Vulnerability & Blame: Making Sense of Unauthorized Access to Smartphones

Diogo Marques
LASIGE
Faculdade de Ciências
Universidade de Lisboa
dmarques@di.fc.ul.pt

Tiago Guerreiro
LASIGE
Faculdade de Ciências
Universidade de Lisboa
tjvg@di.fc.ul.pt

Luís Carriço
LASIGE
Faculdade de Ciências
Universidade de Lisboa
lmc@di.fc.ul.pt

Ivan Beschastnikh
University of British Columbia
bestchai@cs.ubc.ca

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

ABSTRACT

Unauthorized physical access to personal devices by people known to the owner of the device is a common concern, and a common occurrence. But how do people experience incidents of unauthorized access? Using an online survey, we collected 102 accounts of unauthorized access. Participants wrote stories about past situations in which either they accessed the smartphone of someone they know, or someone they know accessed theirs. We describe the context leading up to these incidents, the course of events, and the consequences. We then identify two orthogonal themes in how participants conceptualized these incidents. First, participants understood trust as performative vulnerability: trust was necessary to sustain relationships, but building trust required displaying vulnerability to breaches. Second, participants were self-serving in their sensemaking: they blamed the circumstances, or the other person's shortcomings, but rarely themselves. We discuss the implications of our findings for security design and practice.

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**; • **Human-centered computing → Empirical studies in HCI**;

CHI 2019, May 4–9, 2019, Glasgow, Scotland Uk

ACM ISBN 978-1-4503-5970-2/19/05…$15.00
https://doi.org/10.1145/3290605.3300819

ACM Reference Format:
Diogo Marques, Tiago Guerreiro, Luís Carriço, Ivan Beschastnikh, and Konstantin Beznosov. 2019. Vulnerability & Blame: Making Sense of Unauthorized Access to Smartphones. In *CHI Conference on Human Factors in Computing Systems Proceedings (CHI 2019), May 4–9, 2019, Glasgow, Scotland Uk*. ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3290605.3300819

1 INTRODUCTION

Smartphones are highly personal devices. Those who access our smartphones can find the digitized minutiae of our existence — information which may not be interesting to anyone, except to ourselves, and to those closest to us. The possibility of unauthorized access by "insiders" is, for smartphone users, a common concern. Surveys suggest this concern is not unfounded, as incidents of unauthorized access appear to be a common occurrence.

User concerns with unauthorized access have been extensively documented. Muslukhov et al. [28], drawing an analogy with other computing systems, characterized known people as "insiders"; and, in a quantitative comparison, found that smartphone users were equally concerned about strangers and insiders accessing their devices. It is unclear whether current security technologies, such as smartphone locks, can alleviate such concerns. Egelman et al. [10] interviewed participants who expressed that they could manage their concerns about strangers with unlock authentication; however, they had more difficulty in managing access by people they knew. One source of difficulty is that intrusion-prevention is not the only important dimension to users. Users also value the ability to access their devices easily [10, 16, 17], and the ability to allow limited access, or signal allowance, to some people [15, 19, 23, 25]. Today, signaling non-allowance, much less enforcing it, is not viable for many smartphone users, notably those subjected to intimate partner abuse [9, 24].

Surveys also indicate that unauthorized access is not unusual [22, 28, 34]. A Pew survey [34] found that 12% of US mobile phone owners reported having had another person

access the content of their phone in a way that they perceived as an invasion of their privacy. Muslukhov et al. [28] reported that 9% of participants in an online survey indicated having used someone else's mobile phone without their permission, with the objective of looking at their data. Marques et al. [22] reported that, in a survey designed to assure anonymity, 31% of participants were estimated to have had "looked through" someone else's phone without permission in the preceding year. The prevalence of engaging in unauthorized access seems to be higher among younger people [22, 28], and those who themselves keep more sensitive data on their mobile devices [22].

Prior research suggests that users of smartphones are concerned about the possibility of unauthorized access, and that incidents are common. However, there has been scarce examination of the ways in which these incidents are experienced when they happen.

In this paper, we ask: *how do people experience incidents of unauthorized access to their smartphones*? To answer this question, we collected 102 stories from participants we recruited online. We solicited stories from both sides in such incidents: participants were prompted to recount past experiences in which either they accessed the smartphone of someone they know, **or** someone they know accessed theirs. We explore *what happens in such incidents*, as well as *how participants describe these incidents*.

Our findings include:

- In the stories we collected, those who accessed devices were most commonly part of an "inner circle" of people close to the device owner.
- We found motivations for accessing devices ranging from benign to malicious. Most stories described unauthorized access motivated by a desire to learn about relationships of the device owner with third parties. Other motivations included playing pranks, convenience, and stealing information or money.
- Incidents of unauthorized access often occurred when devices were briefly unattended, for instance while the owner went to the bathroom.
- Overwhelmingly, the most accessed data were text-based conversations, such as text messages, instant messages, and email.
- Participants understood interpersonal trust as necessary to sustain relationships, but building trust required displaying vulnerability to unauthorized access.
- Participants blamed incidents of unauthorized access on a set of circumstances, or on the other person's shortcomings, but rarely on themselves.

Our findings offer details about incidents of unauthorized access which can inform the development and evaluation of new technologies. Furthermore, our work provides a lens for interpreting the limitations of existing defenses in the face of unauthorized access by parties known to device owners.

2 METHOD

To obtain detailed accounts of unauthorized access, we asked participants in an online study to write open-ended stories about past experiences. Participants could write about an experience of accessing a smartphone of someone they know without permission, or about an experience of someone they know accessing theirs.

We emphasized that stories were anonymous. To that end, we did not ask participants to convey their role. Instead, we asked them to write stories as if they were narrators not involved in the incident. We also suggested they use a set of names we selected in advance (**Ash** for the person whose device is accessed, and **Val** for the person accessing it); we suggested they use gender-neutral pronouns, and asked them to refrain from including any personally-identifiable information.

We also offered some suggestions to facilitate the story-writing process. We suggested participants to include key elements of narrative, such as *when* and *where* the incident took place, the *relationship* between Ash and Val, *what* happened, and *why*. We indicated a good length threshold was having "enough detail so that a reader could understand the story and retell it to someone else." (The story-writing prompt is reproduced, along with all materials, in the online repository linked at the end of this paper.)

Asking for narratives of past events is a well-established method in many disciplines, including HCI and security. The approach we took can be understood as an application of the Critical Incident Technique (CIT) [13]. Unlike what is common in applications of the CIT, which usually rely on direct first-person accounts, we instead asked for stories. Our intention was to provide more anonymity to participants, muting some of the social desirability bias associated with admitting to unauthorized access [22]. Story-writing methods have also been noted to have the potential to gather qualitative data on sensitive topics more effectively [5].

To recruit participants, we used Prolific. Like the better-known Amazon Mechanical Turk service, Prolific recruits people for online tasks, and mediates their compensation. Prolific, however, was specifically created to recruit participants for online research, and has been found to provide better-quality data [33]. We also believe Prolific treats participants better, imposing compensation minimums and, in our experience, being active in preventing abuse.

