

ABSTRACT

Title of Thesis: USERS' PERCEPTIONS OF DATA OWNERSHIP, DATA STORAGE, AND THEIR LOCUS OF CONTROL OVER DATA GENERATED BY SMART PHONE APPLICATIONS

Lisa Rogers, Master of Science 2020

Thesis Directed By: Dr. Michelle Mazurek, Assistant Professor, Department of Computer Science and Institute for Advanced Computer Studies

When users don't understand how their data is stored, managed, and deleted in the cloud, it can leave that data vulnerable to hacking, privacy breaches, and other losses. How aware are users of what data they have in their cloud or other locations? This thesis examines how centralized remote storage affects participants' knowledge of and ability to control and delete their phone app data using qualitative semi-structured interviews with 16 adults in the Washington, DC area.

Results indicate that many users, especially Android users, don't know what data they have backed up, and don't feel they have control or understanding of their cloud account. Some participants thought they could better control their data if they learned more technical skills, but felt too intimidated to try. These results have implications for designing more usable cloud storage, recovery and deletion for mobile devices.

USERS PERCEPTIONS OF DATA OWNERSHIP, DATA STORAGE, AND
THEIR LOCUS OF CONTROL OVER DATA GENERATED BY SMART
PHONE APPLICATIONS

by

Lisa Marie Rogers

Thesis submitted to the Faculty of the Graduate School of the
University of Maryland, College Park, in partial fulfillment
of the requirements for the degree of
Masters of Science
2020

Advisory Committee:
Dr. Michelle Mazurek, Chair
Dr. Marshini Chetty
Dr. Jessica Vitak

© Copyright by
Lisa Marie Rogers
2020

Acknowledgements

To my parents, who never let me forget I still had a thesis to complete once I started in the working world. Also to all their support both with my masters and before, giving me the opportunities for a robust and diverse education. To my mom for offering to correct my horrible grammar for 33 years now, and my father who always supported us to find and pursue a career that makes us happy.

To my grandfather, who taught me from a young age that the world can take away anything from you, but your education. To my sister who kept me supplied on veggies to make sure I stayed healthy under pressure.

To my beloved Veck, who endured countless pilot tests and freak outs during my grad school education. He took me to experience and eat at wonderful far away places to inspire me during grad school. I'll never forget the combination of this that led to him piloting a study for system administrators as we rode a boat around the canals of Amsterdam. Of course he had to answer each question about pianos, but got my confidence in the study flow up. Whenever he is around my glass is always full, be it of caffeine or alcohol.

To my advisor, Michelle, who took in a student from a different department, because I wanted to learn about Usable Security. She taught me more than

just qualitative methodology, she taught me where resources were to attend security conferences all around DC and how to network with academics.

Thank you for all your insights, suggested talks and suggested reading over the years. Also thank you for not giving up on me, even though this project took a long time!

To Marshini, for keeping my research confidence and spirits up during graduate school and looping me into doing interesting work with interesting people. I learned a lot from you to hone my moderating skills as well as brainstorming exercises I use everyday in work. There have been so many times I've had to pull out a design thinking activity to turn the direction of a stakeholder meeting.

To Jessica for her strong command of the English language taking the time to lend insights and suggestions on how to polish up this paper.

To Carol Boston for taking care of all the logistics and leg work to make sure I got through these 5 years. If it wasn't for your emails and reminders, I might have felt too distant from UMD to finish.

To Wei Bai, for working with me my first year of graduate school to teach me about how to recruit participants and to always make sure to keep up with reading to stay sharp.

To Amber Soley, for always brightening my day and supporting me when I doubt myself. For loaning me a computer when mine broke, and always offering me a bed or drink when I needed it.

To “TeaChat” for introducing me to my future husband and being a constant companion these many years as I have moved. For always sympathizing with me during my lows and the xnice, and the wonderful companionship and city foodie meetups over the years. My pocket friends always make me smile. May we have many more years of friendship and delicious caffeine.

To my committee for taking the time to read this, and to all the wonderful teachers and students I learned from during my years at the University of Maryland. I was honored to spend those years learning with you.

Table of Contents

Table of Contents

Acknowledgements	ii
Table of Contents	v
Chapter 1: Introduction	1
Chapter 2: Related Work	5
2.1 What is my data and where does it go?.....	5
2.2 Data Archival and Recovery	7
2.3 Data Deletion.....	8
2.4 Mobile Privacy and Permissions.....	10
Chapter 3: Methods	14
3.1 Recruitment	14
3.2 Participant demographics	16
Table 3.21 Participant Demographics	16
3.3 Interview structure	18
3.3.1 Introduction	18
3.3.2 Applications on their phone.....	19
3.3.3 Recovery.....	20
3.3.4 Content Deletion	21
3.3.5 Data Access and Control	21
3.3.6 Privacy	22
3.3.7 Participant Debrief	23
3.4 Data Analysis	23
3.5 Limitations	24
Chapter 4: Results	25
4.1 Where data lives.....	26
4.1.1 Context 1: Where data lives	26
Table 4.1.0 Where Participants Believe Their Data Lives	27
4.1.2 Context 2: What data applications are collecting	28
Table 4.1.1.0 Data the application collects.....	28
Table 4.1.1.2 Data I put into the application	29
Storage theme 1: How do I know if it is stored somewhere other than on my phone?	30
Storage theme 2: The phone is a portal apps I installed live on, but apps that come with the phone (native apps) behave differently	31
Storage theme 3: The cloud is well known but poorly understood	34
Not understanding what is going in the cloud or how to control it	34
4.2 What can be recovered	36
Recovery theme 1: I can use my computer to help my old phone and new phone speak to each other.....	38
Recovery theme 2: Recovering data from the physical device would be difficult.....	38

Recovery theme 3: My cellular service provider could restore my data, if they can be convinced	41
Recovery theme 4: I can pop my SIM card into my new phone	42
Recovery theme 5: I don't know what is actually backed up	43
4.3 How to actually delete something	46
Deletion Theme 1: I can never delete it	47
Deletion Theme 2: I can delete my account.....	48
Deletion Theme 3: I can send it to my computer to delete it there	49
Deletion Theme 4: I can destroy the physical device	51
4.4 What is being done with my data and what can I do to have more control over it?	51
How long do companies keep the data they collect?	52
Data Retention Theme 1: They delete frequently because they run out of space just like I do	53
Data Retention Theme 2: Companies keep data for a long time in case a third party requests it	56
Google is omniscient and can see everything you do on your phone or computer	61
How much control do smartphone users perceive they have over their data?.....	63
Table 4.4.1 What I can do to get control of my data.....	63
Control theme 1: I can get control of my data if I learn more about technology	64
Control theme 2: I can control my data by choosing which technologies I use	68
Control theme 3: There isn't anything I can do	70
Chapter 5: Discussion & Implications	70
5.1 Where data lives.....	71
5.2 Recovery	73
5.3 Deletion	75
5.4 Mobile Privacy & Control	76
Chapter 6: Conclusion	79
Appendices.....	81
Interview Protocol	81
Full Participant Table	90
Code Book	95
Example of later codes (from February 2018).....	110
Screener	113
Bibliography.....	118

Chapter 1: Introduction

With mobile app usage accounting for around half of digital media usage time (Comscore 2017), a substantial amount of data is being created or used by applications on smartphones. How well do users understand where that data is going and how does this affect their ability to recover or delete that data? Users' understanding of that affects two critical areas: if they are able to get back information that they find important as well as how well they are able to understand and mitigate the privacy and security issues that might arise from where that data goes. In order to restore the data users need to understand at least one place they have a copy of that data, but in order to fully delete that data they need to understand all of the places that has a copy of that data.

There have been high profile cases, such as the 2014 iCloud hack known as the Fappening. It was particularly shocking to one high profile victim, Jennifer Lawrence, because she thought she had deleted those photos but had missed deleting the copies in the cloud as well. This was a traumatizing experience to the actress, even when she was interviewed by Oprah three years after the event she said "I would much prefer my whole house to have been invaded. That's what's so scary about electronic [things]. I have such fear with my phone and my computer and electronics. It's taking somebody's

intellectual property but also my body. It was violating on a sexual level.” (Winfrey 2017) when asked about how she felt that her photos had been exploited in that manner. But she wouldn’t have had her photos hacked that way if she had deleted all of the copies of those photos, namely the ones that had been automatically backed up to her iCloud. We spoke to participants to find out where they thought their data, such as photos they took, went to after they took them, after they sent them to someone, and after they posted them on social media, to see how aware they were of where their data went and how many copies of it there were. What we found was that many of our participants didn’t feel they knew what was being backed up to their cloud accounts and didn’t feel like they had control of it.

In addition, even though it is a real world issue that happened previously to some participants we spoke with, very little is known about the user’s understanding and beliefs regarding recovering data from a lost or damaged mobile phone.

In this study we investigated five specific questions in order to expand our knowledge around the topic of ‘How does cloud storage / backup / otherwise non-local content affect people’s knowledge of and ability to control and delete their phone/app data?’.

- RQ1: What do mobile phone users know about how and where their phone/app data is stored?

- RQ2: What do mobile phone users know about phone/app data recovery processes?
- RQ3: What do mobile phone users know about data deletion processes on their device?
- RQ4: What do mobile users think companies are doing with their data and what do they think they can do about it?

Our study evaluates our participants' understanding of where their data lives, who participants think is able to access that data and what they do with it, how much data on their phone they would be able to recover if they lose or replace their phone, and how they would delete something they wanted to ensure no one would be able to recover. We interviewed 16 adults who live in the Washington DC area about where they thought their information lived, where they could recover it from and how they could be sure it was deleted for good.

What we found was that participants didn't have a clear idea of where their information was stored, including what was backed up or not. Participants relied on cues such as an application having a login to determine if the information was stored anywhere beyond the physical phone. But even those cues weren't enough; half of the participants we spoke to who had previously lost or damaged their device (three/ six), didn't have nearly as much backed up as they thought they had. Most of those participants reverted back to tangible backup methods, such

as a rolodex or paper planner, after their experience trying to recover information.

Participants had even less understanding of how to ensure something was actually deleted on their mobile device. Many of their methods for deleting underscored the deficit of UI elements to visually understand that something is deleted and then be able to confirm it. Participants mentioned ad-hoc methods including connecting their phone to their computer to utilize the familiar Windows recycling bin and even physically destroying the device.

Through doing this study, we hope to identify gaps in understanding in current systems so that designers and policymakers can take steps to lessen the gap and make it easier for people to control and access their data. Our results have implications for the design of interfaces and tools for both applications and mobile providers, as well as for policy makers. While we do not focus too much on what data is actually being collected, as many other studies focus on that, the results of this study can be used in tandem with those to identify gaps in users perceptions of what is happening compared to where data is actually being stored, how many copies of it exist and what companies are doing with their data.

In this thesis, we examine what mobile phone users know about how and where their phone/app data is stored, phone/app data recovery

processes, data deletion processes on their device, and how this knowledge or lack of knowledge affects their mental models of where data lives and what they can do to take control of their data.

Chapter 2: Related Work

Here we discuss work in four key related areas, data ownership and where data lives, research around participants understanding of recovering lost data, research around participants understanding of data deletion and sentiments and understandings around mobile privacy and permissions.

2.1 What is my data and where does it go?

During our study participants were asked a number of questions around data ownership, and where they thought their data lived. While later sections cover the areas of data ownership with recovery and deletion specifically, this section examines related work around the sentiments of participants about their data as well as where they think it is stored.

Yao, Ri, and Wang's 2017 study found four folk models participants fell into related to their beliefs about online behavioral advertising and where the data collected on them goes: that the web-browser pulls and stores all your behavioral data and creates the profile; tracking is done

by the browser but the individual website chooses which ads to display based on that data; companies/websites form a collaborative network that share data across sites; and lastly that individual websites pass the information onto a third party company who decides what advertisements to show. Since we were talking about apps rather than websites, the first two models didn't come up during the study, but both of the latter two did. The two common models we had were that companies shared data with other companies based on their relationship with that company (n=5), and that there was that third-party company that collected and did things with that data (n=9). Google emerged as one of the most commonly talked about third party data companies in their study as well, based on participant quotes.

Kang et al. (2015)'s study also examined participants' understanding of the infrastructure of their data using semi-structured interviews. The primary difference between their study and ours is that they focused on computers and we focused on mobile devices. Their non-technical user group tended to not have much knowledge beyond the surface entities they interacted with such as Facebook or Google. They also found that security action or inaction was taken by participants based on the perceived reputation and size of the company whose site they were on. Some users were concerned about doing banking online because they saw that as a public internet network (the wireless service) as opposed to a more secure private one. When asked where

they think their data is stored, they brought up Google, Cloud Storage, ISPs, and advertisers. There was a division on whether participants thought information would be stored online indefinitely, with some participants who thought it did get deleted saying that web pages come and go so they thought it was possible to delete data, and other participants citing that once something is on the internet you can never delete it. Actions their participants thought they could take to better protect their data included proactive risk management (ex: use an antivirus, change password regularly), event based risk management (ex: be wise about accepting friend requests or giving out their email address), controlling digital traces (ex: deleting cookies, incognito browser mode), and securing their connection (ex: using encryption).

2.2 Data Archival and Recovery

Odom et al. (2012) conducted semi-structured interviews to explore participants' sentiments towards possessions they had stored in the cloud. In their research they found older participants had well organized archives of family photos that were oftentimes backed up to an external harddrive or other form of physical storage backup. They found that younger participants didn't tend to have physical backups of their data in the same way their older counterparts did.

Their research also touched briefly on data deletion (covered in 2.3) and found that participants oftentimes discard possessions because

they evoked painful memories or no longer represented their values or desires. They found that participants' desire to store something online was tied to one of three core reasons: to share content with others, to make things more accessible and not just located on one device, and to back up data in case of hardware failure. They found an area participants were concerned about was with digital possessions, unlike physical possessions, it was difficult to know what they own and where it is. Another concern with storage online they uncovered was the anxiety that an organization or site might block them from being able to access photos or other data they stored on the site. Lastly they discovered that participants are concerned about being able to permanently dispossess their online possessions. We examine these concerns around where people think data lives and how they think they could delete it in RQ1 and RQ3, and delve deeper into the recovery aspects Odom et al. (2012) touched on in RQ2.

2.3 Data Deletion

During our study, we probed into participants' beliefs around how they would permanently delete something both on their phone, as well as on social media.

Similar to Sleeper et al. (2013), our study probed into motivations people had for deleting their data. Sleeper et al. found people were most likely to regret messages they posted that were critical of others

creates challenges for data ownership and deletion. Also, while encryption is a possible solution, it has many usability challenges associated with it. Our study examines this redundancy/recovery problem from the user's perspective rather than the corporate perspective. Ramokapane et al. (2016) also touched on perceived trustworthiness of cloud providers, which is a theme that appears in their later work, as well as in our study. The 2016 paper proposes tenets for assured deletion: that it is fine-grained and only the desired data is deleted; that it doesn't affect use of the product, that users' productivity and use of the product is not influenced; that all copies of the data are deleted; and that data is made inaccessible from the environment immediately after deletion is complete.

2.4 Mobile Privacy and Permissions

This section explores prior work that has been completed regarding participant's understanding of privacy (or lack thereof) on their mobile devices, as well as some solutions researchers have used to increase understanding of what data is being shared or help users wrestle control of their data.

Similar to our study, Tabbassum, Koskinski, and Lipford (2019) looked at data ownership of information, how companies used that data, and how participants could mitigate those risks. They looked specifically at smarthome devices, whereas we focused on smartphone applications.

