"Say I'm in public...I don't want my nudes to pop up." User Threat Models for Using Vault Applications

Chris Geeng, *New York University;* Natalie Chen, *Northeastern University;* Kieron Ivy Turk, *University of Cambridge;* Jevan Hutson, *University of Washington School of Law;* Damon McCoy, *New York University*

https://www.usenix.org/conference/soups2024/presentation/geeng

This paper is included in the Proceedings of the Twentieth Symposium on Usable Privacy and Security.

August 12–13, 2024 • Philadelphia, PA, USA

978-1-939133-42-7

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

"Say I'm in public...I don't want my nudes to pop up." User Threat Models for Using Vault Applications

Chris Geeng
New York University

Natalie Chen
Northeastern University

Kieron Ivy Turk
University of Cambridge

Jevan Hutson
University of Washington School of Law

Damon McCoy
New York University

Abstract

Vault apps and hidden albums are tools used to encrypt and hide sensitive photos, videos, and other files. While security researchers have analyzed how technically secure they are, there is little research to understand how and why users use vault apps, and whether these tools meet their needs. To understand user threat models for vault apps, we conducted semi-structured interviews (N = 18) with U.S. adult vault app users. We find our participants store intimate media, non-sexual body images, photos of partying and drinking, identification documents, and other sensitive files. Participants primarily used vault apps to prevent accidental content exposure from shoulder surfing or phone sharing, whether in public or with and around close ties. Vault apps were not used to prevent a technically proficient adversary from accessing their files. We find that vault apps prevent context collapse when sharing devices, similar to how privacy settings prevent context collapse on social media. We conclude with recommendations for research aligning with user threat models, and design recommendations for vault apps.

1 Introduction

Vault or secure media storage applications, henceforth referred to as "vault apps", are applications that provide a private media storage repository on a user's phone or mobile device with an additional level of data protection. These applications are commonly used to secure private or sensitive photos, videos, and other documents, protecting them from other users who may have access to regular media storage applications on a phone [1].

Prior work has tangentially noted the use of vault apps for storing sensitive media such as intimate images [20, 34], financial documents, as well as other apps [53], protecting it from other users who may access the owner's phone. Security research has explored traditional threat models to study how secure vault apps are to adversaries with some degree of technical ability [51, 65]. Other work has threat-modeled vault apps with the user as the adversary, in the scenario that law enforcement is trying to find criminal evidence in vault apps [12, 66]. However, there is a gap in research exploring how existing vault app users make use of the applications and what threats they are actually concerned about.

In this study, we conducted semi-structured interviews (N=18) with adults who use vault apps from a range of backgrounds to identify what motivates people to use these applications, as well as how these applications are used in practice. We asked participants how and why they use vault apps, what features they like or wish the apps had, what threats they are concerned about, and how they found the vault app they use.

Our results include:

1. File assets that are stored on vault apps include intimate media, identification documents, non-sexual body photos, photos of old partners, photos of partying or drinking, medical photos, or conversations.
2. Participants' primary threat models are preventing accidental content exposure from shoulder surfing, when consensually sharing a device, or when a parent is snooping on a phone. They are aware that vault apps may not prevent targeted hacking.
3. While features of usability and security/privacy through authentication can be in tension with one another, participants cite having both features is the appeal of the vault apps they use.
4. Device and photo gallery sharing also produce context collapse given different media has different intended audiences, similar to social media posting [37]; vault apps provide a privacy function similar to granular audience selection in privacy settings, restoring contextual integrity.

By exploring the range of threat models that are considered by these users, we identify ways vault apps protect vulnerable individuals, and we make design recommendations for vault applications to meet user's security, privacy, and usability requirements.

2 Related Works

2.1 Vault Apps and Hidden Folders

Vault apps are digital tools used to protect the privacy of sensitive photos, videos, documents, and sometimes other apps, using encryption, camouflage, and hiding [65]. The average vault app requires successful authentication through a PIN, swipe pattern, or biometrics to access the content stored in the app. Therefore, even if an adversary had access to a person's unlocked phone, they would be promoted to authenticate again to access the files. They sometimes provide decoy functionality by having an app icon that appears as a calculator app on the phone's home screen. There are also social media apps like Snapchat or file apps like iOS Photos that have a secondary feature to password-protect specific files, such as iOS Photos Hidden Album, Google Photos Locked Folder, Snapchat My Eyes Only Album, and iOS Notes locking. When we refer to vault apps, we are also referring to these secondary hidden albums.

2.1.1 Security Analyses of Vault Apps

Security researchers have previously used forensic or security analysis to identify vault apps and extract hidden files from them [22]. Dorai et al. created a tool to automatically extract data from iOS vault apps, to be used by law enforcement [12]; Duncan & Karabiyik, as well as Zhang et al., were able to extract vault app data on Android devices as well [14,66]. Xie et al. found that for some Android vault apps, they could find the login password or unencrypted information stored in the Android file system [65]. To see if adversaries could extract data without forensic analysis, using the threat assumptions of either unjust search and seizure of civilians by authorities or intimate-partner violence, Ruffin et al. found that "adversaries can infer the existence of most of the popular vault apps and retrieve the stored files with the rudimentary-level knowledge of the Android system" [51]. One limitation of these security analyses was not having empirical evidence on how users actually use vault apps to justify their threat model. Following prior usable security work investigating how different groups threat model their own lives [18,19,32,57,58], our work seeks to fill this gap.

2.1.2 Vault App Usage

There has been little research on how and why people use vault apps and hidden albums and whether these tools meet their security and privacy needs. Sambasivan & Checkley et al. studied the phone privacy practices of women in South Asia, where the cultural expectation is that they should share their phones with family members so their digital activities may be scrutinized [53]. They found women often employ app locks (similar to vault apps[1]) to protect social media apps, photos and videos, as well as menstrual period trackers, banking apps, and adult content. Some challenges they had included PINs being discoverable and the presence of an app lock being incriminating. Geeng et al., focusing on adults in the U.S., found that users store intimate photos in vault apps [20].

2.2 Securing Intimate Media

Sharing intimate media, or sexting, has become a common practice: Herbenick et al. found that 27% of adult women and 24% of adult men in the United States sent nude or semi-nude photos of themselves to someone in 2017 [25]. While early literature on intimate messages treated the phenomena as a high-risk, deviant behavior, current research underscores that sexting can be an important part of adult social life that is just as normal as not sexting [15, 30], and can have a positive role in relationship satisfaction [7, 13, 59]. Supporting safety around intimate messages requires acknowledging both "vulnerability and sexual agency" [15], as well as removing patriarchal norms from sexual expression [54], given in general women, sexual minorities, and ethnic minorities bear a disproportionate burden of harms around sexual expression, such as surveillance, harassment, and abuse [8,9,52,55,56]. And legal scholar Danielle Citron notes that privacy around individuals' intimate lives is a privacy value of the highest order because of its importance to sexual agency, intimacy and equality: "[w]e are free only insofar as we can manage the boundaries around our bodies and intimate activities" [9].

2.2.1 Vault Apps and Intimate Messages

Snapchat is a common app used for sharing intimate messages among young adults [61]. It features a "My Eyes Only" password-protected photo album. Other password-protected storage people have used to store intimate media include Vault and encrypted folders on one's computer [20]. Password protected storage is an often-recommended defense for protecting intimate images [3, 38]. Maas et al. found that, while there has been an incident where high school football players had non-consensually stored nudes of female classmates in vault apps which facilitated posting photos online, non-consensually posting nude images/videos online is not a behavior significantly associated with vault app usage [35].

2.3 Social Media and Device Privacy

Beyond just communication around intimate media, people generally communicate differently based on context and audience [23], and people have different privacy norms in dif-

[1] App locks primarily allow phone users to restrict access to any application on their phone by using a password/swipe pattern/biometrics; some vault apps may also have this functionality, but they primarily lock photos and files.

ferent contexts [46]. Marwick & Boyd coined the term "context collapse" to refer to "when social technologies cause a collision of information norms [that] people experience as privacy violations." [37]. This commonly occurs on social media, where a post may be seen by a variety of audiences, not just the poster's intended audience. This can also occur with device sharing. People who trust each other, e.g., family, friends, and romantic partners, often share accounts and devices [39,47,48], though device sharing may also happen as obligation [48].