Using Prolific's screening questions feature, we were able to only invite participants who had indicated having a prior experience with unauthorized access. Once participants accepted the invitation, they were informed of the researchers' contact information, the purposes of the study, and asked for

consent in our use of their responses for research purposes. Data was collected in two stages. We first collected a set of 35 responses and inspected the stories to verify that our instrument was working as intended. We were satisfied that it did. However, there were many unique stories in the initial set, and we wanted to have as much variation as possible. We thus decided to expand the dataset, with the goal of collecting a total of 100 responses. We ended up collecting 115 responses, but, after inspecting them, we excluded 13 which were either empty, nonsensical or not relevant to the prompt. Our analysis draws from the remaining 102 stories.

Participants whose stories we used identified themselves as female 61 times, and as male 40 times. They reported their ages as 18–24 years in 31 instances, 25–44 in 63 instances, and 45–64 in 8 instances. About 75% of participants were from Europe, and about 25% from the US or Canada. Only three participants were from elsewhere. On average, participants took about nine minutes to complete the task, and the average story was 151 words-long. Participants were compensated at an average hourly rate of £11 (GBP).

We analyzed the data in two steps. First, we engaged in exploratory and descriptive analysis of the qualitative data. We built a codebook, coded all stories, verified inter-rater reliability, and summarized the domains and codes we found. After completing this analysis, we were not entirely satisfied with how our codebook captured the richness of the data. We thus engaged in a second step, which was a thematic analysis (e.g., [39]) of participants' stories. We approached the process of data re-examination mainly through close reading. Since the data was already coded, and thus easy to subset, we could explore latent aspects of participants' experiences from several vantage points. Close reading is an analytical procedure associated with the social sciences and the humanities (for a discussion of humanistic approaches to HCI see [2]). Our process was therefore reflexive. As a result, this analysis cannot be detached from the researchers who were involved in this process.

In the next two sections, we report on each of the two steps of analysis. In the first, we examine *what* happens in incidents of unauthorized access, and, in the second, we examine *how* incidents are represented by participants. More detail on our analysis process is provided at the beginning of each section.

3 UNPACKING INCIDENTS

To explore what happens in incidents of unauthorized access, we encoded essential elements of circumstances described in the stories. We created a codebook, comprising of eight categories of codes, and coded each of the stories.

To build the codebook, one researcher (the first co-author of this paper) inductively created codes from textual evidence in stories. Using this codebook, that researcher, and a second researcher (another co-author), both coded a subset of ten stories. They agreed on 95% of coding decisions (Cohen's κ = 0.90, z-score = 29.2, $p < 0.001$), indicating the coding was reliable. In the process of reaching consensus, we found most disagreements were lapses in code assignment by researchers. We resolved the remaining disagreements by disambiguating some code descriptions. The first researcher then re-coded all stories. Because inter-rater agreement had very little room to improve, we found it unnecessary to repeat the process of parallel rating and consensus.

In the codebook, we formulated code categories as questions about stories, such as *What was the primary motivation for unauthorized access?*; and formulated codes as possible answers, such as *Val wants to play a prank on Ash.* In six of the eight categories, questions called for classification, so we assigned, at most, one code per story. In the remaining two categories, questions called for enumeration, so we assigned as many codes as applicable. Categories are therefore dimensions of stories, and codes describe the variation within these dimensions. Story 54 of 102 was the last in which a new code appeared, indicating that the number of stories we collected was almost double what was needed to capture the variation in the dimensions we found.

The dimensions we captured describe a narrative chain, including the context in which incidents happened, the course of events, and the consequences. To capture context, we classified the **types of relationship** between Ash and Val, and Val's primary **motivation**. To capture the course of events, we classified how **opportunities** for access came about, how Val overcame the **lock** if it was set up, and enumerated Val's **actions** once they obtained access. Finally, to capture consequences, we classified whether and how Ash became **aware** of their device being accessed, enumerated expressions of **emotional aftermath** experienced by either party, and classified whether relationships **ended**. We next describe the codes we found.

The context leading up to incidents

Type of relationship. We classified relationships between parties into five types: **intimate partners**, **friends**, **family** members (who are not intimate partners), **co-workers** (who are not also friends), and **acquaintances**. In the online survey, we prompted participants to write about incidents involving them and "someone they knew", without suggesting relationship types. The stories therefore reflect those relationships that participants judged to be non-strangers. We also suggested for participants to describe the nature of the relationship in their story. In all but 9 stories, participants provided enough evidence for us to classify relationships. **Figure 1.A** shows the relative frequency of relationship types we identified. Two of the codes are outliers: acquaintances and co-workers. These outliers were a story

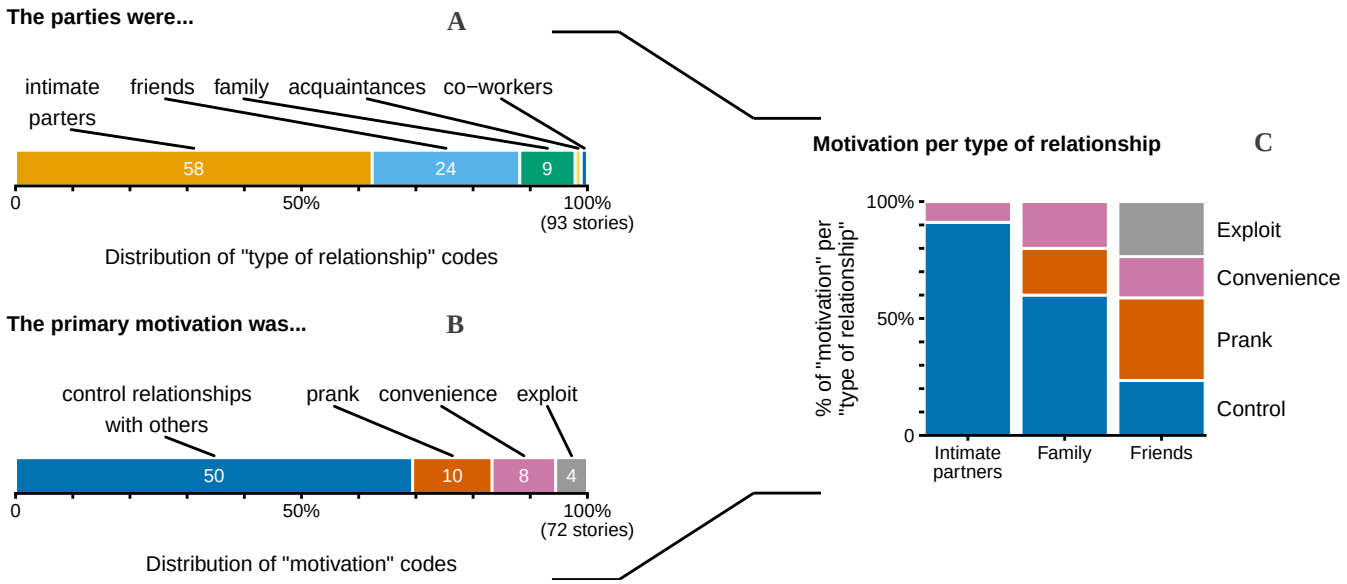

Figure 1: Types of relationships and motivations in stories of unauthorized access to smartphones. (A) Distribution of types of relationships, in the 93 stories with such a code. (B) Distribution of motivations for unauthorized access, in the 72 stories with such a code. (C) Relative frequency of motivation codes for subsets of the data described by the relationship codes, in the 67 stories in which we assigned both codes.

describing an attempt at unauthorized access by a co-worker, who was ultimately unable to unlock the device; and a story in which someone, by accident, accessed an acquaintance's smartphone of equal make and model to theirs. Despite these unique relationship types, we included these stories as they add diversity to our data.

