Multiuser Privacy and Security Conflicts in the Cloud

Eman Alhelali
eman.alhelali@kcl.ac.uk
King's College London
London, UK

Kopo M. Ramokapane
marvin.ramokapane@bristol.ac.uk
University of Bristol
Bristol, UK

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

ABSTRACT

Collaborative cloud platforms make it easier and more convenient for multiple users to work together on files (GoogleDocs, Office365) and store and share them (Dropbox, OneDrive). However, this can lead to privacy and security conflicts between the users involved, for instance when a user adds someone to a shared folder or changes its permissions. Such multiuser conflicts (MCs), though known to happen in the literature, have not yet been studied in-depth. In this paper, we report a study with 1,050 participants about MCs they experienced in the cloud. We show what are the MCs that arise when multiple users work together in the cloud and how and why they arise, what is the prevalence and severity of MCs, what are their consequences on users, and how do users work around MCs. We derive recommendations for designing mechanisms to help users avoid, mitigate, and resolve MCs in the cloud.

CCS CONCEPTS

• **Computer systems organization → Cloud computing**; • **Security and privacy → Usability in security and privacy**.

KEYWORDS

Multiuser Conflicts, Multi-party Privacy Conflicts, Interdependent Privacy, Cloud Security

ACM Reference Format:
Eman Alhelali, Kopo M. Ramokapane, and Jose Such. 2023. Multiuser Privacy and Security Conflicts in the Cloud. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23), April 23–28, 2023, Hamburg, Germany*. ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3544548.3581307

1 INTRODUCTION

Cloud systems allow users to collaborate in the creation, edition, storage, sharing and management of data [3, 43]. It is estimated that over 2 billion users now use cloud systems to store and share hundreds of billions of data items, and by 2025, there will be more than 100 zettabytes of data stored in the cloud [66]. As a result, cloud systems are expected to continue growing in the future years, both in the number of users and the amount of data they store and share. In parallel, the associated privacy and security issues will continue to grow [49]. In this aspect, the inappropriate use of cloud services can result in data loss, denial of service, data theft, privacy issues, hacking, and stealing of data [3].

Because of the cloud's collaborative nature, allowing multiple users to co-create, co-own, co-edit, and co-manage files and folders, cloud systems may also be prone to multiuser conflicts (MCs) between users. MCs in the cloud may occur when a user's action leads to privacy violations, loss of data, or integrity of the data/folder they are sharing with others. While MCs have been studied extensively in other collaborative online systems such as social media [60, 69], they have not yet been studied in-depth in the cloud. Nevertheless, previous literature on usable security and privacy literature in the cloud provides evidence of potential MCs in the cloud [29, 53, 67]. Only two studies considered MCs in the cloud, but they are only restricted to the MCs that arise when some users change the location or names of files [16, 43].

In this paper, we present the first in-depth, empirical study of experienced MCs in the cloud, from identification of any actions that lead to MCs, to communication and/or resolution. We aim to answer the following research questions:

RQ1. What are the characteristics of multiuser conflicts (MCs) in the cloud? How and why do MCs happen?
RQ2. What are the major impacts and consequences of MCs on users?
RQ3. How do users work around MCs; in other words, what strategies do they rely on to address MCs?

To answer these research questions, we conducted a survey with 1,050 participants collecting MCs they experienced following the Critical Incident Technique (CIT) [9] using two questionnaires, with closed- and open-ended questions, which we analyzed quantitatively and qualitatively. In particular, we examine MCs considering both the Initiator users (the users that caused the MC) and the Affected users (those affected by the MC) on both shared files and folders. We specifically asked about the context of the files/folders in question, what was the reason that caused the MC, who was involved, what did they do, the severity of the MC, any communications between Initiator and Affected about the MC, the approach followed to try to resolve the MC, and whether the MC was resolved or not.

By answering our research questions, we provide the following contributions. First, we identify how MCs affect users in the cloud, with most MCs causing *security* and *privacy* issues to Affected users, including loss of confidentiality, loss of integrity, and loss of availability. Second, we uncover the actions (taken by Initiators) that lead to MCs, the reasons behind such actions, and discuss the instances in which those actions lead to MCs. Actions that lead to MCs include sharing, editing, permission setting, restructuring and renaming, and deleting files and folders. Some actions happen due to mistakes, while others result from the lack of technical skill, misjudgment, and security and privacy concerns. Third, we

CHI '23, April 23–28, 2023, Hamburg, Germany

ACM ISBN 978-1-4503-9421-5/23/04…$15.00
https://doi.org/10.1145/3544548.3581307

find that Affected usually communicate with Initiators to make them aware of the problem, to try to resolve it, reprimand them, or avoid the MC from happening in the future. Sometimes Affected users do not communicate with Initiators, particularly if they feel the damage has already been done and there is no point, especially if the severity of the MC is considered to be low. Fourth, we show the technical and non-technical strategies that users utilize to try, but not always or completely succeed, to resolve MCs. Non-technical strategies include discussing the issue and/or apologising/explaining if needed, while some MCs require technical strategies, where the Initiator may have to re-do (or reverse) their actions, adjust permissions, or provide protection for the concerned file or folder. Importantly, we find that some of the MCs do not get resolved due to the irreversible nature of the action, and some MCs have enduring impacts that lead to communication or relationship breakdown. Finally, based on our results, we recommend to have both preventative and recovery mechanisms to support users avoid or manage MCs, with mechanisms to facilitate the detection of sensitive content, more collaborative cloud interfaces, usable mechanisms to facilitate approval and consent of actions done by others, and new communication mechanisms available to support users during MCs.

2 RELATED WORK

2.1 Security and Privacy in the cloud

The prevalence and adoption of the cloud have not come without security and privacy challenges [2, 16, 56, 72, 73]. To further understand users' concerns and pratices, several notable studies have been conducted. For example, Ion et al. [26] investigated cloud consumers' privacy attitudes and beliefs. They indicated that consumers' privacy requirements differ from those of enterprises. When investigating users' general use of cloud office suites, Dominik et al. [67] found that users were mainly concerned about unauthorized access to their documents and believed that the cloud office suite provider was responsible for informing them in the event of unauthorized access. They also indicated that users' threat models remain unclear. Daniel et al. [8] found that trust is a critical factor in reducing uncertainty and the perception of risk, and trust can be increased by the providers' reputation and users' satisfaction. While these prior works highlight the users' security and privacy issues around cloud usage, they do not shed light on the security and privacy issues that result from users sharing or collaborating in the cloud. Actions or situations that lead to multiuser conflicts are missing in the existing literature; what causes these conflicts, their consequences on the initiators, and the affected's security and privacy are yet to be considered. Our study provides insights with regard to multiuser cloud conflicts. Regarding cloud practices, Ramokapane et al. [53] examined cloud users' deletion practices, challenges, and the coping strategies they deploy to alleviate their struggles. They found that users usually refrain from deleting from shared folders, especially files uploaded by other parties. However, they also found that other users did not understand that deletion from shared folders affected every member of the shared folder. In another study [54], they found that when they are many collaborators in a shared folder, users preferred a deletion type that allows recovery to the one that completely deletes data from the shared folder. While users' cloud deletion strategies have been discussed, no prior work has explored the strategies users employ when having conflict while collaborating in the cloud. This work provides strategies that users employ to resolve or prevent multiuser conflicts in the cloud. Khan et al. [29] investigated user experience with cloud computing, including why participants chose to store files in the cloud, the kind of data they stored but forgotten about, and what they wanted to do with that data. The results of the study underlined the need for mechanisms that enable users to manage the risk in the files they have stored and forgotten about in the cloud. However, concerning MCs, no evidence suggests the need for mechanisms to resolve them. Our work is the first to provide evidence on the mechanisms needed for resolving or preventing MCs.

2.2 Multiuser Privacy and Security Conflicts

A number of researchers have explored MCs before, but, mainly, in other domains. This includes research on collaborative access control models (see for instance [48] for a recent literature review), as well as the extensive literature on multiuser and interdependent privacy (see for instance [24, 59] for recent literature reviews on the topic). In all cases, there is a recognition that, in modern online and mobile systems, the privacy and security of one user is no longer an individual matter [4, 15, 24, 32, 38, 59, 61, 68, 70, 71]. That is, the privacy and security of one user does not only depend on what that user does with her data, but it also depends on what other users do with that data. The typical example is that of a group photo that is shared in social media, how the uploader decides to share the photo in social media may have a privacy and/or security impact on all the others depicted in the photo. In fact, the vast majority of the work on MC has focused on social media. From empirical research to study the phenomemon of MCs in social media and how and why they occur [6, 10, 18, 27, 32, 55, 60, 68] all the way to research on methods and systems to prevent MCs from happening in the first instance [19–21, 25, 35, 36, 46] and manage MCs when they may occur to avoid undesired security and privacy consequences [5, 22, 23, 41, 42, 52, 57, 58, 65]. However, no previous work has empirically examined MCs in the cloud. As we will see and discuss later on, our study uncovers crucial differences between social media MCs and cloud MCs. In the cloud domain, MCs have only been considered focusing on two particular aspects discussed next. Harkous and Aberer [16] studied the privacy impact of third-party apps on cloud computing and found that most of these applications ask users to gain full access to not just the user but also their collaborators, potentially causing privacy MCs as their collaborators may not be happy with that. Nebeling et al. [43] studied users of Dropbox and found that they had availability and other security issues when tracking of the files they uploaded as other users could change the location, delete or rename the files.

While these two works focused on two very specific instances of MCs, there is a lack of understanding of MCs in the cloud in general.

3 METHODOLOGY

To answer our research questions, we used a mixed-method survey approach to collect quantitative and qualitative data, and then followed thematic analysis [7] to analyse qualitative data and used descriptive and inferential statistics to analyse quantitative data. As detailed in the next section, we used the Critical Incident Technique (CIT) [9, 14] to collect the MCs that occur when multiple users collaborate using files/folders in the cloud. The CIT involves collecting data from humans having experienced particular incidents [14], and it has been extensively and widely used to collect critical incidents from users in marketing, healthcare, education, psychology, and computer science research [9]. The decision to use CIT to collect and study cloud MCs was due to its success to collect and analyze incidents related to multi-user issues before in other domains, for eaxmple, in social media [60]. It has also been used successfully in other recent human-centred security studies, including the study of security incidents [51], users' experiences updating software [63], and users' perceptions of being discriminated by automated AI-based systems [62]. This study was approved as a minimal risk by our institution's IRB.