Jacobs et al. found that when a partner in a collocated couples share their device, they may accidentally share private content with their partner. And despite device sharing being common, Wu et al. found that few tools allow intimate partners to maintain both their ideal sharing and security behaviors with devices [64]. Device and credential sharing, compared to healthy relationships, can be adversarial in relationships with intimate partner violence [16,17,40]. While device sharing can happen with consent, snooping on smartphones, or non-consensual device access, also occurs: Marques et al. found that 20% of U.S. adults had engaged in phone snooping in a year [36].

Researchers have also explored the tension between parents desiring technology check-ins or surveillance and children wanting privacy from their parents [4,10,11,21,33,41,45,63]. Hawk et al. found that increased parental privacy invasion led to adolescents telling their parents less about their lives [24]. Cranor et al. found that, while parents believe they should be able to monitor all of their teen's possessions, teens felt their phones should be exempt. In terms of vault apps, various parenting articles caution parents to check their children's phones for vault apps hidden as calculators to find content children are hiding from their parents [2]. To better understand what vault app users, from their perspective, store on these apps, and what their security and privacy concerns are, we conducted our research study which we describe below.

3 Methodology

From July to August 2023, we conducted 18 semi-structured interviews with adults living in the U.S. who used any form of vault app or hidden album folder.

3.1 Recruitment and Participants

To recruit participants, one author posted flyers around a major U.S. city. We also shared flyers with our personal networks, social media sites such as Reddit and Lex, as well as university undergraduate email listservs. Recruitment materials linked to a Qualtrics screening survey, which screened for participants 18 or over and who use vault apps. Given the potentially sensitive nature of discussing vault app storage, other demographic questions besides age were voluntary. Based on responses, we selected participants of varying age, race, income, gender,

ID	Gender	Sexual Orientation	Age in Years	Race
1	man	straight	18-24	Latino
2	non-binary / third gender	gay	25-34	Latino
3	woman	bisexual	18-24	Asian
4	man	gay	25-34	White
5	man	gay	25-34	Asian
6	man	gay	25-34	Black
7	non-binary / third gender	N/A	18-24	Asian
8	woman, non-binary / third gender	queer	25-34	White
9	woman	bisexual	18-24	White
10	man	straight	18-24	White
11	man	N/A	18-24	Asian
12	woman	straight	18-24	Black
13	woman	N/A	18-24	Asian
14	man	straight	25-34	Asian
15	man	straight	18-24	Asian
16	man	straight	25-34	Asian
17	man	straight	18-24	Asian
18	non-binary / third gender	queer	25-34	White

Table 1: Demographic information of interview participants ($N = 18$). N/A means the participant did not specify an answer.

Education	#
bachelor's degree	7
graduate or professional degree	7
some college, but no degree	4

Relationship Status	#
single	7
dating	5
partnered	2
N/A	3

Household Income	#
$150,000 or more	1
100,000–149,999	3
75,000–99,000	1
50,000–74,999	2
25,000–49,999	3
less than $25,000	6
N/A	2

Relationship Style	#
monagamous	16
open and monogamous	1
N/A	1

Table 2: Aggregate demographic information of participants. N/A means the participant did not specify an answer.

and level of education. (Despite our attempts at recruitment, we were not able to recruit any participants over 34.) During the interview debrief, we further asked participants about their sexual orientation, relationship status, and relationship style. Participant demographic information can be found in Table 1, with some demographics presented in aggregate for participant privacy in Table 2.

3.2 Interview Protocol

Two of the authors conducted semi-structured interviews. Some interviews were conducted with both authors present and some interviews were conducted by only one of the authors. We conducted interviews remotely via Zoom for an average of 34 minutes. Participants provided written consent prior to the interviews; the interviewer also provided an overview of the consent form again at the beginning of the call to answer any questions. Zoom calls were recorded with participant consent; we retained audio and deleted video. Participants were compensated with a $30 dollar gift card.

The interview protocol covered what vault apps or hidden album apps the participant uses, how they found out about them, what they store, how they handled the files prior to vault app storage, why do they use them, which features they find useful, what features they wish it had, and any other security or privacy concerns that prompted app usage. If participants used the vault apps to store intimate media, we further asked questions around establishing consent as well as storage duration. The full protocol can be found in Appendix 7.

3.3 Data Analysis

We followed an open coding process. First, we used MacWhisper (an AI-based transcription tool; no third-party person was involved) to transcribe the interview audio. Documents were locally transcribed on the first author's computer. The second author flagged any lines that were unclear and manually corrected them. We anonymized the transcripts.

During the open coding process, two authors double-coded 8 of the same interviews. After double-coding every two interviews, the authors met to discuss code development and resolve disagreements. After the codebook became stable, the authors recoded the first 8 interviews and double-coded the rest, meeting together after every few interviews to discuss and resolve disagreements. Inter-rater reliability (IRR) was not calculated because we double-coded all interviews, and because our research goal is the richness and nuance of different experiences, not counts of how often a code occurred [43].

3.4 Positionality

Three authors identify as queer, and two authors identify as straight. Our paper presents findings, particularly around sexting culture amongst queer people and gay men. While social science has a history of positioning gay sexual practices as deviant [44], our position on consensual intimate messaging is one of normativity, particularly in gay communities where it can mediate internalized homophobia and loneliness [60].

3.5 Ethical Considerations

Given the potential sensitivity of discussing intimate images as well as other topics, participants were reminded they could skip any question they felt uncomfortable answering or withdraw from the study without penalty. Participants could end the interview at any time and still be compensated. After the interview, participants could request to review their recording and have all or any portion destroyed. No participants requested this. Participant demographic information is presented partially in aggregate to further anonymize participants. This study was approved by [redacted for review] IRB.

4 Results

In this section, we report on participant threat models for using those apps, i.e., what threats they use vault apps for as a defense and what assets they are protecting through vault app storage. We also report on the tool affordances that are important to them or wish to have, how they picked the tool, and what their storage behaviors were before having the tool. Quotes have been lightly edited to remove filler words for clarity.

The vault apps participants brought up included:

1. Hidden albums within photo gallery apps: iPhone Photos, Google Photos. The hidden albums are accessed within each app by traversing the app's albums/library. These hide photos and videos.
2. Snapchat's My Eyes Only album. Photos and videos in this album are stored on Snapchat's servers. If the user forgets the password, the photos are lost forever; there is no recovery process.
3. Samsung's recommended app Secure Folder. It can lock photos and videos, files, and other apps.
4. Third-party vault apps like Secret Photo Album, Photo Vault, Vault, and App Lock.
5. And locked files within existing note apps: Adobe Acrobat, iOS Notes, OneNote.

All of these tools require authentication to access hidden files stored through the app. Their specific affordances are described in more detail in Appendix 7.

4.1 Threats Towards Using Vault Apps

Users installed a vault app to protect their data from shoulder surfing, accidental exposure, and parental device snooping.

Threats Covered by Vault Apps	Threats Not Covered
Shoulder surfing	File-system access
Accidental exposure when sharing device	App data collection
Parental device snooping	
Adversary: Accidental	**Adversary: Targeted**
Friends	Someone with technical expertise specifically after the participant
Family	
People in a public space	
Co-workers	Vault app corporation
Oneself	

Asset: Sensitive Files
Sexual imagery of others or oneself
Non-sexual body photos
Photos of partying or drinking
Photos of old partners
Sensitive documents, e.g., IDs and password lists
Medical photos or conversations

Table 3: Threats that participants feel vault apps can defend against and cannot defend against.

These threats can be considered with respect to a set of relevant *threat actors*, who have different capabilities that should be considered when designing privacy and security features for the vault apps. A summary of the threats relevant to vault apps are summarised in Table 3. Threats that participants reported as ones not covered by vault apps are discussed in Section 4.3.