Participants more often conveyed incidents involving people in an inner circle of close relationships. The outliers corresponded with the more distant types of relationships - acquaintances and co-workers. Even within the more common types of relationships in the data, upon closer inspection, we found patterns suggesting that most stories were associated with close relationships. In the case of the largest type, intimate relationships, most stories described established relationships. Stories signaled the non-transient nature of relationships with a combination of markers, including commitment labels (e.g., "married", "couple", "in a relationship"), indication of duration (e.g., "long-term relationship", "together for three years"), or reference to having children. We found the same pattern in stories describing incidents between friends: in most cases the relationships were qualified with markers of closeness (e.g., "best friends", "longtime friends", "childhood friends", "real friends"), or with reference to co-habitation. Relationships we coded as "family" only included very close ties: six parent-child relationships; two sibling relationships, and one pibling-child relationship.

How can this pattern be explained? One possibility is that our sample represents a larger reality. In particular, the repetition of the pattern within subsets of data is consistent with unauthorized physical access being more prevalent in close relationships. Our data is also consistent with previous observations that social proximity is associated with physical proximity, offering more opportunities for unauthorized access; and that socially-close people could be specially motivated to obtain access (e.g., [22, 23, 25, 28]). However, the pattern can also be an artifact of our sample. Ours was a small, convenience sample, and the study was not designed to make quantitative generalizations. Another possible explanation for the pattern is that participants chose to recount the incidents that were significant to them. Our sense is that incidents involving people from an "inner circle" often carried a heavy emotional toll. Possibly, this made them easier to recall and reflect upon.

Motivation. We found four types of motivation for unauthorized access: to seek **control** over Ash's relationships with others, to pull a **prank** on Ash, to use some of the device's functionality for **convenience**, or to **exploit** access for personal (e.g., financial) gain. While we suggested participants to describe the motive for device access, we were not able to classify motivation in 30 stories. **Figure 1.B** shows the relative frequency of motivation types we could identify from evidence in the text. Notably, in about two thirds of cases, unauthorized access was control-motivated.

The **control** code covered a wide range of incidents. We used a definition of seeking control which encompassed both surveillance and interference: "Val wants to learn about, or influence, Ash's relationships with other people". The code was initially based on Stark's *coercive control* framework of intimate partner abuse [38], which constructs controlling behaviors, rather than episodes of violence, as markers of abuse. This framework has been previously used in investigating technology-mediated abuse between intimate partners [41]. In our data, controlling behaviors were abundant. Many stories featured incidents between intimate partners, in which one party sought to verify compliance with expectations of monogamy, and sometimes punish perceived infractions. However, since the code definition was merely descriptive of an intent, it also applied to other stories. For instance, there were stories describing incidents in which friends, or family members like parents, sought knowledge or influence over relationships with third parties. In some cases, stories indicated that the parties ultimately perceived these behaviors to be benign, even among intimate partners.

The codes **prank** and **convenience** mirror findings of a previous study of motivations for access to Facebook accounts [40]. As in that study, we used these codes for stories featuring individuals seeking access to play pranks, or to use some of the device's functionality for practical purposes. Of the stories in which we could classify a motive, around one quarter were pranks or convenience-motivated access. The existence of such stories with non-malicious intent, suggests that participants understood the story writing task as encompassing any experiences they thought relevant.

We only classified four stories with the **exploit** code. The four stories are, however, unique: they portray a range of ways in which stealing of valued possessions — a concern often more associated with strangers (e.g., [28]) — is sometimes sought by individuals known to each other. Three of those stories describe people exploiting unauthorized access to benefit financially — in one story by stealing a device, in another by stealing business contacts, and in the third by transferring currency out of a digital account. In the remaining story unauthorized access was a means to steal sexualized media.

The stories participants provided indicate a connection between the relationship type and the motivations for unauthorized access. **Figure 1.C** shows the proportion of classified motivations in relation to the relationship type (excluding the two outliers). We found just two motivation types in stories involving intimate partners: convenience, and control. However, control-motivated unauthorized access was overwhelmingly prevalent. Among family members, the control motive was also prevalent, but playing pranks or convenience were also typical. Among friends, we found all four types of motivation. Exploitation for personal gain occurred exclusively among friends.

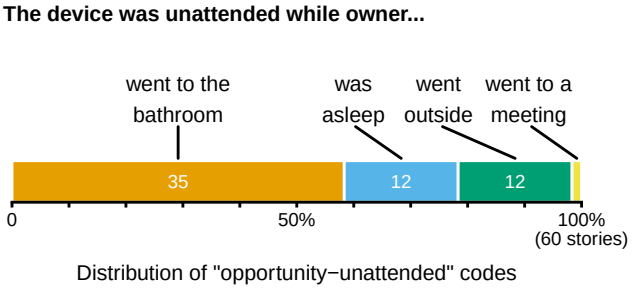

Figure 2: Distribution of circumstances in which devices were accessed while unattended, in stories of unauthorized access to smartphones. Limited to 60 stories in which there was detail about the circumstances, out of 82 stories in which unattended devices were accessed.

The stories also indicate that people access smartphones without permission for many reasons. Some, such as stealing money or data, are clearly nefarious. Some, such as playing pranks or accessing a device for convenience, lean towards being benign. Control-motivated access was, however, often more difficult for us to judge as to its nefariousness. Participants, as prompted, most often described distinct episodes of unauthorized access, not sustained patterns of behavior which could be markers of abusive relationships. Furthermore, equal behaviors can be considered acceptable or not by parties depending on context [6]. In exceptional cases, however, participants did describe what was unequivocally abuse. In our data, these cases appeared predominantly in stories in which parties were not intimate partners at the time of the incident. For instance, in one story, they had "just ended their relationship", yet Val, after accessing Ash's device, turned verbally abusive and threatening; and, in another, Val is described as aspiring to an intimate relationship, but the perception of rejection leads to bullying and harassment. A more rigorous examination of these matters can be found in the growing body of literature on the role of technology in intimate partner abuse [6, 9, 14, 24, 41].

The data we collected thus lends support to prior observations that unauthorized access can be a component of intimate partner abuse, but indicates a wider range of relationships, and relationship states, in which unauthorized access occurs.