3.1 Survey Instruments

Two main questionnaires were designed based on the two roles users can play on an MC. The first questionnaire, the Initiator, was designed to find incidents from the point of view of someone who unknowingly or knowingly had done something on a file or folder that affected others. The second questionnaire, the Affected, was designed to find incidents from the point of view of users affected by someone else's actions while sharing files and folders in the cloud. However, we acknowledge that, in reality, any user can play both roles (obviously, not simultaneously in the same MC). Therefore, the idea to gather incidents considering the two roles users can play is to have a complete perspective, as previous research in social media MCs already found that users' perceptions of the situation may change depending on the role they play in each MC [60]. To avoid making the questionnaires too long, each of these two questionnaires was further sub-divided based on the different nature of files and folders. We designed the four sub-questionnaires (the Initiator shared files, the Initiator shared folders, the Affected shared files, and the Affected shared folders) to be almost identical with small variations/wordings due to the role played (either the Initiator or the Affected) and whether the issue referred to files or folders. The four sub-questionnaires contained around forty questions each (see Survey file in supplementary materials for a sample sub-questionnaire, the one for Affected Shared Files). We studied both contexts (i.e., shared files and folders) because prior studies around cloud collaborations mainly focused on shared files rather than folders. Moreover, due to the lack of studies concerning Cloud MCs in the wild, we wanted to provide an depth understanding of how conflicts manifest in the whole ecosystem.

In a nutshell, the questionnaires followed the CIT guidelines to gather details about the most recent MC [9, 14]. This is important according to CIT in order to avoid guiding participants or biasing the study to the most dramatic or vivid incidents, or some other selected group [64]. This also allows for the study of prevalence, frequency, severity, and to broaden the understanding of the occurrence of the incidents in the wild [60]. This was done based on the role of each participant, so we asked about: a) the last time someone was unhappy because of their actions on a shared file or folder (Initiator); or b) the last time they were unhappy because of somebody else's actions on a shared file or folder (Affected). Then, the questionnaire asked a number of closed and open ended questions about this incident.

The questions were structured based on the stages of interpersonal conflicts [13]: conflict identification, communication, and resolution. We specifically asked about the context [45] of the files/folders in question, what was the reason that caused the problem, who was involved and the relationship between them, what did they do, the self-assessed severity of the MC; the nature of any communications between Initiator and Affected about the MC; and the approach followed to try to resolve the MC, and whether the MC was considered to be resolved or not. Finally, we also asked about demographics at the end of the survey.

3.2 Procedure and Pilot

The four sub-questionnaires were created and hosted on Qualtrics, and Prolific was used to administer the questionnaires to participants. At the beginning of the study, we gave participants a short explanation about our survey and sought their consent to participate before continuing. Before rolling out the study, we conducted a pilot study to check the flow, timing, sufficient variation in responses, how the questions were understood, and question non-response. After running the pilot study, we clarified some of the questions, e.g., the question about the relationship between those involved seemed confusing, so we also asked specifically about the type of it (e.g., friend, family, colleague). The pilot test was done through Prolific on 10 participants for each version of the questionnaires, so there were a total of 40 participants involved in the pilot test. None of the data collected during the pilot study was used in the final data analysis. The final versions of the sub-questionnaires were administered to 1126 participants. Specifically, participants were randomly assigned to one of the sub-questionnaires, that is to the Initiator shared files, the Initiator shared folders, the Affected shared files, or the Affected shared folders version of the questionnaire. To avoid biases, we excluded any participants who took part in one of the survey versions from taking part in the other versions. It took an average of 17 minutes to complete the survey and participants were paid $3 (circa $12/hr).

3.3 Data Reliability

To ensure data quality, we implemented three well-known and widely-used quality control measures when administering the survey instrument [11, 31, 39, 47, 50, 60]. First, we spread two attention checkers across each survey [39, 47]. Second, we applied a reverse coding method in two of the Likert questions to prevent and being able to detect later straight-lining responses from participants [11, 31]. Last but not least, we only recruited participants with a high reputation, with at least 100 submissions and an approval rate of 95% or more during recruitment [50, 60].

		# Participants			# Participants
Gender	Female	440	**Age**	18-24	272
	Male	602		25-34	388
	Other/N/A	8		35-44	235
Education	No formal education	5		45-54	92
	High school/College course	368		55-64	45
	Undergraduate degree	345		65-74	16
	Postgraduate degree	326		75-84	2
	Prefer not to say	6	**Employment status**	Full-Time	336
Nationality	United Kingdom	376		Part-Time	85
	European Union	303		Due to start a new job	8
	United States	182		Not in paid work	40
	Global South	73		Unemployed	44
	Other Global North	49		No answer	537
	No answer	67	**Period cloud usage**	1 year	61
Cloud services	Dropbox	434		2 years	145
	Google Drive	797		3 years	186
	iCloud	287		4 years	86
	OneDrive	413		>4 years	572
	Box	19	**Using cloud to share folders/files**	Daily	140
Cloud Access	Smartphone	723		Weekly	477
	Tablet	185		Monthly	371
	Desktop	495		Yearly	62
	Laptop	746			

Table 1: Participants demographics. Our sample was diverse in gender, age, education, nationality, employment, the cloud services participants used, how they accessed the services, and how long they have been using the cloud.

3.4 Coding Process

To analyze open-ended questions, we used thematic analysis [7]. Two of the authors familiarised themselves with data from the first questionnaire. Then, the lead coder created an initial version of the codebook. The second coder then used the codebook to independently code the responses from the first sub-questionnaire, i.e., the Affected shared folders. The two researchers then met and discussed the codebook. Initially, there were disagreements due to different understandings of cloud conflicts and general cloud usage. The two coders resolved these disagreements through a series of discussions (i.e., arguing to consensus [28]). After the final codebook was agreed the two researchers then independently attempted to code the second sub-questionnaire (i.e., the Initiator shared folders). At that point, the two researchers realized that the codebook might need many different changes to account for the new perspectives brought by Initiators (for the other two sub-questionnaires), so they decided to have two different codebooks for Initiators and Affected. Therefore, the first step after this was to use the first codebook (developed based on the Affected shared folders) on the other Affected shared files. This meant the addition of only a few new codes due to the difference between files and folders. The coders then collaboratively identified possible themes, grouped similar codes, defined and named the themes. The Cohen's Kappa coefficient agreement was 0.74 for the two surveys which is highly acceptable as a good agreement [37]. The two researchers then created the second codebook, which focused on the Initiator. They followed the exact same process as for the first codebook; the two coders independently coded one sub-questionnaire (Initiator shared files) to generate the codebook and then discussed the coding scheme. The two coders discussed the disagreements, identified key themes, and then finalized the codebook. Then, they coded the final sub-questionnaire (i.e., Initiator shared folders). The resulting Cohen's Kappa was 0.77, which again is highly acceptable as a good agreement [37].

3.5 Participants

In total, 1,126 participants were recruited. From them, 14 participants were discarded because of straight-lining 2 failed the two attention check questions, 36 failed one attention check question, 6 had not used the cloud before, 9 reported an incident not related to the cloud, and 9 provided useless answers (e.g., 'blabla'). The remaining 1,050 participants (cf. Table 1 for demographics) were analyzed; 260 respondents completed the Initiator shared files survey, 265 the Initiator shared folders, 266 the Affected shared files, and 259 the Affected shared folders. Regarding diversity, our sample had 440 females (602 males and 8 others), various education qualifications, nationalities, and employment status (40% employed, 4% unemployed). It also included participants from the global north: 376 from the UK (36%), 303 from EU countries such as Germany, France, Netherlands, Italy, Spain and others (29%), 182 from the US (17%), and 49 (5%) from other countries like Australia, Canada and Israel; while some participants, 73 (7%), were from countries in what is considered the global south, including Chile, China, India, Angola, Colombia, Nigeria, and Philippines. Moreover, some of these countries have different security and privacy laws, others not yet, which gives our study deep but broad views on security and privacy in general.

4 GENERAL CHARACTERISTICS OF MC

We start by providing a general characterization of the MCs we collected and analyzed:

Prevalence and Recency: The vast majority of participants (99%) reported a multiuser conflict and only 1% of participants reported that they had never experienced an MC. Therefore, the prevalence of MC is high and has affected most users at some point. Results from four surveys indicate that 20% of participants experienced their last MC within just *one month* from the survey date, 34% of participants had the last MC within 6 months, 22% of participants experienced the last MC within a year, 15% of participants experienced the last MC within more than a year, 8% of participants reported that the MC happened during an event such as COVID-19 quarantine, and only 1% of participants reported that they did not

remember the date. Overall, these results indicate that the majority of the participants experienced their last MC within 6 months of the survey's date (54%) and that most of them experienced their last MC within 1 year of the survey's date (76%).

Platform: From all surveys, based on the kinds of cloud services that the respondents were using, we found that the majority of MCs happened in Google Drive 54%, which is likely related to most participants, 797 (77%), using it as reported in Table 1. After that, with 23% of MCs, came Dropbox, which is also the second most-used service (42%) by participants. The third one is Microsoft OneDrive with 13%, used by 413 (40%) participants. The least reported platform for MCs is Apple iCloud 7%, also related to 287 (28%) of participants using it (see Table 1). Around 2% of participants reported using other cloud platforms such as SharePoint, Huddle, Box, and MEGA. Taken together, these results seem to suggest that MCs happen similarly regardless of the types and platform of cloud service.

Data Type: Our survey respondents indicated that conflicts occurred when different actions (detailed in section 5) were done on files and folders, where the type of files included documents (e.g., Microsoft Office365), photos, audio files, and videos. Regarding ownership of data, 311 (60%) of Initiators stated that they owned the shared folder/file, while 206 (40%) stated that they were not the owners. For the Affected, 271 (52%) indicated that they were the owners of the shared folder/file and 249 (48%) indicated that they were not the owners of it. Overall, these results suggest that MCs occur regardless of the type and ownership of data.

Social Context: Our findings suggest that most MC happen between work colleagues (43%), between friends (32%), within families (16%), in education settings (5%), and others (3%). Conflicts happened on shared folders and files created to serve various purposes, including work, education, social and family events. Power dynamics (2%), though not prevalent, also seemed to play a role, as some of the relationships reported involved individuals with a potential power imbalance, such as manager and co-worker, advisor and student, etc. For instance: *"I was working on a project with a work partner when a disagreement came up on how to handle a certain file. He was the head of the project and restricted my ability to edit the file."* (P160 AffectedFolders).