4.1.1 Proximity-Based Access

The first threat encompasses people who are in the same vicinity as the user. These may include friends, family, co-workers, or strangers in the same space. These users do not have any control over the device itself; however, they are likely to be able to see the content of the users' screen through "shoulder surfing" or because the user is sharing the screen. To prevent this, vault apps move media from applications which would regularly include them (e.g. camera roll, file viewers) into other storage.

> When I'm in public, I'd rather not have some of those [intimate] images that are far back to be shown as I'm scrolling, 'cause I take a lot of public transit. I'm usually around a lot of people. So I wanna make sure that those images aren't accidentally shown when I'm in some of those more social situations. *—P2*

> If [I] open up Snapchat, say I'm in public. I'm recording a drag show or something. I don't want my nudes to pop up. So I just don't want people to see [these photos] when I'm scrolling through. *—P18*

4.1.2 Physical Access to Device

The second threat includes people who have physical access to the user's device. Some of our participants would share their phone with a friend or family member to share some memories, who may accidentally scroll past the intended shared photos.

> Sometimes I share my camera roll with other people. So I wanna make sure that some of those images aren't just shown. *—P2*

P3 and P17 were also concerned about parents accidentally seeing content while they intentionally snooped through one's phone. And some participants had photo memories of a time they would not want to be reminded of unless they were in a specific mood.

Vault apps provide a secondary locking mechanism, which is often (but not always) distinct from the devices' authentication mechanism. This protects against this threat by adding an additional layer of authentication, that users with physical access cannot bypass by accessing the unlocked device alone. Vault apps also separate sensitive content from general folder content, making it more difficult to accidentally send the wrong photo. P9 stated, "I don't want it in my Apple photos because I could accidentally send this to someone."

4.2 Assets Protected by Vault Apps

In general, participants stored types of sensitive files that, when shown to an unintended audience, could bring up feelings of embarrassment or shame, loss of dignity, questions or lectures from family, or old memories in oneself. For example, P17 did not want certain friends, who he describes as "something common here and around in India...they only talk with boys, they only interact with boys, and they have some sort of exclusion from women," to see photos of him with another girl because:

> When they find out those pictures, they might make a fuss around the classroom....They would shout around, shout the girl's name when I'm around, shout my name with the girls around....It's just a friendship thing, but they take it as a crush or whatever....So yeah, [I use a vault app] to avoid that annoying thing and not to embarrass that person as well.'

We discuss specific stored content below.

4.2.1 Asset: Sexual imagery of others or oneself

Many participants mentioned using vault apps or hidden folders to store not-safe-for-work (NSFW) sexual photos of themselves or others. The common threat they were concerned about was accidentally revealing those photos in a public place, in a professional setting, to family or friends, or anyone other than the participant themselves and the person they intend to share it with. These could be nude or semi-nude photos, as well as fetish-related photos. People mentioned using Snapchat's My Eyes Only and Hidden Photos Album in particular.

P6 and P8 in particular mentioned potential harms to others accidentally exposed to one's intimate imagery could cause. P6, a gay man, talked about not wanting his women friends to see his photos:

> But the idea of a woman seeing unsolicited dick pics [is] then just sort of me perpetuating an already existing system or [...] harassment.

And P8, a queer non-binary person said,

> In the work context it would be really bad and I think in any context it could be really alienating for someone, and kind of sexual harassment.

Some participants, while they used vault apps to protect against accidental exposure, were not as concerned if it did occur. P4, a gay man, stated, "I'm also just like very sexually liberated person. So I don't really like, think of too many bad outcomes." He said that while he has the concern of a targeted adversary getting a hold of his images, or his boss accidentally seeing his images, he finds these scenarios quite unlikely.

Storage Practices. Some participants discussed storing a partner's intimate photos prior to saving, while others who sext in casual relationships said that being sent an intimate photo implies consent to store it.

> People, if they don't want something to be saved, would send it over like Snapchat or like the Instagram disappearing photo messages. *—P4, gay man*

P9, a bisexual woman, talked about desiring to discuss storage boundaries:

> I'm bisexual and I think with women, it's a little bit more of an open conversation of what is expected, 'cause you're both a little bit more aware and a little more scared. I think with men, when I talk with men, they don't really care as much what happens with their photos as I do with me. So it is more like on my end, like, hey, don't screenshot, don't do this, don't do that. And obviously I'm like, if you would like, if you want me to do the same, I will, but most of the time they don't care in the sense that women tend to care about their photos.

Some participants did not think about the storage duration of intimate images, while P1, P4, and P9 said they deleted intimate images of partners at the end of the relationship.

4.2.2 Asset: Non-sexual body photos

Several participants mentioned storing non-sexual photos of their bodies for various reasons. This included gym body progress photos, gender-transitioning photos, and swimsuit photos. P3, a 18-24 year old woman, talked about putting body photos from when she had an eating disorder into a vault app so she does not accidentally see it:

> That's another reason that I don't really look back on My Eyes Only 'cause, at least where I'm at right now, I'm trying not to be in that mindset. But at the same time, I don't know that I would necessarily delete it because sometimes it is helpful to look back and [see], this is what I was thinking.

P7 took photos of themselves to track their bodily changes as they started hormone replacement therapy. They keep photos in the iOS Hidden Album to prevent an unintended audience from seeing it, which would cause:

> Embarrassment or loss of dignity or decency, I think particularly because it's my body going through transition, it's something personal to me. Or it's not a version of myself that I present to people now.

They also do not want to accidentally see those photos because as they mentioned, "I don't really want to look at my body", so using a vault app requires conscious access to see the photos.

P8 also put SFW selfies in their Hidden Album:

> I think I felt like I had too many and they didn't need to be in my regular camera roll....But they were kind of clogging my camera roll.

4.2.3 Asset: Photos of partying or drinking

Some participants stored photos of drinking or going to parties with friends that they did not want their more conservative families to see.

P1, an 18-24 year old man, said:

> The earliest memories in [Snapchat My Eyes Only] are from the stupid high school parties where I didn't want my aunt or uncle [to see], if I'm throwing in a picture of a memory or whatever to see [me] drinking.

P16 and P17 mentioned not wanting parents to see photos of alcohol. P17, an 18-24 year old man, talked about using Secure Folder because while he does not drink, he keeps photos of hanging out with friends who drink, which his parents would ground or lecture him over.

> I had to hide [the photos] from my parents because they find [alcohol] unfavorable in their eyes. So me coming from a strict household, I have regular checkups on my phone, even though I'm [18-24] now, I have regular checkups on my mobile phone. My parents do that regularly.

4.2.4 Asset: Old Partners

Several participants mentioned not wanting a new partner to see photos of old partners. P6 said,

> It's not like I'm fearing that relationship would somehow be torn asunder because of the presence of those photos, but it does create a tiny little thorn of just sort of like, ooh.

Some participants kept photos of exes to look back on as an old memory. P5 described:

> I don't feel like if I break up with someone I need to remove that part from me. And I always talk with my current partner about [my] dating history. For example, for some photos, I would just hide them for the purpose of keeping the memory or separating them from the major album.

4.2.5 Assets: Sensitive Documents

Participants mentioned using vault apps for important documents, such as bank statements, identification documents (ID proofs) and for P16 from India, "certificates to prove our caste and religion."

P11 started using a vault app because he was looking for a safe and easily accessible storage mechanism for IDs due to this incident:

> In 2020 when I was traveling, in [the] airport we have to show our ID [as] proof that our names and the passport, or any ID proof, matches. I had an e-ticket and I had my ID proof as a PDF in my phone. I was unable to find [the] PDF because I had saved it in my local chats and everything in my WeChat. There were people in the line and everything so it was a very hassle moment for me.

The vault app made it easy for him to find his IDs on his phone. And his concern if friends or family got access to his IDs was that information would get to a loan shark who would call and harass him, given that happened to a friend.

P1 also uses Dropbox's locked files to store sensitive financial information regarding a project's donors. P1 uses iOS Notes, P13 uses OneNote, and P16 uses AppLock for storing a locked note filled with various passwords, functioning somewhat similarly to a password manager.

