletion in the cloud worked the same way as saving a file. Although this is correct to some extent, that is only so when using a sync folder in a computer. When using sync folder, every file placed in that folder will automatically be uploaded and saved in the cloud. When a file is deleted from a sync folder it will be removed from the user space visible to the user but placed in a *Deleted folder* in the cloud. However, this may not apply in a situation where a user connects to the cloud through another app (e.g., camera app to backup photos). Deleting a photo from the camera app may not necessarily delete it from the cloud. However, some participants expected files to be deleted from the cloud when they deleted them from their mobile devices because they automatically saved to the cloud. One frustrated participant said,

"*I used to think that it[deletion] was kind of automatic that if I deleted from the phone that it would like [delete] because the fact that I save the photos, that it's saved in iCloud I think that if I delete it ,it would delete itself from my iCloud as well.*" P14

The cloud within an app. The use of applications to consume cloud services has left many users not knowing that they can access the cloud independently from those applications. This type of users do not delete from the cloud because they do not know that their data may still be in the cloud and they can access the cloud to delete. Users also do not know that some applications may backup data automatically to the cloud. One participant was surprised when asked if she had ever directly logged in and deleted from her iCloud account:

"*I [have] never come to the conclusion that I could actually go there and delete*" P14

Borrowed deletion models. Some users have transferred their mental models of deletion from other online services such as online social networks to the cloud. When asked about how they would delete a file from a shared folder in the cloud, one Dropbox user responded saying:

"*... I think I will ask my friend to delete it. And if they don't then I can't do anything apart from untag myself. I think it's quite a similar policy like in Instagram or in Facebook when you want to delete it, it always gives you the options either contact your friend to have them delete the photo or you just unfriend them.*" P14

Shared folder: Deletion is one sided. The concept of deleting from a shared folder is a challenging and confusing one for most users. Some users believed that when one deletes from a shared folder, the deletion will only remove a file from their accounts but that particular file would still be available for other members of the shared folder. To these users, deletion from a shared folder is one-sided. We also found out that some users believed that when a file is uploaded to a shared folder in the cloud, the cloud would create multiple copies of the file for all the members of the shared folder. Thus, assuming that when they delete from a shared folder, they are only deleting their own copy and not deleting from everyone. One participant likened deleting from a shared folder to deleting from Whatsapp messenger:

"*... [If she deletes it] it wouldn't get deleted from my side but it will obviously just get deleted from her side [because] she doesn't want it. Like if you send a Whatsapp message. So normally it wouldn't get deleted from my end, it would just get deleted from her end.*" P12

Shared folder: Deletion affects all members. Some users reported that they knew that deleting from a shared folder may remove the file from all other members' accounts as well. Nevertheless, this caused a conflict within the user who no longer needs a shared file within a shared folder and wishes to delete it. Users find it difficult to make the decision whether to delete or not. They believe that there is no alternative way of deleting a file from a shared folder while other members of the folder are still in need of that file. We found that users who possess this model prefer to leave the file in the shared folder undeleted just to be on the safe side.

"*... when I do this it's always after my transcriber has used the material and sent me the transcriptions back so I always think it is safe to delete them now because in my head I'm thinking... if I delete them she won't be able to see them, so I wait for her to finish the job and then I delete them.*" P4

Deletion is permanent and instant. Some of our subjects had a very under-developed model of deletion in the cloud. These subjects did not think about deletion in any depth but concluded that it was instant and permanent. The fact that a file disappears from their sight was enough for them to conclude so. These subjects were unconcerned about their deleted data and believed they were safe after deletion. Our data further suggested that this belief affected their views on recovery from the cloud; according to these subjects data recovery from the cloud is not possible.

We discovered a conflict within the minds of some of the individuals who had this model. On one hand, they believed deletion was permanent because they could not recover deleted data in the cloud. On the other hand, they also believed that deletion in the cloud could not be permanent since cloud is an online service. This conflict was caused by the belief that online services do not delete data therefore cloud being an online service would also not delete data. A handful of participants, however, did not fall into these conflicting models. They suggested deletion in the cloud was not permanent and even constructed attack models for deletion:

"*... you delete something but they still keep a copy of it and then some can hack in and get your information. I think because they keep a copy of everything, so I think after deleting they still keep a copy,... it means that somewhere they keep information that could be retrieved later, but whether that information is kept confidentially or [if] it could be hacked, people hacking in and getting other people's pictures and then blackmailing them and stuff.*" P24

Providers don't delete. A group of participants believed cloud providers do not delete for their own benefit like advertisements and research. They held the view that there is a "secondary" storage where deleted data is stored but users are not able to access it. Although, they reported high privacy concerns, they also exhibited some defeatism:

"*I never read the T&Cs I don't really know if it's deleted forever. It's probably still stored somewhere, but I don't have immediate access to it.*" P11

"*I think the provider might not want that[deletion] to happen because they keep the data and then they want to use it for marketing and, you know, different purposes.*" P24

However, some participants were not concerned about their data being used for adverts because they believed that as long as they could achieve what they wanted to do, this was acceptable.

