[Slides & transcript of presentation at the ACM CHI Conference on Human Factors in Computing Systems, Galsow, May 2019. Report at https://dl.acm.org/citation.cfm?id=3300819]

I'm going to talk about unauthorized access to smartphones – situations where one person physically picks up a smartphone that isn't theirs without permission, and does something with it.

"In the past 12 months, I've looked through someone else's cell phone without their permission."

Estimates from indirect survey (list experiment), N = 1,381 MTurk sample

■ Yes ☐ No

31%	69%
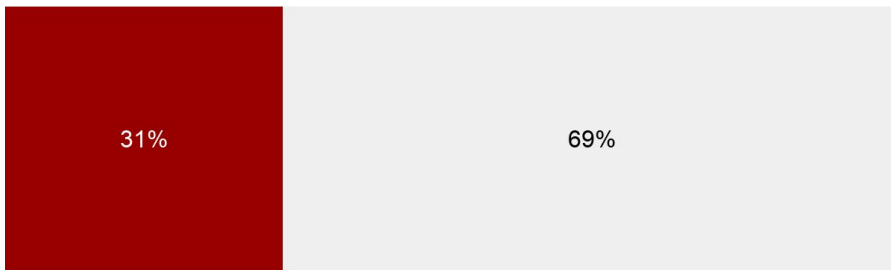
Diogo Marques, Ildar Muslukhov, Tiago Guerreiro, Konstantin Beznosov & Luís Carriço. 2016.
Snooping on Mobile Phones: Prevalence and Trends.
Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS '16).

Smartphones can be highly personal devices. Which means they can also be highly sensitive. One way in which they can be sensitive, is that if someone picks up our smartphone, they have access to the digitized workings of our lives.
And unauthorized access is not unusual.
Me and my collaborators, for instance, have estimated, through a kind of survey designed to assure anonymity, that 31% of participants in a fairly large convenience sample identified with having had "looked through someone else's phone without their permission" in the preceding year.
Smartphones being so sensitive, and unauthorized access so common, it matters who exactly is accessing our smartphones without permission – it matters, for instance, if it's a stranger, or if it's someone who we know. We have been warned about the bad things that can happen if some stranger gets access to our phone. But access by people who we know seemed to us to be a much different experience. And that's the experience that we wanted to examine in this work.

What are incidents of unauthorized access like?

So we set out to answer this question:
What are incidents of unauthorized access like?

What are incidents of unauthorized physical **access** to smartphones involving people known to each other **like?**

Specifically, incidents of unauthorized physical access to smartphones involving people known to each other.
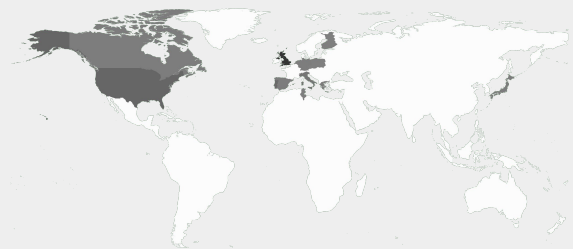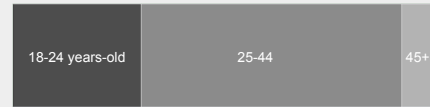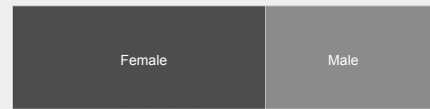We wanted to know: what actually happens? How does it happen? And how do the people involved feel about it?

Approach

Collect accounts of incidents:

- experienced either as smartphone owner or person accessing smartphone
- written as stories

Data: 102 open-text stories collected from Prolific

Participant demographics

To do that, we collected 102 accounts of incidents from participants in study conducted online.

We solicited accounts from participants who had had the experience of someone accessing their smartphone without permission, or the experience of themselves accessing someone else's smartphone without permission.

Because these experiences can be sensitive, we asked participants to write about them as if they were stories. We asked people to use character names instead of their real names, and to use a narrative arc.

