The Burden of Ending Online Account Sharing

Borke Obada-Obieh
University of British Columbia
Vancouver, Canada
borke@ece.ubc.ca

Yue Huang
University of British Columbia
Vancouver, Canada
huang13i@ece.ubc.ca

Konstantin Beznosov
University of British Columbia
Vancouver, Canada
beznosov@ece.ubc.ca

ABSTRACT

Many people share online accounts, even in situations where high privacy and security are expected. Naturally, the sharing of these accounts does not endure forever. This paper reports the privacy and security challenges that people experience when they stop online account sharing. We conducted semi-structured interviews with 25 participants who stopped sharing at least one online account in the 12 months preceding the study. Our results suggest that users experience cognitive and psychosocial burdens when ending account sharing. We offer suggestions for how to improve the design of online accounts to support users better when they end account sharing.

Author Keywords
Online shared accounts; Usable security and privacy

CCS Concepts
•Security and privacy → Social aspects of security and privacy; Usability in security and privacy; •Human-centered computing → User studies; Human computer interaction (HCI);

INTRODUCTION

Sharing online accounts has become a prevalent practice among social groups and individuals. In the US alone, 54% of Americans share accounts, with 41% sharing online shopping accounts (e.g., Amazon Prime), and 75% sharing streaming accounts (e.g., Netflix, Hulu) [6, 24]. A recent discussion via Twitter among the members of the UK's Parliament shows that sharing accounts is a common practice [23], even when a high level of information security is expected [37, 41].

However, privacy and security issues arise when account sharing ends, especially when the account was never designed to be shared in the first place. Online accounts are not always designed to effectively facilitate the ending of sharing between users [9, 25, 35].

While previous work focuses on why people share accounts [33, 40] and how they begin the sharing process [25, 33], we investigated the factors that complicate the ending of online account sharing in various types of interpersonal relationships by asking:

- RQ1: What are the security and privacy challenges people encounter in ending sharing of online accounts?
- RQ2: How can systems be designed to address these challenges and protect users' security and privacy when account sharing ends?

Answering these questions can provide insight into how accounts can be designed to better support users in ending account sharing, thereby improving the user experience and safeguarding users' personal information.

For the sake of clarity, we grouped online accounts into the following categories:

Accounts designed for sharing (DS) are accounts that offer multi-user membership plans. Examples include Netflix, Amazon Household, and Spotify Premium Family accounts. Although these services also provide single-user plans, we will use "DS accounts" or "multi-user accounts" to only refer to the multi-user plans.

Accounts not designed for sharing (NDS) are accounts that are intended for only one user. Examples include WhatsApp, Facebook, Instagram, and LinkedIn accounts. We also include the single-user versions of DS accounts in this category. We'll use "NDS accounts" or "single-user accounts" to refer to such accounts.

Additionally, we define interpersonal relationships as "close association between individuals who share common interests and goals [20]." Examples of these types of relationships include friendship, family, business, or romantic relationships.

We addressed our research questions through conducting semi-structured interviews ($N = 25$) with those participants who had shared at least one account in the 12 months preceding the study. Participants had various types of interpersonal relationships with those who they shared accounts with. The interviews focused on the accounts, why and how the sharing began and ended, and what made the process difficult. We analyzed data using thematic analysis [19].

Our study has three major contributions. First, we discover *reasonable* but unsupported sharing use cases for some NDS accounts. Participants were torn between attempting to satisfy their appropriate need for sharing and maintaining their security and privacy. Our results suggest that companies offering such NDS accounts should consider supporting these use cases. Second is the finding that participants' privacy and security

CHI '20, April 25–30, 2020, Honolulu, HI, USA.
© 2020 Copyright is held by the owner/author(s).
ACM ISBN 978-1-4503-6708-0/20/04.
http://dx.doi.org/10.1145/3313831.3376632

were more at risk when they stopped sharing NDS accounts because the accounts were never designed for sharing. As part of this contribution, we offer specific recommendations for designing these accounts to allow sharing between users without users having to share account passwords. Third, we identify negative impacts of ending the sharing of DS and NDS accounts on users, and group them into *cognitive* and *psychosocial* impacts.

Examples of cognitive impacts are remembering the people with whom accounts are shared, changing passwords, and remembering the accounts across which participants reused passwords. Examples of psychosocial impacts are the uncertainty about whether the sharing ended successfully, the frustration of losing personal content, and the fear of the account being hijacked by the secondary user. Identifying these challenges is important for reducing the cognitive and psychosocial burden of ending account sharing, as well as for reducing corresponding security and privacy risks. We suggest recommendations (and discuss their benefits) for improving the design of online accounts to address the identified challenges. Our contributions provide insight into the burden of ending online account sharing and add new considerations to the many that already exist when considering account privacy and security.

RELATED WORK

Account Sharing

Several studies have focused on account sharing and the reasons behind it. Egelman et al. [11] conducted a survey of households that made use of the Windows operating system on their home computers. The study aimed to find out whether participants shared single-user accounts on their computers and how sharing occurred. The result of the study was a recommendation to provide family accounts on home computers to aid account sharing. A more recent study by Matthews et al. [33] investigated why people share accounts and household devices. Using an inventory survey and a 21-day diary study, the authors discovered 6 types of sharing that are related to the reasons people share accounts: borrowing, mutual use, setup purposes, helping other users, broadcasting, and accidental.

Sharing accounts in the context of romantic relationships has received special attention from the academic community. Singh et al. [49] were among the first to study why couples share accounts. The authors carried out open-ended interviews, group interviews, and focus groups during three months with married and de facto couples. They found that people share accounts as a sign of trust, as a key to survival, and because they had no option (e.g., couples with disabilities). More recently, Jacobs et al. [25] conducted interviews and an 8-day diary study that confirmed the results of previous studies and identified additional reasons for account sharing in romantic relationships, which were the maintenance of the relationship, and to promote intimacy. The aim of another recent study by Park et al. [40] was to understand the account sharing behaviors of people in romantic relationships. Through a survey on Amazon Mechanical Turk, the authors found that couples share accounts to meet goals such as convenience, household maintenance, trust, and relationship maintenance. However, some participants were actively hiding the existence of certain accounts from their partners. Park et al. also suggested design recommendations for better supporting three relationship stages: the start, maintenance, and the end.

Studies of technology in the context of intimate partner abuse (IPA) have described common situations in which abusers coercively access survivors' accounts, and survivors attempt to end this coercive access [14, 15, 34]. Even though some of the account mechanics described in our study with general users may overlap with this prior work, IPA situations are different in that they involve coercive account access and different (potentially severe) consequences for survivors. Multiple studies of how technology affects IPA [14, 15, 34] have described how abusers leveraged coercive control of survivors' accounts and shared household accounts to abuse survivors. For example, an abuser may use coercive access to a survivor's accounts to reset passwords and lock the survivor out, to impersonate the survivor to damage their reputation and relationships, or to surveil the survivor. It should be noted that our study does not explore account ending in the context of abusive situations.