4.2.6 Asset: Medical photos or conversations

P2 mentioned storing photos of a skin problem when they were having intestinal issues in their My Eyes Only Album, because they considered it not-safe-for-work:

> And then when I would go to the doctors, if they needed to see a visual from previous irritation I could also share that with them.

P9 talked about using the Locked Folder in Google Photos in high school for saving screenshots of conversations to discuss with her therapist. She started using it because her friends would play Photo Roulette, which would access her Camera Roll. She moved photos she did not want her friends to see through the game to the Locked Folder, including photos related to her bipolar disorder diagnosis:

> I don't need people learning things about me that I wouldn't tell them willingly because they see something that [..] I didn't want them to see. So I did it for myself. Some things were moved there once I got word [of] things from other people, like you wouldn't want to know that, like when I had a mental health diagnosis. So I was hiding things that were related to that because I didn't want people to know [...] I have bipolar disorder. So other people were like, 'That's not a common enough one. You should hide anything related to that [...] that's a shameful diagnosis or disorder to have'.

She stopped using the tool in college since her parents had stopped going through her phone then, and also,

> I didn't feel my privacy was being invaded as much. I felt more comfortable setting boundaries. So I didn't think I needed to hide everything. And I think also I was like, okay, if I stopped hiding things on my phone, it'll make me feel more secure in telling other people things that maybe, because I was able to hide things that I wasn't able to do beforehand.

4.3 Threats Not Covered By Vault Apps

Participants had other security and privacy concerns for their assets that they did not use vault apps to cover.

4.3.1 Targeted Adversary

Participants also sometimes had concerns of a targeted, skilled adversary, but were generally aware this app would not protect against that kind of threat. In terms of a targeted hacker, P9 stated "But I'm like, so many people use Google. What is the odds that it's mine that gets hacked?"

P6 said,

> I really don't fear too much of somebody going through my phone. What person would be on that chaotic mission of "I'm gonna go try and find all of your [nude] photos right now". If another guy gets in, frankly, I don't have that many straight male friends. If he does get in, I'm just like, well, that's on you. I don't know how you find yourself there, but that's what you got. I may be delusional, but I don't really really fear bad scenarios. I stopped using it once I was a sophomore in college, because by that point [..] I didn't feel my privacy was being invaded as much.

P8, when asked why someone accidentally seeing a photo rather was the bigger concern over a targeted hacker, said,

> I think both should be concerns and I should probably be more concerned about my stuff getting hacked, rather than me accidentally showing something to someone. But I think that I'm a little bit lazy and I tend to not prioritize real privacy concerns I should have. Just for the sake of convenience I skip over and I don't make the effort to really protect things.

4.3.2 Company/Government Data Collection

Participants were concerned about the company of the tool they were using collecting data from them as well. P7, P9, P10, and P13 stated they were concerned about Snapchat having access to their sensitive photos and not knowing how they are using the photos or how well they are protecting those photos.

For P5, he preferred using the iOS hidden album because they did not want to download a third-party vault app and have another company collecting information from him. For P14, he trusts Apple well enough to use their tools, but notes, as an international student, because of the Patriot Act:

> [The government] can basically, no matter the level of encryption or anything that you have, no matter if you're using a phone of Apple, Samsung or anything, they can literally get into your phone.

P9 stated about Google Photos Locked Folder,

> With [the app], I think it was just more concerning 'cause that was at the start of when people started to learn about how data was being mined from us and being sold to companies and all that stuff, that was [..] when people started freaking out about that.

However, she concluded that she already uses many Google products and they already have a lot of information on her.

4.4 Vault App Affordances and Features

We discuss the affordances that met participant needs, and affordances they wished were included. A summary of the affordances that participants mentioned positively can be found in Table 4. Table 5 and Table 6, which lay out which apps participants mentioned have which affordances, can be found in Appendix 7.

4.4.1 Authentication

Customizable Password. P17 mentioned being able to use a different password than his phone password, which makes him feel safer because,

> Since my parents do regular checkups, they know my password to open the phone, but for the secure folder that I have hidden the password from them.

P13 was concerned about not having this feature with Hidden Folders, because knowing how to unlock the iOS phone would allow unlocking the Hidden Folder. For P1, the customizable password determines what folder is opened.

> Based on whatever pin you enter, it'll direct you to a different folder without revealing that there are any other keys in the name system.

Biometric Authentication. Some participants like the ease of biometric authentication, whether through fingerprint or FaceID. P11, discussing opening identification documents said,

> I use frequently the fingerprint one. Because if I have multiple bags in my hand at the airport, keeping them down and then typing the password is going to get pretty complicated.

But P1, P8, and P16 were concerned that biometrics makes authentication too easy for a potential adversary to unlock their files, which we discuss more in Section 4.4.4. Because Google Photos Locked Folder uses the default authentication for the phone, P16 wanted to be able to change the default biometric authentication to a PIN.

4.4.2 Discreteness

P3, P5, P7, P9, and P16 mentioned liking their tool of choice because it was difficult to find in a phone. P9 said they like Snapchat's My Eyes Only because, "[My parents are] not going to understand how to access it." For P16, they liked AppLock because the icon on the phone looks like a calculator. P17 wished that Secure Folder would disguise itself as another kind of app, such as a calculator.

P3 described wanting something similar specifically for locking notes or text messages, in a way "that's like discreet enough to not be a clear sign of if you're hiding something" so that it does not alert her parents or friends that she is hiding something. P3 did not want to download a separate vault app because of questions its existence could invite:

Positively-Mentioned Affordances
Customizable password different from phone authentication
Biometric authentication (fingerprint or FaceID)
Different folders opened by different customizable password
Disguising app icon (e.g., Calculator)
Hidden album is within an already used app (e.g., iOS Photos, Snapchat)
Vault app is separate from an already used app
Locked photos are hidden from Memories (e.g., Snapchat)
Built-in sharing functionality to other social media or messaging apps
Folder creation

Table 4: Summary of existing vault app affordances that participants positively mentioned. Some affordances are contradictory: some participants liked the ease of access that biometric authentication provided, while other participants did not feel as secure that the vault app could only use the device's default authentication, which was often biometrics. In addition, some participants preferred using a hidden album within an existing photo or social media app because it was convenient or because friends/family would not find it suspicious, while other participants preferred having a separate vault app to not create folder artifacts in commonly used apps.

> If my parents or my friends were to see, oh, you have this app just for hiding photos or certain things on your phone, I think that would have been maybe a little weird, felt like I was being overly secretive.

While Grindr does not have a locked photo album feature P4 did like that its existing Albums do not show a preview of the photos contained inside, so he can discretely share albums while other people are around without exposing any photos. P2 and P13 liked how Snapchat, for photos placed in the My Eyes Only album, are automatically removed from Snapchat's Memories, which is where photos are generally saved.

4.4.3 File Separation

P6 describes managing his intimate images as,

> What I want is just take all these photos and pull them out of the general pool. But the real value is them just not being [in] the general pool.

This file separation is enough for folks' threat models, but as others have pointed out in addition to P8, they don't consider it "secure".

> I think from my understanding is it's just putting it in a different album on my phone that is not with the rest of my camera roll, but it's not really protecting it in any way.

For P1 and P14, who use Secret Photo Album to store intimate images and Vault to store non-intimate images of former partners respectively, they like using apps that are not a default on their phones because it does not produce artifacts in popularly known locations. P1 stated he feels Secret Photo Album is more secure than using iPhone Hidden Album because his friends would know of the latter but not the former. And P11 says he likes using a separate vault app instead of Android's built-in locked Gallery album because,

> So for [IDs or other photos], I started using it in Secure Folder[. . .]it's also protected from [the] normal Gallery....I didn't want to get into hassle of those because if someone wanted to access [an album in] the Gallery, lots of questions can pop up.

4.4.4 Ease of Access

P11 prefers PhotoVault to Secure Folder for storing IDs because Secure Folder needs a second click into a folder to open up images, while PhotoVault shows images upon successful authentication.