Severity: Participants were asked to identify on a Likert scale how severe the conflict was, with 7 being extremely severe and 1 not at all severe. Figure 1 represents the number of conflicts and severity, showing a very similar pattern for all surveys of fewer cases as the severity increases. However, it is easy to spot a difference between Initiators and Affected, confirmed with a significant correlation ($r = -0.10$, $p < 0.01868$), i.e., in general, Initiators consider MCs less severe than Affected.

5 WHAT DID INITIATORS DO TO CAUSE THE MC?

We now explain the actions that led Affected to *feel* affected and caused MCs. These actions include sharing (44%), permission setting (19%), editing (17%), deletion (or lack thereof) (13%), lack of expected action (4%), and restructuring or renaming (2%) of files and folders. Table 2 provides a summary of situations where MCs occurred for each action. The first two columns state and describes the actions that led to an MC, and the third column lists the possible reasons why the affected was not happy about the action, which may be different depending on the action. The last column lists the possible explanation from the initiators why the action was made or occurred, with some reasons (e.g., storage management) only reported to lead to some actions (e.g. deleting).

Sharing: Many participants reported MCs when someone shared files or folders. Regarding folders, MCs were mainly due to one member of the shared folder adding someone new to the folder without consulting others, uploading a members' personal files to the folder, sharing inappropriate content, sharing the folder further or outside the shared folder members, or sharing the folder without securing it. The most common action was adding a new person to the shared folder, e.g., "*We were working on a project as a group and decided that only members of the group could view and edit the document. But one member added another person who was not part of the group to view and edit the document. We were worried that this person would take ideas from our project and implement it on his project*" (P179 AffectedFolders). Regarding files, Some MCs happened when one group member shared files outside the group through other cloud or social media platforms. "*I had shared some of my best photos to let some family members see them. One of them copied some and then shared them on social media as if they were their own. They also shared some photos of me on social media. All of this was without my permission (which I would not have given) and without asking me. I only found out that this had occurred through another friend!*" (P85 AffectedFiles). Others reported an MC when a member shared a file without first encrypting or securing it: "*I remember my friend being angry with me for sharing photos with him using google drive. The photos were zipped but not protected by a password, and he was angry with me for even using google drive to share private data*" (P152 InitiatorFiles).

Permission Setting: An MC also occurred when Initiators changed permissions and access rights and one or more members of a shared folder or file could not access it as a result. Regarding shared folders, participants reported that conflicts started when one or more members could not access a secured (password-protected) folder or some of the shared contents and when a member shared a folder using a different cloud service that other members did not have access to, e.g., "*My manager pulled my access to a shared folder at work. It meant I didn't have access to important information, making my days' work very hard.*"(P12 AffectedFolders). Other file MCs were mainly due to not having access, not having the right to edit, or when their permissions were wrong, e.g., "*my friend and I collaborate on a project together. she decided to restrict my ability to edit certain files because she wanted to have full control over certain aspects of the project*" (P234 AffectedFolders). Another participant, (P200 InitiatorFiles) explained that they could not access password-protected files, "*I had the file encrypted for extra security, and went on vacation, they were upset because they were unable to access the file while i was gone and had to wait.*".

Editing: From all the four surveys, participants reported that editing a file without permission, editing the wrong file, editing a file late, making undesirable edits, editing without following an agreed protocol, or any editing that led to corrupted files caused MCs. One member explained: "*We were doing work about a project all together on a shared document on google drive. We said that it was done for the day, but one of my colleagues decided to do things*

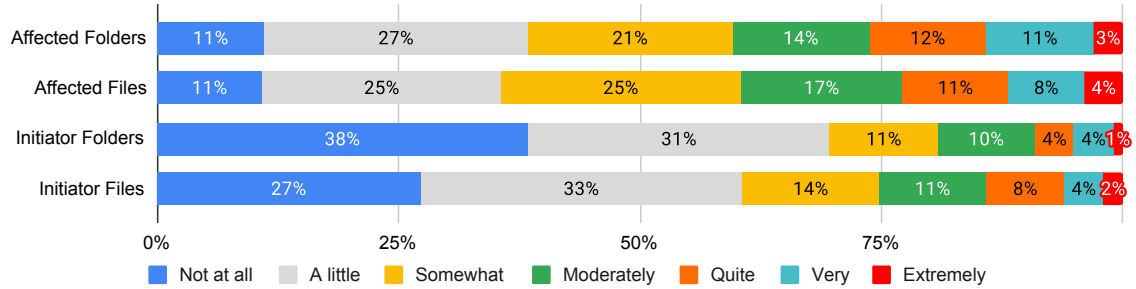

Figure 1: Severity of MCs. Initiators reported MCs as less severe than the affected, while severity was similar for files and folders.

Actions	When conflicts occurred	Reasons from Affected	Reasons from Initiator
Sharing (44%)	- When a member of a shared folder adding someone new - Uploading a member's files to the folder - Sharing inappropriate content - Sharing shared folders/files further (sometimes through another platform) - Sharing the folder without securing it - Sharing content unintentionally (or deliberately) - Sharing a file that is not ready for sharing	Loss of confidentiality Lack of consent Not following agreed rules	Mistakes Lack of technical skill Denying access purposefully Misjudgement
Permission setting (19%)	- Members cannot access shared contents or a secured file or folder - Some members do not have access to files or do not have editing rights - A member has set up the wrong permissions - Members share using a different cloud service that not all members have access to	Loss of availability Lack of consent	Mistakes Lack of technical skill Denying access purposefully Security and privacy concerns
Editing (17%)	- Editing a file - Editing the wrong file - Editing a file late - Making undesirable edits - Editing that leads to corrupted files	Loss of integrity Lack of consent Not following agreed rules	Mistakes Denying access purposefully
Deleting (13%)	- A member permanently deleting a file or folder without consultation - A member failing to delete a file or folder they were supposed to delete	Loss of availability Lack of consent Not following agreed rules	Mistakes Lack of technical skill Misjudgement Storage management
Lack of expected action (4%)	- A member do not complete a required action - A member failing to share, edit or delete	Loss of availability	Mistakes Lack of technical skill
Restructuring and renaming (2%)	- A member changing the organisation/name of the shared folder/file or its contents	Loss of availability Lack of consent Not following agreed rules	Mistakes

Table 2: A summary of specific areas where MCs occurred for each action, Affected reasons for being unhappy, and reasons behind Initiators' actions.

on our backs and change what we had done all together a few hours earlier" (P28 Affected Folders).

Deleting: Participants from all the surveys explained that some MCs started after a member deleted a file or folder permanently or when a member failed to delete a file or folder they were supposed to delete. One participant reported: *"At some point in time, the folder owner decided to delete the folder. No warning was given, and access was lost for good"* (P187 AffectedFolders). Regarding undeleted files, P59 InitiatorFiles explained that forgetting to delete a photo their partner asked them to delete from a folder they shared with his parents caused a conflict between him and their partner: *"She deleted it after she had found out [I didn't], but parents had already seen it."*

Lack of expected action: Our survey indicate that a few MCs arose because of the Initiator did not complete a required action. Participants explained that failure to share, edit or delete sometimes caused issues among members. "*I am very nervous and tend not to do something until I know how to do it. I could not work out how to upload/download - I had no idea.*" (P254 InitiatorFiles). Another participant stated "*Wanted our holiday from 2019 photos together and the person was asked to upload. She never uploaded the photos*" (P88 AffectedFolders).

Restructuring and Renaming: MCs were also caused by the Initiator changing the organisation or name of the shared folder or its contents. Regarding folders, MCs could happen due to chaning the structure of the folder, e.g., "*I reorganized a folder and a team member was annoyed because he had to learn the new organization system*" (P194 InitiatorFolders); or by sharing an unorganised folder. Regarding renaming folders and files, MCs happened when a member renamed a folder without following the agreed naming style or work protocol: "*Several people did not follow my instructions, and they did not name their files the way I asked. It made me spend extra time renaming their files, and it was annoying*" (P121 AffectedFiles). Participants from the Affected folder and file surveys also mentioned that MCs occurred when members created many copies of the same file.

In terms of prevalence of actions in particular situations, Table 3 summarizes the actions that led to the MCs broken down by the social context (as introduced in Section 4). Regardless of the social context, Sharing is the most common action that leads to MCs by far (as the totals in Table 2). For instance, for the most common context (work), Sharing was the most usual action that led to MCs. We can also see that all actions were reported as leading to MCs in all social contexts, with few variations between them. For instance, even in the Friends context, with the highest Sharing proportion over the total number of actions for that context, almost half of the other actions that led to MCs were not sharing but others like

	Actions					
Social context	**Sharing**	**Permission Setting**	**Editing**	**Deleting**	**Lack of expected Action**	**Restructuring and Renaming**
Work	171 (38%)	83 (18%)	102 (23%)	55 (12%)	27 (6%)	11 (2%)
Education	21 (38%)	12 (21%)	12 (21%)	5 (9%)	2 (4%)	4 (7%)
Family	70 (42%)	38 (23%)	22 (13%)	31 (19%)	3 (2%)	2 (1%)
Friends	183 (56%)	60 (18%)	38 (12%)	42 (13%)	1 (0%)	5 (2%)
Others	13 (35%)	8 (22%)	4 (11%)	4 (11%)	6 (16%)	0 (0%)

Table 3: Actions broken down by social context. All actions occurred in all social contexts with only a few variations across contexts.

Permission Setting, Editing, and Deleting. Finally, looking across actions and contexts, even in cases where differences seem higher for one action (e.g. editing in work/education vs family/friends), there is still a sizable amount of that action for all social contexts. Given the low count of many cells in the table, we did not conduct any statistical tests as their results could be unreliable.

5.1 Why and How did the MC affect *Affected* participants?

We now report the main reasons why Affected participants were affected and that led to the MC. Note that the frequency numbers below do not represent all participants because the themes that emerged after our analysis and that are discussed below emanate from a series of questions, i.e., we did not explicitly ask one particular question about this.

Loss of confidentiality: 383 (37%) of participants reported that they were left unhappy because files and folders containing personal, private, or confidential data to them or the group were made accessible to others. They complained they lost the privacy and security of these data when someone new was added to the shared file or folder or when such content was shared outside the cloud in other platforms. Others also explained that they risked losing the rights to their work. Finally, some Affected did not trust those with whom the Initiator shared.