Our research builds on prior work. We expand the scope of investigation with general users by studying the end of account sharing in the context of a variety of interpersonal relationship types, such as friendship, business, school, and acquaintanceship. We also explore how technology supports this process and what can be done to improve support.

Ending Account Sharing

Several studies focused on how digital possessions are managed after breakups. Quan-Haase et al. [43] studied the coping strategies employed by young adults (10 unmarried participants) on Facebook after a romantic breakup. The results indicate that participants remained digitally entangled. For example, because Facebook shows interactions between friends and non-friends, it was possible for participants to continue to learn about their ex-partners' activities, even though they no longer wanted such information. Sas et al., [46] studied how users keep or dispose of their digital possessions after a romantic breakup. The authors conducted semi-structured interviews with 24 students and identified three roles that people take in disposing of their digital possessions: deleters, keepers, and selective disposers.

Researchers from the University of Dundee also studied how users manage their digital possessions after a romantic breakup, with the goal of informing the design of systems aimed at helping people disentangle digitally [22, 35]. The digital possessions studied included videos, chat logs, login details, shared accounts, social media posts, and text messages. The study was carried out with 13 participants. The authors found that after the romantic relationship ended, the role of digital possessions changed, as the possessions now acted as a proof that the relationship existed and was over. Participants managed their digital possessions by hiding, deleting, or abandoning their possessions, and in some cases, letting the possessions fall into disuse.

Our study differs from prior research in two major ways. First, we focus on the end of online shared accounts and we consider different age groups and types of interpersonal relationships. While Sas et al. [46] studied what users do with their digital possessions, we go further to identify the specific security and privacy challenges that users face when managing one type of digital possession — an online shared account. No previous studies have focused their investigation on these challenges. Second, we discuss how systems can be designed to support users during the ending of the sharing of accounts while considering users' security and privacy issues.

METHODOLOGY

Data Collection

We recruited participants by advertising on Facebook and on UBC's paid participants study list. Potential participants filled out an eligibility survey. To be eligible to take part in the study, participants had to be 19 years old or above. Participants had to have stopped sharing at least one account within the last 12 months or be in the process of ending the sharing of an account. We chose to recruit people who were also in the process of ending account sharing to understand any current challenges they might be facing.

We piloted our study procedure with two participants. In the first pilot study, we asked the participant what account she had stopped sharing. We realized that the participant had difficulties remembering most of the accounts she ended sharing. The participant remembered some shared accounts only when the researcher gave examples of commonly shared accounts. Based on this result, we decided to present participants with a list of accounts grouped and categorized by Park et al. [40], to help participants remember their shared accounts. We piloted this approach with a second participant, and we discovered that the participant remembered previously shared accounts easily. We therefore decided to use this approach for the main study. Apart from this change, all other procedures in the pilot interviews were the same as those used in the main study.

After adjusting the study design based on the outcomes of the pilots, we recruited participants for the main study. We carried out semi-structured individual interviews with all recruited participants to allow participants to express their thoughts in their own way and add information as they saw fit, without the restriction of a structured interview [8]. We conducted in-person or video interviews based on the participant's preference. In-person interviews were conducted in a quiet meeting room on UBC campus, while video calls were conducted via Skype. Participants interviewed in person were compensated with $20, sent via e-transfer to those participants whom we interviewed via video call. We conducted 11 interview sessions via Skype video, with the rest (14) in person. Data collection was done from December 2018 to February 2019. The research was approved by the UBC Behavioural Research Ethics Board (ID: H18-03521) before any data collection took place.

Interview Procedure

We proceeded with the interviews after participants gave informed consent to participate in the study. During each interview, we explained the meaning of shared accounts, giving examples of such accounts. We avoided priming the participants by stating that shared accounts were simply accounts used by the participants and other users. Participants were told that the aim of the study was to understand their experiences using shared accounts.

Participants were then asked to identify the accounts they were sharing or had shared with someone. To help participants remember their shared accounts, we presented them with a list of accounts grouped and categorized by Park et al. [40]. This list itemized most online shared accounts at the time, but we explained to participants that the account list was only a guide. As they identified other accounts that did not appear on the list, they were free to tell us about them (and some did).

After participants identified their shared accounts, we asked them which accounts they were currently sharing and which ones they had stopped sharing. Then we asked participants to give more information about the accounts that they had stopped sharing. We also asked questions about the use of passwords on their accounts. Afterward, we asked for demographic information and compensated the participants. One or two researchers took part in each interview session. All interview sessions were audio recorded.

Data Analysis

Two researchers transcribed and coded more than 16 hours of recorded interview sessions, each an average of 40 minutes long. Interviews were analyzed using thematic analysis [19], a "set of procedures designed to identify and examine themes from textual data in a way that is transparent and credible [18]." We followed the data analysis steps outlined by Guest et al. [18]. Two researchers segmented and coded the transcribed interviews into categories, types, and relationships to develop the codebook. Afterward, the researchers identified the themes that emerged from the data. We conducted data analysis concurrently with the collection and reached theoretical saturation after 23 interviews, as no new codes emerged from the last two data collection sessions. Our supplementary material includes a saturation graph depicting the total number of codes after each interview.

To calculate inter-coder reliability, we used the percentage agreement metric described by Graham, Milanowski, and Miller [16]. The calculated agreement was above 90%, which indicates high agreement. In addition, three researchers engaged in a code and theme sorting exercise to come to a consensus on the identified themes.

Participants

We recruited 25 participants (16 women and 9 men), aged 19 to 45 years (the mean and median were 27). Table 1 provides the detailed demographics of the participants. All participants had stopped sharing at least one previously shared account.

RESULTS

Our results suggest that negative impacts accompany the ending of account sharing, and we group them into two categories: cognitive and psychosocial. We define cognitive burden as the mental effort involved in ending account sharing and psychosocial burden as the emotional and social cost of ending account sharing. Although we divided these negative impacts into these two categories, it should be noted that cognitive