Their study showed that while smarthome device users didn't have a clear understanding of how companies were using their data, it didn't greatly affect their behaviors. Additionally, they also found that users' perceptions of risk are largely shaped by their experience with computing in other contexts.

Almuhimedi et al. (2016) explored how users' behavior changed when they received privacy notifications about how applications are using their data. Their notifications alerted the user the data had been shared and then had three actions a user could take: change their privacy settings, dismiss the notification, or show more detail. They found that participants were bothered about apps obtaining so much information about them and would take action to protect their privacy when such action was easily available to them. They also found such notifications worked well when they were "personalized, salient, sticky, and configurable but not annoying," though even with their tool participants still had a limited understanding of what data was being collected by apps. Similar to their study, we looked at participants' awareness and sentiments toward what data was being collected by smartphone applications. Their study focused more on testing behavior with their solution, whereas ours focused deeper on participants' understanding as well as their abilities to delete information that has already been created. Additionally, their study focused only on Android users, while our study focused on both Android and iOS users.

Wijesekera et al.'s (2015) gave 36 participants modified smartphones for a week to gauge how often applications accessed information in real use cases. They found users based their decisions on whether or not an application should be able to access their data on two heuristics: whether they understood why the application needed that data and whether they had concerns around the specific type of data the application was requesting.

Balebako et al. (2013) measured the gap between participants' expectations of what data was being collected on them by two game apps and how much data was really being collected. Similar to MobiPurpose, their study tested a solution to educate users in real time about what data was actually being collected. They found that participants' knowledge of how much data was actually being collected didn't affect their likelihood of recommending the application, but they would let the person they were recommending it to know that data was being collected.

Balebako et al.'s (2013) study found three main classifications of participants understanding of how their data was being collected and used by mobile applications: 1) they had never thought about information leaving their phone, 2) they realized data was being collected but assumed it was only being used internally to improve the

application, or 3) they understood data was being collected for marketing purposes but were still surprised by how much data was actually collected.

TurtleGuard (Tsai et al., 2017) is a technology developed to test out a context-based rule system for mobile application data. They also investigated participants' application usage, but had a more targeted approach by asking which were the two most recent applications to access this device's location. They found that 72.5% of participants incorrectly assumed they were denying access to collecting sensitive data about them. Their technology was driven by the fact that their research had indicated that users want to protect their sensitive information but have a difficult time understanding what data is being accessed and when they are successfully deterring it.

Warshaw, Taft, and Woodruff (2016) found that participants with only a high school education didn't believe companies were capable of making inferences about them with algorithms. They found that their participants mainly believed companies used either demographic data or made straightforward inferences from their behavior (such as tailoring ads based on where you click). Both groups tended to oversimplify and underestimate what companies were capable of inferring from behavioral data collected.

Weinshel et al. (2019) found that applications using tracking were much more common than participants had believed before the start of the study. Similar to our study, their participants already had a general sense that ads were being targeted to them based on browsing behaviors. They also found that participants wanted ways to get more control over their information and privacy. That is a finding that was somewhat in line with our findings, but we found more privacy resignation in our study.

Chapter 3: Methods

We designed an interview study to explore attitudes about data ownership and deletion related to smartphone apps. Below, we discuss recruitment, details on our participants, the interview structure, our analysis approach, and limitations of our study.

3.1 Recruitment

Divided between the spring (7 participants) and fall (9 participants) of 2017, we interviewed 16 participants in the D.C. metro area about their existing beliefs about data ownership and their locus of control over the data created by apps on their smartphone. These participants received \$15 compensation (as well as \$3 parking reimbursement if they came to our lab on campus to complete the study). Interviews averaged 75 minutes and were conducted in a semi-structured format. During the

interview, participants were asked to draw out their thoughts at certain points between interview questions. Topics discussed were: phone and application usage habits, how they thought those applications worked, where they thought their data lived, data recovery, data deletion, and data access/privacy.

Participants were recruited using digital as well as analog methods. Advertisements were placed on NextDoor and Craigslist as well as at local restaurants and stores. Potential participants were invited to fill out a screener to be possibly selected for an interview. The screener questions can be found in the appendix.

Participants were asked for their demographic information as well as how much time a day they spend on their smartphones, how often they used certain applications of interest on their phone, as which type of operating system they ran on their smartphone. Based on this data, we selected interview participants with a focus on balancing age, operating system used, and frequency of phone use. Attempts were made to balance gender as well, but we had a much lower response rate both initially and in scheduling with male participants.

Additionally, two pilot interviews were conducted with family and friends; these were used to refine the moderator guide and to inform

how well the questions were understandable to participants and getting the types of answers we were looking for. These interviews are not included in the final data analysis.

3.2 Participant demographics

Seventeen participants were interviewed for the study, with one faulty recording excluded from the study. Of the 16 participants whose data was collected, transcribed, and coded, there were 11 women and 5 men. Another relevant breakdown was that we surveyed 9 participants who were currently using Android phones and 7 using iPhones, though during the interviews, some participants mentioned switching phone operating systems for various reasons. See Table 3.21 for demographic details on each participant.

Table 3.21 Participant Demographics

PID	Gender	Age	Type of smartphone	How much time do you spend on your smartphone in a day?
P1	Male	22-30	Android Phone	Most of the day
P2	Female	51-60	Apple iPhone	Most of the day
P3	Female	22-30	Apple iPhone	Hours
P4	Female	22-30	Android Phone	Hours

P5	Female	22-30	Apple iPhone	Most of the day
P6	Female	51-60	Android Phone	Most of the day
P7	Female	31-40	Apple iPhone	Hours
P8	Male	60+	Android Phone	Minutes
P9	Female	22-30	Apple iPhone	Most of the day
P10	Female	41-50	Android Phone	Hours
P11	Female	31-40	Android Phone	Hours
P12	Female	41-50	Android Phone	Hours
P13	Male	41-50	Apple iPhone	Most of the day
P14	Female	18-21	Android Phone	Most of the day
P15	Male	41-50	Android Phone	Hours
P16	Male	31-40	Apple iPhone	Most of the day

There were a few factors that went into demographics not being as balanced as would be ideal: It was notably difficult to recruit men, and while many individuals between the ages of 18-21 signed up on the screener, several of the ones we scheduled did not show up to their interview time. Additionally, few potential participants (and only one who scheduled an interview) self-reported “low phone usage.” Android users were also slightly more prevalent in our population than market data suggest they would be. Statistica reports that iOS devices made

up 44.6% of Smartphone market share in October 2017 (citation). Part of this may be due to the low incentive we were able to offer in contrast to the more expensive starting models of iPhone devices.

3.3 Interview structure

In order to delve into participants' beliefs about where their data lives, what is being collected, and who can access it, we utilized a semi-structured interview format. The interview was structured to not prime the participants to think about privacy or data security measures when talking about application use, where the data lives, and recovery. Instead, we asked about those topics only near the end of the interview. Many participants brought up privacy or security independently when talking about the other subjects, and clarifying questions were asked then.

The interview was divided into 8 major sections:

1. Introduction
2. Applications on their phone
3. Recovery
4. Content Deletion
5. Application Deletion
6. Data Access and Control
7. Privacy
8. Conclusion

The full moderator guide can be found in the appendix.

3.3.1 Introduction

During the introduction participants provided background information about what device they have now, how long they have had it, and their most common activities on their phone. While this demographic information was useful, the primary purpose of this section was to build rapport and get participants thinking about their phone usage.

3.3.2 Applications on their phone

For this section participants were asked about their usage of specific applications. The questions were asked in descending order about the applications we speculated would have the most interesting privacy implications, skipping any the participant did not have experience with, until five apps per participant were discussed.

Since during the pilot participants weren't easily able to diagram or express their thoughts about how their technology functioned, we added questions prior to that to get them thinking about how they use the applications and what information they are entering into or receiving from the application.

For each of the five applications, the participant was asked what they use it for, what data they enter into the application, what other information they think that application collects, where the information is stored, and how it gets there. The participants were requested to draw this as they went along, though the ratio of things they talked about versus things they drew varied greatly.

The final question of this section, which was asked to all participants, dealt with where (and in how many locations) a photo they sent to someone else would be. We probed their awareness of whether the picture is located on the phone of the person they sent it too as well.

3.3.3 Recovery

For this portion of the interview, participants were asked to speculate or relay their previous experiences about what information they would be able to recover if their phone stopped working today, if they lost their phone, as well as if their phone was working properly and they got a new phone. This was to get them thinking more in depth about where their data lived, and if it was anywhere other than the device itself. We started by asking participants if their phone stopped working today (but they had the device) what information they would be able to recover. Then discussed what would be different if they lost their phone but it was still working, finally if they had their phone and it was working but wanted to upgrade their phone. The intention behind varying the condition of their phone (functional, damaged or absent) was to give concrete situations which forced participants to consider where the recovered data was coming from. This also helped to pinpoint whether participants had a mismatch between their beliefs on whether the data existed anywhere besides their phone.

Additionally in this section participants were questioned about what data they would be most concerned about losing and what steps they have taken in order to preserve their access to that data.

3.3.4 Content Deletion

Delving deeper into participants' beliefs on whether their data existed elsewhere or not, the next section probes into how they would go about deleting data - both that which existed on their hard drive (like photos) and that which obviously existed elsewhere as well (social networking site). There was also a probe related to motivations for deleting data in the past.

At the end of this section they were referred back to their earlier diagram they made of where all the photos they sent go to, and asked where all they would have to delete it from for it to be gone forever. Then how they would check to see if it was gone. Finally we asked whether the data would exist if they deleted their account/application and rejoined.

3.3.5 Data Access and Control

For this section we started with an organic open-ended question of "Who do you think might be able to access your data?" so as to not prime participants before delving into specific areas. This section asked about the ability of four groups to access their information: people you ask for recovery help, such as technical professionals or

friends; corporate employees; government employees; and hackers.

We started with any entity the participant had mentioned organically earlier in the interview or with the general question at the start of this section and then probed in that order for the remaining parties.

For technical professionals and friends, participants were questioned regarding their beliefs about how difficult it would be to recover information lost during the earlier recovery section of the interview. We asked how difficult they believed it would be for this to be accomplished, both in the sense of skills and tools.

For the corporate employee section, participants were asked what employees who work for the company might be able to access, which employees could access it, and what they might do with it.

The government employee section asked the same question as the corporate employee section with the addition of a question at the end about what information they could obtain from Facebook with a subpoena.

Finally they were asked about what a hacker could access remotely and if they had the device in hand. We also asked whether it was time sensitive as to what hackers would be able to access/ recover.

3.3.6 Privacy

Finally after talking about all of the worst case scenarios, participants were asked if there was any information used by their phone applications that they would be uncomfortable having stored anywhere but the local memory of their phone. Then we asked if they would feel comfortable having a paper copy of this information stored somewhere.

3.3.7 Participant Debrief

At the end of the interview, participants were debriefed and given time to ask any questions about backing up or recovering their data that they were worried about after discussing it during the interview. Here many participants also wanted to know the “right answers” as to what data was being collected and where it was stored.

3.4 Data Analysis

The recordings were transcribed and then analysed by me using an iterative open coding method (Khandkar, 2009), with support from the MaxQDA software package. Codes were created and refined from the data rather than from preset codes. Then, higher level themes were extracted from 27 code families.

Themes were established through discussing the findings as a group and deciding which were worth delving more deeply into. Coding was an iterative process; the first coding took place in MaxQDA, and

subsequent themes and groupings were assembled on word documents and further refined.

Code families were generally formed around questions from the interview, such as “where the data lives...” which then had participants answers tagged by element such as “data base”, “In Google”, “Celltower”, “in the cloud”, “the telecom company”, and “in the app”. The “where data lives group” initially had 26 subcodes, which then like themes were grouped together, and we focused on themes that multiple participants fell into. These codes eventually turned into Recovery theme 3 and Storage theme 1. Another example of codes is the “apps or items that are different” family which had 11 subcategories. This is what eventually took shape as “native apps behave differently” for where data lives and recovery from Storage theme 2. A full list of codes can be found in the appendix.

3.5 Limitations

As in all qualitative research, there were several limitations to this research. While we gathered themes that emerged within our population, we didn’t try to measure how prevalent those themes or beliefs are among the population. Also we are limited to what participants feel comfortable bringing up to us during our brief interview session, and just because they don’t mention things doesn’t mean they don’t think about them. Especially in this case, a lot of them were quite

intimidated sharing their thoughts on technology, since many of them weren't very confident in these beliefs.

Because the data was analyzed by a singler coder, no interrater reliability score can be established for verifying these themes.

Additionally during the screener I forgot to inquire regarding participants' income, limiting the ability to connect the results with previous works that focused on socioeconomic status.

Likely this work is also biased from pulling from a lower income sample (I was only able to offer \$15 for an hour of their time) and is not geographically diverse since participants were drawn from the Washington D.C. metro area.

Chapter 4: Results

In this section, we discuss participants' beliefs about where they think their smartphone data lives, where they think they can recover it from if their phone is lost or being swapped for a newer one, and what they believe they can do to get control of their data or permanently delete it.

A few themes emerged from our conversations. Participants understood logins as a way to let them know information was stored somewhere other than locally on the phone, thought companies needed to delete data pretty regularly to have enough space to

operate, and believed if they wanted to get any control over their data they were going to have to invest time to learn technical skills.

Participants were aware of cloud services such as iCloud and Google Drive backing up their data, but aren't aware and don't feel in control of exactly what is being backed up. Participants needed more visual proof of deletion, and would mistake things such as destroying the device or putting it onto their computer to delete it (using the trash bin) as an item being truly deleted. Below, we expand on these themes in the data.

4.1 Where data lives

This section addresses RQ1, which seeks to ascertain: what do mobile phone users know about how and where their phone/app data is stored? The three main themes we found and discuss below are: how users know if something is stored somewhere beyond the physical memory of their phone; applications that come preinstalled on the phone are perceived to behave different than those downloaded by the participant at the app store; and participants don't feel like they have control or knowledge over what is being backed up to the cloud.

4.1.1 Context 1: Where data lives

During the interview, participants were asked where they thought their data lived, and what apps or other entities it talked to. Table 4.1.0 summarizes their responses.

Table 4.1.0 Where Participants Believe Their Data Lives

Where the data lives	Number of participants who brought this up (N = 16)
On their phone (physical storage)	12
On a company's server/mainframe	11
In a company's database	8
At Google/ On a Google Account	6
The Sim Card	5
"In the app" (app as a location)	5
Other people's phones (awareness of multiple independent files once shared)	5
On their computer	4 (3 because of centralized storage, 1 because of physical device transfer/backup)
In a cell tower	2
The website of the app they are on	2

The two most common places participants talked about their data living were physical storage devices: their phone or the company's computers. Other interesting findings in this section were how the SIM card wasn't talked about much when talking about where their data lives, but nearly a third of participants brought it up later as a place they could recover their data from. In addition, nearly a third of participants (5) mentioned awareness that a photo they shared now lived on the phone of the person they sent it to. Three participants discussed how they could access the data on those apps on another

device they owned, showing awareness of data being stored and actively accessed from a remote location rather than the phone.

4.1.2 Context 2: What data applications are collecting

Before getting too far into where participants think information is stored, let's give some context as to what specific data participants are aware of applications collecting, both with and without action on their part. Table 4.1.1.0 summarizes the most frequently mentioned types of information. The most commonly mentioned items are: location and user activities.

Table 4.1.1.0 Data the application collects

Information the app collects	Number of participants who brought this up (N = 16)
Location	8
User Activities	8
Files from your phone	3
Biometric data from your phone	2
Information from a linked account	2
Contacts	2
Ratings from other users	2

Other interesting pieces of data that were only brought up by single participants are: place of employment, age, phone number, hobbies and things you like, and home address.