Loss of availability: 180 (17%) of participants reported that they were unhappy when they realized they had lost their data and would not recover it, or when they lost access. They explained that this was usually when other members deleted or revoked access without consulting them.

Lack of consent: 156 (15%) of participants indicated Initiators conducted an action without their consent. This included when another person was added to the file/folder or when files were shared further; when content was changed or erased; when files or folders were deleted; and when permissions were changed.

Loss of integrity: Around 155 (15%) participants explained that they were unhappy because the file they were working on was corrupted or the content or their edits were changed. Participants explained that some files got corrupted after other members edited them. Some informed us that their team members kept making changes to their work which led to them redoing it.

Members not following the agreed rules: Our analysis shows that users make rules of engagement and collaboration to protect their shared files and folders concerning sharing, editing, and deleting. When such rules are not maintained, they leave other members unhappy. Thirty-three (3%) of participants reported this.

5.2 Why did Initiators perform the action?

We now report the most common reasons from Initiators on why they performed the action that led to the MC:

Mistakes: When we asked the Initiators the reasons behind their actions that led to MCs, 155 (15%) of participants said it was a genuine mistake. They explained that their intention was not to cause harm or deny others access to Affected. This included all actions, for instance sharing: *"A friend shared a file with me, asked me to check over it, I did, but I sent it to someone else by mistake ... he was really mad at me"* (P24 InitiatorFiles); and editing: "*I accidentally set everyone's permission from editing to viewing by accident, and nobody could work until I undid [it]*" (P141 InitiatorFiles).

Lack of technical skill: 47 (5%) of Initiators explained that their actions were not just mistakes per se but due to their lack of knowledge around using the cloud services. They reported failing to share files and folders using the correct permissions and sometimes deleting files without knowing. "*I really didn't know how to use Google Drive at the time, which is how the file got deleted in the first place*" (P253 InitiatorFiles).

Denying access purposefully: 37 (4%) Initiators said they removed access from the Affected because Affected did not need access anymore, misconducted, or ended their relationship, or because of interpersonal disagreements. When Affected had misused or shared file/folder beyond the team, did not cooperate well or their editing contribution was deemed below par, Initiators removed their access to the file/folder. For example: "*He was messing up the files on purpose, so I took away his permissions, and he got upset*" (P226 InitiatorFolders). Other Initiators revoked access because the Affected was no longer part of the team: "*Due to the sensitivity and job role change of colleague, I had no choice but to restrict access*" (P153 InitiatorFolders).

Cloud security and privacy concerns: 22 (2%) of participants reasoned that their action was due to their concerns. Some had security and privacy concerns: Initiators revoked access to protect their (or group's) privacy or IP: "*Removed access from someone because I didn't want my ideas to be copied*" (P261 InitiatorFiles). Other concerns related to performance issues: "*spent too long accessing the file*" (P120 InitiatorFiles).

Misjudgement: Twenty (or 2%) of Initiators explained that they misjudged the situation that led to a conflict. They usually underestimated the sensitivity of files, the character of the people they added or shared files/folders with, and whether a file was still useful or others had a copy of it. "*I shared a few files I did not know were confidential to a common friend... my other friend (who shares the account with other colleagues and me) was still disappointed in my actions*" P76 InitiatorFile. Also, P3 InitiatorFiles explained they deleted a file before others could download it.

Storage management: 15 (1%) of Initiators explained that they deleted because they wanted to create space. "*Due to the lack of cloud storage, I removed some files, which other people had not stored locally themselves and still wanted to access*" (P84 InitiatorFolders).

6 COMMUNICATING MCS

We focus now on what happened after an MC had happened. For Affected, there were two main cases, either they did or did not communicate their unhappiness with Initiators. In particular, 61% of Affected complained to Initiators while the remaining 39% did not want to communicate their unhappiness for reasons detailed below.

6.1 No complaints

For the 39% Affected participants who did not complain: 20% perceived the MC as a minor issue that was not worth complaining about, e.g., "*I felt like it wasn't a big enough issue to make a big deal out of it*" (P27 AffectedFolders); 17% stated that they did not want to cause more trouble, e.g., "*I did not want to cause more trouble than what existed already*"(165 AffectedFolders), 7% did not want to affect the relationship with the others involved, e.g., "*He was a close friend and didn't want to strain the relationship*" (P43 AffectedFiles), and 5% thought that the MC happened because of a mistake, e.g., "*It was an honest error and I know it would not be repeated again*" (P20 AffectedFiles). Interestingly, there was a significant correlation between the severity of the conflict and whether Affected complained or not (r=0.32, p<0.0000001). That is, the more severe the MC the more the chance that there would be a communication about the MC.

6.2 Complaints

For the 61% who complained, they did so in person (46%), email (29%), messaging through Whatsapp (28%), telephoning (19%), texting (7%), through social media apps such as Facebook(6%), using comments feature in the cloud(5%), and other (4%). These figures were very similar to those reported by Initiators about how Affected communicated with them (obviated to save space). Regarding what the complaints were about, we found the same for Initiators and Affected:

Raising Awareness: Sixty-seven (67)% of the Affected reported that they wanted to make the Initiators aware about the MC, e.g., "*I just thought that they needed to know and they were sorry I got a sorry back*" (P75 AffectedFiles); and to express their feelings. This was echoed by Initiators, who also said that the Affected complained to make them know about the issue and how they feel about it.

Reprimanding the initiator: Ten (10)% of the Affected stated that they complained about the Initiator's lack of consultation and carelessness, which was again echoed by Initiators, which is related to the lack of consent reason given by Affected in the previous section.

Raising security and privacy concerns: Nine (9)% of the Affected stated that they wanted to let Initiators know that they had some privacy and security concerns, this was also echoed by Initiators, who also took some actions because of their own concerns as detalied in the previous section.

Resolving the issue: Seven (7)% of the Affected stated that they complained to try to find a solution or resolve the issue, "*To resolve the issue*" (P73 AffectedFolders). This was also confirmed by some initiators, they explained they received communication that advised them to resolve the issue. For example, P165 InitiatorFolder said: "*Just telling me to kick the guy I accidentally added*"

Preventing the issue from happening again: Finally, seven (7)% of the Affected wanted to prevent MCs from happening again, as one participant (P98 AffectedFolders) said: "*For something like that to not happen again in the future*". This is was also shared by initiators, some explained that the affected member wanted them to be careful in the future.

7 RESOLVING MCS

Overall, 84% of conflicts were resolved and 16% remained unresolved. However, we could observe differences, with Initiators considering 91% of MCs resolved while Affected considered 78% of MCs resolved, confirmed with a chi-squared test ($\chi^2 = 37.43, p < 0.000001$). Nevertheless, the differences also seemd to be related to whether Affected communicated with Initiators or not. When Affected complained to Initiators, they then reported 87% of the MCs resolved, while Affected who did not communicate with the Initiators reported only 26% of MCs resolved.

Therefore, conflict communication plays an important role for MC resolution, consistent with current conflict resolution theories [13] and previous research on social media MCs [60]. There was also a significant correlation between the MC *severity* and whether or not it was resolved (r = - 0.11, p < 0.00015). The higher the level of severity, the less likely MCs are resolved, the reason for this could be because more severe MCs are less likely to be resolved, or they may be perceived as more severe because they could not resolve it, or both could be true.

7.1 Resolution Strategies

To understand how cloud MCs are resolved in the wild, we asked respondents who indicated that their MC was resolved to explain how they were resolved further. Our analysis indicated that users develop and use various strategies to resolve MCs. For instance, most MCs that occurred due to sharing or adding a new member were resolved by conversing about the issue, in some cases adjusting permissions (e.g., revoking access), and where applicable, by deletion. Revoking access was commonly used when a new member was added to the folder or file. Issues concerning editing were mostly resolved by conversing and re-editing documents necessary, while access and edit rights were mostly resolved by readjusting settings. Participants reported changing their cloud use mainly after having conflicts around sharing, and only a few changed their cloud use after incidents around deletion and permission settings. Our analysis also shows that restructuring and renaming issues were mainly resolved by talking about the issues or undoing the changes. Issues related to deletion were resolved by conversing and undoing deletion. Almost all the MCs were resolved by the initiator and affected conversing or conversing and then applying a technical strategy. We provide a summary of these strategies, actions and a contingency of various strategies users may assume to resolve

Actions			Sharing					Permission Setting			Restructuring Renaming					
Strategies			Add a new member	Upload affected's personal files	Share a file further	Share file not ready to be shared	Share a wrong file	Remove affected's access	Restrict permission to edit	Unable to open a secured file	Change location or name file/folder	Share unorganized folders	Editing	Delete a file/folder	Lack of Expected Actions	Total
Nontechnical	Conversing	Converse	28	1	20	1		10	19		5	2	33	7		126
		Explaining	13		4			5	6		2		3	1	13	47
		Promise will not do it again	9		8			2	2				3			24
		Promise will seek approval	7		3								2	1		13
		To apologize	25		10			2	3			1	7	3		51
		Negotiate a new group policy	2	1	5						2		1	1		12
		Asking	12		6	1										19
		Forgive (Affected)	12	1	6			3	2				3	3		30
		Seek help from affected													16	16
Technical	Readjust permission	Remove access from the new member	58													58
		Remove access to file\folder			22				1							23
		Remove initiator's access to file											3			3
		Grant access to file/folder						33								33
		Grant editing permission							56							56
		Only the boss can add a member	1													1
		Restrict permissions to only view files											5			5
	Protecting	Securing file with a password	1													1
		Change file's /folder's password	3													3
		Encrypt folder			1											1
		Decrypt file/folder								1						1
		Provide file/folder's password								5				18		23
	Redoing	Re-creating the file	8		1								2	5		16
		Re-sending					1	4	2				4	26		37
		Re-editing							1				54			55
		Reorganizing									7	3				10
		Return to a previous version	1										13	15		29
		Local copy						1					6	26		33
		Deleting file/folder	22	10	33	1			1				1			68
	Changing their usage	Use an alternative method to share	1		1									2	4	8
		Use a different cloud service												2	3	5
		Set up a new account with limited access	1													1
		Delete or stop using cloud	2		2			1	1							6
		Stop using cloud for sharing							1							1
		Stop using automatic backups		1												1
		Stop sharing personal files (Affected)	1		1											2
		Affected remove his access to folder	1													1
		Block initiator's access	1		3											4
		Did nothing (Initiator)	6	1	5			3	3				2			20
		Non-specified	8		8			1	5				8	2		32
		Grand Total	223	15	139	3	1	65	103	6	16	6	150	112	36	875

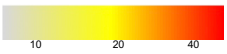

Figure 2: Contingency table with # times each coping strategy was observed for each MCs. Each cell of the heat map shows the number of times participants have mentioned that they have used a particular coping strategy to resolve an MC. Red color indicates higher numbers, while a gray color indicates lower numbers, and blank cells are instances that were not discovered in our dataset.

their MCs in Figure 2. In the next sections,we discuss the strategies more in detail next.