"*I'm not so much concerned with that [deletion] as to the underlying reasons, and the drivers for the business are more important to me than their terms and conditions."* P26

4.3 User interface issues

As expected, we uncovered several cloud interface issues that negatively affected users' deletion process. Poorly designed user interfaces caused a lot of distress to some users which resulted in them losing interest in deleting or left them frustrated. Users are affected by screen sizes, type of interface (i.e., whether it is a web or mobile application), and how the deletion process is completed in that application. Our data also suggests that when users find it difficult to use an interface to delete, they are unlikely to attempt to delete using the same interface in the future. A number of our participants who access the cloud through mobile phones reported that sometimes they do not know where to go in their mobile phone interfaces in order to delete from the cloud.

Effort. Some cloud features (e.g., auto saving) affected users' deletion process. Users who have auto synchronization turned on ended up not deleting from the cloud because a lot of effort may be required from them to delete all the unwanted files synchronized to their cloud storage. One participant who had this feature turned on informed us that sometimes their smart phone accidentally takes photos while in their pocket leaving them with a lot of unwanted photos. It required a lot of effort and time to delete such photos from their phone and then from cloud, as a result sometimes they chose not to delete from the cloud.

"*... often with mobiles these days if the camera goes off in your pocket, which it often does, you can end up with all these blank photographs. Of course they go into OneDrive, so you look at your OneDrive and you want to clear all that. But sometimes it can take ages.*" P23

Buggy software. Buggy applications and unresponsive interfaces left some users not being able to delete. Some users reported that sometimes when they try to delete, the app or web interface would not respond resulting in them abandoning the process. Less satisfying mobile apps and unresponsive web interfaces resulted in users having less desire to delete. For example, some users reported that for them to delete they have to try it a couple of times before the operation successfully completes. Users found this annoying and preferred not to try deleting when they wanted.

4.4 Coping mechanisms

Our analysis reveals that users have developed different coping mechanisms to address or mitigate their failure to delete from the cloud. These mechanisms ranging from ignoring deletion altogether to changing cloud providers through to seeking help from others and ad-hoc strategies. We discuss various coping mechanisms employed by our participants next.

4.4.1 Head in the sand

Most participants who could not delete preferred to leave their files undeleted in the cloud. We identified four reasons why users settled on this strategy: (i) They perceive this method to be easy and quick—it does not require them to put in any effort. Users who felt deletion can be burdensome preferred this method. (ii) When a user has sufficient storage space left on their account, they are highly likely to leave the files in the cloud. (iii) When users perceive the file to be harmless or non-confidential. (iv) Trust in the cloud provider: when users trust the service provider they are more inclined to leave data in the cloud.

4.4.2 Cloud hopping

Those with high privacy concerns or low-levels of trust in providers often opted to stop using certain cloud services or changed their service providers. Although, this may be considered an extreme measure, we discovered that people weighed the benefits of using a cloud service against the cost of their undeleted data being exposed. Others noted that they changed providers because of running out of storage space with their current provider. Interestingly, we found that none of the participants who changed providers deleted or deactivated their accounts with the previous provider.

4.4.3 Excluding certain files from the cloud

Some participants reported that they explicitly decide on what goes in to the cloud before they upload to the cloud. By excluding potentially sensitive or confidential documents and sharing them by offline means, such users believed they were safe and they did not have to worry about undeleted information. This approach is common among people who have high privacy concerns and low trust towards providers. However, this strategy may open up other threats in terms of data exposure, e.g, through lost removable (potentially unencrypted) media—some participants reported using USB sticks to share sensitive files.

4.4.4 Deleting from one device

Some users reported that they only deleted from devices they were more comfortable with and were confident would yield expected results. For example, some users opt to delete from their computers (sync folder) than to delete from the web interface or mobile applications.

"*Yes, I have the app on my phone but I rarely use it, my app. I have downloaded the app on my desktop. So, I delete from there instead... I mostly delete it from the desktop because I found it difficult to delete it on the phone.*" P24

This strategy does delete the file from the cloud, however, this may lead to delays to deleting a file because the user may not always have the device they are comfortable with all the time.

4.4.5 Seeking help

Several users reported that they ask for help from their friends, family and colleagues if they think it is urgent and important that a file should be deleted. Others revealed that they will search online for solutions, for example, from tutorials, forums and blogs. The type of help sought depends on users' motivation to delete. For example, when the motivation to delete is due to high privacy concerns or trust issues, then the user will not hesitate to ask their social network for help. However, when the file to be deleted is sensitive (e.g., explicit photos) or confidential, users have a likelihood of not seeking help from other individuals with the fear of being exposed or shamed. They would opt for looking for solutions online. This strategy leads to high chances of deleting from the cloud and participants who reported they knew how to delete revealed this is how they learnt about deletion.