During the interview, participants were asked what data they put into the application, to differentiate it from information that is collected without their action. Table 4.1.1.2 summarizes what information participants believed were being collected by applications based on their actions.

Table 4.1.1.2 Data I put into the application

Information I put into the app	Number of participants who brought this up (N = 16)
Financial Information	5
Location	4
Photos	4
Weight (fitness apps)	4
Email	3
Phone Number	3
Purchase History	2

Next we asked participants where they thought their information they put into the app (in table 4.1.1.2) was stored and if they thought that entity shared it with anyone else. They thought that it was. The most common reason participants mentioned for knowing applications are

keeping their information they input is because it was able to predict what they wanted. Either by filling in text, labeling an address as home or sending relevant coupons.

“Because I know if you type it in, just barely, part of an address then it will fill it in.” (P16).

Storage theme 1: How do I know if it is stored somewhere other than on my phone?

Participants were asked where all their data was stored (with follow up questions to get them to think deeper). For participants who mentioned the data being stored in a location other than the physical device, two indicators to participants that data was stored in a location other than their physical device that came up were: if the application had a log in and if they could access the information from another device they owned.

Applications with a login gave users more confidence they would be able to recover their information by logging in on a new phone. Half of the participants specifically cited logins giving them confidence they could recover information (seven/16) and/or log in to the same service on other devices and have all of their account information accessible (three/16). For example, P16 said, “*All of my apps have logins so I assume that all of my information would be stored.*” This finding suggests participants understood their information was centrally stored, since they thought it would be the same experience no matter

what device they logged in from. Though they didn't believe all applications behaved this way. P15 noted, *"I'm very confident that I could recover the information from the applications from a number of them, partly because the application on the phone itself isn't doing a lot, the main thing I have to remember to do is load them. The ones I couldn't would be ones storing more stuff on the phone itself."*

For these applications, the process they envisioned was that they would have access to previous information and configurations within the app after re-downloading it from the app store and logging in with their account information. *"I would think if I downloaded the app, I think whatever I have shared in Betterment.com is secure with them. So if I switched phones, as long as I log into the app, I believe I would have access to it"* (P10).

Storage theme 2: The phone is a portal apps I installed live on, but apps that come with the phone (native apps) behave differently

During the interviews, a theme around applications native to the phone appeared. They didn't think that information could be transferred onto a new device, except through creative work arounds. Even participants who understood centralized storage and generally thought you could get a new device, download the application, and recover all of the information in your account with no issues, spoke differently about applications that came preinstalled on the phone, such as texts, voicemails, and notes. While their explanations for this varied, they

were doubtful of their abilities to recover this information when they got a new phone, even if their old phone was still in their possession and working.

Five of the 16 participants cited their information living “in the app” itself. This was a destination that was familiar but undefined to many of them, and veered between being on the physical device and not as they talked about it and thought more deeply about what the applications do.

“I think in an app there is some security that I guess your information must be saved by whoever runs the app as you enter it” (P2) was a common sentiment among those participants when they were first questioned about where their information was. They stopped, prior to follow ups, at it being stored ‘in the app’.

With further probing, participants began to start to talk about the different access points that could reach this ‘app’ in order to help define what they meant by app as a destination. P6 had one of the most complete mental models of the users who participated in this study. She described access in detail, saying, *“My profile is stored in the app somewhere. The suggested destinations are coming from the app itself. It’s coming actually from my phone, from the app, from the uber app. It’s stored in the uber app. It’s not stored in the phone, because this is the uber app we’re talking about. The uber app is on*

the phone, because I downloaded that app on my phone. And it also is connected.. Which is the weirdest thing about uber. So, I can go on my laptop, I can go on my iPad, and look at it. But if I want to order, order the service, you have to do that from your cell phone.“ To her, the app and websites were both access points to Uber and the information was the same on both, but the permissions differed.

One participant went beyond talking about access points and connected the app location to company servers. *“So you take a picture of the... the check. And then, that goes to that Bank of America servers. And then I assume it came back that it's like you know they're depositing it or whatever they do. And then I assume that the app will have to communicate with, um, or the people working with the other banks or that's where the checks are from”* (P7). But she was the exception who was able to take the definition far enough to tie living on the app to being on a company server.

Some participants identified certain pieces of information, most commonly related to native applications like photos and text, that they believed were stored only locally. *“We could save information onto the phone. I don't know that they are going anywhere. Like you have the hard part, the physical part of the app, and then you have the cyber part. I think it gets saved onto the physical part.”* (P4).

This distinction between native apps and other apps was also salient for data recovery, as we will discuss in Section 4.2. below.

Storage theme 3: The cloud is well known but poorly understood

The cloud came up many times in the conversation, as both a place data lived and a place it could be recovered from. While the cloud (most frequently Google Drive/Photos, iCloud, Amazon, OneDrive, and DropBox) was repeatedly mentioned as a place where data lives and can be recovered from, most users didn't feel confident they understood what the cloud was. In fact five participants explicitly stated unprompted how confused they were by the cloud. *"Yeah, and I can't figure out that cloud situation. Like I don't know what is going on. I don't really know what goes into the cloud and what doesn't."* (P16).

Not understanding what is going in the cloud or how to control it

Not understanding the cloud and what goes into it was a common theme with other participants as well. *"I have no idea, because I still don't understand the cloud. You see, the cloud is supposed to be your backup storage, your back up. From what I understand. It's supposed to free up space on any device. So you have all of this information floating around in the air, right, and it's supposed to be free. So, the storage part of air, I really don't think there's any sections that say this is private, this is shared, this is semi-private, in the cloud, it's just this*

how do you direct it. So when you say “where in the cloud”, I have no idea of where in the cloud. I just know it’s not shared.” (P6). P16 said, “I don’t know enough about it to trust it I guess. I don’t feel that I need to. Because I have everything backed up already so this is not a big deal.” (P16)

A few participants recognized the cloud was tied to a physical storage location as well, but didn’t elaborate in depth about it or use the information to go a step further. *“In their corporate offices, or you know... their cloud I guess you would say.” (P2).*

iPhone users understood the cloud somewhat better than Android users

Awareness that their data was stored in the cloud was much more prevalent among iPhone users (seven of the nine users who mentioned data being restored from the cloud) than Android users.

This is likely due to the awareness of iCloud as a service as well as a better UI around the cloud and cloud setup than Android. *“So I’m just gonna like I log in on the iPhone and then it downloads all this stuff. And I think it asks sometimes... I think it asks like what you want sometimes, but you can sort of customize what you put on there” (P7).* Options available for iPhone users mentioned were both the iCloud as well as Google. Android users primarily mentioned using Google or specific cloud storage applications, but many Android hardware producers offer cloud storage as well.

While neither iPhone or Android users were confident they understood the cloud, nor understood how to control what goes into it, there was a difference in sentiment when talking about it. *“So I don’t really understand the iCloud. I think you have to have it on if you’ve lost your iPhone I think your iCloud has to be on. I could be totally wrong. I don’t know a lot about this stuff.”* (p3). While this iPhone user doesn’t fully understand the cloud, they speak of permissions (having it on) and setup (having it on their phone). In contrast, this Android user also speaks of permissions and accounts, but they don’t feel like they had the chance to alter the settings or even know what the settings were. *“I don’t think the information I entered into my gmail account is out there, for instance in gmail. That, I do not know where. I don’t get this communication. I have no idea what pieces of data would transfer automatically. What I’m agreeing to. It’s a completely gray area.”* (P10). The Android users in general felt like they had less control over what went into their Google accounts as well as with controlling what goes into the cloud and when.

4.2 What can be recovered

After discussing what information participants thought was being stored on apps and where it was being stored, we discussed how participants would recover information from those same applications if they lost their phone or switched phones. This section addresses

RQ2, 'What do mobile phone users know about phone/app data recovery processes?'. We identify 5 key themes: People who had experience losing their phones, rather than just replacing their phone, tended to think that less was saved than those who hadn't lost their phone and attempted to recover information previously. Most of the participants who reported that applications native to the phone had data stored and recovered differently were participants who had previously lost their phone and ran into issues recovering those items.

Most participants we spoke to didn't attempt recovery themselves and instead relied on their service provider, device provider (in the case of iPhone users going to an Apple store), or sometimes a technically savvy close tie to assist them with recovery.

Despite confusion about what it is and how it works (Section 4.1, theme 3), the cloud was the most common place more than half (nine) of participants mentioned recovering data from.. Other places participants mentioned being able to recover their data from were: their old device (six/16), the phone company (six/16), or their SIM card (five/16).

There were five major themes that emerged with regards to people recovering data from their phone: participants mentioned using their computer as a 'translator' between their old and new phones; that they thought recovering data from a physical device would be costly and

difficult, especially if the device was damaged; that their cellular service provide can help them restore data; that most of the data on their phone can be recovered from the SIM card; and that they don't have a keen understanding of what is backed up or not.

Recovery theme 1: I can use my computer to help my old phone and new phone speak to each other

Four participants mentioned using their computer as an intermediary when recovering their data. Those were all iPhone users or users who had used iPhones in the past. *"Well I had to download it (the data) onto my desktop. So I then loaded the information back onto my older phone and then updated whatever apps needed to be updated. The desktop stuff is loaded back onto the phone. The 4s (iPhone data) is downloaded onto the desktop and the desktop goes back to the new phone"* (P2).

Another participant mentioned that they thought they could use a computer to move data if they were switching between being an iPhone user to an Android. *"You might be able to like, I guess you could download them like some kind of Excel or CSV I don't know what they are actually, but I think you could download another format and then try to upload it but I don't know how that would work"* (P7).

Recovery theme 2: Recovering data from the physical device would be difficult

As can be seen in the “where data lives” section in 4.1, three-quarters of participants mentioned the physical hard drive of their phone as a place information is stored. But when it came to restoration, they weren’t certain they would be able to recover information from the physical device, even if they were still in possession of it. Participants believed getting information off a physical device would be difficult and expensive, especially if there was any sort of damage to the device.

While the majority of participants (12) brought up the physical device as a place their data was stored, only half of those (six) mentioned the physical device as a place their data could be recovered from. Only two mentioned it in their primary list of where they could recover their data from, while the rest mentioned it only for certain cases where they weren’t able to recover that information any other way.

So why would the physical phone not be a place information could be recovered from, even though they know it stores information? Many participants were concerned with the effort or cost of using this method of restoration. They weren’t sure how a phone could be broken and still have information recovered from it, or how expensive it would be to hire someone to recover information from a damaged phone. For example, P11 said, *“Depending on how damaged the phone was, but I think they would be able to somehow. But it would cost a lot.”*

Additionally some participants saw recovering from physical storage as a redundant action, because they weren’t sure if there was anything on

the phone that wasn't also backed up in a cloud location such as Google or iCloud. *"If it was in the phone's memory, from the memory card, if it's very likely there, from Google backup."* (P15).

Several participants mentioned recovery from the physical device as a last resort for data that was not accessible any other way. This was most frequently data associated applications that came preinstalled on the device, like notepads (three), contacts (three), calendars (three), voicemails (one), and texts (four). This echoes participant comments, discussed in Section 4.1 (theme 2), that native apps store and manage data differently than apps the user downloads.

Specifically, participants reasoned that these apps behave differently because they come pre-installed with the phone, they existed before smartphones, and they have had issues recovering that information when they have changed phones before. *"My text conversations. When I renew my phone usually they don't come back up. My phone history, so like if I got a phone call from someone important and never saved their number, that is gone"* (P3).

Texts were the example that came up most during conversations with participants. *"I think in an app there is some security that I guess your information must be saved by whoever runs the app as you enter it. But if it's just something loose (not a, you know on your own phone, it is your responsibility to back it up. Like texting would be loose."*

(P2). In contrast, only one participant mentioned their texts would transfer to their new device if they changed phones. Others thought that they would be more difficult to recover than most other information on their phone.

Recovery theme 3: My cellular service provider could restore my data, if they can be convinced

Six participants believed their cell phone provider could help them restore information they lost on their phone. While these participants believed the phone company had all of their lost data, they also thought or experienced that it was difficult to obtain their lost data this way. P4 said, *“I’m thinking everything is stored three or four times in different places. That’s what T-Mobile claims, so I think it’s possible for it, it’s not that it’s really, I don’t think it disappears forever, because again, with law enforcement, they’re able to pull from somewhere if they really need to. But I think for us, common you and I, they aren’t going to go through that effort.”*

P4 was the only participant who actually had attempted to contact the cellular service provider, when her mom lost her phone previously. She was unsuccessful in working with the phone company to restore her mom’s data. Despite this, she still believed the ISP had the data and could obtain it and pass it on in a usable form to a higher authority, such as law enforcement, but would not make the effort to recover

it merely for customers. It is noteworthy that this belief persisted after personal experience to the contrary. The other five participants who believed they could recover data this way had not tried it before, but it would be interesting to see how their belief held up to personal experience trying to recover their data this way.

This belief, although common, is not entirely correct. According to the Department of Justice's 2010 look into retention periods by cellular service providers (Department of Justice 2010), the first assumption by those six participants—that cell phone providers can help restore users' data—is not quite correct: metadata rather than data is most of what is stored. The metadata for calls and text messages is stored at least a year, if not longer depending on the provider. Also, metadata for IP information, which presumably would give some insight into app usage, was stored up to a year by Verizon, and 60 days by Sprint and Nextel. At the time only Verizon and Virgin kept any record of text content, and only Verizon and T-Mobile stored picture content for any length of time. This may have changed, however, as storage has gotten cheaper since the report was published in 2010..

Recovery theme 4: I can pop my SIM card into my new phone

Another common site mentioned for recovery was the SIM card (five); this came up both when discussing recovery as well as steps they would take if their phone was lost or stolen. These participants shared

the belief that their data were transferred to the new phone from their SIM card and that someone else could restore data from their SIM card unless the phone company disabled it.

Participants focused more on what data was stored or could be restored from the SIM card, such as when P6 said: *“Basically, almost everything gets saved to the SIM card. When I say everything, it’s like you’re, because the phone number and everything is attached to the SIM card. So anything dealing with that phone number—your security preferences, your storage, and everything like that—is on the SIM card... even though the majority of your apps are on the SIM card, you have some apps that are on the expansion (SD) card . And photos are on the expansion card.”*

Looking into what data SIM cards actually store (Chang, 2018) participants were partially accurate in their assumptions about data storage. Depending on the carrier, the SIM card may hold more than just the account information, number, and network permissions. SIM cards may contain slightly varying data depending on the carrier and country of origin, but may store phone numbers or recent call or text history.

Recovery theme 5: I don’t know what is actually backed up

Of the six participants who had experience with losing a phone unplanned (either through loss, theft, or device failure), half of them

had issues where they weren't able to recover much of their phone information. But none of them were emotionally affected enough to have considered more extreme measures to recover that information. The most common reason for this information being lost was that they didn't have as much backed up as they thought. All three of these participants were Android users. This could be related back to another finding from this study that iPhone users were generally more acquainted with the cloud as well as Apple's backup and recovery framework.

After experiencing technological failures, it wasn't uncommon for participants to revert to low-tech methods of backup and recovery. In total, six participants made mention of having done this in the past, two to back up data and five to recover their lost data, with one participant engaging in both behaviors. For the most part, this involved writing down the contents of the phone (notes or contacts) to back them up manually. Other examples included getting contact information from contacts they weren't able to get back by asking in real life and using social connections, using a physical planner, or reverting back to keeping all of their contacts in a Rolodex. *"You know, especially now I'm in the process of my summer project of going back to an old-fashioned Rolodex. Because if you're not going to use address books anymore, people ain't going to remember a number. So I'm going back, as a backup, I'm going back to a Rolodex."* (P6). These

participants seem to be reverting to something concrete that they can see and touch and know for sure the information is present, unlike the cloud.