7.1.1 Non-technical Strategies. One-way Initiators and the Affected resolved MCs was through conversations. Participants resolved 338 MCs using this method. Initiators used discussions as an element to alleviating the concerns of the affected, e.g., "*I talked to him about it that the other person can be trusted, nothing to worry about*" (P43 InitiatorFolders; or to clarify the situation or the reason behind the action, e.g., "*I explained why I added the person and why they had to have access*" (P193 InitiatorFolders). Initiators also used conversations to reassure the Affected that the situation would not happen again, that they would seek their approval next time, or to apologize. Furthermore, conversing was used to collectively negotiate and set a new sharing, editing, organizing, or deleting policies between the group members, e.g., "*We instituted a new policy about adding people to the Drive: if the person was not a member of the workgroup, everyone in the group had to agree to add them to the Drive, and they could only be added as long as they were involved with our workgroup. My colleague also removed her sensitive documents from the drive, and I made a new shared folder for myself and my collaborators.*" (P110 InitiatorFolders). Lastly, conversing was also used to ask and request something. For example, asking the newly added member not to open specific files/folders or keep contents confidential, e.g., "*I messaged the friend I sent the files that they were confidential and not to open them*" (P74 InitiatorFiles).

7.1.2 Technical strategies. Participants also reported the following technical strategies: **Re-adjusting permissions:** Participants usually removed access or restricted permissions when using this strategy to resolve an MC. This strategy was used by both Initiators and Affected to resolve MCs related to sharing, editing, and permission setting actions. For instance, removing access for the newly added member(s), e.g., "*We revoked access from the new person*" (P158 InitiatorFolders). When the action concerned editing, participants would change permissions from editing to viewing, e.g., "*I corrected the sheet, disabled users from editing unless I authorized it*" (P260 AffectedFiles), or removed their overall access to the file. Lastly, this strategy was used to fix access rights, granting access to others to edit and view files and folders, "*My colleague solved it and gave me access again to the folder*" (P151 AffectedFolders).

Protecting: Participants protected their confidential shared files and folders using a password or changed the password to prevent the newly added members from having access: "*All files with private data are now password-protected*" (P6 InitiatorFiles). Moreover, when some members were unable to open a secured shared file or folder, Initiators provided the password or decrypted it: "*I was able to assist them with the file and help them view it*" (P196 InitiatorFiles).

Re-doing: Some strategies involved redoing the action more adequately or bringing the file to a previous version. This included *re-creating the file* after adding a new member, editing issues or deleting a file. For example, when confidential content was made public after adding a new member, some members would recreate or make a new copy and then change the contents, e.g., "*we just kept working but with different ideas*" (P234 InitiatorFiles). When a file was deleted, they would recover or recreate it: "*I recreated the spreadsheet and started keeping local copies of everything I do.*" (P243 InitiatorFiles). Besides, some of the participants stated that they resolved MCs by *re-sending the file* again, mostly to handle conflicts that occurred because of deleting, but it was also used to resolve editing or denial of access MCs. Another redoing strategy was *re-editing the file* to handle MCs related to editing and when permissions were restricted to viewing. When an MC occurred as a result of sharing an unstructured folder, or changing a file/folder's name, or changing file locations, some participants said that they *reorganized* the folder or returned it to the original arrangement, or changed back the name. Finally, other participants used backups, version history, or local copies to resolve MCs where reverting was possible or when data was deleted to *return to a previous version*. For instance: "*Docs has a history feature that allowed us to roll back to a previous version*" (P245 AffectedFiles); and "*some of the project data was backed up on my hard drive ... so there wasn't much work to do again*" (P42 InitiatorFolders).

Deleting: Some participants deleted the concerned file or folder to resolve conflicts related to sharing, editing, and restricting permission to edit. For example, after a file had been shared, they would delete the file to prevent access: "*I removed the file from google drive so it could no longer be accessed*" (P113 AffectedFiles).

Changing usage: Finally, some cases were resolved by changing the way users utilize the cloud. For instance, some participants change the method to share, e.g., "*I emailed the photos directly*" (P184 InitiatorFolders), or changed to another cloud service, e.g., "*I moved on to the OneDrive cloud*" (P93 AffectedFiles). Others created new accounts or deleted their accounts to manage access, e.g., "*I set up a new google drive account with limited access*" (P136 AffectedFolders). There were also participants who stopped using the cloud altogether or its cloud sharing and backup features.

7.2 Unresolved MCs

There were four main reasons when participants reported MCs could not be solved. First, some MCs could not be resolved as it was impossible to do so. For instance, when personal/confidential content had already been accessed or seen by others: "*the folders and content were already shared which cannot be taken back from the person who was not supposed to read it*" (P190 AffectedFiles); or when files were permanently lost: "*the file could not be retrieved hence I lost all the work I had done, I had to start again from the beginning*" (P71 AffectedFiles). Second, some participants could not resolve MCs because their association ended, so they could not reach any agreements: "*we had a blazing row about it, and we don't speak anymore*" P15 (AffectedFolders). Third, some Initiators did not understand the Affected's concern. Initiators thought Affected were either passive or aggressive, or simply refused to resolve the MC: "*The said person did not want to give me (nor anyone else) editing/admin rights*" (P66 AffectedFolders).

Finally, some Affected indicated that MCs could not be resolved because they decided to ignore or did not have time to deal with it.

7.3 Impact of MCs

Regardless of whether MCs were resolved or not, participants reported subsequent impacts the MCs had on them.

First, and this is the only positive impact reported, participants stated the MC led them to be more careful to avoid MC in the future, e.g., "*It made me aware that I need to be careful when giving*

other people access to our files." (P158 InitiatorFiles). Second, Participants reported that MCs related to editing, permission, and deletion negatively impacted their productivity. MCs wasted their time finishing tasks, affected work progress and quality (redoing work last minute), made them miss deadlines, and left them with a bad reputation in their work and/or study place, e.g., "*The impact was bad, got a bad review from the management.*" (P103 AffectedFolders). Third, some participants no longer considered the Initiator or Affected their friend after the MC, e.g., "*I fell out with the person that added my ex-partner*" (P77 AffectedFolders), or "*the person who used my pictures, it broke down our friendship for ever*" (P15 AffectedFolders). Finally, almost all Initiators and Affected reported having negative emotions after the MC, which included feeling embarrassed, angry, frustrated, disappointed, and annoyed, with no apparent differences between resolved and unresolved MCs.

8 DISCUSSION AND IMPLICATIONS

We now discuss the main findings of our work, their similarities and differences with MCs in other domains like social media, the main similarities and differences between affected and initiators, and design implications.

8.1 Key findings

Figure 3 presents an overview of our key findings: the relationship between the Initiators and Affected, what causes the MCs, their impact and how they resolve them. Summarizing the key findings around our main research questions:

RQ1 *What are the characteristics of multiuser conflicts (MCs) in the cloud? How and why do MCs happen?* Our results indicate that almost all participants experienced MCs at some point, and the majority of them experienced an MC within 6 months of the study date. Also, the majority of MCs happened in work or education related situations, affected different types of data (documents, folders, multimedia files, etc.), and about a third were considered moderately to extremely severe. MCs were the cause of the actions of the Initiators, including: sharing, editing, permission setting, restructuring and renaming, and deleting files and folders. Initiators were led to carry out those actions for different reasons such as due to mistakes, lack of technical skill, misjudgement, security and privacy concerns, or wanting to deny access or deletion files or folders for other reasons. In addition, a particular, recurring theme was that Initiators had not asked for consent from the Affected before conducting these actions.

RQ2 *What are the major consequences and impacts of MCs on users?* Most MCs affect users' security and privacy. This included loss of confidentiality, loss of integrity, and loss of availability. Even when there was an effort to resolve and address the MC after being identified, these losses were many times no-recoverable. In some cases, the consequences of MCs can lead to severe and long-term consequences that may affect people's offline lives, especially when the action leads to some impact that cannot be reversed, e.g., privacy violation. The study also found that the whole process of MCs, from identification to communication to attempted resolution, can lead impacts such as relationship breakdown, poor or reduced productivity, and various negative emotions like anger, frustration, and embarrassment. However, in some cases, the process of going through an MC acted in a positive way, as it would allow users to become aware of the problem as well as increase their literacy of how shared folders and files work.

RQ3 *How do users work around MCs; what strategies do they rely on to address MCs?* When Affected decided to communicate with Initiators about the MC, which was most of the times unless the MC was perceived a minor issue, they did so to try to address the situation, make Initiators aware of the consequences of their actions, such as privacy and security violations, reprimand the initiators or prevent the MCs from happening again. Regarding resolution strategies, some MCs are resolved through non-technical means, e.g. via conversations, with Initiator and Affected, discussing the issue and/or apologising/explaining if needed. This indicates that some MCs result from acts or mistakes that can be quickly resolved by just talking about the issue. Some MCs require technical interventions; the Initiator may have to re-do (or reverse) their actions, adjust permissions, or provide protection for the concerned file or folder. We found that some of the MCs do not get resolved due to the irreversible nature of the action or impact of the MCs, while others are due to personal reasons of the Initiator or Affected. Importantly, our results indicate that MCs can have severe consequences leading to communication or relationship breakdown.

8.2 What are the differences and similarities between cloud MCs and social media MCs?

As detailed in Section 2.2, multiuser privacy and security conflicts occur in other domains too, such as social media, smart homes, mobile phones, autonomous systems, shared accounts, etc. [4, 15, 24, 32, 38, 59, 68, 70, 71]. In particular, the majority of the work on how and why MCs occur has so far focused on social media, with extensive empirical research to study the phenomemon in that domain [6, 10, 18, 27, 32, 55, 60, 68]. Therefore, we compare the evidence we gathered in this study of cloud MCs to social media MCs to highlight important differences and similarities to further our understanding of MCs across platforms.