How events unfolded

Opportunity. We classified how opportunities for unauthorized access came about with three codes, referring to situations in which devices were left **unattended**; situations in which access was obtained through **secondary devices** (i.e., not Ash's current smartphone); and situations in which the

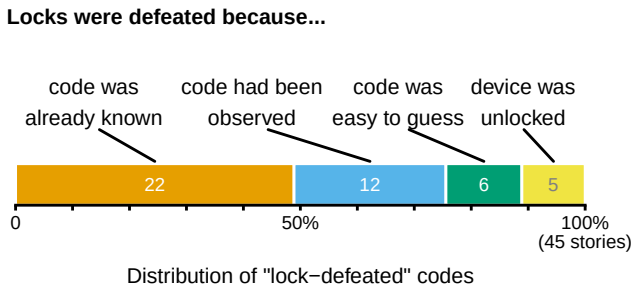

Figure 3: Distribution of ways in which locks were defeated despite being set up, in stories of unauthorized access to smartphones. Limited to 45 stories in which there was enough detail about how locks were defeated. In 16 other cases, locks had not been set up.

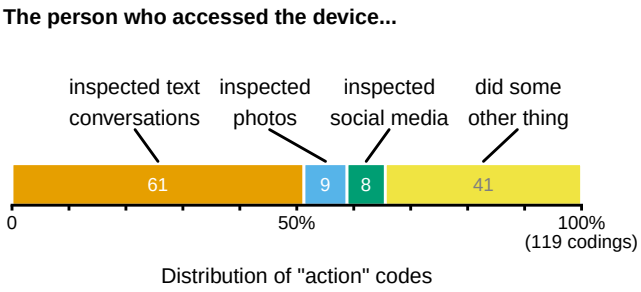

Figure 4: Distribution of the most common types of actions during unauthorized access to smartphones in our stories. We only show the three types of actions which occurred in more than five stories.

person accessing the device used **deception**. Having had suggested that participants provided details about how one person was "able to get access" to the other's device, we were able to classify opportunity in 85 stories from explicit evidence. Overwhelmingly, stories indicated that, when devices were accessed, they had been left unattended (82 cases). We saw few stories with unauthorized access through secondary devices (2 cases) or through deception (1 case). The secondary devices mentioned in the stories were a tablet that was synced with a primary smartphone, and a smartphone that had not been reset after the owner started using a new one. The one case of deception refers to a story in which a person asked for access to "check something on the internet" and then accessed a social media account. Although these stories were outliers, we found that they provided diversity and mostly matched what was asked of participants.

When there was enough detail in the stories, we further classified cases of devices being left unattended into four notable sets of circumstances. **Figure 2** shows the relative proportion of occurrences of these cases. Stories commonly indicated devices had been left unattended while their owners went to the **bathroom** (for instance, to take a shower); while they were **asleep**; and while they went **outside** of their homes (for instance, for shopping or going to class). We found one case of a device being left unattended at work, while the owner was attending a **meeting**. Noticeably, in all these circumstances, devices had been left unattended in locations often deemed trusted by some security software, such as homes or workplaces. For instance, Android's Smart Lock [1] actively suggests users add their home's location to a set of trusted places where unlocking is required less often.

Locks. We found that a considerable number of stories referenced smartphone locks. In 61 stories, we found references to either **locks not being set up** (16 cases), or to **people overcoming locks** that were set up (45 cases). We encountered four notable ways in which locks, despite being set up, were ineffective in preventing unauthorized access. **Figure 3** shows the relative proportion of occurrences of these cases. Most commonly, stories indicated that authentication **codes were already known**, for instance because they had been willingly shared previously. Sharing smartphone authentication secrets is a common behavior in interpersonal relationships (e.g., [7, 10, 17, 23]). In other cases, authentication **codes were discovered through visual observation**. Visual observation, or "shoulder-surfing", is another well-documented vector for unauthorized physical access (e.g., [11, 17]). We also found stories in which characters were described as having **guessed authentication codes**; and stories in which **locks were set up but not active at the time** of unauthorized access, for instance because devices were not inactive long enough to lock.

Participants seemed to perceive smartphone locks as a key element in preventing unauthorized access. We prompted participants to include information about how Val was "able to get access", but did not reference locks. The fact that stories provide such level of detail on locks suggests that participants considered them to be relevant for preventing access by known people, as previous work has documented (e.g., [7, 10]). Our data does not contradict that, absent smartphone locks, unauthorized access by known people would be even more common. In fact, upon closer inspection, we found five stories in which Ash counteracts the possibility of future incidents by setting up a lock or changing the authentication code. In these five stories, either the motivation for the incident had been to play a prank, or Ash was defending the device against family members. Changing of locks was not mentioned in other stories possibly because it was not seen as an effective strategy in other circumstances.

Actions. For each story, we enumerated the actions performed by the person accessing the device. We categorized

actions into four types: **gathering information** by visual inspection, **tampering** with devices by making changes to their state which are not easily observable, **impersonating** the device owner, and **exfiltrating** data. When stories provided enough detail, we further categorized actions by their object. After combining objects of actions with types of action, we ended up with 21 codes. We had suggested that participants included details about what active parties did after obtaining access and, in all but 11 stories, we found direct evidence to attribute at least one code.

Figure 4 shows the types of action we found to occur more than five times. Most commonly, we found stories to provide evidence of information gathering (77/102 stories). The most common object of information gathering we found was **text-based conversations**, such as text messages, instant messages, or emails. Inspection of text-based conversations was so prevalent that it appeared in the majority of stories (61/102), and the code was attributed about as many times as all the remaining 20 codes combined (61/119 code attributions). The only two other codes that we attributed more than five times also concerned information gathering. We found nine stories describing inspection of **media files** such as photos; and eight stories describing inspection **social media activity** other than conversations (e.g., posts). Occurring with less frequency, we found stories indicating the person who accessed the device inspected notifications, contacts, call logs, internet history, apps installed, and calendars. The diversity of objects of information gathering that we encountered largely coincides with types of data smartphones users have described as sensitive in prior research (e.g., [4, 12, 15, 18, 19, 25, 27, 28]). Previous research has also called attention to smartphones having a particular status as to their sensitivity (e.g., [8, 9]). Part of the reason may be a combination of smartphones being more heavily used for personal communication than other devices (e.g., see [26]), and users valuing personal communications more than other digital assets (e.g., see [28, 36]). With the caveat that our sample may not be representative, some of the data users deem as most sensitive, seems to coincide with the data most targeted for inspection by non-strangers.

Although less frequently, we also found several instances of tampering, impersonation, and exfiltration of data. Stories described tampering with devices by changing settings, changing contact records, deleting contents, installing spyware, and capturing new photos; they described impersonation in social media, in text-based conversations, and in financial services; and they described exfiltration of photos, records of conversations, and contacts. Similar behaviors have been previously observed, for instance, in studies of the role of technology in intimate partner abuse (e.g., see [6, 9, 41]). However, in the stories we collected, tampering, impersonation, and exfiltration were not always associated with control-motivated unauthorized access between intimate partners. We found instances of tampering in prank- or convenience-motivated incidents; instances of impersonation in prank- and exploit-motivated incidents; and instances of exfiltration in exploit-motivated incidents. This diversity is consistent with our earlier observation that behaviors associated with intimate partner abuse also occur in a wider spectrum of circumstances.

Consequences

Awareness. We suggested participants included detail on how, if at all, the person whose phone was accessed learned about it. In 22 stories, we found there was evidence indicating that people did not become aware of their phones being accessed; and in 61, that they did become aware. We further classified how people became aware, and found stories to describe three ways: by finding clues leading to a suspicion of unauthorized access, such as unusual device behaviors, or things said by the other person (25 stories); by unprompted own admission, for instance, by confronting the device owner (20 stories); or by encountering another in the act of accessing the device (16 stories).