4.4.6 Deleting a different file

Some of our participants reported that when they are deleting to free up space and they fail to delete a certain file, they will instead choose a different file to delete than the original one. One participant explained that sometimes they get a warning not to delete a file but because they do not fully understand the consequences of deleting that file, they will instead look for a different file to delete.

"*...I will not delete that one, I will try to find something else to delete instead of it, to get more space otherwise I can't. So, at times I will remove a different file because I have not [yet] found a correct solution on how to get over it.*" P24

4.4.7 Ad hoc strategies

We also discovered some ad hoc strategies among our participants. Some of them revealed that they did not have a well-defined method of overcoming the failure to delete. They reported that they will try to find the best possible solution that fits and suitable for that moment in time. Some participants reported that if they cannot delete a file, but they feel it is important to delete such a file from the cloud, they would try deleting it from all their devices including the web interface. One participant revealed that when they are in need of more storage and they cannot delete they will simply buy more storage.

4.5 What deletion experience do users want?

In the previous section we discussed different coping mechanisms employed by users when they struggle to delete. Here we focus on themes and categories that emerged as to what cloud users want. We identified four key themes across our participants.

4.5.1 Transparency in deletion

Participants want providers to be more transparent about deletion of data; they wanted information on how their data is deleted to be made freely available. Participants who struggled to delete suggested that providers should provide tutorials on how to delete, and that deletion information should be made clear when they first sign up for services.

However, those who could delete were not so much interested in such information but rather in knowing more about how deletion is done in the cloud. Some suggested that they should receive notifications when data is completely removed from the cloud. That is they want guarantees that their data is completely gone from the provider. We found that this suggestion was popular among participants with privacy-driven deletion practices.

4.5.2 Complete deletion

Early in our research process, the assumption that cloud deletion was complete and instant emerged and we formulated some interview questions around this belief. As a result, we asked users what deletion meant to them and most of them defined it as "getting rid of" or "destroying data". Our analysis suggests that they believe deletion in the cloud is complete because they use these mental models when they think of the cloud. However, we found that participants who had better knowledge of the cloud and deletion desired complete deletion. They suggested that deletion should mean permanent:

"*I suppose all data should be completely deleted. Once you press 'delete', delete should mean delete, so then you don't have that sort of grey area as to what's sensitive, what's not sensitive. Delete should mean delete, I think.*" P6

"*The moment I delete something from my iCloud, or my laptop, I want it to be deleted completely. I feel like once I [have] said I don't want this on my laptop again, or I don't want it on my phone, I would rather have it deleted everywhere, complete.*" P3

For users who assumed deletion was complete, we explained to them that it is possible that their data may not be completely removed from the cloud [26]. Most of our participants responded with shock to this revelation while others reported they had always thought it might not be deleted.

"*I've always had it in the back of my mind that what you delete does not completely go. I didn't know like it's almost impossible to delete...*" P3

Although most users reported they would want complete deletion, this wasn't true universally. A number of users, understandably, wanted to have the opportunity to recover deleted data especially data deleted by mistake.

With regards to complete deletion, several of our participants exhibited the following beliefs: (1) data perceived important or confidential should be completely deleted, (2) Data belonging to other people or data that contains identifiable information should be completely deleted, and (3) only law abiding citizens should be allowed to completely delete things from the cloud.

With regards to the final point, we discovered that users who perceived themselves as harmless and law abiding citizens did not mind if their data was not completely deleted. However, they reported that if the data did not belong to them or contained other people's identifiable information then they would want it gone. Some users believed that complete dele-

tion would enable law breaking citizens to commit and hide their crimes on the cloud. Despite this, other users reasoned that they would still choose permanent deletion because it is their data and no one has the right to access it after deletion. With regards to recovery, such users reported they would change the way they work and just be careful when deleting data. We found that participants who belong to this group were people who had high privacy concerns about the cloud and would rather lose data because of mistakes than have it undeleted in the cloud.

4.5.3 Contact Point

During the interviews, some users reported that it was hard for them to get verifiable information on using the cloud. They suggested that a service dedicated to resolving their cloud queries would be useful especially when they cannot ask anyone. One participant put it this way:

"*[First thing is,] I don't know whom to call. If I want my data back I don't know whom to call, whom to contact because I don't think they have any helpline or service like this where a customer can call and say, 'I deleted by mistake, send it me back,' or I don't know whether the provider has the access to retrieve particular data of a customer.*" P24

4.5.4 Control over deletion

Our analysis suggests that users feel the need control over deletion in the cloud. They wanted to be the ones who decide when a file should be permanently deleted or held for potential recovery. Our data also shows that users want control over what is synced over to the cloud so that they will not have to delete.