Several participants began to or liked using their chosen tool because it already existed on their phones.

> It's just convenient that it's already on my phone. I didn't have to download anything else. —*P7*

> It's convenient in the sense that I have Snapchat on my phone. I use Snapchat pretty often, so it's easy access. —*P9*

Some participants saw this ease of access as a security cost. P3 wished that My Eyes Only would have an additional pop-up question of "Are you sure you want to send this?". P8 wished there was an additional step to authentication for the iOS Hidden Album after FaceID.

> I guess I have one concern if I was asleep or something and I don't know if face ID works when your eyes are closed. Or if I accidentally clicked the hidden album and then it immediately scanned my face and opened it up. It would be nice to have extra questions or require extra actions.

P1 felt similarly about accidentally unlocking the iOS Hidden Album with his finger and wanted an extra prompt asking for authentication rather than automatically doing so.

4.4.5 Ease of Sharing

While P2 liked how easy it was to share within Snapchat and download photos from the My Eyes Only album, a common desire amongst participants who shared intimate messages was being able to easily share a photo from a different vault app or hidden album to a messaging or social media app. P4, P5, and P6 wished more apps would have access to the iOS Hidden Album when uploading photos. P14, who has Vault on his iPhone, wished there was an easy way to locally transfer files from it to his PC without having to use Vault's Cloud feature.

4.4.6 (Absence of) Backups

P1 was concerned about losing his stored photos if he forgot his My Eyes Only PIN. He could reset it, but Snapchat will delete the images in the album.

Conversely, P3 was concerned with not wanting Hidden Album photos to be backed up with iOS. P14 complained that by default with iCloud featured turned on, the Hidden Album photos will also get stored, which she does not want and has turned off. They would not want that automatically.

P7 stated he wanted more transparency around what happens to files with iOS backups:

> I think, in particular, like when you back up your phone, I don't know where those photos go like on your computer....But I guess like [I want] more transparency and like, if they're committed at all to protecting what you have in there, because I guess the assumption for me as a user that like hiding photos would have, would that be like things are private or people like want them to be hidden for some reason or another that I would presume be private.'

4.4.7 Desiring more "Security"

Meanwhile, P11 had a specific request for more security. If someone opened and failed to authenticate for Photo Vault, he wanted it to discretely take a photo of the person so he could find it later. P14 talked about an app feature that would automatically filter more private photos from the general photo pool based on a country's specific norms of what is considered private. And P17 wanted an explanation of My Eyes Only when he first found it:

> If they would just give me a little tutorial or something, break down of the feature and its security, that would probably be good.

4.4.8 Other Desired Features

P2 and P14 wanted more editing features. P2 wanted to be able to send blurred out photos through My Eyes Only, similar to how iMessage can send blurred photos where the blur is slowly removed. P1 wished Secret Photo Album could store files other than just photos or videos, such as PDFs of important documents.

P11 and P13 did not like how the free version of vault apps have a lot of ads. While none of the participants mentioned paying for a vault app, we note certain affordances only being available in paid app versions in Table 5.

4.5 Tool Discovery Process

Participants mentioned finding the tool they use either through friends/family, personal discovery while going through an existing app, or doing an Internet search for a vault app (similar to how people have looked for security advice [50]).

P1, P5, P7, P8, P13, and P17 found the Hidden Album feature while using the built-in Photos app on their iPhones. P2 and P12 said they found the My Eyes Only album through their regular use of Snapchat, while P10 said he always knew that tool was there. P14 discovered Adobe Acrobat's locked file feature when he was sent bank statements with a password. P15 had Secure Folder recommended by their Samsung phone, and P16 found Google Photos' locked folder through their regular use of the app.

P1, P3, P9, P11, P13, P14, and P15 mentioned doing an Internet search to either find a tool to meet their needs or to see if an existing tool they had (like OneNote or iPhone Photos) could hide or protect certain files. P11 compared reviews of different vault apps to make a download decision. P14 and P16 mentioned discovering the vault app they use by seeing their friends use a vault app and asking about it.

4.6 Pre-Vault App Behavior

Participants had different asset storage practices before using a vault app or hidden album. P1 would hold his phone close while scrolling past sensitive partying videos rather than scrolling with his phone screen out in the open. P3 would either not take "embarrassing" photos of herself or delete them right after taking them. P1, P8, and P17 did not take nude photos before having a vault app.

P16 would delete photos of himself with friends drinking after taking a look at the photo. P4, P5, and P9 would delete their nudes from their phone after sending it to someone. P9 stated,

> More so with nudes...it would be taken directly on Snapchat and immediately deleted. And then I realized how annoying that was, but I didn't want them so openly on my camera roll....Then once I

> discovered [Snapchat] For My Eyes Only existed, I was like, okay, this is great.

P8 would not have stored any or would have deleted nudes of themself and others. For other participants, before using a vault app they had their photos or documents stored on other apps, including their regular Camera Roll, WeChat files, Gmail files, Grindr, and Snapchat.

5 Discussion

5.1 Perspective Determines Technological Security

While prior work has explored vault app security either from the threat modeling standpoint that the vault app user is the adversary [12, 14, 66], or from the threat modeling standpoint that a vault app user faces law enforcement [22] or IPV [51], our work begins from learning user threat models towards using vault apps. We show how our participant pool uses vault apps towards less capable adversaries than a targeted hacker or law enforcement: our participants were primarily concerned with stopping unintended exposures to the public or close ties around them (which prior research also recommends as the use case for vault apps [22]). While they had an understanding that vault apps would not stop a targeted adversary, for preventing accidental exposure they found vault apps to meet their needs (though any technology can never be proven to be fully secure [27]). Herley writes, "In the absence of actual compromise data the security community often speaks of worst-case risk" [26]. Prior vault app security analyses focused on worst-case risk, but our findings show that for users with different adversaries in mind, the security of vault apps needs to be evaluated differently. For research, evaluating tool security for what threats users care about is just as important as evaluating security for worst-case threats. Therefore, it is important to conduct user studies so users can define their own security concerns and contexts for what mitigations are useful to them, beyond just security experts determining threats for users, as prior work has also shown [19, 58].

5.2 Context Collapse and Device Sharing

While context collapse was initially coined to refer to posts on social media where multiple audiences may see content [37], our results show how context collapse also exists amongst device sharing and screen sharing. Our participants have opened their devices and photo galleries in professional settings, amongst friends and family, and in public, which are not always the intended audiences for all device content. For example, while one may have consensually stored intimate images on one's phone, it would be inappropriate to be seen in a workplace. Given that photo galleries and file apps store media for different purposes and audiences, from public to private, personal to professional, similar to social media, tools are needed to support device privacy similar to how privacy settings prevent context collapse on social media.

Jacobs et al. describe accidental content sharing when partners have access to each other's phones as breaking contextual integrity [28], or breaking adequate privacy based on norms in a specific context [46]. Vault apps allow people to regain contextual integrity through more granular app-level authentication, providing selective content visibility. As shown in Section 4.6, some participants would not have stored intimate media or party memories with friends before using a vault app. This shows how vault apps can provide the necessary granular device privacy that Wu et al. states is lacking on devices for privacy-supporting consensual device sharing [64].

5.3 Vault Apps For Vulnerabilities

While contextual integrity can explain the desire to keep certain media private based on social norms [28, 46], McDonald & Forte argue that privacy theory should move away from protecting norms towards protecting vulnerable populations, who are "not only more likely to be susceptible to privacy violations but whose safety and wellbeing are disproportionately affected by such violations" [42].

We had several participants who had privacy vulnerabilities, either on a societal, community, or familial level: P17 wanted to keep photos of drinking private from his conservative Christian family, and P9 had expectations of keeping her bipolar disorder diagnosis quiet in her town, while also having concerns about her intimate media being exposed as a woman. In the former's case, a parent's desire to know everything about their child comes into tension with their child's desires and values; as Levy & Schneier note, "The balance between essential caretaking and privacy invasion can be unclear" [33] . Regardless, in a parent-child relationship the child often has less power than a parent, even as an adult. And in P9's case, there is much research supporting the higher degree of harm women face from their intimate photos being exposed [5, 6, 8, 31]. Vault apps can provide privacy protection in these contexts of differential power. While vault apps can be used for harmful purposes [12, 35], and some parental articles have flagged it as something to look out for on a child's phone [2], its existence on a phone should not necessarily imply harmful behavior on the user's part because it is also a tool that supports privacy for vulnerable populations.