Cloud MCs are not just about sharing: Like social media MCs, our analysis revealed that most cloud MCs are due to sharing. MCs occurred when initiators gave new people access to shared folders or files, shared data further or outside the cloud platform, or sharing inappropriate files. This is similar to what has been reported in social media [6, 10, 32, 55, 60, 68]. However, unlike social media, we also found that sharing a file on its own may not be the problem but the lack of security measures applied to it, such as not encrypting or protecting it with a password. Moreover, unlike in social media, where most conflicts happen due to sharing, cloud MCs can also occur due to other actions or functionalities offered in the cloud like editing, changing permissions, sharing unfinished work, unfulfilled expected action, and restructuring, or renaming files and folders. Note that this happened across social contexts. In all contexts, including work, education, family and friends, the action most frequently leading to MCs was sharing, but many MCs happened due to other actions like deleting, editing, or changing permissions. This suggests that cloud computing may provide a larger surface for MCs to happen than social media.

Cloud MCs happen more often at work: Around half of MCs reported by our participants occurred or were related to work. This

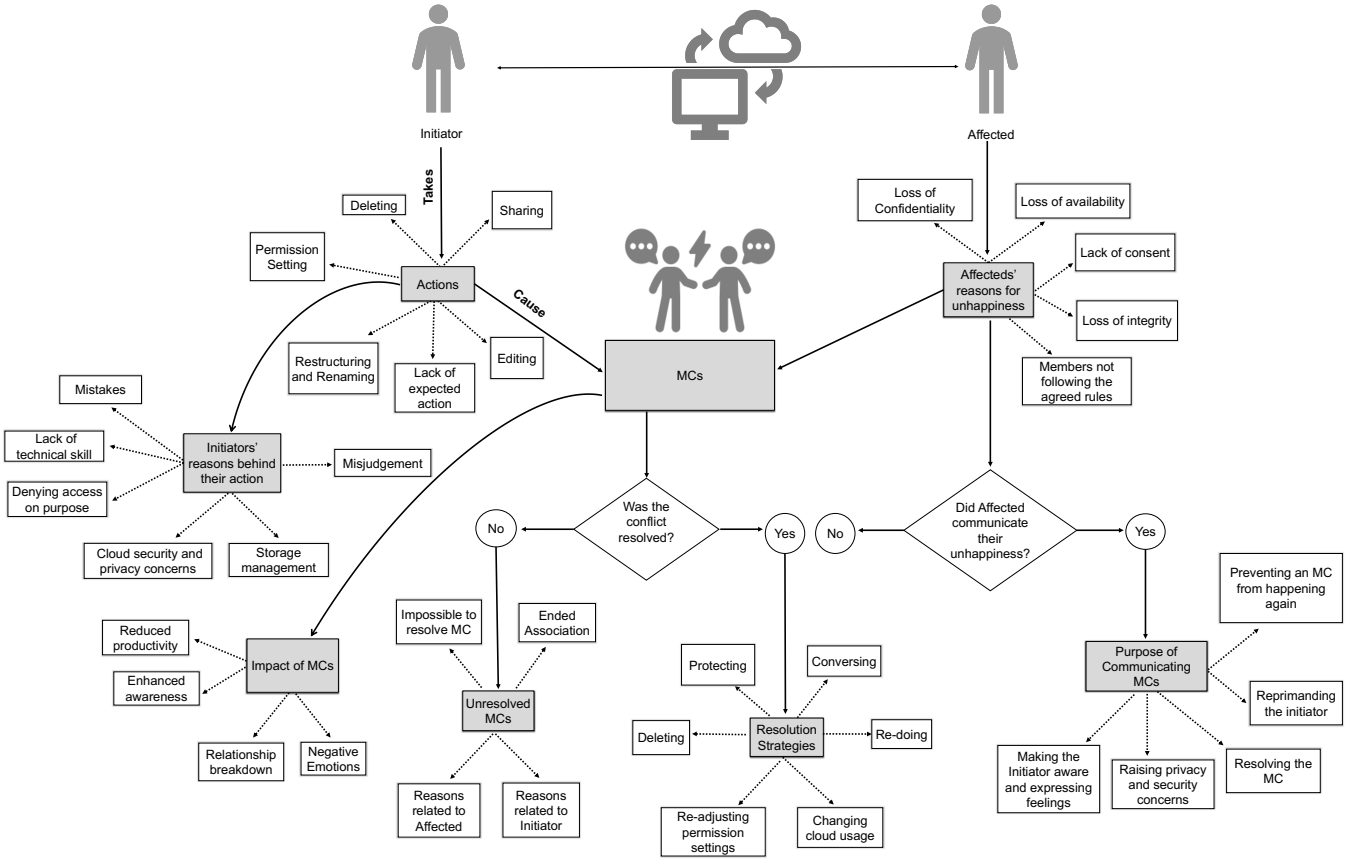

Figure 3: Key Findings: The figure provides an overall view of the relationship between our main findings. It shows the Initiators' actions that can lead to MCs and their reasons. In terms of the affected, it shows why the affected were not happy and how they chose to (or not) communicate their displeasure. Moreover, this figure also shows the journey to resolving MCs, the strategies used by Initiators and Affected to address the MCs when it is possible to do so, and reasons why some MCs were not resolved. Lastly, it shows the impact MCs have on relationships, work, awareness, and emotions.

finding was reflected throughout the study, including the impact of MCs; for instance, MCs reduced productivity. While users do share cloud folders and files with friends and family for social purposes too, they also do it for work. This is rather different from what has been reported in social media studies [6, 10, 32, 55, 60, 68], where most MCs occur between friends and families. This is expected and understandable, as many users use the cloud for multiple purposes, notably including work purposes. The main point is that it adds potential issues and impacts less present in social media, such as reduced productivity, that need to be considered in cloud MCs.

Cloud MCs also share similarities with MCs in social media: We also observed similarities with MCs found in social media, particularly when attempting to resolve MCs. Cloud users employ offline, corrective, and preventive strategies, similar to those developed in social media [5, 32, 60, 68]. Participants often used non-tech offline strategies like conversing, explaining, apologizing, and negotiating a group policy reported in social media studies. Regarding corrective strategies, our participants would delete or adjust the permission to suit collaborators' desires, similarly to what social media users employ to control the visibility of unwanted content using built-in privacy management features, such as untagging or sharing content within close circles. Meanwhile, for preventative strategies our participants stated that they sometimes have to revoke or change a member's access rights or revoke/block the initiator's total access to prevent further harm. Social media studies also report this; users may constrain the audience or block other users. Another similarity we observed besides strategies was concerning reasons for unhappiness; some MCs were due to a lack of consent or engagement from the initiator. In social media, users explained they were not happy because initiators did not consult them when putting or removing content online [10, 32, 60, 68].

8.3 Differences and similarities between Affected and Initiators

Our study indicates that when participants are Initiators, they would mainly report the severity of MCs as less severe than Affected. It seemed like Initiators slightly downplayed the impact of the MCs. We also observed this concerning whether an MC was considered to be resolved or not; with Initiators reporting that the MCs were resolved significantly and substantially more often than

Affected. Moreover, we also observed these differences regarding feelings after an MC has occurred; 82% of the affected reported a negative emotion, while only 18% of the initiators reported having negative emotions after the incident. Overall, these results suggest that when participants were playing the role of Initiator, they might not fully realize the impact of their actions on others (Affected), the severity, and the possible consequences of the action.

In terms of similarities, both groups described the same types of conflicts or similar actions leading to MCs. We did not observe any particular action being prevalent in one group but missing in another group. Both groups also used similar tools to communicate MCs. These similarities suggest that common ground on which intervention mechanisms could be based. For instance, interventions could focus on aligning parts or concepts which are not perceived as similar by both groups, like the potential consequences as discussed above.

8.4 Design implications

We finally discuss some design implications for mechanisms to avoid and/or support users through MCs in the cloud.

Preventative and Recovery support for Cloud MCs: Our findings indicate that sometimes users revert changes or redo work to resolve some MCs. However, some consequences, for example, loss of privacy or confidentiality, cannot easily be reversed. These consequences can endure even when the action has been reversed or the matter is considered closed by the parties involved. Consequently, we recommend that mechanisms to support users should focus on reversible actions but also target non-reversible results. For reversible consequences, designers could propose recovery mechanisms. Most of these mechanisms exist already, for instance, undoing changes and recovering deleted files. The usability of such mechanisms could be improved. However, for unredeemable consequences, designers should prioritize mechanisms that limit actions that can potentially lead to severe consequences. Users could be warned or made aware of severe consequences. Existing efforts in this area are limited; Nebeling et al. [43] proposed MUBox, which introduced key aspects to managing shared folders, such as notifying collaborators of changes (in the name, location, or content of the files within the folder) and letting them vote on their approval. However, the resulting user experience is not completely clear; for example, there could be delays in adequate changes.

New mechanisms for detecting the sensitivity of content: Some reported MCs in our study were associated with the sensitivity of the content. Initiators revealed that they did not think the content was sensitive before they shared files/folders or added a new member to the shared content. This finding suggests varying perceptions of sensitivity. Potentially, there may be a way to know in advance if the content can be considered sensitive. To address this issue in social media, researchers have used computer vision-based algorithms [1, 19, 25] to detect content that may lead to privacy conflicts. While these efforts are promising, they were limited to face detection in photos and videos. In the cloud, users share other content which may be sensitive but not contain faces or photos/videos, such as office documents. Research efforts around classifying cloud data are still in their infancy but promising. For instance, Khan et al. [30] and Ramokapane et al. [54] attempted to classify cloud files according to their sensitivity and usefulness. Classifying data according to sensitivity would help users make informed decisions about sharing data or files.