We collected the data through Prolific from a reasonably diverse sample. Prolific is a crowdwork service, like Amazon Mechanical Turk, but specifically targeted for online research.

[These & remaining charts, and map, made with ggplot2]

Ash and Val had been dating for about two years, and things were rocky.

Ash seemed distant and uninterested in Val most of the time, which became a large problem in their relationship. Ash progressively became more distant and absent, and Val could hardly stand it.

One night while Ash was fast asleep in their bed, Val decided to look through Ash's phone on the bedside table. Signs of infidelity, possibly from the beginning of their relationship were on the phone. There were text messages with sexually explicit photos and pet names.

Val waited until the morning to mention what was found to Ash. When Ash woke up, the phone was displaying one of the photos and the jig was up. It was obvious that Val had found out what had been going on.

Val had already packed up everything and was ready to leave. Ash never saw Val again.

(P54)

This slide shows the shape of the 102 stories participants provided. Some stories were very short. Some were very long and detailed. The story that's highlighted here is close to the average size. I've changed some personally identifiable information, but the gist of it is that "Ash and Val had been dating" // "One night while Ash was asleep Val decided to look through Ash's phone. There were some compromising text messages and photos. When Ash woke up, the phone was displaying one of the photos and the jig was up. Ash never saw Val again."
[Page visualization made with ggpage]

Analysis

1. Unpacking incidents

   ○ **What happens** in incidents of unauthorized access to smartphones?

2. Making sense of incidents

   ○ **How did participants represent incidents,** and what does that tell us?

With this data, we did two kinds of analysis.

First, we tried to unpack incidents. We wanted to answer "What happens in incidents of unauthorized access to smartphones". To do that, we did an exploratory qualitative analysis, by which we mean we provided some quantitative structure to the underlying qualitative data through a coding process.

Second, we tried to make sense of incidents. We wanted to see "How participants represented these incidents?" And to do that, we did thematic analysis, by which we mean that we took in the data, and then looked at patterns and meanings that were not necessarily at the surface.

For the rest of this presentation I'll give a glimpse into the two steps of analysis.

Unpacking incidents

- Coding of stories from explicit evidence in the text
- Two raters coded subset of 10 stories, with 95% agreement

Outcome: 61 codes, in 8 categories

Ash and Val had been dating for about two years, and things were rocky.

Ash seemed distant and uninterested in Val most of the time, which became a large problem in their relationship. Ash progressively became more distant and absent, and Val could hardly stand it.

One night while Ash was fast asleep in their bed, Val decided to look through Ash's phone on the bedside table. Signs of infidelity, possibly from the beginning of their relationship were on the phone. There were text messages with sexually explicit photos and pet names.

Val waited until the morning to mention what was found to Ash. When Ash woke up, the phone was displaying one of the photos and the jig was up. It was obvious that Val had found out what had been going on.

Val had already packed up everything and was ready to leave. Ash never saw Val again.

(P54)

| Type of relationship |
| Motivation |
| Opportunity |
| Use of locks |
| Val's actions |
| Awareness |
| Aftermath |
| Relationship termination |

First, unpacking incidents. To give structure to the data, we coded the stories with semantic codes. Semantic codes are codes for which there is direct, explicit evidence in the text. To check whether our coding process was reliable, we had two raters code a subset of stories, and they almost always agreed with their coding decisions. The outcome of this process was that we found 61 codes, divided among 8 code categories. I'm going to go through some of them. [Remaining in the paper, more detail in my doctoral thesis.]

Convention: Val accessed Ash's smartphone without permission

Before I do that, just a note. I'm going to follow a convention to name the people involved in incidents. When I speak about Val, I'm always referring to the person who accessed a smartphone without permission. And when I speak about Ash, I'm always referring to the person whose device was accessed.
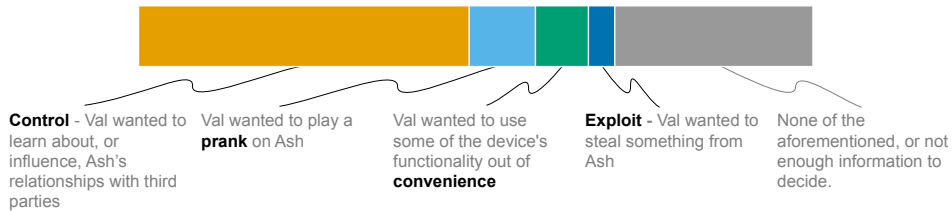
What was the relationship between Ash and Val?