5.4 Design Recommendations

Most of our participants wanted both security and privacy, as well as usability with their vault apps. Sometimes these values came into tension with one another, e.g., biometric authentication provides easy access but introduces the concern of easy access by an adversary. In accordance with these tensions, we make some recommendations for vault app design. Vault apps

and hidden albums should allow authentication choices in addition to or instead of the phone's default authentication. This includes both PIN and biometric options, as well as options for friction pop-ups to prevent accidental access to the app from a fingerprint or FaceID.

We also note that while all the apps mentioned were free, some had ads while others had paywalled features. Both Android and iOS have default hidden/locked albums within default photo apps (iOS Photos and Android Gallery). If one wants other functionalities like decoy vaults, one has to turn to another app. Prior work has discussed the digital divide between higher-income and lower-income users, with the former having better access to paywalled privacy or security services [49]. While the default vault app feature of authentication-protected storage is available on iOS and Android phones, other features require payment. We recommend phone OS developers continue developing vault app features for default apps to support users with less financial privilege.

Finally, several participants mentioned not fully understanding how the technical aspects of vault apps work, in terms of security. Vault apps could provide an overview of encryption and other security features in-app, similar to the Privacy Center on Facebook. Some participants also mentioned difficulty in determining whether hidden media is backed up on a cloud server or another device. Some vault apps like Snapchat My Eyes Only do not have a recovery process for photos if the password is lost; photos are deleted if the password is changed. Meanwhile, hidden photos on the iPhone are automatically backed up to iCloud if Photos is enabled for iCloud sync. To better provide information on data storage and access, vault apps could have a privacy nutrition label [29] that notes if there are any other devices or servers the files are stored on. Also, for people who have a photo or file backup sync turned on, there should be granular settings to bulk-remove an album/folder from being backed up.

6 Limitations and Future Work

We do not perform a technical analysis of vault app security, as that is out of the scope of this paper. As our research method is qualitative, we cannot provide results on the frequency of behaviors, threat models, or app usage; instead, our interview results provide rich and contextualized insights on participant privacy concerns, motivations, and how that affects their behaviors. Future work should take quantitative approaches to understand the frequency of vault app usage and storage of different media types. Moreover, future work should study how vault apps represent their security to users and whether this maps to actual technical practice.

While we recruited a diverse U.S. population across gender, sexual orientation, race, education, and household income, our participants were almost all monogamous, and participant ages ranged from 18-34. Future work is needed to determine if this reflects the typical vault app user age range. Our participants being largely LGBTQ+ is likely due to additional recruiting through queer communities; other groups that we did not specifically recruit from may have different usage patterns with these tools. Also, we cannot speak to mental models of people who have considered using vault apps for shoulder surfing and accidental exposure threats but decided not to use them. We also did not specifically recruit for certain vulnerable populations, such as IPV survivors, who may have different or differently prioritized security and privacy requirements [62], e.g. stealthiness or deniability. Future work should study how different vulnerable populations may use vault apps to understand their more specific threat models.

Finally, we only describe vault app usability and affordances for the tools our participants mentioned. Future work should explore user evaluations of other vault apps and other features they provide, such as Face Down Lock, which closes the vault app and opens a different app when the phone is placed face down.

7 Conclusion

To understand user threat models for using vault apps, we conducted semi-structured interviews with 18 adults in the U.S. who use vault apps or hidden folders. We found the primary threats participants use vault apps to defend against are accidental content exposure through shoulder surfing, when consensually sharing a device, or when a parent is snooping on a phone. Participants stored files including intimate media, identification documents, non-sexual body photos, photos of old partners, photos of partying or drinking, and medical photos or conversations. Given phones store a range of public to private, professional to personal media, we show how vault apps can prevent context collapse and protect contextual integrity when sharing devices. We also show how vault apps can preserve privacy for vulnerable individuals and its existence should not by default imply harmful behavior. We conclude with design recommendations to improve balancing the usability/security tension of vault apps.

Acknowledgments

We would like to thank Calvin Liang, Kentrell Owens, Lucy Qin, Franziska Roesner, Elissa Redmiles, Lucy Simko, Miranda Wei, and Eric Zeng for their valuable expertise. This research is supported in part by the National Science Foundation under Award #2016061, and the EPSRC.

References

[1] Vault - hide pics, app lock - apps on google play. https://play.google.com/store/apps/details?id=com.netqin.ps&hl=en_US&gl=US. (Accessed on 02/14/2024).

[2] Parents warned of vault apps on their children's smartphones. https://www.moms.com/fake-calculator-app-kids-hide-photos/, 2021. (Accessed on 02/09/2024).

[3] Toward safer intimate futures: Recommendations for tech platforms to reduce image based sexual abuse - european sex workers' rights alliance. https://www.eswalliance.org/toward_safer_intimate_futures_recommendations_tech_platforms_reduce_image_based_abuse, 2023. (Accessed on 02/07/2024).

[4] Mamtaj Akter, Amy J Godfrey, Jess Kropczynski, Heather R Lipford, and Pamela J Wisniewski. From parental control to joint family oversight: Can parents and teens manage mobile online safety and privacy as equals? *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW1):1–28, 2022.

[5] Rikke Amundsen. 'The Price of Admission': On Notions of Risk and Responsibility in Women's Sexting Practices. In Karen Lumsden and Emily Harmer, editors, *Online Othering: Exploring Digital Violence and Discrimination on the Web*, Palgrave Studies in Cybercrime and Cybersecurity. Palgrave Macmillan, 2019.

[6] Rikke Amundsen. The turn to trust: adult women, hetero-sexting, and the use of trust as sexting risk mitigation. *Feminist Media Studies*, pages 1–16, 2023.

[7] Melissa Burkett. Sex (t) talk: A qualitative analysis of young adults' negotiations of the pleasures and perils of sexting. *Sexuality & Culture*, 19(4):835–863, 2015.

[8] Danielle Keats Citron. *Hate crimes in cyberspace*. Harvard University Press, 2014.

[9] Danielle Keats Citron. Sexual privacy. *128 Yale Law Journal 1870 (2019); U of Maryland Legal Studies Research Paper No. 2018-25*, 2019.

[10] Lorrie Faith Cranor, Adam L Durity, Abigail Marsh, and Blase Ur. {Parents'} and {Teens'} perspectives on privacy in a {Technology-Filled} world. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 19–35, 2014.

[11] Alexei Czeskis, Ivayla Dermendjieva, Hussein Yapit, Alan Borning, Batya Friedman, Brian Gill, and Tadayoshi Kohno. Parenting from the pocket: Value tensions and technical directions for secure and private parent-teen mobile safety. In *Proceedings of the sixth symposium on usable privacy and security*, pages 1–15, 2010.

[12] Gokila Dorai, Sudhir Aggarwal, Neet Patel, and Charisa Powell. Vide-vault app identification and extraction system for ios devices. *Forensic Science International: Digital Investigation*, 33:301007, 2020.

[13] Michelle Drouin, Manda Coupe, and Jeff R. Temple. Is sexting good for your relationship? It depends.... *Computers in Human Behavior*, 75:749–756, 2017.

[14] Michaila Duncan and Umit Karabiyik. Detection and recovery of anti-forensic (vault) applications on android devices. 2018.

[15] Nicola Döring. Consensual sexting among adolescents: Risk prevention through abstinence education or safer sexting? *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 8, 01 2014.

[16] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. "A stalker's paradise": How intimate partner abusers exploit technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, New York, NY, USA, 2018. Association for Computing Machinery.

[17] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders. *Proceedings of the ACM on Human-Computer Interaction*, 1(CSCW):1–22, 2017.