One participant (P1) took it a step further and mentioned a low-tech method to recover the data as well. They planned to actually recover the information by finding the people and asking their contact information, *“I could recover my contact information just like finding family members and stuff. Maybe like a note file on the cloud, but I’d probably write it down. That’s probably the easiest way. People that already are around would be easier, but people who moved away, like farther away would probably be hard. Like people that I don’t see in the area that’s probably the hardest thing.”*

It was surprising how unconcerned many participants were about losing their information. They didn’t go through as many steps contacting companies or looking into technical solutions as other participants we spoke to in this study. Instead they reverted back to something they saw as familiar and simpler to deal with. P11 described how their feelings toward losing phone information evolved from feeling upset to feeling refreshed, saying: *“At first I was pretty upset but then I said ‘everything happens for a reason’ so it’s ok. I’m just going to try different concrete methods of keeping my information and scheduling different things like that, since it’s so important. We can never tell*

what's going to happen with the phone that you're going to lose something important so I just then switched back over to my book schedule and yeah. The contacts were backed up on my, yeah, and the people I talk to all the time, I would need their number. It was ok. People that I didn't always talk to, I mean, I didn't need to keep their number so it was pointless in keeping all that information that I didn't need. I found it was kind of a reviving thing for me, I guess. Refreshing, A Renaissance kind of thing. It was like you refresh your whole perspective on things.” (P11).

Even among participants who hadn't lost their phone previously, they mentioned being more concerned about the expense of getting a new phone than the possible loss of any data on it. *“I think everything else is not actually stored on the phone, so (I'd be upset about losing), probably just the text messages really. And the phone itself, cause you know, it's very expensive.” (P7).* Who it should be noted falls under the category of believing the phone is a portal applications live on, as discussed previously in 4.1 Storage Theme 2.

4.3 How to actually delete something

After discussing what data participants had access to and would be able to recover, we focused on how participants would do the inverse, ensure a piece of data wasn't able to be recovered. This section

addresses RQ3: 'What do mobile phone users know about data deletion processes on their device?'. We found that participants didn't have much confidence in their ability to make sure that something was fully deleted, so nearly a third of our participants didn't think there was any way to delete something once it is on the internet. The other two thirds had strategies they thought would assist them in ensuring deletion including: deleting their account; using a computer to delete it there; and destroying the physical device the data is on.

Deletion Theme 1: I can never delete it

When asked how they would ensure that a piece of data was fully deleted and couldn't be recovered by anyone, five participants believed that once you put something on the internet, there was no possible way to ever fully delete it. *"And then, if it's on the internet, it's never really going away. But that's how you can deal with it."* (p5). The two reasons that emerged for why they didn't think it was possible to ever fully delete it were: redundant copies from backups and other people having copies.

As far as copies not local to the device, there was a sense that the user did not have control over any copies not local to the device. *"I think in a lot of ways that's hard, I mean yes I can delete it locally, but if it's been backed up, then it sort of, I think i can get it to the point where*

it's probably gone, but getting it to a hundred percent is close to impossible.” (p15).

Five participants had awareness that the photos they sent out either by text, email, or social media, also existed on other people's devices; they would need to delete them from those other devices if they wanted it to be gone entirely. Participants talked about the companies that backed up their data in an anthropomorphized way as well that was similar to how they talked about individuals they had shared a file, photo or text with. *“Yeah, definitely. When somebody got your information they can tell you I shredded it... but they never shred it. Once information is stored in the cloud, it is stored forever. Of course. They never delete anything.” (P13).*

Deletion Theme 2: I can delete my account

Two participants believed their data would be fully erased if they deleted the accounts associated with that data. What they differed on was whether they thought their data would be deleted automatically or not. P11 believed special settings were needed to fully delete data when deleting an account, so she asked her husband to help with deletion: *“It was easy for me, I mean my husband just deleted my account. I guess he had to choose some different settings where they delete all the comments and stuff.”* In contrast, P16 thought there were only the two states, deleted or active, and didn't mention any special

settings, but also wasn't quite sure the data would truly be gone after deleting their account. *"Ok... well... if it was on my phone, there is nothing I can do... I guess I would deactivate my iCloud account... and hopefully all of that stuff would be trashed. If I deleted my account then I think everything would be deleted."*

Deletion Theme 3: I can send it to my computer to delete it there

Two older participants mentioned connecting their phone to their computer, because they knew how to fully delete things there. *"Well on the Mac, my desktop, there is a way to show history. And then you can pull up the recent history and pull up stuff that you did that maybe you didn't delete. But then there is a way to delete it permanently. So I think I would send it over to my Mac for the sake of security and delete it that way"* (P2). Similarly, P6 said, *"The basic thing that you are supposed to do is to delete it, go to your deleted files and delete it again, go to your recycle bin and delete that and make sure everything is empty."* These comments suggest they felt reassured by the trash can UI and the act of 'emptying' the trash can with the warning that they wouldn't be able to recover the information. They have projected this habitual way of doing things to believing that it will also take care of deleting it from other locations.

Both participants had the sense that deleting something from a computer was more powerful and secure. In addition to seeking

confirmation from the computer UI for deletion, they may also be confounding other factors with the computer being a more secure way to delete -- either because that would have been enough to fully delete things in the past, before cloud storage, or because they saw confirmation of it being deleted in one location so projected that to it being deleted in all locations. What can be concluded from these interviews is that users are looking for some visual confirmation or record that their data has been deleted, and they can get that from the classic trash bin on the computer more than from locations on their phone.

Two of the four users who backed up their phone using their computer (in section 4.1 Recovery Theme 1) also had the mental model they could delete things from their phone the same way they do on a computer. Whereas only one Android user mentioned that as a way to recover data *“The basic thing that you are supposed to do is to delete it, go to your deleted files and delete it again, go to your recycle bin and delete that and make sure everything is empty.”* (P6). These users were among those who saw their computer as a way to recover their data, either from being backed up there or from their computer acting as an intermediary between phones. So deletion was not the only digital task they felt more comfortable completing using a computer than a mobile device.

Deletion Theme 4: I can destroy the physical device

One participant didn't think data would ever be truly unable to be recovered until they physically destroyed the device it was on. "*And then my actual phone... I mean... I guess I would physically destroy it. That is the only thing I can think of that would be foolproof. I wouldn't trust just deleting it*" (p16). Like the previous section, this user is projecting seeing proof of deletion in one location to proof it has been deleted in all locations. Physically destroying the phone would likely only local, not backed up data, as seen in the recovery section, rather than being 'a foolproof' method to truly delete data.

4.4 What is being done with my data and what can I do to have more control over it?

In this section we explore participants' thoughts about how long companies store data and what they do with it, as well as what participants believe they can do to gain more control over how their data is used. This addresses RQ4: 'What do mobile users think companies are doing with their data and what do they think they can do about it?' The main themes that emerged were that participants either thought companies deleted data often because they were worried about running out of space, or they keep it a long time in case a third party, such as law enforcement, requests it. After exploring participants' thoughts on what is being done with their data, we asked

them what they thought they could do to control it. Themes that emerged were that participants thought they could gain control either by learning more about technology or choosing which technologies to opt in or out of. Though many participants thought that there wasn't anything they could do to control their privacy.

How long do companies keep the data they collect?

We asked participants how long companies store the data they collect and where that information is kept. Many participants cited the common adage at some point during the interview that they weren't sure anything that was ever put on the internet ever really went away; this is expanded on in section 4.3 Deletion, Theme 1. It seemed to not be something they had really considered before beyond the mantra they had heard after various news scandals where data had been recovered.

There were a multitude of places participants believed their information lives, though almost universally they were speculating because they did not have firmly held previous beliefs or knowledge on the matter. Participants' responses suggest they didn't spend much time thinking about where their information went, which contrasted with how fluidly they spoke during the sections about what apps they use and issues they have had with losing their phones before.

When asked an open ended question about how long they thought a company kept their data for, a multitude of answers were given. At least a year and at least ten years were tied as the most common responses, at three participants a piece. Other guesses were a month (2), more than five years (1), more than 30 years (1). None of these guesses were very firmly held by participants, and with the large and inconsistent range, there is strong evidence that people don't have any idea how long data is stored by companies.

But a few main themes emerged from participants' beliefs about data permanence: participants believed companies delete data to make room for new data, and participants believed companies kept data in case customers or the government requested it later. Each of these themes is explored in more detail below.

Data Retention Theme 1: They delete frequently because they run out of space just like I do

By far the most commonly cited place data lived was in that company's server or "mainframe." Eleven participants listed that as a place their phone's data could be found. Of those, seven believed that the server was located at the company headquarters. The majority of participants believed the company stored their data on something closely resembling a home computer with similar UI/file structures as well as space limitations. This was a bit of a contrast to Ramokapane, Rashid

& Such's 2017 finding that their participants didn't think companies ever deleted data.

Only one participant mentioned those servers might be rented, and only two mentioned server farms. The rest of the participants talked about these servers akin to at-home computers, and seemed unaware of the scope of commercial server rooms. Many participants believed companies didn't keep information on hand for too long because they would run out of storage.

While participants were likely correct in assuming their data was stored on company servers, their perception of the scope of these servers was likely incorrect, at least for larger companies. They envisioned a server to be a computer or room at a company headquarters that behaved a lot like their personal computers. *"Like if they have like, this is a computer screen, they could search me up if they wanted to. They have some search button and then... they find me, and they click on me. They open like another new window again, and it's just me and my information stuff. And that's it"* (P14). In this example, the participant even brings up specific UI elements from their home computer that they envision servers to have, like a file browser, a search bar and an individual monitor.

Many participants projected their struggles with storage space onto companies. *"They must delete it on a regular basis, you know,*

because otherwise they really couldn't function I don't think. Like I think it would have to be about the day after you deleted it." (P2). Some participants thought all companies dealt with that, while for others there was a difference between how long large and small companies held data. *"With Facebook I can log in from pretty much anywhere and get the same information. I would just assume like storage space for smaller companies. Like if you don't have enough... I'm assuming that's expensive to have, so if you don't have enough of it, you're not going to pay to keep someone's information for very long if they aren't using your app or your site or whatever"* (P7).

Slightly less common than a "server" or "mainframe" was participants believing that their information lived in a company's database. Eight participants believed this, with some overlap between the two groups. How participants talked about "databases" though was much more nebulous and less concrete than how participants talked about servers.

Whereas servers were talked about more like participants' computers at home, databases were spoken of in a very undefined way. Unlike the "server" the "database" wasn't tied to a location—such as a company headquarters—as strongly. *"It's in their database, like it's a cloud, sort of cloud thing. I don't know. So a database somewhere, I*

guess” (P11). People who believed this way didn’t fall into any specific category of self-reported frequency of smartphone usage or age.

But similar to participants who described the servers to have UI and storage elements common to their home computers, so did participants who framed servers as databases. *“ I guess they keep you in a database of like, like I saw like a movie and stuff and they keep the database in the big things. In folders and stuff like that.”* (P1). Both groups described these servers as having a classic file structure UI like their home computer.

Data Retention Theme 2: Companies keep data for a long time in case a third party requests it

Participants’ reasons for why they believed companies didn’t delete data were primarily related to third party usage rather than internal usage. The two main reasons participants mentioned companies retaining their data were either in case law enforcement requested it for a case, or in case the user wanted to rejoin/restore their account. *“I don’t think it (my data) disappears forever, because again, with law enforcement, they are able to pull from somewhere if they really need to.”* (P4).

“I don’t even know if accounts [that people don’t use] like go inactive anymore... I think nowadays, I mean they last for quite some time. I think they store them for a while.” (P7).

Who do companies share data with?

In general, participants had awareness their information was being shared, but a wide array of beliefs with what companies share information and who they share it with. There also wasn't any emerging opinions or ideas about what companies did with the information they shared or why they shared it beyond creating targeted ads. It was a very surface level and unformed topic that participants hadn't given much thought to prior to this discussion. Twelve participants brought up information sharing between companies unprompted. In contrast only three participants thought companies didn't share information.

Other noteworthy information sharing mentioned included companies sharing information with the government—brought up by three participants—and companies sharing information with other users on the service—brought up by three participants. “I think it is definitely sold to other companies, so it's definitely somewhere else for marketing purposes.” (P3).

By far the most pervasive information sharing cited was with advertisers, with nine participants mentioning it. This is likely the most visible form of information sharing in most people's daily lives, since they see the effects of that data sharing in the form of ads or recommendations from companies. “*Mostly it's annoying with the*

marketing stuff like the ads and that kind of thing. Especially if they're like making money off of like selling that data. I mean, I guess it's kind of expected at some point." (P7).

Five participants commented that they thought apps shared information with partner companies or other companies under the same umbrella company. The most common companies mentioned for this were Google or Uber, with pop-up notifications being mentioned as proof of this. *"They share their information with their partners. Uber partners that I've seen, I know Uber has Uber Eats, and Uber Eats partners are fast food or restaurants. They (use my data to) suggest where I should eat. Uber also has the thing with attractions, i forget what it's called. With the attractions it makes suggestions of places I might want to go visit or that is near the location I'm going. So I'm sure they share with the partner companies, because they are sharing with me."* (P6). As far as Uber goes, there was the thought that they would share the destination data with partner companies, and that is why they would get notifications about things nearby or to rate a location. *"I know Waze and Google Maps share information, so I would assume yes, at least within in house with their own stuff they do. I don't know about Uber. I would think that they might sell like some things or share some things maybe."* (P7). The Google reviews rating system was interpreted by a couple of participants as a partnership between Google and the company they are being asked about.

There were also some mentions that data would be shared/passed on in the event of a company buying or merging with another company, though there was not much discussion around this point. For example, P11 said, *“I was just going to say like a merger or something. I know, I think if that was the case then, they would be able to keep our information unless there was bad blood between them, but I still think it would be available and it would still be there”*

Participants mentioned their perception of that companies do with their data being influenced by news reports, as well as anecdotes of their own personal experience. *“I am kind of put off by some of the corporate shenanigans, It’s kind of like there is one brand in the spotlight and then that gets a lot of media attention... things have to come up to be a big story for that one to get center stage”* (P15).

Four participants brought up information sharing between companies, either among similar or complementary applications. This is in line with what Yao, Ri and Wang (2017) found with their finding participants think that partner companies share user information. *“Probably [Google’s] their sister companies but I’m not sure. Because when you sign up with lots of companies, usually they say they don’t share information, but you never can tell.”* (P11). As with previous sections in 4.4 of how companies share information, most of this section is created off users trying to sense make of their experiences. A theme in the

interviews was that geofenced notifications (notifications that are triggered by being within range of a physical location) may play a part in participants' perceptions that location-based apps are sharing their data with other applications. This is an example of how participants create mental models to make sense of complex technologies they have very little information about or possibly even awareness of. Many technologies are being used by businesses for marketing that interact with mobile phones such as Beacons that can track where you are in a store and send personalized coupons when you are near a product, geofenced push notifications from an application when you are in proximity to a store, and so forth. Participants we spoke with did not seem to be aware of the existence of these technologies, and were trying to find explanations for why they were getting tailored pop ups when they were in certain locations. They were aware of companies sharing or selling data from news articles, so saw that as a likely explanation for how a company knew where they were and targeted them for marketing a place or product.