Emotional aftermath. We also suggested that participants included details about "any consequences". From the evidence provided in stories, we enumerated expressions of positive or negative sentiments resulting from incidents of unauthorized access. Positive sentiments included amusement, satisfaction, or relief; negative sentiments included annoyance, anger, guilt, humiliation, pain, regret, sadness, or shame. We found negative sentiment to be expressed more often. Negative sentiments were expressed in 36 stories; while positive sentiments were expressed in 9.

Relationship termination. A consequence in some stories was the ending of relationships. Many stories did not provide enough direct evidence to classify them. In those that did, we found 21 stories indicated relationships had ended at least in part due to incidents of unauthorized access, and 25 stories indicating relationships had persisted.

In comparison to codes describing the context of incidents or the course of action, we found the codes for consequences to provide much less insight into participants' experiences. Participants often emphasized how consequential incidents of unauthorized access had been their lives. However, we could not capture that richness with a coding process that required direct and unambiguous evidence in the text of stories. Stories indicated an array of consequences that could not be captured by relationships having ended or not, nor by sentiments being explicitly positive or negative. There were relationships which did not end, but their persistence was painful. There were relationships which ended, but were

eventually mended and made stronger. Participants sometimes described reactions to incidents which implied strong emotional states, but did not describe precise sentiments — the reactions spoke for themselves.

The qualitative analysis we started with, and described in this section, was informative in important aspects of participants ' experiences, but was insufficient to capture consequences. To address this limitation, we engaged in a second, more reflexive, type of analysis, which we discuss next.

4 MAKING SENSE OF UNAUTHORIZED ACCESS

To offer a more rigorous account of participants' experiences with unauthorized access, we turned to thematic analysis. The codes we used in the previous section, based on direct assertions in the text, are *semantic codes*. Semantic codes are believed to be unsuitable for capturing latent meanings in qualitative data [39]. Our data called for a more reflexive approach.

To understand how participants made sense of their experiences, we turned our attention to *how* they described them. We developed two themes to capture key aspects of participants' experiences — trust as performative vulnerability, and self-serving sensemaking.

Our process for developing these themes was inductive. We re-engaged with the data in multiple rounds of close reading. In each round, we used categories of semantic codes as lenses to look at the data. For instance, in the first round, we used the lenses from the *relationship type* code category, and closely read all stories with a focus on how relationships are represented, and how these relate to how incidents are experienced. In this process, we marked-up text, drafted thematic maps, collected quotes, and articulated patterns in written notes. Gradually, we distilled our analysis into two organizing themes which, to our satisfaction, conveyed what was missing in our code-based analysis.

We next lay out these two themes. We lightly edited the quotes to make them easier to read, and to elide gender or other information that could de-anonymize the stories. The names of characters in quotes follow the convention we suggested to participants: **Ash** refers to the owner of the device, and **Val** refers to the person who accessed Ash's device without permission.

Trust as performative vulnerability

Central to participant's experiences of unauthorized access was seeing expectations of trust, which they believed were binding, being violated. Many stories conveyed a belief that mutual trust was not only desirable, but necessary to maintain relationships. However, to maintain trustworthiness, participants had to make themselves vulnerable to violations. This rationale is vividly illustrated in two of the stories of control-motivated unauthorized access among intimate partners, told from opposing perspectives:

> "Ash had nothing to hide but feared not being trusted if they kept their phone with them at all times" – S43

> "Val was suspicious. Ash would take their smartphone everywhere including when they were showering. Ash would turn their smartphone off if they had to leave it in a room with Val." – S75

In these stories, Ash not displaying vulnerability was detrimental to their trustworthiness, which was reciprocated by Val accessing Ash's smartphone without permission. Participants' representation of trust evoked other conceptions of trust rooted in vulnerability. In a review of trust development, Lewicki et al. distinguish a "psychological tradition", wherein trust is understood as one's willingness to accept vulnerability, conditioned on positive (or at least neutral) expectations of another's conduct [21]. Trust as a marker of relationship health also frequently comes up in empirical work on privacy and security attitudes towards known people (e.g., [23, 25, 32]). For instance, a recent study of account sharing among intimate partners found that one common explanation for sharing was a feeling that trust was necessary in relationships [32]. However, in the stories we collected, it was not enough to be vulnerable. People had to overtly display vulnerability, by very visibly taking on risks. Performatively taking on risks could mean not visibly engage in risk-averting behaviors, such as in the case of S43. The alternative, of engaging in risk-averting behaviors, such as in the case of S75, could have interpreted as meaning Ash was not trustworthy, which in turn revealed that the relationship was in peril.

The corollary to this conception of trust it that unauthorized access by someone close is not experienced as a security problem. Security problems could perhaps be fixed with stricter security regimens. Instead, the prevailing experience of unauthorized access was one of breach of trust, and hence existentially consequential to relationships. Participants' perceptions were that when the vulnerability they displayed was abused, changing a lock code was hardly a solution – instead, there *had* to be consequences for the relationship. This imperative is sometimes represented as a lack of rationale for the consequences, such as in these examples:

> "Ash discovered what had been done to their phone from unusual battery consumption. It was the end of their relationship." – S1

> "Ash found out about what Val did by new apps being open, and the phone being in a different place. Consequentially, Ash and Val are no longer roommates, and do no longer talk." – S45

In both stories, device owners terminated relationships immediately upon finding out that their devices had been accessed. Notably, the narrator does not find it necessary to articulate a rationale. The causal link was so obvious to them that including it in the story would indicate a choice, when there was none.

Through the same mechanics, unauthorized access could also benefit relationships. When displays of vulnerability were reciprocated with actions perceived by owners as not violating expectations, and instead being benign, relationships were strengthened. We saw that pattern in some episodes among intimate partners, in which the person accessing the phone used it to for practical tasks: for instance, in story 12, where the phone is accessed while the owner is showering to facilitate planning a gathering with other people; or in story 44, where the phone is accessed to check the calendar for an open date for a surprise party. We also saw that pattern in some of the stories describing pranks. As long as an invisible line was not crossed, pranks served to build rapport. Whether in stories of beneficial access or pranks, these episodes are portrayed as illustrations of well-functioning relationships.

In most of our data, displaying vulnerability, by taking risks with unauthorized access, seemed to be more of a choice than an obligation. That is not always the case. Research on technology-mediated intimate partner abuse has noted that taking such risks is often needed for personal safety (e.g., [24, 41]). Research on privacy-enhancing practices in non-Western geographies also indicates there are expectations of openness affecting women, which make taking risks more of an obligation [35]. Taking the patterns we saw in our data, and considering other accounts of risk-taking, the reasons for displaying vulnerability can be understood as existing in a spectrum. To what extent risk-taking is a choice or an obligation may be unclear, both to us and to those conveying their experiences. Nonetheless, it seems clear that displaying vulnerability is ultimately a need.

Self-serving sensemaking

Stories conveyed a stark pattern of attribution: when told from Ash's perspective, they blamed Val's intrinsic traits; when told from Val's perspective, they blamed the situation. With very few exceptions, stories were charitable to the narrator.