ID	Age	Gender	Educational Level	Occupation	Ended Sharing	Ended Sharing With
P1	21	W	Bachelor’s (Ongoing)	Student	Netflix (s)	Friends
P2	32	M	Master’s	Teacher in High School	Netflix (p)	Ex-girlfriend
					Telus (p)	Father
					LinkedIn (p)	Friends
					LinkedIn (p)	Professionals
					Skype (p)	Friends
					Gmail (p)	Friends
P3	45	M	Master’s	Information Technology	Amazon (j)	Partner
					Fantasy League Game (p)	Colleague
P4	27	M	Master’s (Ongoing)	Master’s Student	Netflix (p)	Friend
					Netflix (p)	Wife
P5	25	M	Bachelor’s	Finance Clerk	Email Account (p)	Employer
					Bank Account (s)	Father
					Amazon (p)	Mother
P6	28	M	Diploma	Circus Artist Instructor	Bank Account (s)	Parents
					Online Calendar (s)	Colleague
P7	31	M	Master’s	Research Assistant	Amazon (p)	Wife
					Amazon (s)	Friend
P8	23	W	Bachelor’s	Tutor	Netflix (s)	Boyfriend
					OkCupid (p)	Ex-boyfriend
P9	29	W	Bachelor’s	Administrative Assistant	Netflix (s)	Boyfriend
					Apple (p)	Family
P10	29	W	Bachelor’s	Tutor	Amazon (s)	Father
P11	29	W	Master’s	PhD Student	WeChat (s)	Sister
					Gmail (s)	Sister
					Sephora (p)	Friend
					Game Account (p)	Friend
					Apple (p)	Family
					Baidu (p)	Sister
P12	30	W	Master’s	Human Resource Specialist	Bank Account (p)	Parents
					Netflix (p)	Parents
					Gmail (p)	Ex-boyfriend
					Facebook (p)	Friend
P13	27	W	Bachelor’s	Unemployed	League of Legends (p)	Brother
					League of Legends (p)	Ex-boyfriend
					Netflix (p)	Brother
					Booking.com (p)	Friend
P14	20	W	Bachelor’s	Student	Amazon (p)	Brother
					Facebook (p)	Ex-boyfriend
					Gmail (p)	Classmates
					Craigslist (s)	Roommates
					Netflix (s)	Family
					Soundcloud (s)	Ex-boyfriend
					Xbox (s)	Brother
					Dropbox (s)	Friends
P15	22	M	Bachelor’s (Ongoing)	Student	Bank Account (s)	Parents
					iTunes (p)	Father
					Spotify (p)	Sister
					Dropbox (s)	Colleagues
P16	24	M	Bachelor’s	General Manager	Bank Account (p)	Ex-girlfriend
					Facebook (p)	Ex-girlfriend
					Yahoo (p)	Ex-girlfriend
					Gmail (p)	Friend
P17	23	W	Bachelor’s	Admin in Insurance	Netflix (s)	Boyfriend
					New York Times (p)	Friend
					Bank Account (p)	Parents
P18	25	W	Bachelor’s	Respiratory Therapist	Bank Account (s)	Mother
					Nextopia (p)	Friend
					Facebook (s)	Friend
					Instagram (s)	Friend
					Netflix (s)	Friend
P19	21	W	Bachelor’s (Ongoing)	Student	Bank Account (p)	Brother
					Netflix (p)	Friend
P20	19	W	Bachelor’s (Ongoing)	Student	Bank Account (s)	Mother
					Tumblr (p)	Ex-boyfriend
					Snapchat (p)	Ex-boyfriend
					Amazon (s)	Ex-boyfriend’s Friend
					Netflix (s)	Ex-boyfriend
					Uber Eats (s)	Ex-boyfriend
					Office365 (p)	Ex-boyfriend
P21	36	W	Bachelor’s	Office Admin	Netflix (s)	Husband
P22	20	W	Bachelor’s	Student and Sales Personnel	Google Drive (s)	Ex-boyfriend
P23	32	W	Bachelor’s	Secretary	Facebook (p)	Friend
P24	42	M	Master’s	Model and Writer	Netflix (p)	Ex-partner
					Bank Account (p)	Ex-partner
					iTunes (p)	Sister
P25	23	W	College (Ongoing)	Student and Part-Time in Insurance	Netflix (s)	Boyfriend
					Bank Account (s)	Mother

Table 1. Detailed demographics of participants. P, S, and J represent primary, secondary, and joint users respectively.

and psychosocial burdens are linked together. All cognitive burdens come with an indirect psychosocial cost, and they often tax users in the form of frustration. We discuss these categories of burden below.

In the rest of the paper, we refer to each participant using the suffixes "P,""S," and "J" along with their ID, to indicate whether the participant was a primary, secondary, or joint user of the shared account. A primary user is the owner of the shared account. A secondary user is not an owner of the account, but shares it with the primary user. *Joint* users both own the shared account with the intent to have equal rights and privileges.

Cognitive Burden

Remembering secondary users. Our participants found it challenging to remember the people with whom specific accounts were shared. Sometimes participants forgot that they shared a particular account. As a result, they forgot to end the sharing of that account, even after the sharing was no longer desired. For example, it was during our interview that P20-P remembered that, apart from her mother, she still shared her Microsoft Office 365 account with her ex-boyfriend: *"Oh my gosh. I still share [my Microsoft 365 account] with my ex!"* She didn't want to continue sharing the account; however, she had forgotten that the account was still shared. Similarly, P22-S, who tagged herself as a "self-imposed" secondary user, also described a scenario where the primary user forgot to log out: *"... it was [during] a movie night [with people from a school club] and I was the one who brought the laptop but I don't have [a] Netflix account. So [an acquaintance] logged in with my laptop and then she forgot to sign out, so I've been taking advantage of [the account] [laughs]."* P22-S has been using the Netflix account for about 18 months.

Changing passwords. Password changes were described as both useful to end account sharing, but also problematic in the cognitive burden they introduced. P20-S described the value of password changes in a story about her boyfriend's Netflix account that was shared with multiple people: *"At least 9 people [used his Netflix account] because there were about 5 profiles and then I think each of them has their own people they were sharing it with. [My boyfriend at the time] had to change his password a lot because there were too many people logged in at [once] ... Whoever he shared it with shared it with other people. So if he wants to watch [Netflix] he couldn't, because there were too many people on it, so he would change his password. [That] would log everyone out and then he would be able to watch it and then [he would] share the password and just repeat that cycle."*

When sharing ends, changing passwords can be a tedious process. P2-P, for example, shared his LinkedIn account multiple times with his friends and paid professionals because he needed help in making his account look professional. However, every time he shared his LinkedIn account, he had to change his password after his friends (or professionals) finished editing his account content. P2-P commented on the burden of having to change his passwords multiple times: *"... it's annoying [to change passwords] because I do forget [the new password] ... I've had that problem a few times before where I've lost track of my passwords and answered some [security] questions [or] ... go through the security feature where they email me [on some other platform] just to verify that it is me."*

To avoid the cognitive burden of changing passwords, sometimes participants would request that the secondary user(s) stop logging into the account. P8 illustrated this while describing an incident between her boyfriend (secondary user) and his ex-girlfriend (primary user): *"I happened to be calling [my boyfriend, and he said] ... 'I just got a text from my ex saying, "Can you log out of the Netflix account?"' [My boyfriend's ex] was also sharing [her Netflix account] with other people. So instead of [changing the password for everyone] ... it's easier to just kick one person out."* In this case, changing the password for multiple users who were sharing a Netflix account would have proved even more challenging. This coping mechanism is, however, linked to the burden of remembering secondary users. For this strategy to be carried out effectively, primary users have to remember that a particular secondary user still has access to the account.