Ash and Val were **intimate partners**, former intimate partners, or one of them aspired to an intimate relationship with the other

Ash and Val were **friends**, including people from work or school who are considered friends

Ash and Val were **family** members other than intimate partners

Ash and Val were **acquaintances**.

Ash and Val were **co-workers** who were not considered to be friends

None of the aforementioned, or not enough information to decide.

Val

Ash

This is the first code category I want to tell you about, represented here in a barchart. The category is defined by the question "What was the relationship between Ash and Val?" Each of the possible answers to this question is a code.

We see in this barchart that in most stories we collected, Ash and Val were intimate partners. Also commonly they were friends or family members. In 1 story they were acquaintances, and in one story they were co-workers. When we invited participants, we only asked them to write stories involving them and someone they knew. From this barchart, it seems that participants mostly wrote about incidents involving people in very close social circles. Incidents involving intimate partners, friends or family, are the ones that participants chose to reflect upon.

What was the primary motivation for unauthorized access?

Control - Val wanted to learn about, or influence, Ash's relationships with third parties
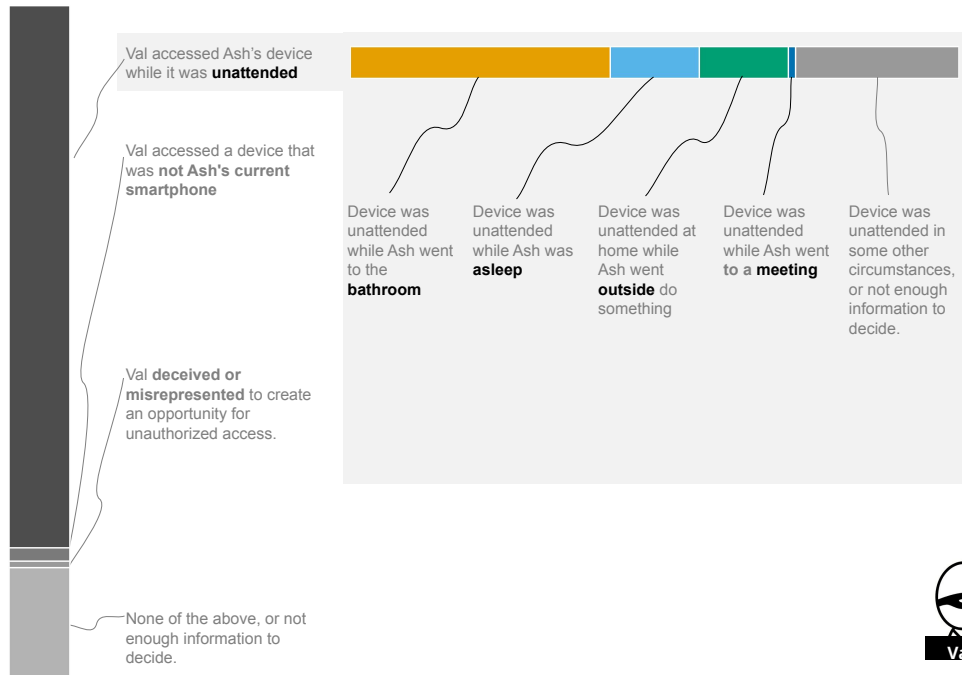
Val wanted to play a **prank** on Ash

Val wanted to use some of the device's functionality out of **convenience**

Exploit - Val wanted to steal something from Ash

None of the aforementioned, or not enough information to decide.