When told from Ash's perspective, strong statements assigning negative character traits to Val were common. A commonly assigned negative trait was being "jealous"; other related character flaws included:

> "[being] the controlling type" – S2
>
> "[being] quite possessive" – S5
>
> "[being] a lunatic" – S69
>
> "[having a] mind [which] works in a suspicious manner" – S40

When stories were told from Val's perspective, situational factors were invoked. Commonly, anomalous events, or a change in behavior, were portrayed as valid justifications for unauthorized access, such as in these examples:

> "Ash's smartphone received a notification from a person Val did not like" – S51
>
> "Val caught Ash in their bedroom talking on the phone at 3AM" – S53
>
> "Val was worried because Ash received many texts in the last days" – S101
>
> "Val started to think about how Ash had seemed distant lately" – S37
>
> "They had been arguing more and more" – S47

The pattern of self-serving attribution, and the fact that it is so pronounced, indicates that incidents were experienced as significant episodes. Similar patterns of self-serving attribution have been found, for instance, when people describe experiences of being angered by someone they know, versus angering others (e.g., [3, 20, 42]). In our data, the pattern of attribution is also consistent. Although it is most pronounced in stories of control-motivated intrusions, we saw it in many kinds of stories. For instance, in stories about pranks, expressions of negative emotional consequences were concentrated in stories told from the perspective of the target of the prank. In stories told from the perspective of parents accessing their children's phones, the parent's actions are almost always represented as arising from an obligation to carry out protective responsibilities. Only in the one story told from the perspective of the child is that justification called into question: the parent is called out for meddling in private affairs.

Participants also described forgiving transgressions, and mending their relationships. Previous research suggests that forgiveness is associated with a reduction in self-serving attributions [42]. We found an echo of that phenomenon in our participants' sensemaking. When stories were told from Ash's perspective, but relationships survived violations of trust, stories tended to not associate negative traits with Val. One common way to minimize incidents was to note that the relationship was still nascent. Another strategy was to normalize access to devices as part of trust display, as in story 93:

> "Ash was a little hurt at the lack of trust but decided to forgive Val quickly. Ash now tries to let Val be more involved in Ash's smartphone activity so Val doesn't feel so anxious."

Similarly, when stories were told from Val's point of view and there were no long-term repercussions to the episode,

situational explanations were muted. However, stories also avoided assigning strong negative traits to the Val. To reconcile the lack of either situational or character explanations, stories typically expressed that unauthorized access had not been motivated by nefarious reasons, just "curiosity". Constructing Val as "nosey" (S6), "intrigued" (S35), or acting out of "boredom" (S64) avoided further self-reflection.

The few exceptions to self-serving attributions were also insightful. It was in these stories that we found most self-reflection on the narrator's own shortcomings, such as in the following stories:

> "I'm terribly ashamed. Ash didn't do anything to justify my mistrust. My last partner did and it has made me paranoid. I feel horrible now for doing it because it was a total invasion of Ash's privacy, and it was utterly unwarranted. The only reason I would now tell Ash would be to alleviate my own conscience. So I'm not saying anything, I'm forcing myself to feel the guilt and the pain." – S20

> "In reality, Val was experiencing some low self-esteem issues. Val wasn't aware of it until now. It was a hard journey to learn this fact." – S37

When there was self-reflection, the significance of incidents of unauthorized access came into full display. For those who had accessed smartphones without permission, the emotional toll of dealing with their actions could be substantial. Recognizing that they had violated expectations of trust also meant that they had put the relationship at peril.

The existence of a pattern of attribution suggests a possible fragility in our data collection method. We had asked participants to provide anonymous stories and, yet, we could often discern which story character the participants identified with. Since participants experienced incidents from a particular perspective, the narrator's description could only provide insight from that perspective. With the benefit of hindsight, we cannot exclude that we could have collected richer accounts had we asked for direct first-person descriptions of incidents instead of stories. However, offering at least some plausible deniability is expected to have had an effect on how forthcoming the participants felt they could be in their writing. Furthermore, asking for stories, it seemed to us, encouraged participants not only to describe, but to also reflect on their experiences.

5 IMPLICATIONS FOR COMPUTER SECURITY

Our analysis can inform the design and implementation of techniques and processes to prevent unauthorized access to personal devices by non-strangers.

Knowing what happens in incidents of unauthorized access can inform threat models. Security, or lack thereof, can only be defined in relation to the threats. Previous research has indicated, and ours corroborates, that non-strangers should be considered part of any reasonable threat model for unauthorized physical access [14, 22, 28, 40]. Some researchers have developed tentative threat models for personal devices, encompassing threats posed by non-strangers in general [28], or more specifically to model threats posed by abusers of their intimate partners [14]. Our analysis can add realistic detail to these models. For instance, using some of the most prevalent codes in our data, we could define a *shower time attack*, in which an individual, having previously gained knowledge of their intimate partner's authentication code, accesses their smartphone while they are in the shower, and inspects communications with third parties. Such a scenario could be useful for making a number of security design decisions: it could inform whether to consider users' homes as safe locations, or how much technical know-how an adversary would need, or how little time would be needed for a successful intrusion, or the kind of data that an adversary would likely target.

Addressing the role of trust. Our data suggests that people in close relationships overtly display vulnerability to intrusions to signal trust. The implication is that, to display trust, people may act in ways that negate the effectiveness of any countermeasures designed to mitigate unauthorized access. Our analysis corroborates previous findings that smartphone locks are often ineffective in preventing unauthorized access by people who are close, for example, because authentication codes are shared in displays of trust (e.g., [7, 10, 23]). In the stories, we also found some instances of unauthorized access to devices that had fingerprint authentication, since users added fingerprints of close people to signal trust, or shared fallback authentication codes. We predict that, as people increasingly adopt biometric authentication, these behaviors will become more noticeable. Other research has also shed light on similar behaviors that negate the effectiveness of other technologies. For instance, having close people use guest accounts is often regarded as inappropriate, since it signals mistrust [18, 19, 25]. These prior observations, we believe, can be explained by the conception of trust we observed in the stories. We cannot, however, make immediate recommendations for how to design security technologies that can accommodate people's need to signal trust. A good starting point may be to, in the process of design, ask the question: how will this artifact be used to signal trust?

6 LIMITATIONS

The methods we employed to address the question we set out to answer have some limitations. We next highlight two major limitations. First, we asked participants to remember

and write about past experiences. The experiences we collected are thus not a representative sample of experiences participants had, but of experiences which were salient to them. Furthermore, the set of participants who chose to take part in our study is also not a representative sample of a larger population. Second, by approaching our analysis qualitatively, our findings are explicitly imbued with our frames of reference. Our combined backgrounds, previous knowledge, styles, and other factors, permeate every aspect of this research, from how we designed a data collection instrument, to how we built the codebook, to how we explored semantic codes, and to how we selected cross-cutting themes.

7 CONCLUSION

Modern smartphone ownership requires continual negotiation of trust boundaries with those who surround us, such as our family and friends. Although unauthorized access to smartphones by those close to us is not unusual, it has received little research notice.