Remembering which passwords are reused on which accounts. Participants found it challenging to remember the accounts across which they had reused passwords. P13-P, for instance, used the same password on her game, bank, Netflix, and university student accounts. She had shared her game account with her boyfriend but changed the password when she had a disagreement with him. However, she had forgotten that she used the same password on the other accounts. P13-P only realized this during the interview and noted that she would change the passwords for the other accounts as well.

Some participants coped with the challenge of remembering many passwords by reusing them across shared and non-shared accounts. P16's example illustrates this behaviour: *"[I know reusing passwords] is wrong, but I do [reuse passwords] because it's easier to remember ... I know you should have different passwords for different accounts, but I'm just too lazy ... because I might forget them."* P22 explains further: *"I tend to use the same password for a lot of websites, and just because I told my password to someone for one website means the person basically knows a lot of passwords for many websites."* Previous research [27, 55] also shows that people reuse passwords to avoid remembering multiple passwords.

To lighten the cognitive burden of remembering many passwords, participants sometimes also derived similar passwords. Passwords used on shared accounts were similar or the same to those used on non-shared accounts. P23, who used similar passwords on shared accounts, explained how she modified her password across accounts: *"I have just one password but then ... I tweak the password a little differently for all of the accounts. Maybe I add an exclamation mark to one, [then] add a number ... ."* Similar passwords are, however, easy to guess. Zhang et al. [57] discovered that if an attacker has access to a password, they can correctly guess the future passwords in 41% of accounts in an offline attack under 3 seconds, and 17% of accounts in an online attack.

Psychosocial Burden

The uncertainty of whether the sharing was successfully stopped. Participants were not always sure that changing password was enough to end sharing. Modern devices are kept logged into online services for extended periods of time without re-authentication (thanks to access tokens in OAuth [36] and similar authentication technologies). While this feature is very convenient in single-user scenarios, it leaves primary users uncertain whether and when changing password "kicks out" secondary users. It was particularly problematic when primary users were unwilling to ask the secondary users to stop using the account. For instance, P20-P no longer talked to her ex-boyfriend after their romantic breakup. During the relationship, she shared her private blog hosted on Tumblr [52] with him. When asked if she was still sharing the account, P20-P remarked: *"... I don't know ... I changed my password, and I hoped that it would log him out ... I think the [Tumblr] app is still [on his phone], but I hope he's logged out."*

The annoyance of being unable to migrate content to a new account. Transferring previously shared content to a new account sometimes proved difficult. P15-S, who had shared his father's Apple ID account, explained the challenges he experienced when sharing ended: *"[On migrating the free apps] I would have preferred to be able to transfer [the free apps] automatically [to the new account] because ... that way I [don't] have to manually re-download all the free apps [from] the app store ... It would be nice to save time."* Similarly, participants discussed lost Netflix profiles and the corresponding movie lists recommendations when sharing ended. P4-P commented: *"I used to share my [Netflix] account with other group of people ... Having that account established and then switching over to another [Netflix] account [to be shared with a new group of people], [it] was difficult to manage all the [profile] list that I create[d]. [I had to] re-establish my entire profile all over again. It's time-consuming and something that you should not [have] to worry about ... ."*

The inability to delete a joint account and its content. It was a challenge to be unable to control what happened to the shared account and its content when sharing ended. It was especially hard to control the previously shared content in NDS accounts. For instance, P22-J and her boyfriend at the time created a Gmail account using the combination of both their names as the email ID. They created the account so they could upload their shared pictures on Google drive. Both, therefore, had joint ownership of the account. However, her ex-boyfriend used his email account as a recovery email address, so the account designated him as the account owner. The end of their relationship also coincided with the end of sharing this account. P22-J, who stopped logging into the account after the breakup, remarked: *"... It would be nice if he didn't have [the] pictures [on the shared Google drive anymore] because we're done."* Explaining her current difficulty, she stated: *"... I want to actually get rid of the account, but I can't because it's sort of his account [and] Google doesn't know that it's two people using it. So ... I can't delete [the account]."* Here, while P22-J wanted to stop sharing the account (and to delete its content) altogether, she had no means of achieving this.

The frustration of losing personal content. Some participants reported losing their personal content. P11-P shared her gaming account with her online friends so they could help her play the game. One of the secondary users, however, traded her game characters without her permission. After ending the sharing by changing the account password, she contacted the game administrators to help her reacquire her traded content: *"[The game administrators asked] ... if someone hack[ed] into the account. I said, no, [my game characters were traded away by my friend] because I gave my friend the account [login details]. [The game administrators] said [that there was] nothing [they] could do because [I] voluntarily trade[ed] [my game characters and I] cannot prove that [someone else traded them] without my permission."* For P11-P, there was no means to prove that, while she granted permission to her friends to play the game, P11-P gave no permission to trade her game characters.

Personal content can be also lost when the end of an interpersonal relationship triggered the end of account sharing. For example, P2-P stopped sharing his Netflix account with his ex-girlfriend without notifying her, as he did not feel comfortable bringing this up with her. As a result, his ex lost all of her personalized content (such as her profile) on the Netflix account without notice.

The risk of an account being hijacked by a secondary user. Account hijacking by the ex-partner is a possible risk when a romantic relationship ends. P8-P shared login details for her online dating account (on OkCupid [38]) with her then boyfriend. After they broke up and before she changed her password, her ex hijacked the account and impersonated her: *"[My ex] ended up impersonating me online ... He took control of my account, and he changed the password [and was asking people on my account] to meet up [while pretending to be me] ... I wasn't able to log in [to my OkCupid account], but based on the messages I was getting in my emails, I was able to piece together what was happening."* Issues like hijacking, impersonation, and abuse are covered more extensively in abuse-focused literature [15, 34].

The burden of avoiding awkward conversations. Avoiding awkward conversations was a major reason why participants' attempts at ending account sharing failed. This is because participants were trying to avoid situations where the end of account sharing would signal the end of their relationship. For example, P11-P had an NDS online shopping account with French multinational chain of personal care and beauty stores (Sephora [48]). As a top-level customer, P11-P received more shopping privileges than regular customers, such as free delivery and store promotions. P11-P was sharing this account with her friend. One reason P11-P wanted to stop sharing the account was that her friend occasionally used up P11-P's store points. P11-P explained why she ended up continuing to share the account: *"... if I change the password, she'll know I don't want to share [the account] with her. But I don't know how to tell her! ... She's my friend; I [can't] tell her, 'Stop using [the account], because you annoy me.' It's not a polite thing to do."* P11-P also shared her Apple ID account on her family's shared iPad Mini. When the device was first set up, P11-P found it easier to just use her existing personal Apple ID account than to create a family account. However, she realized later that she had lost part of her privacy, because she was using the same Apple ID on her personal phone, and the users of iPad Mini could see her browsing and search history. Although P11-P wanted to stop sharing the account and regain her privacy, she felt uncomfortable explaining to her family why she wanted to change the account on the device, so she kept using the device as is.