Two participants mentioned that they thought certain companies wouldn't share information in order to maintain or create a competitive edge with that data. When asked why he thought Google shared information with their partner companies but Lyft didn't, he responded *"Not in my mind. Because I think the ride sharing thing is so split that everyone does not want to share with the other*

companies. With Nest I don't feel like that is competing in the same way. It's not a controversial thing with something that is so public. Like who runs around talking about their thermostat that much. People, especially in big cities, take taxis, Uber, Lyft, Via. So that comes up a lot. So I think those don't want any interaction with anyone else." (P16).

Google is omniscient and can see everything you do on your phone or computer

In addition to the already well documented (Dinev et al 2006) phenomena that many US citizens think the government sees everything they do online, but have privacy resignation around it, there was a less pervasive trend of participants thinking Google is the hub of the internet and much of their data passes through and is seen by Google, no matter who the app or site is owned by. *"I think the vast majority of data used by regular everyday people passes through Google"* (P10).

Almost half of users (seven) mentioned Google possessing the power to be able to see information not related to one of its own products. *"I know everything is connected on Google, but I just don't use it that often, as most people, I guess"* (P11).

Even though there was no mention of Google and Apple being partner companies who share data, some participants thought their iCloud was also stored at Google. *"I think all of the information I have stored in my*

iCloud is also stored in a Google Warehouse, wherever they store Google information at.” (p13). In fact, unlike other companies, participants weren’t even sure Google needed your permission or opt in to collect all of the information about you. For example, P7 said, “I would assume like any of the companies, so like Apple if like, even I didn’t give them my consent, they can access the stuff. And Google. I think they’re, they have the ability to do it, whether they do it without your permission is another thing.”

Nearly half of the participants (seven), Android and iPhone users alike, believed that some or all of the information they have on their phone is also stored at Google. *“I don’t know how I connect to Google. Any picture that I take, Google has it. I don’t know why, I don’t know why they connect my phone with Google. I don’t know, but the thing is, that Google, as soon as I take the picture, they ask, ‘Do you want to share the picture?’.” (p12).*

An interesting trend was the additional level of privacy resignation whenever the participants were talking about Google. Participants felt even less control trying to keep Google from getting their information than they did with most of the apps they were talking about in the study. Above it is noticeable the participants used language such as *“even if I didn’t give them my consent” (P7) and “I don’t know why they connect my phone with Google” (P12).*

How much control do smartphone users perceive they have over their data?

During the interviews, we asked participants what they felt they could do to prevent their data being shared, as well as how they would be able to truly delete data if they wanted to.

None of the methods participants cited to control their data were overly surprising. A quarter of users surveyed felt like nothing they did would make any kind of difference.

Table 4.4.1 gives details on what measures participants brought up that they could do to get control of their data. The counts for each are low because this was an open ended question.

Table 4.4.1 What I can do to get control of my data

What I can do to control my data	Number of participants who brought this up (n = 16)
Read the fine print	5
I can't do anything	4
Learn more technical skills	4
Alter my account settings	3
Not use that app	3
Delete Cookies or Browser History	2
Not use public wi-fi	1

Not store personal things on my phone	1
Keep important documents in a local drive	1
Delete the app	1
Keep an eye out for suspicious actions	1

Control theme 1: I can get control of my data if I learn more about technology

A significant facet of many of the things participants felt they could do to get control of their data, was that many believed it just required time and focus, rather than other resources, yet many of them didn't do them or feel capable of attempting to do them. They weren't sure where to find these settings, or where to begin learning technical skills or felt like it was *"out of their skill range"* (p15). *"I mean, I wouldn't even know how to begin to like encrypt stuff. So I am sure if you are using their app, it would be hard to [get them to stop selling data to advertisers]."* (P7).

The most pervasive method participants (five) thought they could use to have better control of their data was to read the terms of service on apps when installing them. And that once you agreed to the terms, the company would have access to your data. *"I feel that a lot of harvesting of data happens. If you're in a system somewhere, data automatically crosses over if you say "yes" to use a particular*

application.” (P4). Previous studies have been conducted showing how few participants actually read the terms of service before accepting them (Obar & Oeldorf-Hirsch 2018), in fact 74% skipped reading the policies all together and those that did click to read the privacy policy, 81% spent less than a minute reading it, and 96% spent less than 5 minutes reading it, when it was estimated to be a 15-17 minute read. So even though participants think it is something they could do to get control of their data, it is unlikely they will actually engage in such behaviors with policies written as they are today.

But sometimes they felt like they had a choice as to how companies would use their data during setup. *“That’s how, if I have a choice. If there is a prompt: if I want to save a message to Gmail or save to my phone, I always choose just my phone. So the stuff that’s in Gmail, I don’t know how it got there. And every time that I am given that Google automatic thing, I turn it off or opt out”* (P10).

Three participants mentioned being able to control some of companies’ use of their data through modifying account settings. Participants mentioned both being able to control what they store as well as what they share with third parties. *“I know that like there’s an option you can choose if you want them to share it or not. So, I guess if you don’t mark it, they will share it. It’s just like a check.”* (P5). This is in line with Tsai et al.’s (2017) finding that people assumed not agreeing to the

application being able to access their location they were also denying the company to collect sensitive information about them.

“It shows up like here’s the name of the app, and it has some lines where it asks you for some information and then you click a button, and then it takes you to another page. And then it takes you to a map of everything and it shows you where you are, it shows you your current address, because you allow, and in between this, it asks if you would allow - yes or no, to allow us to access your location and other information stored, whatever, and you say yes and then it brings you to where you are.” (P9).

Two participants mentioned being able to mitigate how many places their data goes by clearing their cookies and browsing history. *“I’m pretty sure you can change it (where your data goes). Collect your cookies, delete your browsing history. And then, if it’s on the internet, it’s never really going away. But that’s how you can deal with it.” (P5).*

A quarter of participants thought they would be able to learn technical skills to take better control of their information. It was noteworthy that of those four participants, three of them mentioned being able to use readily available public sources, such as Google or Youtube, to learn these skills. *“I guess I would do a Google search to find out how to permanently and completely delete photos from my phone. That would*

be my method. Was there some secret holding place out there.”

(P10).

It is worth noting there was even one overlapping participant here with the users who felt they couldn't do anything to control their data. Upon thinking more, one participant initially said that even though there was nothing he could do right now to take ownership of his data and fully delete something (see Section 4.4.3 below), he could possibly learn the technological set of skills to do so on YouTube. *“You got to be smart, computer savvy, you gotta be willing to sit in front of a computer screen and learn hacking. You can teach yourself hacking, data breaching,.. Umm... encryptology... and all of that stuff. It's easy. Well it's not easy, but if you set your mind to it you can learn how to do it. Everything you want to, YouTube it, they will teach you how to break into an iPhone on YouTube.”* (P13).

As stated above though, participants felt like this was out of their skill range, and even though the resources were out there for them to learn how to do this, they didn't feel like they themselves had the ability to learn to do these things when they were asked follow up questions. The only one who felt it was in their abilities was P13 above, and he mentioned he lacked the patience to learn those skills.

Control theme 2: I can control my data by choosing which technologies I use

Eleven participants were aware of the fact many free apps were monetizing their data, and three participants believed the only way they could control their data from those apps was to not use them.

“Especially if they’re like making money off of like selling that data. I mean, I guess it’s kind of expected at some point. ... I’m sure it says like somewhere in that thing that you sign when you sign up that they can do that. So if you didn’t want them to do that then you just wouldn’t sign up.” (P7). Though only four made any mention of actually not using an application because of this, even though they were aware of it.

A strategy employed by a participant who was very privacy sensitive due to her job working with children was to use the website version of the service instead of the app, as she believed she would have more control over what information was being collected from there. *“Well, not necessarily an application, although they do have the app version. I met my husband on OKCupid. They have the app version, but I never downloaded it. Partly the reason I did it was I thought they were saving certain pieces of information I didn’t want them to, so I just used the browser.”* (P4).

Two participants made mention of controlling what went on their phone/cloud in the first place as a way to prevent unwanted information from getting to other entities. *“I don’t know what to do. That would be hard. Put less personal things on my phone.”* (P11).

The cloud is a security and privacy risk

Some participants had strong negative feelings about the cloud and saw it as a technology they might be more secure if they opt out of using it. They believed it was causing their privacy to be out of their control, but they hadn’t taken steps to stop using it. *“I suppose if I slowed down, I could disengage that ‘cause I hate the cloud! It’s the idea of the intrusion on my personal information by some nebulous corporation, the government; whoever... So I do not really care for the whole automated. I’m not truly convinced the cloud is truly secure.”* (P10).

Participants didn’t have a clear idea of how the cloud was partitioned, how it knew what data was theirs, or how file permissions worked. *“So you have all this information just floating around, as they say in the air. Right. That is supposed to be free. So the storage part of where, I don’t really think there is sections that say this is private, this is shared, this is semi private in the cloud. It’s just how you direct it.”*

One participant was extremely concerned about the security of cloud storage and did their backups with external hard drives and disabled

cloud backup. *“The biggest thing for me is if I don’t want something to get out there, keep it local only. I think J’s backup might do this, back it up to a PC, or an external hard drive, but I think I would prefer to do that, have that be local rather than cloud based.”* (p15)

Control theme 3: There isn’t anything I can do

A quarter of participants (four) didn’t think there was anything they could do to control their data. None of them expressed much negative sentiment towards this, more an acceptance of fact. *“I mean the best you can do is hope for the people there to be honest, and hope for the best. That’s all.”* (P16). This is in line with earlier findings about privacy resignation (Turow et al 2015).

A theme with this group was the pervasive mention of how it is now in the hands of other people, and they were at the mercy of what that person chose to do with it. While they didn’t think there was anything they could do about it, it also wasn’t an inevitable bad thing that would occur. *“Whatever information you give to someone, they have the human right to share it with anybody that you wouldn’t know they are sharing it with.”* (P13).

Chapter 5: Discussion & Implications

As an exploratory qualitative study, there are a few topics this study brings up that could use more through answering, namely around

recovery. During this study we learned that not much research has been done in the space of helping people recover their data when they lose a device. Many technologists seem to be leaning too heavy into the cloud for recovery, which this study showed that many participants weren't comfortable using for a multitude of reasons. There is a lot of room to improve the UI and services for recovery that could be refined with further research.

Additionally, companies should use a bit of caution adopting new technologies that interact with mobile devices. If they aren't done in a way that the user has a way to understand 'how the technology is behaving so intelligently' they might extrapolate on how a company 'knew that about them' and associate it with a story they saw on the news and make assumptions worse about the company's ethics than what they are really doing. We see this especially in the case of how participants assumed geofence notifications were really companies selling their data. Finding ways to give users context as to how their data is being used without requiring too much cognitive load on their part, would be an area both academics and industry researchers could look into further and refine.

5.1 Where data lives

Most participants we spoke to didn't have a firm grasp of where their information was stored and even less sense of how to fully delete

something. At the end of the interviews, many times participants thanked the interviewer for making them think of things in a different way. This suggests that most of them hadn't taken the time to consider their beliefs about these topics in much depth before. This is in line with what Kang et al. found in their 2015 study with their non technical user group who weren't aware of where things lived and spoke mainly of the surface level entities. This was very much in line with our participant pool as well, it was difficult to get many of them to speak of the ecosystem of where their data was stored beyond the names of the apps and companies they use. In addition, there was no consensus or strong opinion on how long data was stored; this lends credence to the previous assertion of a weak mental model regarding information storage. This suggests more consideration should be given to interfaces that deal with the storage and deletion of data.

Application designers should take note that participants do not have a clear mental model of where data lives. A common belief was that data "lived in the application." Five participants made mention of this. This has implications for application designers when customers are interacting with existing media or creating new media in the application. If a participant creates or alters media in the application, they should be able to find it again using a menu or user interface within the application. Applications that save those to other portions of the phone, such as a camera roll, could confuse users.

5.2 Recovery

One of the main topics we covered in this study was participants' beliefs around their abilities or inability to recover data if they lost, damaged or were replacing their phone. Our findings provided a glimpse into the understudied topic of mobile data recovery and highlighted the need for further research as well as UI refinements on recovery tools.

Based on the differences between participants with and without experience losing their device, it is likely not as much is backed up or recoverable as participants believe from their experiences of switching devices. Further, very few of the people we spoke to took active ownership over recovering their data. Most relied on their cellular provider or the app itself to recover data. Generally, logins were a sign to users that their account was backed up and that they would be able to access the data in the app from a new phone or even another device such as a tablet or computer. Participants were greatly dependent on services like iCloud or Google to back up things for them automatically, though didn't have a clear idea of what was being backed up or not.

This creates an opportunity for cellular providers or device producers to offer recovery services for their customers, since many participants

viewed these companies as a resource they could use to recover information, even though no one in this study had successfully recovered information this way previously. Most participants didn't know where or how to find a specialist to recover their data, so this could be a useful additional service or partnership existing cellular providers or device manufacturers could have.

Another implication of the participants' limited understanding and control regarding cloud backup and storage is that a more guided setup when starting a cloud storage account might be helpful. In general, users didn't have a good sense of what was being backed up or not, tied together with the finding that they haven't backed up as much as they had thought. Having a guided setup as well as some clearer guidance in the settings could be immensely helpful for helping users back up the things they care about as well as feel more in control of what is backed up. Another option could be using predictive notifications in line with the user's recent actions, e.g., 'Since you deleted this file from this location, would you also like to delete it from these other locations that you have it backed up?' This might help to make participants' mental models of cloud storage and recovery more robust and accurate.

Additionally, it might be helpful to prompt at install/setup time, as well as during any major configuration changes or if device storage nears

capacity, for a simple high level setup for what gets backed up. This isn't an activity most users will seek out themselves, so the system needs to be decently intelligent when it prompts users to alter their settings. Of course, it shouldn't be too frequent or long of an activity, otherwise it would affect the overall user experience, and it should be done at a time that feels relevant to the task at hand for the user, so there is a greater chance they will read the alert and give meaningful thought to the settings. Ideas for tying it to a natural workflow could be something similar to Almuhimedi et al.'s (2016) privacy nudger, which sent the user nudges about how applications were using their data. Something similar might be helpful to help users understand what is being backed up by applications and where. Notifications should follow Almuhimedi's guidelines to be "personalized, salient, sticky, and configurable but not annoying."

5.3 Deletion

During our study we found a deficiency in understanding information on the UI for deleting things from the cloud or phone. Participants felt much more confident in deleting things from their computer, even if the information was not originally stored there. Having a way for users to better understand what and where they are deleting or backing things up, as well as a place they can verify it has been deleted, would be helpful to provide users a greater sense of control and ownership over their data. While high profile cases such as the Fappening mentioned

in the introduction happen to celebrities, it is likely other people deal with unfavorable outcomes in their personal lives from information they thought they had deleted resurfacing in damaging ways. This is related to the suggested improvements in mobile UI for deletion mentioned in Sections 5.1 and 5.2 . One that might be particularly useful would be prompts after a user deletes data in one location to ask them if they would also like to delete it in other suggested locations.

The primary motivations for deleting our participants talked about were in line with Ramokapane et al.'s (2017) study: participants most often deleted because they ran out of space. But there were some emotional drivers: we heard incidences of deleting pictures to forget, to distance themselves from a time or place, or to avoid conflict with present relationships. Both our study and Ramokapane et al.'s found that some users felt more comfortable deleting from certain devices (namely computers) than others.

5.4 Mobile Privacy & Control

Near the end of the study we discussed with participants if they thought the app companies were sharing the information with anyone else and what they could do about it. About a third of our participants didn't think there was anything they could do about it, while the remaining two thirds thought if they could learn more about technology or the settings they would be able to have more control of their data.