Val   Ash

Another thing that we coded was the motivation for unauthorized access. We found four kinds of motivations. More common was what we called "control". We defined control as "Val wanting to learn about, or influence, relationships between Ash and third parties". Other kinds of motivations were playing pranks, another accessing just for convenience, to use something. And the last one is what we called exploit -- in computer security there is typically a lot of focus on these types of incidents, where a perpetrator wants to steal something valuable from a victim, such as money, or a device, or business information.

Again, we should look at this distribution as reflecting the kinds of experiences participants chose to reflect upon. From that perspective, control-motivated access appears to be something that troubled participants a lot.

How did the opportunity for unauthorized access came about?

Val accessed Ash's device while it was **unattended**

Val accessed a device that was **not Ash's current smartphone**

Val **deceived or misrepresented** to create an opportunity for unauthorized access.

None of the above, or not enough information to decide.
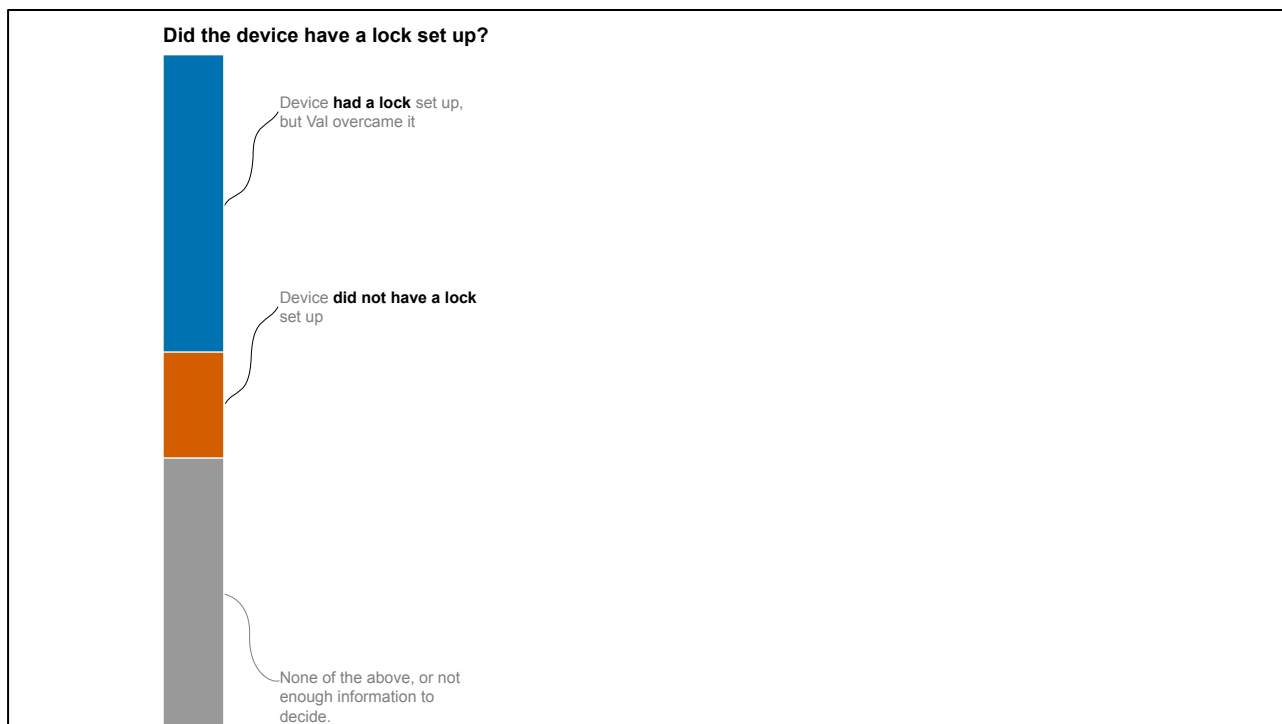
Val