Participants sometimes preferred to stop using an account, rather than having awkward conversations with the secondary users. P23-P, for example, shared her Facebook login details with her friend, but she wanted to stop sharing the account to regain her privacy. However, P23-P felt that deleting the account was a safer option: *"Imagine you were my best friend and then I told you, 'Hey, I want to change the password [because I no longer want to share the account with you], but I don't want to let you know.' I think that's a bit of an awkward situation and [I] don't want to go through that, [so] I asked Facebook to delete my account ... [my friend and I are] still best friends till today."* If P23-P had changed her Facebook password, she would have to explain to her friend the reason behind the password change. P23-P told her friend she deleted her Facebook account because she no longer wanted to continue using Facebook at the time. For P23-P, this was an easier option than to explain that she wanted to stop sharing the account. P2-P did not want to have an awkward conversation with his ex-girlfriend about the Netflix account that he shared with her: *"You know what? I was a coward. I didn't even tell her [I was going to stop sharing the account]. I just went and changed the account plan, and she probably figured out what was happening ... ."*

The stress of ending the sharing of utility accounts when the primary user moves out. Ending the sharing of a utility account was difficult. P6-P, for example, moved out of a household but he was having challenges with ending account sharing, as the Bell internet account "recognized" him as the sole user: *"[My former housemates and I] wanted to transfer the [Bell] account to [one of] my roommate's name [but] we had a lot of trouble [doing that]. It was ridiculous."* Explaining the process, P6-P remarked: *"[To stop sharing the account, my roommate, and I] had to both be on the phone line at the same time ... or we had to go into [Bell] store at the same time, and it's hard because people's schedules are so different. I ended up closing the account, which is more trouble because now we have to mail back the modem to Bell, and [my former roommate] has to open up her own account [for the household]."* In this situation, the utility company treated the account as a single-user account and hence required a new account to be set up for another household member. Similarly to Moncur et al. [35] we report the difficulty of transferring utility accounts at the end of relationships. The novelty of our work is in exploring these challenges beyond romantic partnerships.

DISCUSSION

Limitations

Our sample could have been more balanced and diverse. It had more women (64%) participants. We were also unable to get data from older population groups, though we did collect data from multiple age groups. In addition, although we investigated various types of interpersonal relationships, among romantic relationships, we only investigated monogamous relationships.

While all participants stopped sharing at least one online account in the 12 months preceding the study, some of the experiences that participants reported occurred more than a year before the interviews. This may have affected how well participants recalled their experience. Also, only two participants were attempting to end sharing when the interviews were conducted. In addition, as with any interviews, the data was self-reported and may have been affected by a number of systematic biases such as halo effect, social desirability, and acquiescence response bias [10].

Nonetheless, we believe that the results from our study can serve as a basis for further research and technology development in supporting the life cycle of account sharing.

General Discussion

The key contribution of this paper is the discovery and categorization of negative impacts of ending the sharing of DS and NDS accounts on users. This contribution may inform the design and evaluation of technology support for various ending scenarios. The prevalence of ending account sharing is yet to be investigated. Most recent estimates, however, suggest that sharing of online accounts in the US alone is widespread: 22% of Spotify users, 45% of Netflix users, and 64% of HBO NOW users share their passwords [5]. We assume that most of this sharing eventually ends. We extend previous studies done on shared online accounts [25, 33, 40], and we contribute to the research on the management of digital possessions after a romantic breakup [22, 35]. While previous research mainly investigates why and how people share accounts [33, 40], we explore challenges involved in ending sharing for both single and multi-user accounts.

Below we highlight two overarching themes synthesized from our results, which characterize user challenges in account sharing and ending.

Access to a shared account could lead to accessing non-shared accounts. In our study, we asked participants about their behaviors regarding their password usage. We do not report all our findings on password behaviors, as they are similar to the previous findings [21, 26, 27, 55]. Our results suggest that people reuse passwords (or use similar passwords) across shared and non-shared accounts. Sometimes, participants seem to forget that their shared accounts have the same or similar passwords with other accounts, as it was with P13-P, who realized that the password for her online bank account was the same as the one for a game account shared with her boyfriend. Besides, some participants reported changing their passwords only when requested by the system, or, occasionally, when they ended account sharing. Access to a shared account, therefore, could facilitate unauthorized access to other accounts. Also, with infrequent password changes, unauthorized users can have access to certain accounts for long periods, which is a security and privacy concern. These concerns emphasize the need for better support of secure account sharing (without sharing passwords) and its ending.

The end of account sharing does not always coincide with the end of the relationship. This is in contrast to previous work, which suggests that the end of a relationship implies the end of sharing and vice versa [17, 40, 50]. While we saw this link in those cases when sharing ended because of the end of dependence or loss of trust (also see Marques et al. [31] on trust and sharing), this link did not always exist in our data. In fact, one challenge that primary users faced was finding ways of ending account sharing while still maintaining their relationship with the secondary user(s). One particular burden was having or avoiding awkward conversations about ending access to the account.

Implications for Design

In the next two subsections, we suggest how system design can address some of the challenges in ending account sharing. We acknowledge that there may be non-technical means, e.g., helping people to develop ethical and moral values, or to improve their communication skills. At the same time, technology researchers and developers can explore options for improving support for reasonable use cases and help users avoid unreasonable sharing, while following the path of least resistance.

We believe (but did not verify) that implementing our suggestions may benefit some users and service providers. All the design suggestions could result in improved protection of accounts' privacy and security, as well as better customer satisfaction. Most of these design improvements could lead to greater sense of control among some primary users, and, as a result, reduce some users' anxiety about their accounts.

Service providers may also benefit, directly and indirectly, from addressing the identified challenges. We expect that improved user experience could result in improved customer satisfaction and fewer customers switching to competing services [45, 51, 54]. More generally, the lower the cognitive and psychosocial cost of securely using an account is, the more compliance budget [4] is left for users to comply with other requirements and rules of the service provider. In addition, service providers might see reduced customer support costs, as the proposed measures may improve account security and reduce abuse and conflict among account sharing users. It should be noted that a thorough analysis of the usability, deployability, and effectiveness of these design suggestions is a subject for future research. Further, we did not consider all user contexts, including abuse contexts, and need further evaluation to determine if and how the design suggestions presented here might work for users coping with abuse or other circumstances not explored in this study.

Designing for Ending DS Account Sharing

Support transfer of user profiles from an existing to a new account. This would reduce the effort needed to transfer profiles and recommendations to new accounts when sharing ends. For instance, when a secondary user of a Netflix-like service is ending account sharing and wants to create their own account with the same provider, the provider could offer the option of transferring the profile to the new account. The transfer can be done by "linking" the old profile to the new account or by exporting the profile data to the user, who can import it into the new account later. This would help users keep their personal preferences, history, movie lists, etc. This is related to the suggestion by Park et al. [40] for romantic relationship maintenance. We go further by offering a more concrete design recommendation. We also note that such support may not only benefit relationship maintenance but could also aid the ending of account sharing. Such a feature could reduce the burden of "branching off" a shared account, which might increase the likelihood a user would continue with the same service provider, rather than switching to a competitor.