While participants still believe the government can see more than private companies, they are becoming aware of data sharing and data brokers, as well as the hidden costs of free services. Because of this, it may behoove many companies to be transparent with how they use their users' data, since trust is starting to erode with more public awareness. Since the public is more aware that their data is being used, companies have the opportunity to frame this information themselves before users make assumptions based on folk models of their own experiences, or through news articles.

There are also interesting tangential implications for STEM and security education. Participants had the perception that they could learn an array of technical skills for free on the internet if they spent the time to do so. They also believed these skills would help protect them and help them gain ownership over their data, if they had the patience to learn and become a "technical person." This was something they mentioned they were aware they could do, not something they necessarily wanted to do. Having more science and technology education earlier, perhaps centering on data management and basic data literacy, could help so people don't feel like they have to be a special type of person to learn these skills.

Though participants are aware of some surface-level threats, either through personal experience or the media, of what companies, the

government or other people can do with their data, in line with previous research in the area, most participants weren't overly concerned.

Similar to prior work, many participants didn't think their information was valuable or of interest to other people since they weren't famous or a criminal (Solove 2007). The importance of data ownership and the effects of not being able to delete their data completely is another area that could be addressed through STEM education.

Chapter 6: Conclusion

In order to understand participants' mental models of data storage, control, and deletion, we interviewed 16 people about their perceptions of where data lived, what companies did with it, how they'd recover their information if they lost or were replacing their phone, and how they'd ensure something was deleted for good.

Themes that emerged centered around participants not having an understanding of where their data lived and what they would be able to recover or not. There were some cues that helped users understand their data might be stored in a location other than the physical device, such as having logins and being able to access the same account on multiple devices, but for the most part they didn't know what they would be able to recover until experiencing a lost device. Participants who had experienced a lost device generally weren't able to recover as much as they thought they would be able to. While they were commonly aware of cloud services, such as iCloud or Google Drive, backing up their data, they didn't have a strong grasp of what was being backed up or not. Additionally deletion was a nebulous concept to most of them, though was not seen as impactful to their lives as recovery.

Though mobile interfaces have been around for over two decades, they haven't developed a user interface that participants understand

nearly as well as the desktop recycling bin for confirming that an item has been deleted. This, combined with the increasingly complex ecosystem of cloud and central data storage, has made it so participants don't have a clear idea of where all their data is living nor how to delete it. This, in tandem with the growing understanding that companies are sharing their data for such things as targeted advertising, has made it so participants don't feel like there is much they can do to take ownership of their data unless they invest the time to learn technological skills or spend the time to read the terms of service or adjust their settings.

Appendices

Interview Protocol

We've included all of the interview questions/ follow-ups. But the nature of this protocol is a semi-structured interview, so not all questions will be asked, but a few follow ups not listed may be asked if the participant brings a topic up related to the study, and clarification is necessary. Not all questions will be asked, but are present in case a participant has not provided detailed responses to key questions for our study. Additionally, more questions are provided than we will cover with each participant. Not all participants use all of the applications we are studying, so we will be asking questions about 5 of the applications, rather than the 13 listed.

Hello. My name is [INSERT NAME] and this is [INTRODUCE OTHER PERSON]. Thank you for taking the time to come in and talk to us today. We greatly appreciate you helping us with our research.

Before we begin, I'll give you an idea of how this interview will go and what you can expect from us. We have several open-ended questions for you about how you use your smartphone and will ask you to draw a couple of pictures about how you think certain features work. We expect that this portion of the study will take approximately 45 minutes.

Before we get started, could you please state your name? Thank you.

Describe everything in the consent form

This interview will include an audio recording, as well as photographs of your drawings. By consenting to the study, you are consenting to this interview being audio recorded. All of your answers will be kept anonymous and your answers will not be tied to you in any identifiable way. The recordings will only be listened to by the researchers in our lab working on this project and will be stored on password protected servers. Any material we use from this interview for academic publication, such as a quote, will not have any personal identifying information attached.

If you feel uncomfortable answering any of the questions we ask you during this interview, just let us know and we can skip them.

Do you have any questions at this point?

Give subject the consent form

Please take a look at this consent form. It tells you whom to contact if you want to report any concerns. I'll give you two copies – one is for

you to keep, and the other is for you to sign. [POINT OUT THE PLACES THE SUBJECT NEEDS TO SIGN]

If you have any questions or concerns for us at any point during this interview process, don't hesitate to bring them to our attention.

Introduction

- What type of phone do you have? How long have you had it?
- What is your favorite feature of your phone?
- When did you get your first smartphone?
- What are the 5 activities you use your phone for most often?

Application Driven Questions

Pick five

For the next few questions, we are going to ask you about specific mobile applications you use, or have used in the past.

I am going to give you a sheet of paper so that you can draw a diagram and then add information from each of the apps your phone communicates with.

- Why do you use this app, how does it benefit you?
- What kinds of information do you enter into this application?
 - (Can you give me a specific example?)
- What other information do you think the application collects?
- What information do you think this application automatically collects about you or your phone?
- **Where does this information go? Can you indicate on the diagram where it goes and how it gets there?**
 - **Who does this information go to (Add them to the diagram)?**
 - **What does it mean that it goes to _____?**
 - **How does it get there? Where does it go?**
 - **Does it go anywhere else?**
- Do you think this information is stored anywhere?
 - Where do you think it is stored?
 - Do you think it is stored anywhere else?
- Do you think [entity said before in the who question] shares this information with anyone else?
- (if use more than 1) Do you think there is a difference between how _____ and _____ work?

Type of Application	Used in part 1
Have you ever used a navigation, ride request, or public transportation tracking application?	
Do you have any “smart home” devices that you control from your phone?	
Do you use any cloud storage or applications?	
Do you use anything similar to a fitbit or diet tracking application?	
Do you use any financial applications?	
Do you have any applications that deal with your health, healthcare or car insurance?	
Have you ever used an application to meet people online? Either to network professionally, find people with similar hobbies, or potential dates?	
Do you use any applications to give you discounts or special deals on in store items?	
<p>Do you ever purchase items on your phone?</p> <ul style="list-style-type: none"> • Do you use a specific application for it or the browser on your phone? 	
<p>Do you use a calendar or other type of scheduling application on your phone?</p> <ul style="list-style-type: none"> • Let’s say you receive notice that an appointment is being rescheduled. You use the calendar on your phone to note this change. If you check the calendar on your computer after that, will it display the old or new appointment time? What about your tablet/ other devices? 	
Do you use any note taking, memo or document application on your phone? Such as Evernote or Google Documents?	
<p>Do you play any games on your phone?</p> <ul style="list-style-type: none"> • When you signed up, did you use an existing account such as a facebook, apple or google account, to log into the game? 	

<p><u>Ask Everyone Questions - Photos</u></p> <ul style="list-style-type: none"> • Think of an event you have been to recently with family or close friends. The pictures you took at that event are on your phone. Where else would they be? • Pushback: Did you send them to anybody? Are they in any cloud account or service? • With the ___ marker, can you sketch how your picture gets from your phone to your friends? How does it travel from your phone to theirs? Where is this data stored? • Which application did you use to take them? • Did you use any applications to edit them or post them? 	X
---	---

Recovery

- If something caused your phone to stop working today, what stuff on your phone would you be most concerned about losing?
- Do you think most of your data would be lost for good?
- How much of your data would you be able to recover?
 - (push back: What data would you be able to recover? Where is the data coming from? How would you recover it?)
- What information do you think you would be able to get back?
- How would you get it back?
- How difficult would it be to get it back?
- How do you know you would be able to get it back?
- Is your data being recovered from the physical device or from somewhere else? Where is the recovered data coming from?
- What information are you pretty sure you wouldn't be able to get back?
- What would you be most disappointed about not being able to get back? (Push back: How disappointed would you be about losing this data?)
- If disappointed: Why don't you back this up somewhere? Why haven't you?
- Is there anything good about not being able to recover these items?
- Which items in this category would you be most concerned about losing?

- Are there any steps you think would be helpful in making these items easier to recover?
- How likely would you be to do this? Why?

Now think about the phone applications we discussed earlier. One of the applications we discussed was _____. With this application in mind, if you lost your phone and got a new one...

- What information from _____ do you think you would be able to recover?
 - Does it matter how soon after you lost your phone you attempted to recover this data?
 - Do you have a specific time frame you need to recover this data in?
 - Is there a point in time where your data is more difficult to recover? Is there a point in time where your data becomes impossible to recover?
- What information from _____ do you think you wouldn't be able to recover?
- If you lost your phone, is there anywhere else you'd be able to access the information from that application?
 - Would you be able to remove information or delete your account from there?
 - If you could, would it prevent someone who has your phone from being able to access your data?
- How disappointed would you be if you weren't able to recover the information from this application?
- Now imagine you got a brand-new phone. What information would you be able to recover if you had the old phone, rather than lost it? Are there any differences?

Do you think any of the other applications you use would be any different?

- Pushback: How about _____?
- Why is this one different?
- Why are they the same?

Type of Application	Used in part 1	Asked in part 2
Photos	x	

Diet		
Financial		
IOT		
Healthcare		
Dating		
Cloud Storage		
Travel/ Rideshare		
Shopping/ Coupon		
Scheduling		
Note Taking/ Documents		
Games		
<u>Ask Everyone- Phone Functions</u> Now think about some features from your old phone. <ul style="list-style-type: none"> • Text • Voicemail • Photos • Contacts 	na	

- **Could you draw me a picture of where the data from your old phone, you are transferring to the new one, is stored?**
- **(pushback: Where is the data from your old phone coming from? Is it from the hard drive of the device or somewhere else?)**
- **Also pushbacks to get them to ID the locations/ symbols**
- **Is the new phone the same brand as the old one or new?**
- **If new: What if it's the same brand as your old one (_____ marker)? What would be different?**
- **If same: What if it is a new brand (_____ marker)? What would be different?**

Content Deletion

- Have you ever deleted content or photos from a social networking site? What about from your phone or computer? What reasons did you have for deleting them?

- Do you think anyone would be able to recover these?
- How difficult would it be, how much time would it take?
- Could anyone learn how to do this, or do you need to have a very specialized skillset?
- Would most people be able to obtain the tools needed to do this, or would they be very expensive or hard to get?
- If you wanted to get that photo back, what would you do? Assuming you had already deleted it from your phone.
- **Looking at the drawing you made earlier of where your photos go, could you show me of where all you would have to delete the photo from for it to be gone?**
- **Pushback: to get them to ID the locations/ symbols**
- **How will you know when it's really gone?**
- **Is there any way you can verify this?**
- With your current knowledge and abilities, what would you do if you needed to make sure something was deleted and is not recoverable?
- Pushback: Are there tools you can get, people you can hire or skills that you can learn to ensure that your information is deleted?
- How concerned are you about someone being able to see content or files you have deleted?
 - Is there any specific audience you'd be worried about seeing these items?

Application Deletion

- If you deleted the application, but rejoined later, would you be able to recover your previous information? What if you deleted your account?
 - Would it be any different for _____?
 - Are there any of the applications that you use you think would behave differently?

OTHER PEOPLE

"We've talked a lot about your abilities to find and recover your data [optional: maybe you mentioned some others : technical friends, hackers, professionals, company employees] but let's talk about some other people who might be able to get access or help you access your info

Who do you think might be able to access your data?

TECHNICAL FRIENDS / PROFESSIONALS

- Earlier we talked about things you would not be able to recover if you lost your phone...
- Would you be sad enough to lose these that you would consider hiring someone to recover them?
- Do you think a professional would be able to recover these? If so, how difficult would it be? How long would it take?
- Do you think a professional would be able to recover these? If so, how difficult would it be? How long would it take? How much would it cost? Where would they recover the information from? Would it be from the device itself or somewhere else?
- Could anyone learn how to do this, or do you need to have a very specialized skillset?
- Would most people be able to obtain the tools needed to do this, or would they be very expensive or hard to get?

CORPORATE EMPLOYEES

name companies from specific apps of the five
What can they access / How long does it take / What do you think they might do / what can you do about it...

GOVERNMENT EMPLOYEES

What can they access / How long does it take / What do you think they might do / what can you do about it...

- If the government subpoenaed the company you had the account with, which you had since deleted, would your information be included in that dataset?

HACKERS

If Facebook was hacked, would a hacker be able to see your deleted photos and posts?

- What if that company was hacked? Would your account information, and your content, be visible to the hacker?
 - Is this time sensitive? Is there any point in which the company will no longer have your data?

- How concerned are you about someone being able to recover account information from an application you have deleted?
- How would this be different from if someone found your phone on the bus? Would they be able to access the same information?

Privacy

- Is there any information this application uses that you would feel uncomfortable being stored in a location other than your phone?
 - [You said that this was only on your phone - if it was somewhere else how would you feel about that]
 - Would you be comfortable having a paper copy of this information?
- Would you be more concerned about someone you know having your phone or having a password you reuse for many accounts?
 - If phone: What would you be most concerned about them seeing?
 - What are the three worst things they could do while having possession of your device? (Make sure they are willing to tell you this, say it is OK if they can't tell you exactly, but have them think about it)
 - Are there any passwords you'd be more concerned with them having than the device?
 - If password: Which passwords are you most concerned about them having?
 - What are the three worst things they could do with your accounts they had passwords to?
 - Are there any passwords you'd be less concerned with them having than the device?
 - Would it make a difference if it was someone you didn't know?
 - What would you be most concerned about them seeing or doing?
 - What are the three worst things they could do with your device/ passwords?

Do you have anything else you might like to add?

Do you have any questions for us?

Thank you for answering our questions about your perceptions of how applications use, backup and store your data. Your participation and

time are greatly valued by us. If you have any questions or concerns about the study, you may ask them at this time, or email _____ at a later date. Once again, thank you so much for your time!