Ash
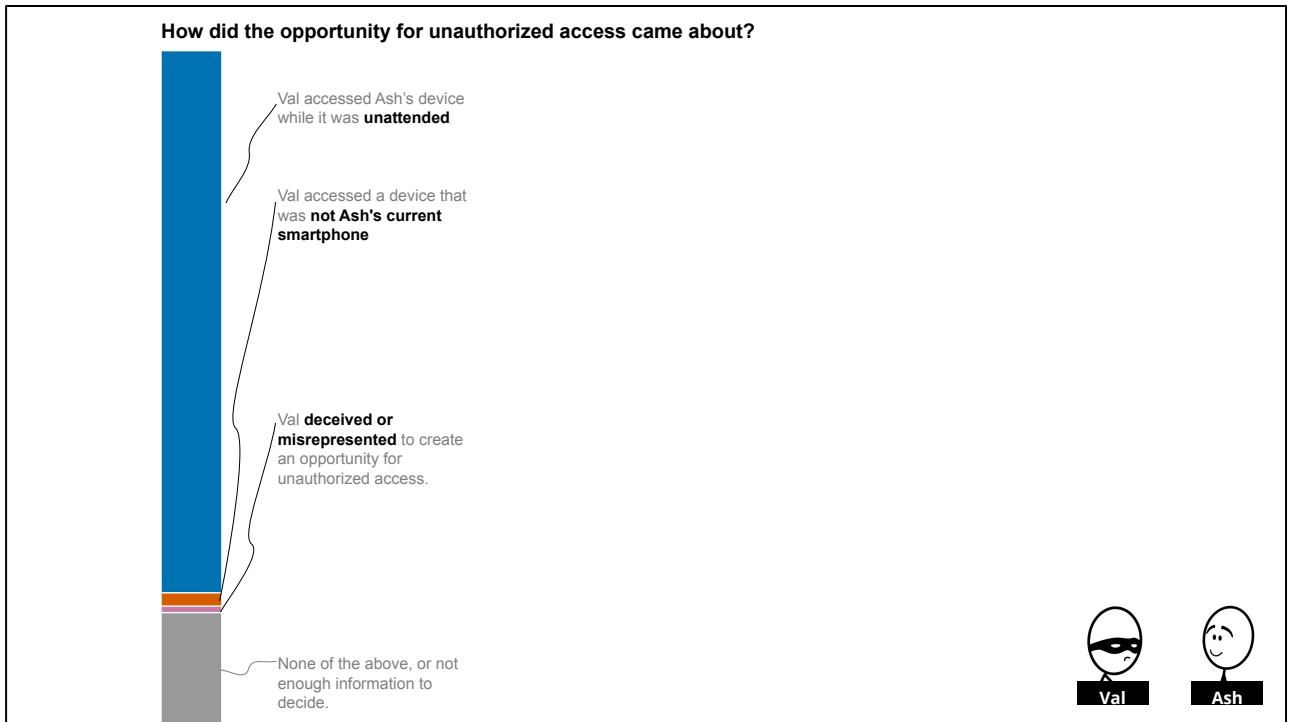
We also coded the circumstances in which devices were accessed. We found a couple of cases of access through secondary devices, and one case of Val deceiving Ash in order to get access. But, what was most common was that devices were accessed while they were unattended.

How did the opportunity for unauthorized access came about?

Val accessed Ash's device while it was **unattended**

Val accessed a device that was **not Ash's current smartphone**

Val **deceived or misrepresented** to create an opportunity for unauthorized access.

None of the above, or not enough information to decide.