Help primary users to remember which accounts they share and with whom, and help them to end sharing if needed. Service providers could support users in these tasks by displaying all the devices that have accessed the account recently or since the last password change, and allowing the user to end account access for some devices. The account could also be designed to allow the primary user to label devices, so that the user can easily identify the devices accessing the account. This design could benefit both the user and the provider by improving the transparency of the access to the account, which might increase the likelihood of the user detecting an account compromise early. In turn, early detection of account compromise might reduce, or even eliminate, the cost of investigation by the provider's technical staff. Some account providers (such as Microsoft, Google, Facebook, and more) already offer some of the features listed, but not all providers do and we note that they would be helpful in many account ending situations.

Allow users to label devices as primary or secondary. This design might grant additional privileges to users when they access the account from a primary device. For example, to help primary users to be aware of which devices are currently logged into their accounts, the system might also occasionally prompt users (when logged in from a primary device) to log secondary devices out. This account design may benefit users like P20-P, whose boyfriend at the time used her login credentials to log in to the Tumblr app on his phone, but she was not sure whether he could still access her account after the breakup. This design may save primary users from the anxiety of being unsure about access to the account by secondary users. Also, the design may help some users to have a sense of control over which secondary users and secondary devices are logged in to their account.

Allow users to limit the duration of a sign in. Users could also be allowed to set a duration for how long they want to remain logged in. If users do not select this option, then they are automatically logged out of that device after a set time. While a "Keep me logged in" option is available on some accounts, we suggest that developers make it available on all online accounts with the option to specify how long the user remains logged in. For instance, P22-S had been sharing a Netflix account for about 18 months, without the knowledge of the primary user. With this option, P22-S would have been logged out of the account after the set time has expired, protecting the privacy of the primary user.

Ensure that the primary user always stays in control of the account. Sometimes the primary users face a "racing problem" when ending password-based sharing. When account sharing ends, whoever resets the account password first wins the race by taking control of the account (e.g., the ex-boyfriend of P8-P hijacked her dating site account by resetting its password). This racing problem is also seen in accounts of some banks. For example, to open a joint account at TD Canada Trust, both co-owners need to be present, but either co-owner can close the account (and appropriate the account funds) [2]. We suggest that service providers could make sure that the primary user keeps control of the account independently of the actions by the secondary user(s).

Provide an option of equal account sharing. Our results and studies by others [25] suggest that romantic couples create cloud storage and email accounts that they intend to share equally and use them for digital assets and communications specific to that relationship. The technology could consider providing an option of "equal" sharing, in which a single primary user cannot just "walk away" with the account. This design reassures users that they will not lose the control of shared digital content when account sharing ends.

Designing for Ending NDS Account Sharing

There are cases of reasonable and unreasonable sharing of NDS accounts. Although NDS accounts are not designed to be shared, participants still shared some of these accounts because they needed to carry out essential tasks that they could only accomplish through account sharing. Since such sharing of NDS accounts does not reduce the revenue of the service providers, we classify it as *reasonable*. More precisely, we define as *reasonable* such cases of sharing NDS accounts that (1) violate the accounts' Terms of Service (ToS) but (2) do not reduce the revenue of the service provider (see Table 2). We believe that it would be beneficial (for both the users and the service providers) if it were easier for users to do reasonable sharing of these accounts. We discuss later in this subsection how support for reasonable sharing of NDS accounts and its ending can be improved. We also define *unreasonable* sharing of NDS accounts if it (1) violates ToS and, compared to the case when each user has their own account with the provider, (2) reduces its revenue, e.g., multiple users sharing a single-user Netflix account. This dichotomy of sharing cases is used solely for the purpose of guiding the reader through the discussion of our recommendations, and with the understanding that service providers have many factors to consider when deciding whether and how to support sharing, and our investigation does not explore them all.

	ToS Violated	Revenue Reduced
Sharing of DS	No	Not applicable
Reasonable Sharing of NDS	Yes	No
Unreasonable Sharing of NDS	Yes	Yes

Table 2. The differences between reasonable and unreasonable cases of account sharing. "ToS" is terms of service.

We suggest that service providers reduce sharing in unreasonable instances by making sure that the path of least resistance [56] for using their products is via non-shared accounts. This suggestion may be difficult to implement, as people circumvent the current barriers put in place to make sharing under unreasonable instances hard. For example, some participants reported sharing Spotify's single-user account. They used Spotify offline, in airplane mode, when they wanted to listen to songs. This trick prevented Spotify servers from detecting and logging out such concurrent listeners. Participants did so to avoid paying the subscription fee for separate accounts. Apart from lost revenue [7] for the service provider, users' privacy and security are more at risk when NDS accounts are shared. Exploring design trade-offs for reducing unreasonable sharing of NDS accounts appears to be an intriguing open research problem.

Supporting Reasonable Sharing of NDS Accounts.

Some NDS accounts could support safer and easier sharing. As we report in Cognitive Burden subsection of Results, P2-P shared his LinkedIn account with his friends and freelancers because he needed help in improving his profile. The availability of many online services that assist users in creating and updating their LinkedIn profiles [28, 30, 42] suggests that many people have similar needs [44]. The participant had to change and remember his new LinkedIn password each time the profile edit was completed and sharing ended. Frequent password changes increase users' cognitive load and nudge them into the unsafe behavior of sharing their passwords with others. It also likely uses up their security compliance budget [4], which can lead to choosing easy-to-guess passwords or even reusing passwords across their accounts (as our participants reported). Findings from our and other studies [31, 33] suggest that users share their social media accounts for convenience and to signal trust (see Results section and Table 1). For example, a friend of P18-S shared his Facebook and Instagram accounts because he wanted P18-S to check his social media messages, to help him keep in touch with his contacts during exams and other hectic periods of his life. In this scenario, it was convenient for the user to share his account, but doing so by sharing his password was unnecessary.

Support password-less sharing of account personal content. Rather than pushing users toward violating terms of use (which make users to agree to "(1) try to choose a strong and secure password; (2) keep your password secure and confidential" [29]), LinkedIn, Facebook, and similar services could create easier means for users to provide others with access to (parts of) their profile/content without sharing the passwords for their individual accounts. For instance, LinkedIn could design users' personal accounts to have sharing functionality, similar to Google Docs, Overleaf [39], or Facebook Business Pages [12]. Users would be able to share their personal content (in this case users' social networking profile or personal posts and direct messages) by granting others edit or review rights. Since our and others' findings [13] indicate that passwords are commonly reused across online accounts, eliminating cases where users have to share their passwords may benefit both users and service providers by improving security of the accounts.