"*Because if I have deleted something, I am saying, 'I don't need it anymore,' or, 'I don't want evidence of it anymore,' then surely it should be deleted completely because I no longer have use for it. Who's meant to still have use of what I've deleted?*" P22

5. DISCUSSION

Table 2: A summary of motivations to delete and coping strategies

Motivation to delete	Coping Strategy
Privacy-driven	Seeking help
	Deleting from single device
	Excluding certain files from the cloud
	Cloud hopping
	Ad hoc strategies
Expertise-driven	Head in the sand
	Ad hoc strategies
	Seeking help
	Excluding certain files from the cloud
	Cloud hopping
Policy-driven	Ad hoc strategies
	Deleting from single device
	Seeking help
	Excluding certain files from the cloud
Storage-driven	Cloud hopping
	Delete a different file
	Deleting from a single device
	Ad hoc strategies

5.1 Deletion motivations and coping strategies

Our findings reveal that users' choices and development of coping strategies are dependent on their motivation to delete. These relationships are summarized in Table 2 and discussed next.

Motivation: Privacy-driven. Users whose motivation to delete is privacy-driven are always quick to seek help in deleting or have a higher chance of employing some ad hoc methods to try to delete from the cloud. Seeking help from other cloud users has a likelihood of deleting a file from the cloud. Ad hoc strategies do not always guarantee data will be deleted from the cloud. When struggling to delete some of these users may opt to delete from the device they are most comfortable with or confident that they will manage to delete data using it. This choice is normally based on users' past experience; the user chooses it because it has worked for them before. Users who try all the above strategies and still fail, are inclined to change their provider or decide not to ever upload files they perceive to be confidential. These strategies are perceived to provide maximum privacy by the user as sensitive files would never reach the cloud from which they struggle to delete.

Motivation: Expertise-driven. Expertise-driven users often resort to ad hoc strategies when they cannot delete. If ad hoc strategies do not work, those with high self-confidence would either decide to leave the file in the cloud or hop to another provider. Such users do not normally ask for help because of their self-belief. Users with less skill and low confidence in using the cloud are likely to leave the file undeleted but not change the provider. They will only change the provider if they are confident of using the platforms/interfaces from the new provider, because they do not want to go through the process of having to relearn how to use the new cloud provider. Expertise-driven users may also resort to excluding sensitive files when using the cloud to avoid the anxiety associated with not being able to delete the file from the cloud.

Motivation: Policy-driven. Users whose motivation to delete is policy-driven usually fear the consequences of having that data not deleted in the public cloud. They usually adopt ad hoc strategies as their first coping mechanism, and if they still cannot delete from the cloud, they would then attempt to delete from the device they are confident in using. They would finally ask for help if everything they tried has failed. Nonetheless, prior failure to get data deleted causes them to exclude valuable or work-related files from the cloud.

Motivation: Storage-driven. Users who delete for storage reasons adopt strategies such as deleting a different file, deleting from a single device, cloud hopping and some ad hoc strategies. Deleting a different file may temporarily create space, but as the number of files that the user cannot delete increases, the user eventually runs out of space. Deleting from a single device and some ad hoc strategies may yield results since files get deleted. However, ad hoc strategies like buying more storage cost the user but do not lead to fulfilling the initial goal – that of deleting from the cloud. The results of cloud hopping are temporary; it only works until the user fills out all the new storage provided. In general, a cloud hopping strategy does not scale as users are unlikely

to keep changing providers regularly.

5.2 Mental models and coping strategies

We also observed a potential connection between users' mental models and coping strategies. In Table 3 we summarize how users' mental models and coping strategies are linked.

Table 3: A summary of users' mental models and their coping strategies

Mental models	Coping Strategy
The cloud within an app	Seeking help Deleting from single device Excluding certain files from the cloud Cloud hopping Ad hoc strategies Head in the sand
Borrowed mental models	Head in the sand Ad hoc strategies Seeking help Cloud hopping
Sync folders are not the cloud	Ad hoc strategies Deleting from single device Seeking help
Providers don't delete	Cloud hopping Excluding certain files from the cloud
Shared folder: Deletion is one sided	Head in the sand
Shared folder: Deletion affects all members	Head in the sand Seeking help
Deleting and saving work the same way	Seeking help Cloud hopping
Deletion is permanent and instant	Head in the sand

The cloud within an app. Users who believe the cloud is inaccessible are likely to seek help in order to delete since they do not believe they can actually log on and delete. Others may just try to delete using the single device that they believe is connected to the cloud, which may not be effective as discussed earlier. Some users may choose to cloud hop in search for a cloud that they believe they can access and delete data from, or they may leave files undeleted. Some privacy-driven users with this mental model may opt to exclude files from the cloud, only storing files they perceive to be not confidential.

Borrowed mental models. Upon realizing that their deletion understanding is different from cloud deletion, users may choose head in the sand approach, change to a new provider, seek help, or try other ad hoc strategies. They may choose head in the sand approach because they recognize the mismatch and unexpected outcome. Such users may hop to another cloud where such mental models may yield expected results, and they may finally seek help after trying some ad hoc strategies.