[18] Alisa Frik, Leysan Nurgalieva, Julia Bernd, Joyce Lee, Florian Schaub, and Serge Egelman. Privacy and security threat models and mitigation strategies of older adults. In *Fifteenth symposium on usable privacy and security (SOUPS 2019)*, pages 21–40, 2019.

[19] Christine Geeng, Mike Harris, Elissa Redmiles, and Franziska Roesner. "Like lesbians walking the perimeter": Experiences of US. LGBTQ+ folks with online security, safety, and privacy advice. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 305–322, 2022.

[20] Christine Geeng, Jevan Hutson, and Franziska Roesner. Usable sexurity: Studying People's concerns and strategies when sexting. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, pages 127–144, 2020.

[21] Arup Kumar Ghosh, Karla Badillo-Urquiola, Shion Guha, Joseph J LaViola Jr, and Pamela J Wisniewski. Safety vs. surveillance: what children have to say about mobile apps for parental control. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2018.

[22] Alissa Gilbert and Kathryn C Seigfried-Spellar. Forensic discoverability of ios vault applications. *Journal of Digital Forensics, Security and Law*, 17(1):1, 2022.

[23] Erving Goffman. The presentation of self in everyday life. In *Social Theory Re-Wired*, pages 482–493. Routledge, 2016.

[24] Skyler T Hawk, Loes Keijsers, Tom Frijns, William W Hale III, Susan Branje, and Wim Meeus. "i still haven't found what i'm looking for": Parental privacy invasion predicts reduced parental knowledge. *Developmental Psychology*, 49(7):1286, 2013.

[25] Debby Herbenick, Jessamyn Bowling, Tsung-Chieh (Jane) Fu, Brian Dodge, Lucia Guerra-Reyes, and Stephanie Sanders. Sexual diversity in the United States: Results from a nationally representative probability sample of adult women and men. *PLOS ONE*, 12(7):e0181198, July 2017.

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

[27] Cormac Herley. Unfalsifiability of security claims. *Proceedings of the National Academy of Sciences*, 113(23):6415–6420, 2016.

[28] Maia Jacobs, Henriette Cramer, and Louise Barkhuus. Caring about sharing: Couples' practices in single user device access. In *Proceedings of the 2016 ACM International Conference on Supporting Group Work*, pages 235–243, 2016.

[29] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W Reeder. A" nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, pages 1–12, 2009.

[30] Kami Kosenko, Geoffrey Luurs, and Andrew R Binder. Sexting and sexual behavior, 2011–2015: A critical review and meta-analysis of a growing literature. *Journal of computer-mediated communication*, 22(3):141–160, 2017.

[31] Amanda Lenhart, Michele Ybarra, and Myeshia Price-Feeney. Nonconsensual image sharing: one in 25 americans has been a victim of" revenge porn". 2016.

[32] Ada Lerner, Helen Yuxun He, Anna Kawakami, Silvia Catherine Zeamer, and Roberto Hoyle. Privacy and activism in the transgender community. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2020.

[33] Karen Levy and Bruce Schneier. Privacy threats in intimate relationships. *Journal of Cybersecurity*, 6(1), 2020.

[34] Ben Lovejoy. 'Nude' app uses coreml to automatically detect & protect intimate photos on an iphone - 9to5mac. https://9to5mac.com/2017/10/17/nude-photos-iphone/, 2017. (Accessed on 02/14/2024).

[35] Megan K Maas, Kyla M Cary, Elizabeth M Clancy, Bianca Klettke, Heather L McCauley, and Jeff R Temple. Slutpage use among us college students: the secret and social platforms of image-based sexual abuse. *Archives of sexual behavior*, 50:2203–2214, 2021.

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

[37] Alice E Marwick and danah boyd. Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, 16(7):1051–1067, 2014.

[38] Louise Matsakis. The Motherboard guide to sexting securely, 2017. https://www.vice.com/en_us/article/mb3nd4/how-to-sext-securely-safely-what-apps-to-use-sexting.

[39] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. "She'll just grab any device that's closer": A study of everyday device & account sharing in households. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 2016.

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

[41] Jane Mavoa, Simon Coghlan, and Bjørn Nansen. "it's about safety not snooping": Parental attitudes to child tracking technologies and geolocation data. *Surveillance & Society*, 21(1):45–60, 2023.

[42] Nora McDonald and Andrea Forte. The politics of privacy theories: Moving from norms to vulnerabilities. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2020.

[43] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–23, 2019.

[44] Henry L Minton. *Departing from deviance: A history of homosexual rights and emancipatory science in America*. University of Chicago Press, 2002.

[45] Maryam Mustafa, Abdul Moeed Asad, Shehrbano Hassan, Urooj Haider, Zainab Durrani, and Katharina Krombholz. Pakistani teens and privacy-how gender disparities, religion and family values impact the privacy design space. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, pages 195–209, 2023.

[46] Helen Nissenbaum. Privacy as contextual integrity. *Wash. L. Rev.*, 79:119, 2004.

[47] Cheul Young Park, Cori Faklaris, Siyan Zhao, Alex Sciuto, Laura Dabbish, and Jason Hong. Share and share alike? An exploration of secure behaviors in romantic relationships. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 83–102, Baltimore, MD, August 2018. USENIX Association.

[48] Rizu Paudel, Prakriti Dumaru, Ankit Shrestha, Huzeyfe Kocabas, and Mahdi Nasrullah Al-Ameen. A deep dive into user's preferences and behavior around mobile phone sharing. *Proceedings of the ACM on Human-Computer Interaction*, 7(CSCW1):1–22, 2023.

[49] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. Where is the digital divide? a survey of security, privacy, and socioeconomics. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 931–936, 2017.

[50] Elissa M Redmiles, Amelia R Malone, and Michelle L Mazurek. I think they're trying to tell me something: Advice sources and selection for digital security. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 272–288. IEEE, 2016.

[51] Margie Ruffin, Israel Lopez-Toldeo, Kirill Levchenko, and Gang Wang. Casing the vault: Security analysis of vault applications. In *Proceedings of the 21st Workshop on Privacy in the Electronic Society*, pages 175–180, 2022.

[52] Nithya Sambasivan, Amna Batool, Nova Ahmed, Tara Matthews, Kurt Thomas, Laura Sanely Gaytán-Lugo, David Nemer, Elie Bursztein, Elizabeth Churchill, and Sunny Consolvo. "They don't leave us alone anywhere we go": Gender and digital abuse in South Asia. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, New York, NY, USA, 2019. Association for Computing Machinery.

[53] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. "Privacy is not for me, it's for those rich women": Performative privacy practices on mobile phones by women in south asia. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 127–142, 2018.

[54] Emily Setty. A rights-based approach to youth sexting: Challenging risk, shame, and the denial of rights to bodily and sexual expression within youth digital sexual culture. *International Journal of Bullying Prevention*, 1:298–311, 2019.

[55] Scott Skinner-Thompson. Performative privacy. *UCDL Rev.*, 50:1673, 2016.

[56] Scott Skinner-Thompson. Privacy's double standards. *Wash. L. Rev.*, 93:2051, 2018.

[57] Julia Slupska, Selina Cho, Marissa Begonia, Ruba Abu-Salma, Nayanatara Prakash, and Mallika Balakrishnan. "They look at vulnerability and use that to abuse you": Participatory threat modelling with migrant domestic workers. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 323–340, 2022.

[58] Julia Slupska, Scarlet Dawson Dawson Duckworth, Linda Ma, and Gina Neff. Participatory threat modelling: Exploring paths to reconfigure cybersecurity. In *extended abstracts of the 2021 CHI conference on human factors in computing systems*, pages 1–6, 2021.

[59] Emily C. Stasko and Pamela A. Geller. Reframing sexting as a positive relationship behavior. Drexel University, 2015. https://www.apa.org/news/press/releases/2015/08/reframing-sexting.pdf.

[60] Samuel Hardman Taylor, Jevan Alexander Hutson, and Tyler Richard Alicea. Social consequences of Grindr use: Extending the internet-enhanced self-disclosure hypothesis. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 6645–6657, 2017.