Support granting of fine-grained permissions to other users. We recommend that users be able to give fine-grained permissions rather than an all-or-nothing access to their personal content. Social networking sites could design personal accounts to enable users to give other users the right to view and/or modify certain parts of their personal content. This could include being able to view messages, reply to messages, and make posts on the shared accounts. To end the sharing of the accounts, the primary user would remove the permissions of the secondary user(s) in the account settings.

These designs may be beneficial to both users and service providers. This is because for some users, the cost of changing passwords is higher than the cost of giving secondary users the right to edit a profile. With such designs in place, users would not even have to share their passwords to begin with. Therefore, ending account sharing could be simplified without primary users changing their passwords for the shared account or remembering to avoid using passwords similar to the ones on their other accounts. This design could also reduce users' cognitive load (and indirectly the use of their compliance budget) due to remembering new passwords. The feasibility of this suggestion has been demonstrated by Twitter, which has recently enabled multiple users to share a personal account without sharing its password [53]. Further, shared passwords give full access to the user's account, which violates the principle of least privilege [47]. This design may also benefit the company by reducing customer support costs arising from secondary users hijacking accounts.

Design household utility accounts with multiple users in mind. There are many challenges involved in using a single utility account. There is an entanglement of service accounts (i.e., accounts used for providing services) and user accounts that hold billing transaction history, preferences, and information specific to the user. This entanglement needs to be removed to support the ending of sharing utility accounts. We suggest that each household could have a set utility account, e.g., "Apt 131 Electricity," and the system would be designed to support Relationship-Based Access Control (RelBAC) [3]. For example, when people move into apartment 131, their individual accounts are added to the "Apt 131 Electricity" utility account, and at least one person is designated as a primary user. With RelBAC, the primary user can assign other users to specific roles. To end sharing when a user moves out of the apartment, a primary user would remove that user from the shared account. Such a design would benefit users by making it easier to transfer the responsibilities for the account. Also, apart from reducing the support cost for the company, the cost of closing one shared account and opening another one may be less for both users and the utility providers. There may also be higher customer satisfaction.

Support household accounts on shared devices. We suggest encouraging users to set up multi-user "household" accounts on shared devices, rather than sharing single-user accounts, by explicitly designing support for such accounts. For example, while Apple provides a "Family Sharing" capability to support the sharing of purchased content across individual accounts [1], it requires each device still to be activated with one individual's Apple ID. As our data suggests, privacy issues arise when single-user accounts are used on the devices shared in households, and, with time, the psychosocial burden of ending the sharing of such accounts only increases. Device manufacturers and service providers could consider making household accounts first-class citizens. One option could be to include a step during the device setup process to indicate whether the device is designated to be shared. If so, then the device could be specifically configured for sharing, so that each user would use their own account/profile on the device. A benefit for the users could be the protection of their privacy and security, which is particularly important given the potential threat from social insiders [31, 32]. Even though service providers may prefer that each user possess their own device, our and others' findings suggest that sharing of devices is common [33]. The potential improvement in user experience and reduction of psychosocial burden could benefit users and, indirectly, the service providers.

CONCLUSION

We report various security and privacy challenges involved in the ending of account sharing. Our findings suggest the need for developers to consider the various challenges and the different contexts when designing online shared accounts.

ACKNOWLEDGEMENTS

This research has been supported in part by a gift from Scotiabank to UBC. We would like to thank members of the Laboratory for Education and Research in Secure Systems Engineering (LERSSE) who provided their feedback on the reported research and the earlier versions of the paper. We thank our anonymous reviewers for all the feedback and suggestions they provided for improving the paper. Stylistic and copy editing by Eva van Emden helped to improve readability of this paper. Special thanks go to the anonymous shepherd who went above and beyond in helping to improve this paper.

REFERENCES

[1] Apple. 2019. Apple support. http://support.apple.com/en-ca/HT204976. (2019). Accessed: 2019-12-23.

[2] TD Bank. 2019. TD bank joint account. http://tdbank.intelliresponse.com/?requestType=NormalRequest&source=3&question=How+do+I+open+or+close+a+joint+account. (2019). Accessed: 2019-12-23.

[3] John Barkley, Konstantin Beznosov, and Jinny Uppal. 1999. Supporting relationships in access control using role based access control. In *Proceedings of the fourth ACM workshop on Role-based access control*. ACM, 55–65.

[4] Adam Beautement, M Angela Sasse, and Mike Wonham. 2009. The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 New Security Paradigms Workshop*. ACM, 47–58.

[5] Paul Bischoff. March 2019. Nearly Half of Netflix Subscribers Share their Account Passwords. https://www.comparitech.com/blog/vpn-privacy/sharing-netflix-passwords/. (March 2019). Accessed: 2019-12-16.

[6] Pew Research Center. January 2017. Password management and mobile security. http://www.pewinternet.org/2017/01/26/2-password-management-and-mobile-security. (January 2017). Accessed: 2019-02-27.

[7] CNBC. August 2018. User Agreement. https://www.cnbc.com/2018/08/19/millennials-are-going-to-extreme-lengths-to-share-streaming-passwords-.html. (August 2018). Accessed: 2019-02-28.

[8] Deborah Cohen and Benjamin Crabtree. 2006. Qualitative research guidelines project. (2006).

[9] The Conversation. February 2018. How to digitally disentangle after a break up, some new rules. http://theconversation.com/how-to-digitally-disentangle-after-a-break-up-some-new-rules-90592. (February 2018). Accessed: 2019-02-27.

[10] Diane Dodd-McCue and Alexander Tartaglia. 2010. Self-report response bias: Learning how to live with its diagnosis in chaplaincy research. *Chaplaincy Today* 26, 1 (2010), 2–8.

[11] Serge Egelman, AJ Brush, and Kori M Inkpen. 2008. Family accounts: a new paradigm for user accounts within the home environment. In *Proceedings of the 2008 ACM conference on Computer supported cooperative work*. ACM, 669–678.

[12] Facebook. 2019. Facebook business page. facebook.com/business/pages. (2019). Accessed: 2019-12-23.

[13] Dinei Florencio and Cormac Herley. 2007. A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web*. ACM, 657–666.

[14] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, 667.

[15] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2017. Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (2017), 46.

[16] Matthew Graham, Anthony Milanowski, and Jackson Miller. 2012. Measuring and Promoting Inter-Rater Agreement of Teacher and Principal Performance Ratings. *Online Submission* (2012).

[17] The Guardian. 2018. From ghosting to oversharing: the new rules of breakups. https://www.theguardian.com/lifeandstyle/2018/nov/15/new-rules-of-breakups. (2018). Accessed: 2019-02-27.

[18] Gregory Guest, Kathleen M MacQueen, and Emily E Namey. 2011. Applied thematic analysis. (2011).

[19] Gregory Guest, Kathleen M MacQueen, and Emily E Namey. 2012. Introduction to applied thematic analysis. *Applied thematic analysis* 3 (2012), 20.