In this paper, we collected and analyzed 102 anonymous stories to understand what happens when people access the smartphones of those closest to them. We described the salient features of these incidents, and explored how people make sense of their experiences. Our analysis portrays these incidents as personally significant experiences, sometimes with severe consequences, and deeply entwined with interpersonal trust arrangements. We also discuss what these findings may mean for computer security.

This work contributes to the literature in several ways. We provide finer-grained details on the diversity of circumstances involved in incidents of unauthorized access. We advance a framework to reason about how people's conceptions of interpersonal trust interact with security practices and user-facing security technologies. And, we observed how self-serving rationalizations from participants can offer a window into sensitive topics related to security.

We find it difficult, however, to speculate on ways to reduce or prevent unauthorized access by non-strangers. We set out to address the question of *how people experience incidents*, remaining as much as possible neutral on whether these incidents should be seen as threats worth confronting. The insights we gathered can nevertheless help designers of security technologies to create defenses and anticipating potential outcomes of their adoption. Particularly useful, we think, is our prediction that, whenever possible, people will subvert access controls to signal trust to those who are close to them. We encourage usable security researchers to test this prediction on new security technologies that are being increasingly adopted, such as biometric authentication, two-factor authentication tokens, and password managers.

Palen & Dourish [31] argue that when issues of security are discussed, the specter of sinister outside forces — thieves, or a Big Brother — finds a level of prominence that is not reflective of people's experiences. In their words, *"it is interpersonal privacy matters that figure primarily in decisions about technology use on an everyday basis"*. The experiences we attempt to understand are "mundane", but they are significant and sometimes life-changing, to those involved. The personal significance of the experiences cannot be detached from people's relationships with their smartphones. Personal mobile devices can be understood as extensions of self [29, 37], and, by some accounts, as bodily appendages [30].

Much remains to be learned about these incidents and their impact on users. We hope that our study stimulates further empirical research in this domain, as well as new security mechanisms that can improve people's daily negotiations of security and privacy with those who surround them.

REPLICATION

Materials, codebook, analysis scripts, and code frequency data, available at https://osf.io/mwuc8.

ACKNOWLEDGMENTS

This work was supported by FCT - Fundação para a Ciência e a Tecnologia, I.P., through a PhD studentship (SFRH/BD/-98527/2013), and funding of project mIDR (AAC 02/SAICT/-2017, project 30347, cofunded by COMPETE/FEDER/FNR), and of the LASIGE Research Unit (UID/CEC/00408/2013). We thank anonymous reviewers for their suggestions, and study participants for kindly sharing their stories.

REFERENCES

[1] Android Help [n. d.]. Set your Android device to automatically unlock. Retrieved Sep. 1, 2018 from https://support.google.com/android/answer/9075927

[2] Jeffrey Bardzell and Shaowen Bardzell. 2016. Humanistic HCI. *interactions* 23, 2 (Feb. 2016), 20–29. https://doi.org/10.1145/2888576

[3] Roy F. Baumeister, Arlene Stillwell, and Sara R. Wotman. 1990. Victim and perpetrator accounts of interpersonal conflict: Autobiographical narratives about anger. *Journal of Personality and Social Psychology* 59, 5 (1990), 994–1005. https://doi.org/10.1037/0022-3514.59.5.994

[4] Noam Ben-Asher, Niklas Kirschnick, Hanul Sieger, Joachim Meyer, Asaf Ben-Oved, and Sebastian Möller. 2011. On the Need for Different Security Methods on Mobile Phones. In *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services - MobileHCI '11*. ACM, New York, 465–473. https://doi.org/10.1145/2037373.2037442

[5] Virginia Braun, Victoria Clarke, Nikki Hayfield, Naomi Moller, and Irmgard Tischner. 2017. Qualitative Story Completion. In *Handbook of Research Methods in Health Social Sciences*. Springer, Singapore, 1–18. https://doi.org/10.1007/978-981-10-2779-6_14-1

[6] Sloane C. Burke, Michele Wallen, Karen Vail-Smith, and David Knox. 2011. Using technology to control intimate partners: An exploratory study of college undergraduates. *Computers in Human Behavior* 27, 3 (2011), 1162–1167. https://doi.org/10.1016/j.chb.2010.12.010

[7] Ivan Cherapau, Ildar Muslukhov, Nalin Asanka, and Konstantin Beznosov. 2015. On the Impact of Touch ID on iPhone Passcodes.

In *Proceedings of the Eleventh Symposium On Usable Privacy and Security (SOUPS '15)*. USENIX Association, Berkeley, CA, USA, 257–276. https://www.usenix.org/conference/soups2015/proceedings/presentation/cherapau

[8] Erika Chin, Adrienne Porter Felt, Vyas Sekar, and David Wagner. 2012. Measuring User Confidence in Smartphone Security and Privacy. In *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12)*. ACM, New York, 1–16. https://doi.org/10.1145/2335356.2335358

[9] Jill P. Dimond, Casey Fiesler, and Amy S. Bruckman. 2011. Domestic violence and information communication technologies. *Interacting with Computers* 23, 5 (2011), 413–421. https://doi.org/10.1016/j.intcom.2011.04.006

[10] Serge Egelman, Sakshi Jain, Rebecca S Portnoff, Kerwell Liao, Sunny Consolvo, and David Wagner. 2014. Are You Ready to Lock? Understanding User Motivations for Smartphone Locking Behaviors. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS '14)*. ACM, New York, 750–761. https://doi.org/10.1145/2660267.2660273

[11] Malin Eiband, Mohamed Khamis, Emanuel von Zezschwitz, Heinrich Hussmann, and Florian Alt. 2017. Understanding Shoulder Surfing in the Wild: Stories from Users and Observers. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, 4254–4265. https://doi.org/10.1145/3025453.3025636

[12] Adrienne Porter Felt, Serge Egelman, and David Wagner. 2012. I'Ve Got 99 Problems, but Vibration Ain'T One: A Survey of Smartphone Users' Concerns. In *Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM '12)*. ACM, New York, 33–44. https://doi.org/10.1145/2381934.2381943

[13] John C Flanagan. 1954. The critical incident technique. *Psychological bulletin* 51, 4 (1954), 327. https://www.apa.org/pubs/databases/psycinfo/cit-article.pdf

[14] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, 667–667. https://doi.org/10.1145/3173574.3174241

[15] Alina Hang, Emanuel von Zezschwitz, Alexander De Luca, and Heinrich Hussmann. 2012. Too Much Information!: User Attitudes Towards Smartphone Sharing. In *Proceedings of the 7th Nordic Conference on Human-Computer Interaction (NordiCHI '12)*. ACM, New York, 284–287. https://doi.org/10.1145/2399016.2399061

[16] Marian Harbach, Alexander De Luca, and Serge Egelman. 2016. The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, 4806–4817. https://doi.org/10.1145/2858036.2858267

[17] Marian Harbach, Emanuel von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. 2014. It's a Hard Lock Life: A Field Study of Smartphone (Un)Locking Behavior and Risk Perception. In *Proceedings of the Tenth Symposium On Usable Privacy and Security (SOUPS '14)*. USENIX Association, Berkeley, CA, USA, 213–230. https://www.usenix.org/conference/soups2014/proceedings/presentation/harbach