Sync folders are not the cloud. Users who believe sync folders are not part of the cloud may adopt ad hoc strategies to delete from the cloud. Some may seek help to delete while others may delete from web interface instead of the sync folder.

Providers don't delete. These users are likely to change providers or choose to exclude files they perceive to be important from the cloud. Although changing a provider does not solve their deletion issues, they believe the new provider will provide a certain assurance of deletion.

Shared folder: deletion models. Interestingly, though shared folder mental models are different, in both cases, users employ the same coping strategy, head in the sand. Users who perceive deletion to be one sided may choose to leave the files undeleted believing that deleting would not delete the files from other members of the shared folder, while, those who perceive that deletion affects all the members of the shared folder may choose to ignore the file because they do not want to delete files which other users are still using. Users who believe that deletion affects all members of the shared folder often seek help to confirm whether they could delete from the shared folder.

Deleting is permanent and instant. The main challenge faced by users with this model is decision making when it comes to deciding whether a file should be deleted or not. They will believe that it will get deleted forever and instantly, as a result, these users often resort to leaving files undeleted in the cloud with a belief that they might need them again.

Deleting and saving work the same way. Users who possess this model tend to seek help when encountering problems with deletion. Some may also choose to delete from the device where this mental model accurately applies, hence leading to successful outcomes. In this case users rely on recalling previous successful deletion experiences.

5.3 Design implications

Our results revealed a major gap in users' understanding of how the cloud and deletion work. Although the responsibility to delete lies between the providers and the users, our study pointed out that cloud users want more transparency regarding cloud deletion policies. Information on deletion should be clear and easily made available for users especially about how data is disposed after use. Users would also benefit from cloud providers making deletion mechanisms easy to understand and accessible.

Regarding help, cloud users would like to have the option to contact someone directly concerning their deletion problems. This implies that some cloud interfaces provide users with not enough feedback or complicated information which is hard to understand. Something akin to Deletion Service Points would help users resolve their problems quickly. With regards to user interfaces, improving user feedback (e.g., notifications during deletion) would inform users on the end results of their actions therefore influencing or improving their weak mental models.

Another possible avenue for improving the current situation is improving users' understanding and awareness-building. Our study found that users possess different mental models at the same time, of which most are incomplete and lead to failure to delete. We argue that these differences make user education a challenging task hence such education should be customized. Also, since not all incomplete mental models lead to failure to delete, we suggest that user education

should focus on maturing mental models that are weak or those that lead to failure to delete.

5.4 Limitations

Our study is a qualitative inquiry – based on a sample size of 26 participants. This sample is significant for such a study and saturation in grounded theory was reached by 13 transcripts. As such we can be confident that the motivations, failures, coping strategies and desires discussed in Section 4 are grounded in the data from the study. We also accounted for coding bias by using a second researcher to verify the codes emerging from the grounded theory analysis. However, some of our participants who reported that they used the cloud for editing documents could not distinguish between Microsoft Office Online, Office 365 and Office 2016. This may have influenced their judgment and perception of deletion from the cloud. At the same time, it further reflects the inaccuracy of users' mental models with regards to the cloud. Future studies ought to explore the users' mental models of the cloud in general and their impact on various user interactions with the cloud with regards to security and privacy.

5.5 Further research

Our study can form the basis of a number of research directions that can contribute to better understanding and supporting users' needs with regards to deletion in the cloud and associated security and privacy goals.

Deep understanding of cloud users' mental models

In this study, we uncovered different mental models constructed mainly by those participants who could not delete, and we observed that these mental models seem to have an influence on users' deletion practices and behaviors. Hence, we realize the importance of understanding other deletion models constructed by users, and also mental models about the cloud in general, particularly focusing on whether users use or transfer these models to the cloud from other domains (computers, smartphones, etc.) or whether they develop new ones to cope with a new reality. This is important in order to understand the extent of the influence of mental models regarding cloud users' practices and behaviors, as well as their adoption of the cloud. It would also be interesting to study security experts about their cloud usage with respect to deletion. Understanding how they use and delete from the cloud could shed light on the differences between them and the findings of this paper.

Understanding the impact of users' practices and behaviors

In our study, we found that people were using the public cloud for their work purposes without any security tools such as encryption. However, we are yet not sure what motivates this behavior and whether users are aware of the risks associated with this behavior, and how do they decide what goes into a public cloud and what does not. Future research should explore this issue in order to develop further insights into how these behaviors affect users' privacy and security, and the privacy and security of their organizations.

Cloud deletion in specific domains

Cloud usage and deletion could also be explored considering different types of organizations, such as governmental organizations, and across different type of industry organizations. It would be interesting to explore if deletion strategies, failures and coping mechanisms are domain-dependent.