Improving support in collaborative interfaces: Overall, our results on actions that lead to MCs suggest the need to improve the collaborative interfaces currently used in the cloud. Future research could focus on building new mechanisms to de-centralize administration rights, taking power from one user but involving everyone in the decision-making. Most reported MCs in our study were associated with non-consensual actions by collaborators, sharing, revoking, editing, and deleting without consulting others. Moreover, de-centralising administration rights would also be helpful to the remaining collaborators when members are no longer in contact. Research efforts should also focus on finding ways in which specific cloud actions could affect users differently. For instance, deletion could be one-sided; a collaborator could choose how an action should affect other members. This approach would be useful in cases where other members are still using the resource. Another example is to flag actions that could potentially lead to more severe MCs. In general, collaborative interfaces should incorporate usable mechanisms that facilitate the strategies that users mostly employ to resolve MCs if they happen. For instance, easy-to-use, embedded mechanisms that protect files and folders could help resolve MCs around the security and privacy of files and folders.

Consent to avoid MCs: One of the reasons that led to MCs in our study was lack of consent; that is, lack of consent before sharing, editing, deleting, permission setting or restructuring/renaming. The initiators reported using preventative strategies such as promising to take approval and consent before doing the action to avoid MCs in the future. While it seems, in principle, possible that consent collection techniques [34, 46] developed for social media to avoid MCs could be proposed for the cloud, building these techniques could be challenging and even impracticable in the cloud; taking consent for each cloud action may be complex, burdensome, and/or inefficient. For example, some users might not respond (or do it in a timely fashion), which may have negative consequences, particularly for those using the cloud for work. Therefore, it would be essential to study the applicability and usability of such techniques to support consent collection in the cloud. Designers could also explore new ways of collecting consent for the cloud.

New communication support *during* MCs: When MCs cannot be prevented or easily recovered from, users may still need to manage and communicate about them as effectively as possible. Our study shows that most participants complained through mechanisms other than the in-built tools like the comments feature. Participants reported complaining mostly in person, email, and messaging apps. This is similar to what has been reported in social media conflicts, with fewer participants using the in-built communication features [60]. Therefore, there is a need to improve communication—allow the affected to complain—allow the initiators to explain—or both to resolve their issues. Communication is vital to resolving conflicts [40]. Other studies suggest using mediators during conflicts; research should propose and test how mediators could be used in the cloud [44]. Prior efforts in other domains have focused on using conversational agents [12, 17, 33] and explainable and value-based AI methods [41, 42].

8.5 Limitations and Future Work

While our sample collected through prolific may be diverse in age, gender and income, it does not represent the whole population of cloud users. It is also possible that our sample may contain people who mostly stay at home. Nonetheless, this sample may also include people conversant with technology and using the cloud very often. Our study was based on participants' reports, and the might not have disclosed all the information about what they experienced. Moreover, those who completed the Initiator surveys may have downplayed incidents to try not to look bad, while the Affected may have exaggerated the incidents to prevent their stories from sounding like they overreacted. That is why it was important to consider both roles to build a more complete picture of MCs. We also acknowledge that our study targeted participants representing many countries from the global north. Hence, even if some participants were from global south countries, the views presented in this paper may be skewed to the global north. However, the sample did include ample representation of different data protection legislation and known privacy perceptions (e.g., US vs EU).

As future work, our results also suggest the need for further empirical research that would help understand cloud MCs, including:

Further understanding the differences between Initiators and Affected: Our results showed differences in how both groups of participants perceived MCs and their consequences based on the role they played on an MC (Initiators vs Affected). We believe that individuals' perception of severity may play a crucial role in deciding how, when, or whether the MC is resolved. Thus, we posit that the solution to adequately support users in resolving these issues may lie in further understanding the differences that seem to exist between the perceptions of users who play the role of Initiator in an MC and those of the users who play the role of Affected to align their positions and perspectives during MCs.

Understanding users' mistakes: In some cases, Initiators argued that mistakes were the cause of the action that led to MCs. For example, some Initiators revealed they shared files with the wrong person by mistake. We are unsure what led to these mistakes, since we did not ask participants what could have led to mistakes. Could mistakes be due to faulty and confusing interfaces or users' cloud mental models? Further research should investigate the usability of various cloud mechanisms and the role of usability in these mistakes that lead to MCs.

9 CONCLUSION

We reported the first in-depth study of multiuser conflicts over shared files and folders in the cloud, from identification to resolution, using a survey designed following a critical incident methodology to collect experienced MCs by cloud users. This allowed us to establish an empirical basis for the prevalence, severity and impacts of MCs. Based on the results of our analysis, we uncovered users' actions (sharing, permission setting, editing, restructuring and renaming, deleting) or lack of expected action that led to MCs, and the main reasons behind unhappiness for each action, with the main reasons being security and privacy consequences such as loss of confidentiality, integrity and availability or lack of consent. Additionally, this study examined communication before and after MCs happened and the coping strategies that users develop to resolve MCs. We plan to share a sanitized and anonymized version of the large-scale dataset of cloud MCs we gathered to foster further research in this area.

DATA STATEMENT

The dataset containing a cleaned and anonymized version of the conflicts gathered can be found here: https://osf.io/d5kej

ACKNOWLEDGMENTS

We would like to thank the anonymous AC and reviewers for their very helpful comments. We would also like to thank Ruba Abu-Salma for her useful comments on a previous version of this paper.

REFERENCES

[1] Paarijaat Aditya, Rijurekha Sen, Peter Druschel, Seong Joon Oh, Rodrigo Benenson, Mario Fritz, Bernt Schiele, Bobby Bhattacharjee, and Tong Tong Wu. 2016. I-pic: A platform for privacy-compliant image capture. In *Proceedings of the 14th annual international conference on mobile systems, applications, and services*. 235–248.

[2] Sultan Aldossary, William Allen, et al. 2016. Data security, privacy, availability and integrity in cloud computing: issues and current solutions. *International Journal of Advanced Computer Science and Applications* 7, 4 (2016), 485–498.

[3] YZ An, ZF Zaaba, and NF Samsudin. 2016. Reviews on security issues and challenges in cloud computing. In *IOP Conference Series: Materials Science and Engineering*, Vol. 160. IOP Publishing, 012106.

[4] Julia Bernd, Ruba Abu-Salma, and Alisa Frik. 2020. {Bystanders'} Privacy: The Perspectives of Nannies on Smart Home Surveillance. In *10th USENIX Workshop on Free and Open Communications on the Internet (FOCI 20)*.

[5] Andrew Besmer and Heather Richter Lipford. 2010. Moving beyond untagging: photo privacy in a tagged world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 1563–1572.

[6] Danah Boyd and Alice E Marwick. 2011. Social privacy in networked publics: Teens' attitudes, practices, and strategies. In *A decade in internet time: Symposium on the dynamics of the internet and society*.

[7] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101.

[8] Daniel Burda and Frank Teuteberg. 2014. The role of trust and risk perceptions in cloud archiving—Results from an empirical study. *The Journal of High Technology Management Research* 25, 2 (2014), 172–187.

[9] Lee D. Butterfield, William A. Borgen, Norman E. Amundson, and Asa Sophia T. Maglio. 2005. Fifty years of the critical incident technique: 1954-2004 and beyond. *Qualitative Research* 5, 4 (2005), 475–497. https://doi.org/10.1177/1468794105056924

[10] Mauro Cherubini, Kavous Salehzadeh Niksirat, Marc-Olivier Boldi, Henri Keopraseuth, Jose Such, and Kévin Huguenin. 2021. When Forcing Collaboration is the Most Sensible Choice: Desirability of Precautionary and Dissuasive Mechanisms to Manage Multiparty Privacy Conflicts. In *PACM on Human-Computer Interaction - ACM Conference on Computer-Supported Cooperative Work and Social Computing (CSCW)*.

[11] Seung Youn Chyung, Julie R Barkin, and Jennifer A Shamsy. 2018. Evidence-based survey design: The use of negatively worded items in surveys. *Performance Improvement* 57, 3 (2018), 16–25.

[12] Leigh Clark, Nadia Pantidi, Orla Cooney, Philip Doyle, Diego Garaialde, Justin Edwards, Brendan Spillane, Emer Gilmartin, Christine Murad, Cosmin Munteanu, et al. 2019. What makes a good conversation? Challenges in designing truly conversational agents. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–12.

[13] Morton Deutsch, Peter T Coleman, and Eric C Marcus. 2011. *The handbook of conflict resolution: Theory and practice*. John Wiley & Sons.

[14] John C Flanagan. 1954. The critical incident technique. *Psychological bulletin* 51, 4 (1954), 327.

[15] Christine Geeng and Franziska Roesner. 2019. Who's in control? Interactions in multi-user smart homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–13.

[16] Hamza Harkous and Karl Aberer. 2017. If You Can't Beat them, Join them: A Usability Approach to Interdependent Privacy in Cloud Apps. In *Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy*. ACM, 127–138.

[17] Hamza Harkous, Kassem Fawaz, Kang G Shin, and Karl Aberer. 2016. {PriBots}: Conversational Privacy with Chatbots. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*.

[18] Rakibul Hasan, Bennett I Bertenthal, Kurt Hugenberg, and Apu Kapadia. 2021. Your photo is so funny that i don't mind violating your privacy by sharing it: effects of individual humor styles on online photo-sharing behaviors. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–14.

[19] Rakibul Hasan, David Crandall, Mario Fritz, and Apu Kapadia. 2020. Automatically detecting bystanders in photos to reduce privacy risks. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 318–335.

[20] Rakibul Hasan, Eman Hassan, Yifang Li, Kelly Caine, David J Crandall, Roberto Hoyle, and Apu Kapadia. 2018. Viewer experience of obscuring scene elements in photos to enhance privacy. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–13.

[21] Rakibul Hasan, Yifang Li, Eman Hassan, Kelly Caine, David J Crandall, Roberto Hoyle, and Apu Kapadia. 2019. Can privacy be satisfying? on improving viewer satisfaction for privacy-enhanced photos using aesthetic transforms. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–13.

[22] Hongxin Hu, Gail-Joon Ahn, and Jan Jorgensen. 2011. Detecting and resolving privacy conflicts for collaborative data sharing in online social networks. In *Proceedings of the 27th Annual Computer Security Applications Conference*. 103–112.

[23] Hongxin Hu, Gail-Joon Ahn, and Jan Jorgensen. 2012. Multiparty access control for online social networks: model and mechanisms. *IEEE Transactions on Knowledge and Data Engineering* 25, 7 (2012), 1614–1627.

[24] M. Humbert, B. Trubert, and K. Huguenin. 2019. A Survey on Interdependent Privacy. *Comput. Surveys* (2019), 35.