Device was unattended while Ash went to the **bathroom**

Device was unattended while Ash was **asleep**

Device was unattended at home while Ash went **outside** do something

Device was unattended while Ash went **to a meeting**

Device was unattended in some other circumstances, or not enough information to decide.
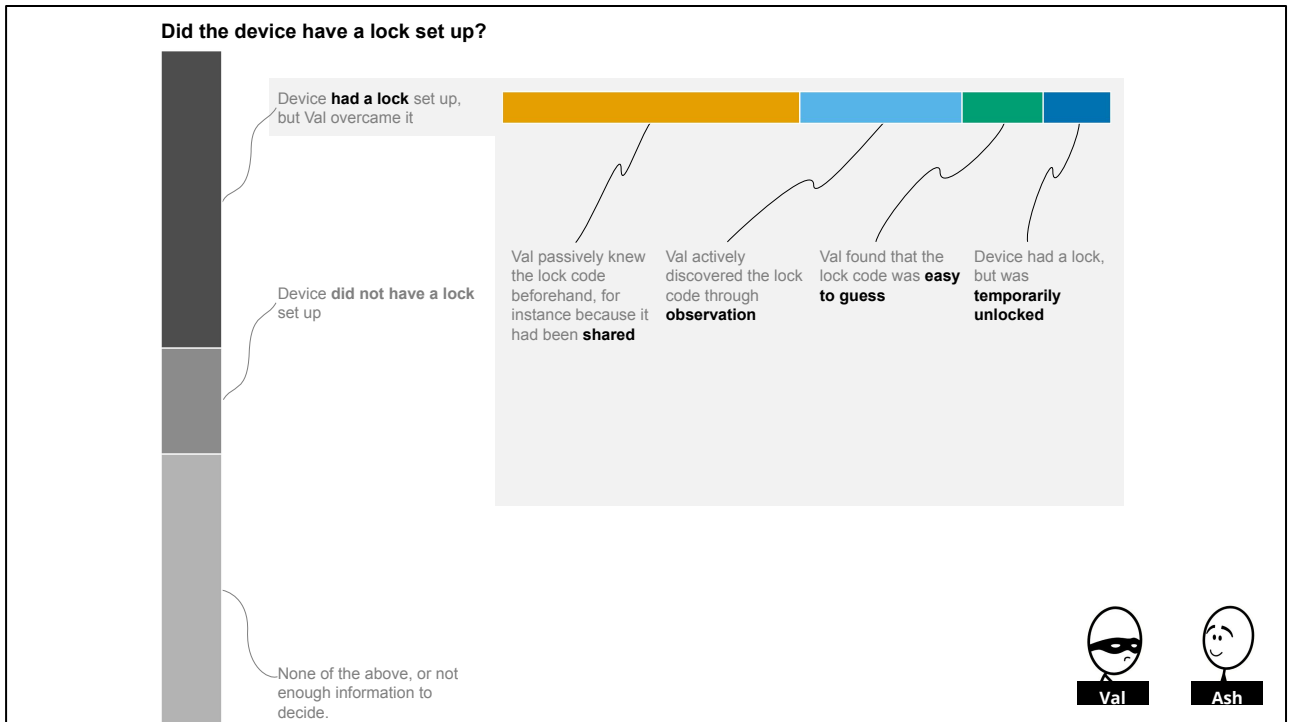
Val

Ash

We found a few notable circumstances by which devices were unattended. The most common was that Ash went to the bathroom, and left their phone behind. Also commonly Ash was asleep, or went outside of their home to run some errands. And in one case Ash went to a meeting.

What's notable here is that these incidents happened in places we may sometimes call "trusted locations" -- homes and workplaces. Another striking aspect, especially with this bathroom scenario is how little time it took for these incidents to unfold.

Did the device have a lock set up?

Device **had a lock** set up,
but Val overcame it

Device **did not have a lock**
set up

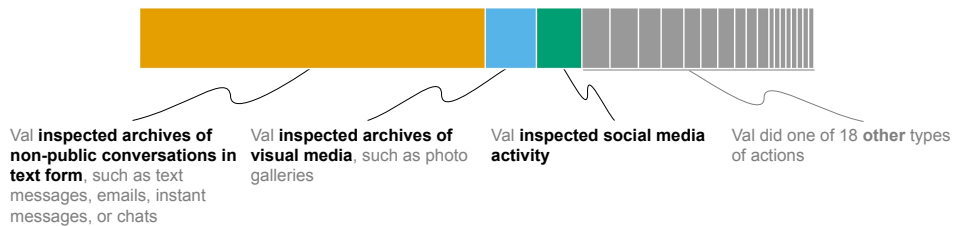None of the above, or not
enough information to
decide.