[20] Management Study Guide. 2019. Different Types of Interpersonal Relationships. https://www.managementstudyguide.com/types-of-interpersonal-relationships.htm. (2019). Accessed: 2019-09-18.

[21] Cormac Herley. 2009. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop*. ACM, 133–144.

[22] Daniel Herron, Wendy Moncur, and Elise van den Hoven. 2017. Digital decoupling and disentangling: towards design for romantic break up. (2017).

[23] Troy Hunt. 2017. The Trouble with Politicians Sharing Passwords. https://www.troyhunt.com/the-trouble-with-politicians-sharing-passwords/. (2017). Accessed: 2019-07-30.

[24] Country Financial Security Index. September 2018. Survey: More than Half of Americans Are Using Shared Services Like Uber, Lyft and Airbnb. https://www.countryfinancial.com/en/about-us/newsroom/year2018/More-than-Half-of-Americans-Are-Using-Shared-Services.html. (September 2018). Accessed: 2019-02-27.

[25] Maia Jacobs, Henriette Cramer, and Louise Barkhuus. 2016. Caring About Sharing: Couples' Practices in Single User Device Access. (2016).

[26] DS Jeslet, G Sivaraman, M Uma, K Thangadurai, and M Punithavalli. 2010. Survey on awareness and security issues in password management strategies. *IJCSNS* 10, 4 (2010).

[27] Joseph Jofish Kaye. 2011. Self-reported password sharing strategies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2619–2622.

[28] Klaxos.com. 2009. LinkedIn Profile Writing Service. https://ca.linkedin.com/company/linkedin-profile-service. (2009). Accessed: 2019-02-28.

[29] LinkedIn. May 2018. User Agreement. https://www.linkedin.com/legal/user-agreement. (May 2018). Accessed: 2019-02-28.

[30] LinkedIn Makeover. 2019. Order Your LinkedIn Makeover Today. https://www.linkedin-makeover.com/order-today/. (2019). Accessed: 2019-02-28.

[31] Diogo Marques, Tiago Guerreiro, Luís Carriço, Ivan Beschastnikh, and Konstantin Beznosov. 2019. Vulnerability & Blame: Making Sense of Unauthorized Access to Smartphones. (2019).

[32] Diogo Marques, Ildar Muslukhov, Tiago Guerreiro, Luís Carriço, and Konstantin Beznosov. 2016. Snooping on mobile phones: Prevalence and trends. In *Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016)*. 159–174.

[33] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. 2016. She'll just grab any device that's closer: A Study of Everyday Device & Account Sharing in Households. (2016).

[34] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F Churchill, and Sunny Consolvo. 2017. Stories from survivors: Privacy & security practices when coping with intimate partner abuse. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 2189–2201.

[35] Wendy Moncur, Lorna Gibson, and Daniel Herron. 2016. The role of digital technologies during relationship breakdowns. (2016).

[36] OAuth. 2019. The OAuth 2.0 Authorization Framework. https://tools.ietf.org/html/rfc6749. (2019). Accessed: 2019-12-26.

[37] House of Commons. 2017. House of Commons Staff Handbook-Information Security Responsibilities. https://www.parliament.uk/documents/commons-resources/Staff-handbook/chapter-23-information-security.pdf. (2017). Accessed: 2019-09-17.

[38] OkCupid. 2019. OkCupid's homepage. https://www.okcupid.com. (2019). Accessed: 2019-12-22.

[39] Overleaf. 2019. Overleaf about us. www.overleaf.com/about. (2019). Accessed: 2019-12-23.

[40] Cheul Young Park, Cori Faklaris, Siyan Zhao, Alex Sciuto, Laura Dabbish, and Jason Hong. 2018. Share and Share Alike? An Exploration of Secure Behaviors in Romantic Relationships. (2018).

[41] UK Parliament. 2019. Advice for Members and their Staff. https://www.parliament.uk/documents/upload/advice-for-members-offices.pdf. (2019). Accessed: 2019-09-17.

[42] ProfileLinked. 2009. We Create Your Professional Linkedin Profile. https://ca.linkedin.com/company/professional-linkedin-profiles-services-for-executives. (2009). Accessed: 2019-02-28.

[43] Anabel Quan-Haase, Andrew D Nevin, and Veronika Lukacs. 2018. Romantic Dissolution and Facebook Life: a Typology of Coping Strategies for Breakups. In *Networks, Hacking, and Media–CITA MS@ 30: Now and Then and Tomorrow*. Emerald Publishing Limited, 73–98.

[44] Quora. November 2018. Is it possible to share access to a LinkedIn profile? https://www.quora.com/Is-it-possible-to-share-access-to-a-LinkedIn-profile. (November 2018). Accessed: 2019-02-28.

[45] Jim Ross. 2014. The Business Value of User Experience. *Cranbury: D3 Infragistics* (2014).

[46] Corina Sas and Steve Whittaker. 2013. Design for forgetting: disposing of digital possessions after a breakup. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 1823–1832.

[47] Fred B Schneider. 2003. Least privilege and more [computer security]. *IEEE Security & Privacy* 1, 5 (2003), 55–59.

[48] Sephora. 2019. Sephora's about us page. https://www.sephora.com/beauty/about-us. (2019). Accessed: 2019-12-22.

[49] Supriya Singh, Anuja Cabraal, Catherine Demosthenous, Gunela Astbrink, and Michele Furlong. 2007. Password sharing: implications for security design based on social practice. (2007).

[50] Erica B Slotter, Wendi L Gardner, and Eli J Finkel. 2010. Who am I without you? The influence of romantic breakup on the self-concept. *Personality and Social Psychology Bulletin* 36, 2 (2010), 147–160.

[51] David Sward. 2007. User experience design: a strategy for competitive advantage. *AMCIS 2007 Proceedings* (2007), 163.

[52] Tumblr. 2019. Tumblr's homepage. https://www.tumblr.com. (2019). Accessed: 2019-12-22.

[53] Twitter. 2019. How to Use the Teams Feature on TweetDeck. https://help.twitter.com/en/using-twitter/tweetdeck-teams. (2019). Accessed: 2019-09-18.

[54] UXPlanet. 2019. Why Better Web User Experience Leads to Better Branding. https://uxplanet.org/why-better-web-user-experience-leads-to-better-branding-e2194ff0d081. (2019). Accessed: 2019-09-18.

[55] Monica Whitty, James Doodson, Sadie Creese, and Duncan Hodges. 2015. Individual differences in cyber security behaviors: an examination of who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking* 18, 1 (2015), 3–7.

[56] Ka-Ping Yee. 2002. User interaction design for secure systems. In *International Conference on Information and Communications Security*. Springer, 278–290.

[57] Yinqian Zhang, Fabian Monrose, and Michael K Reiter. 2010. The security of modern password expiration: An algorithmic framework and empirical analysis. In *Proceedings of the 17th ACM conference on Computer and communications security*. ACM, 176–186.