Evaluation of encryption tools and deletion

Some studies (e.g., Tang et al. [29], Rahumed et al. [25] and Ramokapane et al. [26]) recommend the use of encryption tools in the cloud to protect users' privacy after deletion. However, none of our participants mentioned the use of encryption as a means to assured deletion. It is not clear whether users are not using such mechanisms because of a lack of awareness or due to usability issues. Usability studies in this area would help understand how such tools could be improved, or how users could be encouraged to adopt them.

Multiparty access control

In our study, we revealed that cloud users possess incomplete mental models about deleting from *shared* folders, which are managed by one or more users. Even if these models were complete and accurate, the issue of data management, and in particular data deletion, when multiple users are involved in the cloud is an under-explored area. Such multi-party access control has been studied in other domains such as social networks [28] and it would be interesting to study the applicability and usability of such techniques in order to support deletion in the cloud.

Follow-up confirmatory studies

Since our study was of an exploratory nature, we identified factors that play a role in deletion in the cloud and potential relationships between them grounded in the data obtained through semi-structured interviews. The next step would be to undertake confirmatory studies, to further understand these concepts and confirm the extent of their relationships.

6. CONCLUSIONS

Although it is generally assumed that deletion is an easy task, our study shows that cloud users struggle to delete. Their failure to delete leads to construction or development of coping mechanisms to address the problem. Users develop these strategies if they believe that it is important that data is deleted from the cloud. However, information on deletion affects how users construct deletion mental models. A lack of information on deletion leads to construction of incomplete or inaccurate mental models which eventually leads to a failure to delete. These mental models have a direct impact on the choices and the development of coping strategies. Incomplete or inaccurate mental models may lead to development of strategies which do not delete data from the cloud, or strategies which only solve the problem temporarily or bring up additional problems. All in all, our investigations bear out the intuition that usability of deletion or lack thereof in the cloud is a key privacy and security challenge that needs significant attention.

7. ACKNOWLEDGMENTS

We thank all the people who took part in our study. We also thank Dr. Asad Naqvi for his assistance in coding and analyzing our data, and all the anonymous reviewers for their helpful comments and suggestions.

8. REFERENCES

[1] A. Adams and M. A. Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, 1999.

[2] H. Almuhimedi, S. Wilson, B. Liu, N. Sadeh, and A. Acquisti. Tweets are forever: a large-scale quantitative analysis of deleted tweets. In *Proceedings of the 2013 conference on Computer supported cooperative work*, pages 897–908. ACM, 2013.

[3] C. Bravo-Lillo, L. F. Cranor, J. Downs, and S. Komanduri. Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy*, 9(2):18–26, 2011.

[4] A. Bryman. *Social research methods*. Oxford university press, 2015.

[5] D. Burda and F. Teuteberg. The role of trust and risk perceptions in cloud archivingâĂŤresults from an empirical study. *The Journal of High Technology Management Research*, 25(2):172–187, 2014.

[6] C. Cachin, K. Haralambiev, H.-C. Hsiao, and A. Sorniotti. Policy-based secure deletion. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 259–270. ACM, 2013.

[7] L. J. Camp. Mental models of privacy and security. *IEEE Technology and society magazine*, 28(3), 2009.

[8] K. Charmaz. *Constructing grounded theory*. Sage, 2014.

[9] J. W. Clark, P. Snyder, D. McCoy, and C. Kanich. I saw images i didn't even know i had: Understanding user perceptions of cloud storage privacy. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 1641–1644. ACM, 2015.

[10] S. Clark, T. Goodspeed, P. Metzger, Z. Wasserman, K. Xu, and M. Blaze. Why (special agent) johnny (still) can't encrypt: A security analysis of the APCO project 25 two-way radio system. In *20th USENIX Security Symposium, San Francisco, CA, USA, August 8-12, 2011, Proceedings*, 2011.

[11] B. Computer. *Dropbox Deleted files*, 2017 (accessed February, 27 2017). `https://www.bleepingcomputer.com/news/software/dropbox-kept-files-around-for-years-due-to-delete-bug/`.

[12] L. F. Cranor. Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *J. on Telecomm. & High Tech. L.*, 10:273, 2012.

[13] Forbes.com. *Apple safari web history*, 2017 (accessed February 28, 2017). `https://www.forbes.com/sites/thomasbrewster/2017/02/09/apple-safari-web-history-deleted-stored-icloud/#7e58cad76328`.

[14] J. P. G. Gashami, Y. Chang, J. J. Rho, and M.-C. Park. Privacy concerns and benefits in saas adoption by individual users: A trade-off approach. *Information Development*, 32(4):837–852, 2016.

[15] B. G. Glaser and A. L. Strauss. *The discovery of grounded theory: Strategies for qualitative research*. Transaction publishers, 2009.

[16] P. Ilia, I. Polakis, E. Athanasopoulos, F. Maggi, and S. Ioannidis. Face/off: Preventing privacy leakage from photos in social networks. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 781–792. ACM, 2015.