[25] Panagiotis Ilia, Iasonas Polakis, Elias Athanasopoulos, Federico Maggi, and Sotiris Ioannidis. 2015. Face/off: Preventing privacy leakage from photos in social networks. In *Proceedings of the 22nd ACM SIGSAC Conference on computer and communications security*. 781–792.

[26] Iulia Ion, Niharika Sachdeva, Ponnurangam Kumaraguru, and Srdjan Čapkun. 2011. Home is safer than the cloud! Privacy concerns for consumer cloud storage. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*. 1–20.

[27] Maritza Johnson, Serge Egelman, and Steven M Bellovin. 2012. Facebook and privacy: it's complicated. In *Proceedings of the eighth symposium on usable privacy and security*. 1–15.

[28] Barbara Johnstone. 2017. *Discourse analysis*. John Wiley & Sons.

[29] Mohammad Taha Khan, Maria Hyun, Chris Kanich, and Blase Ur. 2018. Forgotten but not gone: Identifying the need for longitudinal data management in cloud storage. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, 543.

[30] Mohammad Taha Khan, Christopher Tran, Shubham Singh, Dimitri Vasilkov, Chris Kanich, Blase Ur, and Elena Zheleva. 2021. Helping Users Automatically Find and Manage Sensitive, Expendable Files in Cloud Storage. In *30th {USENIX} Security Symposium ({USENIX} Security 21)*.

[31] Yujin Kim, Jennifer Dykema, John Stevenson, Penny Black, and D Paul Moberg. 2019. Straightlining: overview of measurement, comparison of indicators, and effects in mail–web mixed-mode surveys. *Social Science Computer Review* 37, 2 (2019), 214–233.

[32] Airi Lampinen, Vilma Lehtinen, Asko Lehmuskallio, and Sakari Tamminen. 2011. We're in it together: interpersonal management of disclosure in social network services. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 3217–3226.

[33] Liliana Laranjo, Adam G Dunn, Huong Ly Tong, Ahmet Baki Kocaballi, Jessica Chen, Rabia Bashir, Didi Surian, Blanca Gallego, Farah Magrabi, Annie YS Lau, et al. 2018. Conversational agents in healthcare: a systematic review. *Journal of the American Medical Informatics Association* 25, 9 (2018), 1248–1258.

[34] Fenghua Li, Zhe Sun, Ang Li, Ben Niu, Hui Li, and Guohong Cao. 2019. Hideme: Privacy-preserving photo sharing on social networks. In *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*. IEEE, 154–162.

[35] Yifang Li and Kelly Caine. 2022. Obfuscation Remedies Harms Arising from Content Flagging of Photos. In *CHI Conference on Human Factors in Computing Systems*. 1–25.

[36] Yifang Li, Nishant Vishwamitra, Bart P Knijnenburg, Hongxin Hu, and Kelly Caine. 2017. Effectiveness and users' experience of obfuscation as a privacy-enhancing technology for sharing photos. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (2017), 1–24.

[37] Kathleen M MacQueen, Eleanor McLellan, Kelly Kay, and Bobby Milstein. 1998. Codebook development for team-based qualitative analysis. *Cam Journal* 10, 2 (1998), 31–36.

[38] Maximilian Marsch, Jens Grossklags, and Sameer Patil. 2021. Won't You Think of Others?: Interdependent Privacy in Smartphone App Permissions. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (2021), 1–35.

[39] Winter Mason and Siddharth Suri. 2012. Conducting behavioral research on Amazon's Mechanical Turk. *Behavior research methods* 44, 1 (2012), 1–23.

[40] Ersilia Menesini, Virginia Sanchez, Ada Fonzi, Rosario Ortega, Angela Costabile, and Giorgio Lo Feudo. 2003. Moral emotions and bullying: A cross-national comparison of differences between bullies, victims and outsiders. *Aggressive Behavior: Official Journal of the International Society for Research on Aggression* 29, 6 (2003), 515–530.

[41] Francesca Mosca and Jose Such. 2021. ELVIRA: an Explainable Agent for Value and Utility-driven Multiuser Privacy. In *International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS)*. 916–924.

[42] Francesca Mosca and Jose Such. 2022. An explainable assistant for multiuser privacy. *Autonomous Agents and Multi-Agent Systems (JAAMAS)* 36, 10 (2022), 1–45.

[43] Michael Nebeling, Matthias Geel, Oleksiy Syrotkin, and Moira C Norrie. 2015. MUBox: Multi-user aware personal cloud storage. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 1855–1864.

[44] Kavous Salehzadeh Niksirat, Evanne Anthoine-Milhomme, Samuel Randin, Kévin Huguenin, and Mauro Cherubini. 2021. "I thought you were okay": Participatory Design with Young Adults to Fight Multiparty Privacy Conflicts in Online Social Networks. (2021).

[45] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Wash. L. Rev.* 79 (2004), 119.

[46] Alexandra-Mihaela Olteanu, Kévin Huguenin, Italo Dacosta, and J-P Hubaux. 2018. Consensual and privacy-preserving sharing of multi-subject and interdependent data. In *Proceedings of the 25th network and distributed system security symposium (NDSS)*. Internet Society, 1–16.

[47] Leonard J Paas and Meike Morren. 2018. Please do not answer if you are reading this: Respondent attention in online panels. *Marketing Letters* 29, 1 (2018), 13–21.

[48] F. Paci, A. Squicciarini, and N. Zannone. 2018. Survey on access control for community-centered collaborative systems. *Comput. Surveys* 51, 1 (2018).

[49] Siani Pearson. 2009. Taking account of privacy when designing cloud computing services. In *2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing*. IEEE, 44–52.

[50] Eyal Peer, Joachim Vosgerau, and Alessandro Acquisti. 2014. Reputation as a sufficient condition for data quality on Amazon Mechanical Turk. *Behavior research methods* 46, 4 (2014), 1023–1031.

[51] Emilee Rader, Rick Wash, and Brandon Brooks. 2012. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*. ACM, 6.

[52] Sarah Rajtmajer, Anna Squicciarini, Christopher Griffin, Sushama Karumanchi, and Alpana Tyagi. 2016. Constrained social-energy minimization for multiparty sharing in online social networks. In *proceedings of the 2016 international conference on autonomous agents & multiagent systems*. 680–688.

[53] Kopo M. Ramokapane, Awais Rashid, and Jose Such. 2017. "I feel stupid I can't delete...": A Study of Users' Cloud Deletion Practices and Coping Strategies. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*. 241–256.

[54] Kopo M. Ramokapane, Jose Such, and Awais Rashid. 2022. What Users Want From Cloud Deletion and the Information They Need: A Participatory Action Study. *ACM Transactions on Privacy and Security (TOPS)* (2022).

[55] Yasmeen Rashidi, Tousif Ahmed, Felicia Patel, Emily Fath, Apu Kapadia, Christena Nippert-Eng, and Norman Makoto Su. 2018. " You don't want to be the next meme": College Students' Workarounds to Manage Privacy in the Era of Pervasive Photography. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. 143–157.

[56] G Shanmugasundaram, V Aswini, and G Suganya. 2017. A comprehensive review on cloud computing security. In *2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*. IEEE, 1–5.

[57] Anna Cinzia Squicciarini, Mohamed Shehab, and Federica Paci. 2009. Collective privacy management in social networks. In *Proceedings of the 18th international conference on World wide web*. 521–530.

[58] Jose Such and Natalia Criado. 2016. Resolving multi-party privacy conflicts in social media. *IEEE Transactions on Knowledge and Data Engineering* 28, 7 (2016), 1851–1863.

[59] Jose Such and Natalia Criado. 2018. Multiparty Privacy in Social Media. *Communications of the ACM (CACM)* 61, 8 (2018), 74–81.

[60] Jose Such, Joel Porter, Sören Preibusch, and Adam Joinson. 2017. Photo privacy conflicts in social media: A large-scale empirical study. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 3821–3832.

[61] Jose Such and Michael Rovatsos. 2016. Privacy policy negotiation in social media. *ACM Transactions on Autonomous and Adaptive Systems (TAAS)* 11, 1 (2016), 1–29.

[62] Tom van Nuenen, Jose Such, and Mark Coté. 2022. Intersectional Experiences of Unfair Treatment Caused by Automated Computational Systems. *Proceedings of the ACM on Human-Computer Interaction-CSCW* (2022).

[63] Kami Vaniea and Yasmeen Rashidi. 2016. Tales of software updates: The process of updating software. In *Proceedings of the 2016 chi conference on human factors in computing systems*. ACM, 3215–3226.

[64] Roderik F Viergever. 2019. The critical incident technique: method or methodology? *Qualitative health research* 29, 7 (2019), 1065–1079.

[65] Nishant Vishwamitra, Yifang Li, Kevin Wang, Hongxin Hu, Kelly Caine, and Gail-Joon Ahn. 2017. Towards pii-based multiparty access control for photo sharing in online social networks. In *Proceedings of the 22nd ACM on Symposium*

on Access Control Models and Technologies. 155–166.
[66] Sumina Vladimir. 2021. 26 Cloud Computing Statistics, Facts & Trends for 2022. https://www.cloudwards.net/cloud-computing-statistics/.
[67] Dominik Wermke, Nicolas Huaman, Christian Stransky, Niklas Busch, Yasemin Acar, and Sascha Fahl. 2020. Cloudy with a chance of misconceptions: exploring users' perceptions and expectations of security and privacy in cloud office suites. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. 359–377.
[68] Pamela Wisniewski, Heather Lipford, and David Wilson. 2012. Fighting for my space: Coping mechanisms for SNS boundary regulation. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 609–618.
[69] Heng Xu. 2011. Reframing privacy 2.0 in online social network. *U. Pa. J. Const. L.* 14 (2011), 1077.
[70] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy perceptions and designs of bystanders in smart homes. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–24.
[71] Yaxing Yao, Huichuan Xia, Yun Huang, and Yang Wang. 2017. Privacy mechanisms for drones: Perceptions of drone controllers and bystanders. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 6777–6788.
[72] Faheem Zafar, Abid Khan, Saif Ur Rehman Malik, Mansoor Ahmed, Adeel Anjum, Majid Iqbal Khan, Nadeem Javed, Masoom Alam, and Fuzel Jamil. 2017. A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends. *Computers & Security* 65 (2017), 29–49.
[73] Dimitrios Zissis and Dimitrios Lekkas. 2012. Addressing cloud computing security issues. *Future Generation computer systems* 28, 3 (2012), 583–592.