[18] Eiji Hayashi, Oriana Riva, Karin Strauss, A. J. Bernheim Brush, and Stuart Schechter. 2012. Goldilocks and the Two Mobile Devices: Going Beyond All-or-nothing Access to a Device's Applications. In *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12)*. ACM, New York, 1–11. https://doi.org/10.1145/2335356.2335359

[19] Amy K. Karlson, A.J. Bernheim Brush, and Stuart Schechter. 2009. Can I Borrow Your Phone?: Understanding Concerns when Sharing Mobile Phones. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '09)*. ACM, New York, 1647–1650. https://doi.org/10.1145/1518701.1518953

[20] Jill N. Kearns and Frank D. Fincham. 2005. Victim and Perpetrator Accounts of Interpersonal Transgressions: Self-Serving or Relationship-Serving Biases? *Personality and Social Psychology Bulletin* 31, 3 (2005), 321–333. https://doi.org/10.1177/0146167204271594

[21] Roy J. Lewicki, Edward C. Tomlinson, and Nicole Gillespie. 2006. Models of Interpersonal Trust Development: Theoretical Approaches, Empirical Evidence, and Future Directions. *Journal of Management* 32, 6 (2006), 991–1022. https://doi.org/10.1177/0149206306294405

[22] Diogo Marques, Ildar Muslukhov, Tiago Guerreiro, Luís Carriço, and Konstantin Beznosov. 2016. Snooping on Mobile Phones: Prevalence and Trends. In *Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS '16)*. USENIX Association, Berkeley, CA, USA, 159–174. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/marques

[23] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. 2016. "She'l 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 (CHI '16)*. ACM, New York, 5921–5932. https://doi.org/10.1145/2858036.2858051

[24] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F. Churchill, and Sunny Consolvo. 2017. Stories from Survivors: Privacy & Security Practices when Coping with Intimate Partner Abuse. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, 2189–2201. https://doi.org/10.1145/3025453.3025875

[25] Michelle L. Mazurek, J. P. Arsenault, Joanna Bresee, Nitin Gupta, Iulia Ion, Christina Johns, Daniel Lee, Yuan Liang, Jenny Olsen, Brandon Salmon, Richard Shay, Kami Vaniea, Lujo Bauer, Lorrie Faith Cranor, Gregory R. Ganger, and Michael K. Reiter. 2010. Access Control for Home Data Sharing: Attitudes, Needs and Practices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. ACM, New York, 645–654. https://doi.org/10.1145/1753326.1753421

[26] Hendrik Müller, Jennifer L. Gove, John S. Webb, and Aaron Cheang. 2015. Understanding and Comparing Smartphone and Tablet Use: Insights from a Large-Scale Diary Study. In *Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction (OzCHI '15)*. ACM, New York, 427–436. https://doi.org/10.1145/2838739.2838748

[27] Ildar Muslukhov, Yazan Boshmaf, Cynthia Kuo, Jonathan Lester, and Konstantin Beznosov. 2012. Understanding Users' Requirements for Data Protection in Smartphones. In *IEEE 28th International Conference on Data Engineering Workshops (ICDEW 2012)*. IEEE, New York, 228–235. https://doi.org/10.1109/ICDEW.2012.83

[28] Ildar Muslukhov, Yazan Boshmaf, Cynthia Kuo, Jonathan Lester, and Konstantin Beznosov. 2013. Know Your Enemy: The Risk of Unauthorized Access in Smartphones by Insiders. In *Proceedings of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services (MobileHCI '13)*. ACM, New York, 271–280. https://doi.org/10.1145/2493190.2493223

[29] Dawn Nafus and Karina Tracey. 2002. Mobile phone consumption and concepts of personhood. In *Perpetual Contact: Mobile Communication, Private Talk, Public Performance*, James E. Katz and Mark Aakhus (Eds.). Cambridge University Press, Cambridge, UK, 206–222. https://doi.org/10.1017/CBO9780511489471.016

[30] Virpi Oksman and Pirio Rautianen. 2003. "Perhaps it is a Body Part": How the Mobile Phone Became an Organic Part of the Everyday Lives of Finnish Children and Teenagers. In *Machines That Become Us*,

James E. Katz (Ed.). Transaction Publishers, New Brunswick, NJ, USA, 293 – 308.

[31] Leysia Palen and Paul Dourish. 2003. Unpacking "Privacy" for a Networked World. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '03)*. ACM, New York, 129–136. https://doi.org/10.1145/642611.642635

[32] Cheul Young Park, Cori Faklaris, Siyan Zhao, Alex Sciuto, Laura Dabbish, and Jason Hong. 2018. Share and Share Alike? An Exploration of Secure Behaviors in Romantic Relationships. In *Proceedings of the Fourteenth Symposium on Usable Privacy and Security (SOUPS '18)*. USENIX Association, Berkeley, CA, USA, 83–102. https://www.usenix.org/conference/soups2018/presentation/park

[33] Eyal Peer, Laura Brandimarte, Sonam Samat, and Alessandro Acquisti. 2017. Beyond the Turk: Alternative platforms for crowdsourcing behavioral research. *Journal of Experimental Social Psychology* 70 (may 2017), 153–163. https://doi.org/10.1016/j.jesp.2017.01.006

[34] Pew Research Center. 2012. Privacy and Data Management on Mobile Devices. Retrieved Sep. 1, 2018 from http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/

[35] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. 2018. "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)*. USENIX Association, Berkeley, CA, USA, 127–142. https://www.usenix.org/conference/soups2018/presentation/sambasivan

[36] Richard Shay, Iulia Ion, Robert W. Reeder, and Sunny Consolvo. 2014. "My Religious Aunt Asked Why I Was Trying to Sell Her Viagra": Experiences with Account Hijacking. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, 2657–2666. https://doi.org/10.1145/2556288.2557330

[37] Irina Shklovski, Scott D. Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. 2014. Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, 2347–2356. https://doi.org/10.1145/2556288.2557421

[38] Evan Stark. 2007. *Coercive control: The entrapment of women in personal life*. Oxford University Press, New York.

[39] Gareth Terry, Nikki Hayfield, Victoria Clarke, and Virginia Braun. 2017. Thematic Analysis. In *The SAGE Handbook of Qualitative Research in Psychology*. SAGE Publications Ltd, London, UK, 17–36. https://doi.org/10.4135/9781526405555.n2

[40] Wali Ahmed Usmani, Diogo Marques, Ivan Beschastnikh, Konstantin Beznosov, Tiago Guerreiro, and Luís Carriço. 2017. Characterizing Social Insider Attacks on Facebook. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, 3810–3820. https://doi.org/10.1145/3025453.3025901

[41] Delanie Woodlock. 2017. The Abuse of Technology in Domestic Violence and Stalking. *Violence Against Women* 23, 5 (2017), 584–602. https://doi.org/10.1177/1077801216646277

[42] Jeanne S. Zechmeister and Catherine Romero. 2002. Victim and offender accounts of interpersonal conflict: Autobiographical narratives of forgiveness and unforgiveness. *Journal of Personality and Social Psychology* 82, 4 (2002), 675–686. https://doi.org/10.1037/0022-3514.82.4.675