[17] I. Ion, R. Reeder, and S. Consolvo. ... no one can hack my mind": Comparing expert and non-expert security practices. In *Proc. SOUPS*, 2015.

[18] I. Ion, N. Sachdeva, P. Kumaraguru, and S. Čapkun. Home is safer than the cloud!: privacy concerns for consumer cloud storage. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, page 13. ACM, 2011.

[19] M. Johnson, S. Egelman, and S. M. Bellovin. Facebook and privacy: it's complicated. In *Proceedings of the eighth symposium on usable privacy and security*, page 9. ACM, 2012.

[20] K. M. MacQueen, E. McLellan, K. Kay, and B. Milstein. Codebook development for team-based qualitative analysis. *CAM Journal*, 10(2):31–36, 1998.

[21] A. E. Marwick et al. Social privacy in networked publics: TeensâĂŹ attitudes, practices, and strategies. 2011.

[22] A. M. McDonald and L. F. Cranor. The cost of reading privacy policies. *ISJLP*, 4:543, 2008.

[23] S. E. McGregor, P. Charters, T. Holliday, and F. Roesner. Investigating the computer security practices and needs of journalists. In *USENIX Security*, pages 399–414, 2015.

[24] S. Portigal. *Interviewing users*. Rosenfeld Media, 2013.

[25] A. Rahumed, H. C. Chen, Y. Tang, P. P. Lee, and J. C. Lui. A secure cloud backup system with assured deletion and version control. In *Parallel Processing Workshops (ICPPW), 2011 40th International Conference on*, pages 160–167. IEEE, 2011.

[26] K. M. Ramokapane, A. Rashid, and J. M. Such. Assured deletion in the cloud: requirements, challenges and future directions. In *Proceedings of the 2016 ACM on Cloud Computing Security Workshop*, pages 97–108. ACM, 2016.

[27] M. Sleeper, J. Cranshaw, P. G. Kelley, B. Ur, A. Acquisti, L. F. Cranor, and N. Sadeh. I read my twitter the next morning and was astonished: A conversational perspective on twitter regrets. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 3277–3286. ACM, 2013.

[28] J. M. Such and N. Criado. Resolving Multi-Party Privacy Conflicts in Social Media. *IEEE Transactions on Knowledge and Data Engineering*, 28(7):1851–1863, 2016.

[29] Y. Tang, P. P. Lee, J. C. Lui, and R. Perlman. Fade: Secure overlay cloud storage with file assured deletion. In *International Conference on Security and Privacy in Communication Systems*, pages 380–397. Springer, 2010.

[30] B. Ur, J. Bees, S. M. Segreti, L. Bauer, N. Christin, and L. F. Cranor. Do users' perceptions of password security match reality? In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 3748–3760. ACM, 2016.

[31] Y. Wang, G. Norcie, S. Komanduri, A. Acquisti, P. G. Leon, and L. F. Cranor. I regretted the minute i

pressed share: A qualitative study of regrets on facebook. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, page 10. ACM, 2011.

[32] R. Wash. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, page 11. ACM, 2010.

[33] A. Whitten and J. D. Tygar. Why johnny can't encrypt: A usability evaluation of pgp 5.0. In *Usenix Security*, volume 1999, 1999.

APPENDIX

A. DEMOGRAPHICS

A.1 Respondents Demographics

Table 4: Summary: Respondents Demographics.
A total of 48 people responded to our advert, the table below summarizes their demographics.

	No. of participants
Gender	
Male	16
Female	32
Age	
18 - 20	10
21 - 25	18
26 - 30	11
31 - 35	5
36 - 40	2
41 - 45	0
46 - 50	1
51 - 55	1
Educational Background	
High school/College course	14
Bachelors	13
Masters	11
PhD	9
Preferred not to say	1
Employment status	
Unemployed/Retired	2
Full time	15
Part-time	3
Student	28
Cloud services	
Dropbox	22
iCloud	20
OneDrive	22
Google Drive	21
Box	13
Microsoft Office 365	35
Google Docs	29
OneNote	6
Cloud Access	
Smartphone	48
Tablet	24
Desktop	30
Laptop	43
Cloud activities	
Uploaded files	48
Deleted data	47
Shared folder/files	46
Deleted an account	30
Recovered deleted files	15
Downloaded files	36
Read a service agreement	12
None of the above	1

A.2 Interview Demographics

Table 5: Summary: Interview Demographics.
26 people were invited to take part in our interviews.