[61] Joris Van Ouytsel, Ellen Van Gool, Michel Walrave, Koen Ponnet, and Emilie Peeters. Sexting: Adolescents' perceptions of the applications used for, motives for, and consequences of sexting. *Journal of Youth Studies*, 20(4):446–470, 2017.

[62] Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L Mazurek, Manya Sleeper, and Kurt Thomas. Sok: A framework for unifying at-risk user research. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 2344–2360. IEEE, 2022.

[63] Miranda Wei, Eric Zeng, Tadayoshi Kohno, and Franziska Roesner. Anti-Privacy and Anti-Security advice on TikTok: Case studies of Technology-Enabled surveillance and control in intimate partner and Parent-Child relationships. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 447–462, 2022.

[64] Yuxi Wu, W Keith Edwards, and Sauvik Das. Sok: Social cybersecurity. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 1863–1879. IEEE, 2022.

[65] Nannan Xie, Hongpeng Bai, Rui Sun, and Xiaoqiang Di. Android vault application behavior analysis and detection. In *Data Science: 6th International Conference of Pioneering Computer Scientists, Engineers and Educators, ICPCSEE 2020, Taiyuan, China, September 18-21, 2020, Proceedings, Part I 6*, pages 428–439. Springer, 2020.

[66] Xiaolu Zhang, Ibrahim Baggili, and Frank Breitinger. Breaking into the vault: Privacy, security and forensic analysis of android vault applications. *Computers & Security*, 70:516–531, 2017.

Appendix

Interview Protocol

1. Vault apps or hidden album apps are tools that store content on a mobile device so people won't accidentally see it. What vault apps or hidden album tools do you use or have used?
2. For each tool: When did you start using the tool?
3. Why did you start using it? a. Was there a specific incident or story that prompted getting it? b. Did anyone else's opinion affect your decision on it?
4. How did you learn about this tool? a. How did you pick that tool over others? b. If they use multiple tools, ask about both of them
5. Did you have any concerns or questions about using it?
6. If we don't know if it's free: Did you have to pay for the tool? What led to this decision?
7. What phone do use?

If participant stores intimate media and stores other types of content, ask the "non-intimate media" line of questioning first, and based on time left get as far with the "intimate media" line of questioning as possible. If decision to use involves storing intimate media:

1. What types of images do you store? a. If storing person's images: Whose images do you store?
2. How did you store them before getting this tool?
3. How do you store them with this tool? a. E.g., directly saving, screenshotting, etc.
4. Do you plan on storing this media indefinitely? a. Is there any scenario you could imagine where you would delete the media?
5. If storing person's images: For the person in the photos you've saved, what expectations did you and that person have when they sent you the photo?
6. Do you ever share these photos? a. Does this app have sharing functionality?
7. What concerns do you have that prompted you to use this tool?
8. You mentioned x concerns prompting you to use this tool. Do you feel like this tool addresses all of these concerns? a. Why or why not?
9. Are there other features of this tool that you find useful? a. Why or why not? b. Can you provide an example of a useful feature? c. Are there features you want that they don't provide?
10. Do you have any concerns that this tool doesn't address?
11. Is there anything you'd like to see changed in the app to help prevent these concerns?
12. Do you have any concerns with the tool itself?
13. What settings do you feel comfortable opening the tool?
14. Is there a way to access these files through your computer?

If decision to use involves storing non-intimate media:

1. What kind of files do you store?
2. What concerns do you have that prompted you to use this tool?
3. You mentioned x concerns prompting you to use this tool. Do you feel like this tool addresses all of these concerns? a. Why or why not?
4. Are there other features of this tool that you find useful? a. Why? b. Can you provide an example of a useful feature? c. Are there features you want that they don't provide?
5. Do you have any concerns that this tool doesn't address?

6. Is there anything you'd like to see changed in the app to help prevent these concerns?
7. Do you have any concerns with the tool itself or the company?
8. In what settings do you feel comfortable opening the tool?
9. Do you plan on storing this media indefinitely? a. Is there any scenario you could imagine where you would delete the media?
10. How did you store them before getting this tool?
11. Is there a way to access these files through your computer?

Final Questions (for every participant)

1. Ask these questions per each type of media stored: What kind of people are you concerned about seeing x content? a. Assuming its for privacy or security usage: Are there outcomes you are concerned about if x sees that content? i. If yes: What are the outcomes?
2. Have you tried any other way of preventing that from happening besides vault apps?
3. Do you feel like the vault app has successfully prevented that?
4. Is there anything you'd like to see changed in the app to help prevent that?

Demographics
You can say pass if you want to skip any of these questions.

1. Relationship style? E.g., monogamous, polyamorous, etc.
2. Relationship status
3. Sexual orientation

Anything else you want to tell us that we haven't asked?

App Affordance Tables

List of Apps	PIN?	Biometrics?	Swipe Pattern?	Selective Access (different "accounts")	Steps to Access
Snapchat My Eyes Only	4 digits	N	N	N	2 swipes
iOS Photos Hidden Album	Screen Lock		N	N	2 clicks
Google Photos (hidden album)	Screen Lock			N	3 clicks
Dropbox (locked file)	Password (Paid version only)	N	N	Y - select who has access	2 clicks
Secret Photo Album	Y	N	Y	N	Open + unlock
Secure Folder (Android Files)	4 digits	N	Y	N	2 clicks + unlock
Photo Vault (KeepSafe)	4 digits	Fingerprint	Y	decoy vault (2nd PIN) No seperate accounts	Open + unlock
Vault	15 digits	Fingerprint	Y	decoy vaults (PAID ONLY)	Open + unlock
Adobe Acrobat (locked file)	Password (Paid version only)	N	N	N	Open + unlock each file
App Lock	N	N	Y	Y - "Profiles"	Open + unlock
iOS Notes (locked file)	Y	Y screen lock	N	N	Open + unlock
OneNote	Password	N	N	N	Open + unlock

Table 5: Authentication and access-related affordances in vault apps and hidden folders participants mentioned. Screen lock authentication refers to the app requiring the same type of authentication as for unlocking the phone. Swipe pattern refers to graphical passwords. Selective access refers to either account-based access permissions or to PIN-based access to different file folders, i.e., providing a different PIN leads to different storage on a vault app. Steps to Access refers to opening a vault app or hidden album from the step prior to authentication; e.g., if one is opening a Hidden Album from iOS Photos, we assume they already have the app Photos open.

List of Apps	Independent from OS	Discreet Icon / Within App	Hide Content In-App	Hidden from Memories	Folders	Share / Download Content
Snapchat My Eyes Only	Y	Snapchat	N	Y	N	Share
iOS Photos Hidden Album	N	Photos	N	Y	N	Y
Google Photos (hidden album)	Y	Photos	N	Y	N	N
Dropbox (locked file)	Y	Dropbox	N	N/A	Y	Share / Download
Secret Photo Album	Y	Y	N	N/A	Y	Y
Secure Folder (Android Files)	Y	Files	N	N/A	N	N
Photo Vault (KeepSafe)	Y	Y	Y - decoy vault with second PIN	N/A	Y	Share
Vault	Y	"Stealth Mode"*	Y - decoy vault with second PIN	N/A	Y	Y
Adobe Acrobat (locked file)	Y	Acrobat	Y - per file passwords	N/A	Y	Y - keeps password
App Lock	Y	N	N	N/A	N	Share
iOS Notes (locked file)	N	Notes	Y	N/A	N	Y
OneNote	Y	OneNote	Y - per section passwords	N/A	Y	Y

Table 6: Discreteness and organizational-related affordances in vault apps and hidden folders participants mentioned. Distinct from Device refers to an app not being a default installation with the operating system. Discreet Icon refers to having a camoflaging icon, such as that of a Calculator app, and Within App refers to the tool being hidden within a non-vault app. Hide Content In-App refers to . Hidden from Memories refers to removing authentication-protected photos from app-curated photo collections. Folders refers to being able to make separate folders for files. *Doesn't work on modern phones.