Full Participant Table

PID	Gender	Age	OS	Time on smartphone in a day	Phone Calls	Text	Email	Video Chat	Memos/Notes	Taking Photos
P1	M	22-30	Android	Most of the day	A Few Times a Day	All the Time	A Few Times a Day	A Few Times a Day	A Few Times a Day	All the Time
P2	F	51-60	iOS	Most of the day	A Few Times a Day	A Few Times a Day	A Few Times a Day	A Few Times a Month	A Few Times a Day	A Few Times a Day
P3	F	22-30	iOS	Hours	A Few Times a Day	All the Time	All the Time	A Few Times a Month	Never	A Few Times a Month
P4	F	22-30	Android	Hours	A Few Times a Day	All the Time	A Few Times a Day	A Few Times a Week	A Few Times a Week	A Few Times a Week
P5	F	22-30	iOS	Most of the day	A Few Times a Day	All the Time	All the Time	A Few Times a Week	A Few Times a Day	All the Time
P6	F	51-60	Android	Most of the day	All the Time	All the Time	All the Time	A Few Times a Month	A Few Times a Week	A Few Times a Week
P7	F	31-40	iOS	Hours	A Few Times a Week	A Few Times a Day	All the Time	A Few Times a Month	A Few Times a Day	A Few Times a Week
P8	M	60+	Android	Minutes	A Few Times a Week	A Few Times a Day	A Few Times a Day	Never	A Few Times a Month	A Few Times a Month

P9	F	22-30	iOS	Most of the day	All the Time	All the Time	All the Time	A Few Times a Day	A Few Times a Day	A Few Times a Day
P10	F	41-50	Android	Hours	A Few Times a Week	A Few Times a Day	A Few Times a Day	Never	A Few Times a Month	A Few Times a Week
P11	F	31-40	Android	Hours	A Few Times a Week	A Few Times a Day	All the Time	Never	A Few Times a Month	All the Time
P12	F	41-50	Android	Hours	All the Time	All the Time	All the Time	All the Time	All the Time	All the Time
P13	M	41-50	iOS	Most of the day	All the Time	A Few Times a Day	A Few Times a Day	A Few Times a Day	A Few Times a Day	A Few Times a Day
P14	F	18-21	Android	Most of the day	A Few Times a Week	A Few Times a Week	All the Time	A Few Times a Month	A Few Times a Month	A Few Times a Day
P15	M	41-50	Android	Hours	A Few Times a Week	All the Time	All the Time	Never	A Few Times a Week	A Few Times a Week
P16	M	31-40	iOS	Most of the day	All the Time	All the Time	All the Time	All the Time	A Few Times a Day	All the Time

		Online Shopping	Social Media - Posting	Social Media - Reading	Playing Games	Watching Movies/Videos	Reading Books	Listening to Music	Reading/Editing Documents	Banking/Other Financial Activities	Managing Health Information
P1	All the Time	A Few Times a Day	All the Time	All the Time	A Few Times a Day	A Few Times a Day	A Few Times a Day	All the Time	A Few Times a Day	A Few Times a Day	A Few Times a Day
P2	A Few Times a Day	A Few Times	A Few Time	A Few Time	A Few Time	A Few Times a Week	A Few Time	A Few Times a Day	A Few Times a Week	A Few Times a Week	A Few Times a Week

		a Week	s a Week	s a Week	s a Month		s a Month				
P3	A Few Times a Week	Never	A Few Times a Week	A Few Times a Day	Never	Never	Never	All the Time	Never	Never	Never
P4	A Few Times a Day	A Few Times a Month	All the Time	All the Time	A Few Times a Month	A Few Times a Week	A Few Times a Week	A Few Times a Week	A Few Times a Week	A Few Times a Week	A Few Times a Week
P5	All the Time	All the Time	All the Time	All the Time	A Few Times a Day	All the Time	All the Time	All the Time	All the Time	All the Time	All the Time
P6	All the Time	A Few Times a Week	A Few Times a Day	A Few Times a Day	A Few Times a Day	A Few Times a Month	Never	A Few Times a Month	A Few Times a Week	A Few Times a Week	A Few Times a Week
P7	All the Time	All the Time	A Few Times a Week	All the Time	A Few Times a Week	A Few Times a Week	A Few Times a Day	A Few Times a Week	A Few Times a Week	A Few Times a Week	A Few Times a Week
P8	A Few Times a Day	A Few Times a Week	A Few Times a Month	A Few Times a Week	Never	Never	Never	Never	Never	Never	Never
P9	All the Time	A Few Times a Week	A Few Times a Week	All the Time	A Few Times a Day	A Few Times a Day	A Few Times a Week	All the Time	All the Time	A Few Times a Day	All the Time

P10	A Few Times a Week	A Few Times a Month	A Few Times a Month	A Few Times a Week	Never	A Few Times a Week	Never	Never	A Few Times a Month	A Few Times a Month	Never
P11	All the Time	All the Time	Never	A Few Times a Week	Never	All the Time	Never	A Few Times a Month	A Few Times a Month	Never	A Few Times a Month
P12	All the Time	All the Time	All the Time	All the Time		All the Time	All the Time	All the Time		All the Time	All the Time
P13	All the Time	A Few Times a Day	All the Time	All the Time	A Few Times a Month	A Few Times a Week	A Few Times a Week	A Few Times a Week	A Few Times a Week	A Few Times a Day	A Few Times a Week
P14	All the Time	A Few Times a Month	A Few Times a Day	A Few Times a Day	A Few Times a Month	A Few Times a Week	Never	All the Time	A Few Times a Month	A Few Times a Month	Never
P15	A Few Times a Day	A Few Times a Month	A Few Times a Month	A Few Times a Day	Never	Never	Never	Never	A Few Times a Month	A Few Times a Week	Never
P16	All the Time	A Few Times a Week	A Few Times a Day	All the Time	All the Time	All the Time	All the Time	All the Time	A Few Times a Day	A Few Times a Week	A Few Times a Day

PI D	Calendar/Scheduling	Maps/GPS/Transit Information	Job-Related Technical Work	Home Monitoring/Security	Dating/Networking	File/Data Storage
------	---------------------	------------------------------	----------------------------	--------------------------	-------------------	-------------------

			or Job Tracking			
P1	All the Time	A Few Times a Day	A Few Times a Day	A Few Times a Day	All the Time	All the Time
P2	A Few Times a Week	A Few Times a Week	All the Time	Never	A Few Times a Week	A Few Times a Week
P3	A Few Times a Month	A Few Times a Week	Never	Never	A Few Times a Week	Never
P4	A Few Times a Week	A Few Times a Week	Never	Never	A Few Times a Month	A Few Times a Week
P5	All the Time	All the Time	A Few Times a Day	Never	A Few Times a Day	All the Time
P6	All the Time	A Few Times a Day	A Few Times a Week	Never	A Few Times a Week	A Few Times a Day
P7	A Few Times a Day	A Few Times a Day	A Few Times a Week	Never	A Few Times a Month	A Few Times a Week
P8	A Few Times a Day	A Few Times a Day	Never	Never	Never	A Few Times a Month
P9	All the Time	All the Time	All the Time	Never	Never	All the Time
P10	A Few Times a Month	A Few Times a Month	Never	Never	Never	A Few Times a Month
P11	All the Time	All the Time	Never	Never	Never	A Few Times a Month
P12	All the Time	All the Time				
P13	A Few Times a Week	A Few Times a Day	A Few Times a Week	A Few Times a Day	A Few Times a Day	A Few Times a Week

P1 4	A Few Times a Month	A Few Times a Month	A Few Times a Week	Never	Never	A Few Times a Month
P1 5	A Few Times a Week	A Few Times a Week	Never	Never	A Few Times a Week	A Few Times a Week
P1 6	All the Time	All the Time	All the Time	Never	A Few Times a Day	A Few Times a Day

For specific items, the question participants saw was: “For each option, there will be choices for All the Time, A Few Times a Day, A Few Times a Week, A Few Times a Month, Never During those times, what activities do you usually do on your smartphone?” On a table.

Code Book

Code System	#
Code System	879
astonished	1
embarrassed	0
Trust in companies	0
Banks	1
Facebook	1
OKC	1
Amazon	1

Apple	2
Is more secure than android	1
Google	6
Has the ability to see your data permission or not	1
Deletion Beliefs	0
Send to computer to delete	1
Things are easier to access for a short period of time	1
Special Skills Needed	2
Delete from as many places as you can and hope	1
You can't	0
Similar to PC behaviors	2
Type of Phone	0
Android	4
iPhone	5
How does the information get to where it lives	0
I don't understand	1
"The App Cloud"	2
Bluetooth	1

—	Waves	1
—	Wireless	2
—	Experience losing phone	0
—	Close tie	0
—	Self	3
—	Dmg	2
—	Lost	1
—	Replaced	0
—	Destroyed	4
—	Things I can do to control...	0
—	Not use public wifi	1
—	Don't have location on	0
—	Not store personal things on phone	1
—	Delete app	2
—	Hire someone	2
—	Vigilance	1
—	Keep it local and not on the cloud	2
—	Security/ Privacy aware actions	2
—		

—	Learn more tech skills	6
—	Awareness of audience	1
—	What I post	1
—	Account settings	2
—	Not use X	6
—	Read the fine print	9
—	I can't	9
—	Who can access my data	0
—	Hacker	2
—	Anyone who works at the company	2
—	Some people who work at the company	3
—	Only if needed to do their job	1
—	Depends on skill	1
—	Depends on rank	5
—	Family/ friends	1
—	Recovery issues/ non issues	1
—	Some data is harder to get back than others	1
—	I should be able to recover everything/ most everything	1
—		

Depends on usage level of device (buried by newer data)	1
I don't think anyone could recover it	0
I don't think I could recover it	1
Same whether upgrade or lost	0
same	1
Different upgraded or lost	0
I wasn't able to recover...	2
and I don't think anyone can	1
But I don't care enough to hire someone to get it back	3
The app isn't in the app store any longer so I can't recover	2
Anyone can do it	0
Need technical expertise	2
Easy	4
Difficult	1
Free	1
Expensive	1
My data is being restored from...	0
SIM card	7

—	Trash can	1
—	The phone company	8
—	My Computer	3
—	My Old Device	9
—	The Cloud	13
—	Most concerned about losing...	1
—	Emails	1
—	Notes	1
—	Voicemails	1
—	Texts	1
—	Sensitive Data	2
—	Nothing	1
—	Music	0
—	Contacts	7
—	Photos	10
—	How long is it stored by companies	0
—	Some info is kept others aren't	1
—	Depends on mergers/ company stuff	2
—		

Delete Regularly for Space	1
More than 5 years	2
Depends on how big the company is (\$ for storage)	1
I don't think accounts go inactive anymore	1
30 years	1
At least 3 months	1
A month	2
Forever	1
At least 10 years	4
At least 1 Year	3
Information sharing	3
You can opt in	1
Connected Apps	3
Unsure	3
Govt	4
With other users	5
Advertising etc	10
Not shared	6

With other branches of their company	5
With other companies	27
Data the app collects	1
Varies by type of app	2
Access to special info helps app run better on phone	1
Depends on company's goals	3
By the tech skills of the company	2
Things the App collects	1
Device info	2
Phone number	1
Contacts	2
Special Info from Phone	3
Date	1
Biometrics	2
User activities	12
Camera access	2
Profile	1
Age	1

Work place	1
Info from a linked account	2
Files	5
I don't know what, but I know they are	1
Ratings from other users	3
Location	19
Hobbies/ Things you Like	1
Weight	0
Name	1
Home Address	2
Address	2
Financial Information	2
Photo	2
Things I put in...	1
Device info	1
bday	1
gender	1
Barcodes	1

—	PCI	1
—	Policy info	1
—	Phone Number	3
—	Email	7
—	Customer Complaints	1
—	Age	0
—	Work place	0
—	Linked account login	2
—	Hobbies/ Things you Like	2
—	Weight	4
—	Name	8
—	Home Address	3
—	Address	4
—	Name of business heading to	1
—	Financial Information	10
—	Purchase history	2
—	Photo	5
—	Financial transactions	2
—		

Location	6
Doesn't Collect Additional Information about you or your phone	6
Because it doesn't need it	2
It can only collect things i do in the app	9
I know it keeps track, because it knew what I wanted...	11
Automatically	7
Because I put it in	8
Reasons for app use	0
To work	3
Social motivations	0
Convenience	3
Back up	0
I try not to keep info I'd be sad if I lost on my phone	1
Reliance on a friend or family member to back up	1
Email Myself	1
I haven't had personal experience, so hope for the best	1
I don't think I have everything backed up	1
Redundant Backup	2

I feel confident in my back up system	8
I back up onto a physical device	12
iCloud thru Computer	3
I back up with the cloud	1
Because of settings from the company/ app	8
Intentionally	3
I didn't have as much backed up as I thought	6
I don't know what is backed up or not	2
The Cloud	1
Spreads out	1
I don't feel like I need it	2
I don't trust the cloud	2
Confuses me	6
Moving to a new device...	0
Download files from old company to put on new phone	3
Moving to a different type (android/iphone) would be difficult	2
Attitudes about companies/ brands	10
Ideals	2

Concerns from the news	2
Log ins/ App Accounts	0
Let me log in to the service on other devices	3
Give me confidence I can recover information	13
Where the data lives...	0
Cookies/cache	1
The internet	2
database	14
App Website	2
SIM card	2
Other devices they own	3
My data gets encrypted	2
In the app	7
Social Media	2
Department of the company (for purpose other than storage)	1
A computer	1
Some information lives one place some lives another	1
In Google	20

Celltower	8
Space	2
Other people's phones	7
Other people's phones	1
Online	2
In the cloud	27
Is seen by a person (at the company)	4
Used by algorithm	7
The app's server/ mainframe/ etc	43
headquarters	1
The phone maker	1
The telecom company	3
Their computer	5
Phone	17
Deletion Reasons	0
I have no use for X	7
I didn't like X	1
For Social Reasons	2

For Space	6
Physical or Low Tech Methods Employed as Fixes	0
To back up data	2
To recover data	6
Apps or Items that are different	0
Cloud	3
Can't recover info from native apps	1
Banking	1
Cloud Storage	4
IOT	1
Voicemail	2
Notepad/ Memo	4
Calendar	3
Texts	10
Photos	2
Contacts	5
Reliance on companies	2
App companies	2

—	Device Brand Companies	3
—	Phone Companies	7
—	Could have recovered it	2
—	You can never delete it...	3
—	Unless you delete the app	1
—	Unless you delete your account	2
—	From your device	1
—	The cloud...	4
—	The company saves it forever	7
—	Things you save	1
—	Things you do in the app	0
—	Things you post	3
—	The government sees all	13
—	Mentions of privacy laws	2
—	And maybe companies do too?	5
—		

Example of later codes (from February 2018)

Even people with iPhones had some version of their data living at or going through Google
6/14 coded participants

ex p10

“A. This is revealing, even to me, so I’m going to say this (referring to drawing) is what I think it goes to Google, then to Betterment.com. I see Google as the home of electronic transfer. That’s my impression.

Q. So you think all information goes through Google?

A. I think the vast majority of data used by regular everyday people passes through Google and Google is my search engine of choice Because I think they’re the best of it. I don’t know how the people feel. I’m thinking a lot of people agree that Google is the best. I mean I’ve tried other search engines and the results are horrible! But when we use a Google search engine, the results are relevant and fast. I have tried other engines and I’m thinking what in the world are the returns. This is NOT what I requested.”

People talked a lot about data living on servers (10/14) or in the cloud (11/14) other than that.

5/14 mentioned the data living in the app (whatever that means – it seemed to mean diff things to them tho when pressed) - but the is their default answer to the line of questioning.

Common methods people think they can use to control their data ownership (in descending order of popularity)

They can’t

Read the fine print

Not use x (with some controversy on whether deleting x later is 100% effective)

Learn more tech skills

Account settings

A few (5/14) people used low tech solutions to either backup or recover data – need to dig more about related factors (if I had to guess based on talking with them I would have surmised income related but since we didn’t gather that x.x)

P12, 13, 16, 6, 1

How long it is stored by companies was all over the place and need to look for relations with that

4/14 people reported not being able to recover as much as they thought they would be able to... need to explore the why further

Data is being restored from

Most commonly: the cloud

Second most common: my old device

Rest of responses are one offs

2/14 mentioned being protected by privacy laws at all
(with 5/14 gov’t sees all models and 3/14 companies do too)

Apps that come with phone or existed before smartphones considered different.
While photos were mentioned more often as something people are afraid of losing,

people seem to have methods in place to backup their photos but worry about recovering their contacts. Many people due to the experience of trying to recover contacts and failing at some point. To a lesser extent memos, texts and voicemails. Not being able to recover text messages came up a few times, but people didn't seem concerned about that.

People seem split between having control over what information an application collects on them – explore more --- also how affect control of how stored

Backing up physically, on the cloud or both

4/14 mention being confused by the cloud

P3, 6, 10, 16

P10/14 were the most negative towards t saying they didn't trust it or need it

Information sharing

7/14 mentioned at least some companies they used sharing their data with other companies

8/14 mentioned their information being used for advertising, either internal or external to the company

3/14 didn't think their information was shared

3/14 mentioned their data being shared with partner apps

3/14 thought their information was shared with the government

2/14 mentioned data being shared with other users (maybe more need to reread for this one)

At least 6 users mentioned an application collecting their location... that was by far the most common data "collected" by the app rather than inputed

4/14 users mentioned that they knew the application was collecting data on them because it was able to predict what they wanted

P9, 6, 13, 16

5/14 participants mentioned the phone company being able to help recover their data... the phone companies also gave some odd advice such as:

- What I don't recommend is open your Wifi because if you open your Wifi, any person can (? in storage) can have access to your phone and get your information so you have to turn off your Wifi. That's why I never turn on my Wifi.