	No. of participants
Gender	
Male	12
Female	14
Age	
18 - 20	3
21 - 25	8
26 - 30	6
31 - 40	7
45 +	2
Educational Background	
High school/College course	5
Bachelors	9
Masters	5
PhD	6
Preferred not to say	1
Employment status	
Unemployed/Retired	1
Full time	12
Part-time	3
Student	10
Cloud services	
Dropbox	15
iCloud	9
OneDrive	6
Google Drive	17
Box	17
Microsoft Office 365	15
Google Docs	14
OneNote	2
Cloud Access	
Smartphone	26
Tablet	13
Desktop	23
Laptop	25

B. INTERVIEW GUIDE

Thank you for participating in our study. As you read in the consent form, we will be recording the session so we can review it to make sure that we don't miss any part of our conversation. Your information will be kept confidential and will only be accessed by us. Your name will not be associated with any data I collect. Do you have any questions regarding the consent form? Do I have your permission to start the recording?

1. Do you use any of the following services or similar services? Examples: Dropbox, Box, iCloud, G-Drive, One-drive.
   - Follow-up-1: How often do you use them?
     (a) Prompt: Would you say you use them every day?

- Follow-up-2:What do you use these services for?
  (a) Prompt: Is it for work or its personal?
- Follow-up-3: You mentioned that you use [service/services], how do you use [it/them].

2. Do you use any of the following services or related services? Examples: Office365, Google Docs etc.
   - Follow-up-1: How often do you use them?
   - Follow-up-2: What do you use these services for?
     (a) Prompt: Is it for work or its personal?
   - Follow-up-3: Can you describe to me how you use [name of the service]?
3. Do you have any particular reason why you use these services?
4. When you store your files in [service mentioned in Q1] or create a document in [service mentioned in Q2] what happens?
   - Prompt: Do you know where they are stored?
5. Have you ever deleted something you uploaded on [service mentioned in question 1]?
   - Prompt: Have you ever thought of deleting something you have uploaded online?
   - Follow-up-1: Why?
   - Follow-up-2: Can you share with me how you go about deleting a file in [service mentioned by user in Q1]?
     (a) Prompt: You mentioned that you use [name of the service], how do you delete data from [name of the service]?
6. Have you ever deleted something you uploaded on [service mentioned in question 2]?
   - Follow-up-1: Why?
   - Follow-up-2: Can you share with me how you go about deleting a file in [service mentioned by user in Q2]?
     (a) Prompt: You mentioned that you use [name of the service], how do you delete data from [name of the service]?

   [NOTE: If the participant claims to have never deleted anything from the cloud before, ask the following question otherwise skip it]
7. You have mentioned that you have never deleted or been asked to delete anything before, how come?
   - Follow-up-1: How do you deal with information that you no longer need?
8. Have you ever faced problems or challenges when trying to delete your data from any of your services?
   - Prompt: Can you recall a time when you wanted to delete something but could not figure out how to delete it or you could simply not just delete.

   [If participant says Yes]
   - Follow-up-1: Which service was that and how did you resolve or get around those challenges? Or how did you finally delete then?
9. Have you ever been required to recover information you have previously deleted?
   - Prompt: Have you ever needed a document or file that you had previously deleted from [service mentioned in Q1 or Q2].
   - Follow-up-1: Were you successful?
   - Follow-up-2: How did you do it?
10. Do you ever think the information [e.g., files, documents] you have previously deleted still exist somewhere online or can be shared by your service provider?

    [If participant says Yes]
    - Follow-up-1: Why?
    - Follow-up-2: What do you do to ensure that your deleted information can never be shared after you have deleted it?

    [If participant says No]
    - Follow-up-1: You mentioned that you don't think your information could be shared after it has been deleted, why?
11. After you delete your files, do you know how long it takes for [service mentioned at Q1 or Q2] to delete them from their side?
    - Prompt: How long does deletion process take?

    [Explain to the participant that you will share a scenario with them and then ask questions using the scenario. Choose one scenario per interview depending on the interviewee occupation, for example, if the interviewee is a student ask them scenario one.]

    Scenario 1
    After a [late night out/party/picnic], your [friend/colleague] creates a folder in [service mentioned] and shares it with you and your other friend. He then tries to be funny and decides to upload 3 embarrassing photos of you three that you took on the night out. You are embarrassed and decide to delete all the photos from the shared folder.

    Scenario 2
    You have just joined a new team at work. Your new supervisor creates a folder in [service mentioned by participant] and shares it with you and your other colleagues. Your supervisor uploads some documents for you and your team to work on. Upon a discussion between you and your supervisor, s/he realizes you don't need one of the documents so s/he asks you to delete the document.

    [Scenario Questions]

12. What do you think will happen when you delete the [photos/document]?
    - Prompt: Will [they/it] be deleted from the shared folder or just your computer or device?
13. Will the [photos/document] be deleted from all your [friends'/colleagues'] accounts or they will only be deleted from your account?
    - Prompt: Will the deletion process affect your [friends/colleagues] too?

    [End of scenario questions]
    Explain to the interviewee that the questions on the scenario have ended.

14. If you were told that information you delete may never be completely deleted, what would you do differently?
15. Do you know anything about the "right to be forgotten" European ruling?

[Explain to the user that you are at the end of the interview, ask them if they do have any questions or anything they want to share about deletion from the cloud.]