Q. Even when you are at home?

- Yes. Even in my home, I don't open Wifi.

Q. And how do you find out about that?

- When I went to the Verizon store, I went to get a phone, the guy told me that. When I got my phone Verizon.

Q. He said never use any Wifi networks?

- Yes

A few mentioned app companies or device companies being able to help them, especially in the case of the apple genius bar

If they think it will be there a long time - how much power to change it?

What are the implications of thinking their data lives in the cloud

Screener

7/15/2020

Edit Survey | Qualtrics Survey Software

<input type="checkbox"/> Q16 	Project Title	University of Maryland Smartphone Backup Study Screening Survey	
	Purpose of the Study	This research is being conducted by Michelle L. Mazurek and Lisa Rogers at the University of Maryland, College Park. The purpose of this research project is to assess different aspects of your smartphone usage, particularly pertaining to internet backup. This is a screening questionnaire that will be used to determine if you are eligible to participate in the study.	
	Procedures	The procedure involves completing a short (5 minute) initial survey to tell us a little about yourself and your smartphone usage. Sample survey question: <i>What type of smartphone do you have?</i> <ul style="list-style-type: none"> • Apple iPhone • Android Phone • Microsoft Phone • Blackberry • Other _____ If you are selected to participate in the study, you will be asked to attend an interview session, which is expected to take no more than an hour. You will be asked to bring your smartphone to the interview. The interview will take place at the University of Maryland in College Park, MD, or in a mutually agreeable public location (library, etc.) in the DC metropolitan area.	
	Confidentiality	Any potential loss of confidentiality will be minimized by storing data in a locked office and/or on password-protected computers. Only authorized researchers will be allowed access to this data. If we write a report or article about this research project, your identity will be protected to the maximum extent possible. Your information may be shared with representatives of the University of Maryland, College Park or governmental authorities if you or someone else is in danger or if we are required to do so by law.	
	Right to Withdraw and Questions	Your participation in this research is completely voluntary. You may choose not to take part at all. If you decide to participate in this research, you may stop participating at any time. If you decide not to participate in this study or if you stop participating at any time, you will not be penalized or lose any benefits to which you otherwise qualify. If you are a student at the University of Maryland, your grades or standing with the university will not be positively or negatively affected by your decision to participate in this research project. If you decide to stop taking part in the study, if you have questions, concerns, or complaints, or if you need to report an injury related to the research, please contact the investigators: <table style="width: 100%; border: none;"> <tr> <td style="width: 50%; vertical-align: top;"> Michelle L. Mazurek University of Maryland 5421 A.V. Williams Building College Park, MD 20742 301-405-6463 mmazurek@umd.edu </td> <td style="width: 50%; vertical-align: top;"> Lisa Rogers University of Maryland College Park, MD 20742 573-880-5472 lmrogers@umd.edu </td> </tr> </table>	Michelle L. Mazurek University of Maryland 5421 A.V. Williams Building College Park, MD 20742 301-405-6463 mmazurek@umd.edu
Michelle L. Mazurek University of Maryland 5421 A.V. Williams Building College Park, MD 20742 301-405-6463 mmazurek@umd.edu	Lisa Rogers University of Maryland College Park, MD 20742 573-880-5472 lmrogers@umd.edu		
Participant Rights	If you have questions about your rights as a research participant or wish to report a research-related injury, please contact: <p style="text-align: center;"> University of Maryland College Park Institutional Review Board Office 1204 Marie Mount Hall College Park, Maryland, 20742 E-mail: irb@umd.edu Telephone: 301-405-0678 </p> This research has been reviewed according to the University of Maryland, College Park IRB procedures for research involving human subjects.		

You may print this page for your records:

Q9 I am 18 years old or older.
 Yes
 *

I have read this consent form or had it read to me.
Q10 Yes

I voluntarily agree to participate in this research and I want to continue with the survey
Q11 Yes

Signature
Q12

-----#EditSection.PageBreak-----

#EditSection.AddBlock

▼ Default Question Block #EditSection.BlockOptions ▼

Q1 What type of smartphone do you have?
 Apple iPhone
 Android Phone
 Microsoft Phone
 Blackberry
 Other

Q2 How much time do you spend on your smartphone in a day?
 Minutes
 Hours
 Most of the day

Q3 For each option, there will be choices for All the Time, A Few Times a Day, A Few Times a Week, A Few Times a Month, Never
 During those times, what activities do you usually do on your smartphone?

	Never	A Few Times a Month	A Few Times a Week	A Few Times a Day	All the Time
Phone Calls	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Text Messages	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Email	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Video Chat	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Memos/Notes	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Taking Photos	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Browsing/Searching	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Online Shopping	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Social Media - Posting	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Social Media - Reading	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Playing Games	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Watching Movies/Videos	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Reading Books	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Listening to Music	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Reading/ Editing Documents	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Banking/Other Financial Activities	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Managing Health Information	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Calendar/Scheduling	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Maps/GPS/Transit Information	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Job-Related Technical Work or Job Tracking	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Home Monitoring/Security	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Dating/Networking	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
File/Data Storage	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Other <input type="text"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Q4 What is your gender?

- Male
- Female
- Other

Q5 What is your age?

- 18-21
- 22-30
- 31-40
- 41-50
- 51-60
- Over 60

■ Q6 Your contact information will only be used to invite you to participate and arrange your participation in the study. After the study, your contact information will be destroyed.

What is your email?

■ Q7 What is your phone number?

■ Q8 How can we best get in touch with you?

#EditSection.AddBlock

⚠ #SiteWide.EndofSurvey #EditSection.SurveyTerminationOptionsEllipsis



Bibliography

Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., Cranor, L.F., Agarwal, Y.. [Your Location has been Shared 5,398 Times!: A Field Study on Mobile App Privacy Nudging](#). In Proceedings of CHI 2016.

Balebako, R., Jung, J., Lu, W., Cranor, L., Nguyen, C., "Little Brothers Watching You:" Raising Awareness of Data Leaks on Smartphones. In Proceedings of SOUPS 2013.

Bashir, M.A., Farooq, U., Shahid, M., Zaffar, M.F., Wilson, C. Quantity vs. Quality: Evaluating User Interest Profiles Using Ad Preference Managers. In Proc. NDSS, 2019.

Blase Ur, Pedro G. Leon, Lorrie Faith Cranor, Richard Shay, Yang Wang. Smart, Useful, Scary, Creepy: Perceptions of Behavioral Advertising. In Proceedings of SOUPS 2012.

Chang, E. (2018). What does a SIM card do and why do you need one? Retrieved from: <https://www.thestreet.com/technology/what-does-sim-card-do-14796633>

Comscore (2017). The 2017 US Mobile App Report. Retrieved from: [https://www.comscore.com/layout/set/popup/Request/Presentations/2017/The-2017-US-Mobile-App-Report?logo=0&c=12?utm_campaign=CONFIRMED OPT IN AUTO RESPONDER ALL&utm_medium=email&utm_source=comscore elq OCT2018 OPTIN CONFIRMATION CONTENT ALL AR](https://www.comscore.com/layout/set/popup/Request/Presentations/2017/The-2017-US-Mobile-App-Report?logo=0&c=12?utm_campaign=CONFIRMED_OPT_IN_AUTO_RESPONDER_ALL&utm_medium=email&utm_source=comscore_elq_OCT2018_OPTIN_CONFIRMATION_CONTENT_ALL_AR)

Department of Justice (2010). Retention periods of major cellular service providers. Retrieved from: https://www.wired.com/images_blogs/threatlevel/2011/09/retentionpolicy.pdf

Dinev, T., Bellotto, M., Hart, P.J., Russo, V., & Serra, I. (2006). Internet Users' Privacy Concerns and Beliefs About Government Surveillance: An Exploratory Study of Differences Between Italy and the United States. JGIM, 14, 57-93. Retrieved from: [https://domino.fov.unimb.si/proceedings.nsf/0/055bc8fcd5e7a733c1257014004b80e5/\\$FILE/41Dinev.pdf](https://domino.fov.unimb.si/proceedings.nsf/0/055bc8fcd5e7a733c1257014004b80e5/$FILE/41Dinev.pdf)

Dolin, Claire, Ben Weinshel, Shawn Shan, Chang Min Hahn, Euirim Choi, Michelle L. Mazurek, and Blase Ur. Unpacking perceptions of data-driven inferences underlying online targeting and personalization.

In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, pp. 1-12. 2018.

Englehardt, S., Han, J., & Narayanan, A. (2018). I never signed up for this! Privacy implications of email tracking, Proceedings on Privacy Enhancing Technologies, 2018(1), 109-126. doi: <https://doi.org/10.1515/popets-2018-0006>

Englehardt, S., Reisman, D., Eubank, C., Zimmerman, P., Mayer, J., Narayanan, A., & Felten, E.W. (2015). Cookies That Give You Away: The Surveillance Implications of Web Tracking. WWW.

Gross, R., & Acquisti, A. (2005, November). Information revelation and privacy in online social networks (The Facebook case). Proceedings of ACM Workshop on Privacy in the Electronic Society (pp. 71–80). Alexandria, VA: Association for Computing Machinery.

Jin, Haojian, Minyi Liu, Kevan Dodhia, Yuanchun Li, Gaurav Srivastava, Matthew Fredrikson, Yuvraj Agarwal, and Jason I. Hong. [Why Are They Collecting My Data? Inferring the Purposes of Network Traffic in Mobile Apps](#). *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, no. 4 (2018): 1-27.

Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. (2015). “My Data Just Goes Everywhere:” User mental models of the internet and implications for privacy and security. In Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015) (pp. 39-52).

Khandkar, S. H. (2009). Open coding. University of Calgary, 23, 2009.

M. T. Khan, M. Hyun, C. Kanick, and B. Ur. Forgotten but not gone: identifying the need for longitudinal data management in cloud storage. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* paper 543. ACM 2018

Leister, W., & Tjøstheim, I. (2018). Which Generation Shows the Most Prudent Data Sharing Behaviour?. arXiv preprint arXiv:1810.04964.

NISSENBAUM, H. Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press, 2009.
Redmiles, E., Kross, S., and Mazurek, M. [How I Learned to be Secure: a Census-Representative Survey of Security Advice Sources and Behavior](#). In *Proceedings of ACM CCS*, 2016

Obar, Jonathan A. and Oeldorf-Hirsch, Anne, The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of

Social Networking Services (June 1, 2018). TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy, 2016.. Available at SSRN: <https://ssrn.com/abstract=2757465> or <http://dx.doi.org/10.2139/ssrn.2757465>

O'Dea, S. Subscriber share held by smartphone operating systems in the United States from 2012 to 2019. 2019. Accessed from <https://www.statista.com/statistics/266572/market-share-held-by-smartphone-platforms-in-the-united-states/>

Odom, A. Sellen, R. Harper, and E. Thereska. Lost in translation: Understanding the possession of digital things in the cloud. In CHI '12: Proceedings of the International Conference on Human Factors in Computing Systems, Austin, TX, 2012

Pagliery, J. Naked celeb hack lesson: 'Delete' doesn't mean delete. CNN Business September 2, 2014. Retrieved from: <https://money.cnn.com/2014/09/02/technology/security/cloud-delete/index.html>

I. Papagiannis and P. Pietzuch, "CloudFilter: practical control of sensitive data propagation to the cloud", ACM Workshop on Cloud computing security workshop, CCSW '12, Oct. 19 2012.

Vasilis Pappas , Vasileios P. Kemerlis , Angeliki Zavou , Michalis Polychronakis , Angelos D. Keromytis, CloudFence: Data Flow Tracking as a Cloud Service, Proceedings of the 16th International Symposium on Research in Attacks, Intrusions, and Defenses, October 23-25, 2013, Rodney Bay, St. Lucia

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

K.M. Ramokapane, A. Rashid, and J.M. Such. "I feel stupid I can't delete...": A study of users' cloud deletion practices and coping strategies. In Proc. SOUPS. 2017

Thomas Ristenpart, Eran Tromer, Hovav Shacham, and Stefan Savage. 2009. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In Proceedings of the 16th ACM conference on Computer and communications security (CCS '09). ACM, New York, NY, USA, 199-212. DOI: <https://doi.org/10.1145/1653662.1653687>

- Samat, Sonam, Alessandro Acquisti, and Linda Babcock. Raise the curtains: The effect of awareness about targeting on consumer attitudes and purchase intentions. In Proc. SOUPS, 2017.
- Sleeper, M., Balebako, R., Das, S., McConahy, A., Wiese, J., Faith, L. Cranor. [The Post that Wasn't: Exploring Self-Censorship on Facebook](#). In Proceedings of CSCW 2013.
- M. Sleeper, J. Cranshaw, P.G. Kelley, B. Ur, A. Acquisti, L.G. Cranor, and N. Sadeh. I read my twitter the next morning and was astonished: A conversational perspective on twitter regrets. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 3277-3286. ACM, 2013.
- Soghoian, C. (2011). An end to privacy theater: Exposing and discouraging corporate disclosure of user data to the government. *Minn. JL Sci. & Tech.*, 12, 191.
- Solove, D. J. (2007). I've got nothing to hide and other misunderstandings of privacy. *San Diego L. Rev.*, 44, 745.
- Tabassum, M., Kosinski, T., Lipford, H. ["I don't own the data": End User Perceptions of Smart Home Device Data Practices and Risks](#). In Proc SOUPS, 2019.
- Y. Tang, P. Lee, J. Lui, and R. Perlman. FADE: Secure Overlay Cloud Storage with File Assured Deletion. In Proc. of SecureComm, 2010.
- Tsai, Lynn, Primal Wijesekera, Joel Reardon, Irwin Reyes, Serge Egelman, David Wagner, Nathan Good, and Jung-Wei Chen. 2017. "Turtle Guard: Helping Android Users Apply Contextual Privacy Preferences." In Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017). USENIX Association, Santa Clara, CA.
- Warshaw, J., Taft, N., & Woodruff, A. Intuitions, analytics, and killing ants: Inference literacy of high school-educated adults in the US. In Symposium on Usable Privacy and Security (SOUPS). 2016.
- Weinshel, Ben, Miranda Wei, Mainack Mondal, Euirim Choi, Shawn Shan, Claire Dolin, Michelle L. Mazurek, and Blase Ur. Oh, the Places You've Been! User Reactions to Longitudinal Transparency About Third-Party Web Tracking and Inferencing. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, pp. 149-166. 2019.

Wijesekera, P., Baokar, A., Hosseini, A., Egelman, S., Wagner, D., & Beznosov, K. [Android Permissions Remystified: A Field Study on Contextual Integrity](#). In *USENIX Security Symposium*. 2015.

Winfrey, O. The Jennifer Lawrence Interview, by Oprah Winfrey. The Hollywood Reporter. December 6, 2017. Retrieved from: <https://www.hollywoodreporter.com/features/jennifer-lawrence-interview-by-oprah-winfrey-1064576>

Y. Yao, D. Lo Re, Y. Wang. Folk Models of Online Behavioral Advertising. Proceedings of the ACM Conference on Computer-Supported Cooperative Work and Social Computing (CSCW 2017).