A more practical issue that we coded was about the use of locks. Authentication locks
are the main security feature by which smartphones are supposed to be protected
from unauthorized physical access. We observed was common for people to not have
locks set up. But, it was also common for people to have locks set up but them not
preventing unauthorized access.

Did the device have a lock set up?

Device **had a lock** set up, but Val overcame it

Device **did not have a lock** set up

None of the above, or not enough information to decide.

Val passively knew the lock code beforehand, for instance because it had been **shared**

Val actively discovered the lock code through **observation**

Val found that the lock code was **easy to guess**

Device had a lock, but was **temporarily unlocked**

Val

Ash

We found 4 ways in which locks were overcame. Most commonly, Val already knew the authentication code, often because it had been shared beforehand with the expectation of limited use. Also commonly, authentication codes were discovered through observation, or shoulder-surfing. Codes were also sometimes discovered by guessing. And sometimes Val took advantage of the device being temporarily unlocked.

All these cases underline how it's very different to prevent unauthorized access from strangers, in which case a lock may be effective, than it is to prevent unauthorized access from known people.

What did Val do once they gained access?

Val **inspected archives of non-public conversations in text form**, such as text messages, emails, instant messages, or chats

Val **inspected archives of visual media**, such as photo galleries

Val **inspected social media activity**

Val did one of 18 **other** types of actions

Val   Ash

The last category I want to talk about is "What did Val do once they gained access?". What we found here was a very long-tailed distribution. There were 21 types of actions that we coded, but only three appeared in more than five stories. We can see that inspecting text-based communications, such as emails or instant messages, was overwhelmingly prevalent. In fact, in more than half the stories we found evidence of this kind of action. The only two other types of actions that appeared in more than 5 stories were inspecting photos and inspecting social media activity.

Making sense of incidents

- Close reading of stories
- Reflexive process of finding latent meanings

Outcome: two themes

To have a fuller picture of what these experiences are like, in our second step of analysis we looked into how participants wrote about them. To do that, we went back to the data and did thematic analysis. Our process for doing that was centered around close reading. We did many rounds of close reading using the codes from our previous analysis as vantage points. For instance, we could find the subset of stories in which Ash and Val were friends, and then closely read how those friendships were represented. Through this process, we found a few patterns of meanings, from which we developed two themes.

Trust as performative vulnerability

"**Ash** had nothing to hide but **feared not being trusted if they kept their phone with them** at all times" - P43

"**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." - P75

Val   Ash

The first theme is organized around this idea of trust as performative vulnerability. Trust and trustworthiness were central participants' experiences. I have two excerpts here that illustrate that idea.

"Ash feared not being trusted if they kept their phone with them at all times" || "Val was suspicious. Ash would take their smartphone everywhere including when they were showering."

Participants thought of trust as an important part of their relationships. And when it came to their smartphones, this conception of trust created a tension. The tension was that, in order to be perceived as trustworthy, people had to display vulnerability. They had to put themselves in a position where their trust could be violated.

The implication of this conception of trust, is that when people went to great lengths to display vulnerability, and were reciprocated with actions that went against their expectations, the consequences could only be severe.

Trust as performative vulnerability

"Ash discovered what had been done to their phone from unusual battery consumption. **It was the end of their relationship.**" - P1

"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.**" – P45

Val   Ash

And this is what I mean by severe:
"It was the end of their relationship."
"Ash and Val are no longer roommates, and do no longer talk."
These two excerpts illustrate the case of expectations being violated, and therefore relationships being negatively affected or even terminated. But sometimes, by the exact same mechanics, relationships were positively affected. For instance, when people displayed trust, and were reciprocated with help in doing a task when they were busy, or a funny prank, stories tended to portray those relationships as getting stronger.

Self-serving sensemaking

"Val is the **controlling type**" - P2

"Val is quite **possessive**" - P5

"Val is a **lunatic**" - P69

"Val has a mind which works in a suspicious manner" - P40

Ash

The second theme we developed is organized around this idea of self-serving sensemaking. Often, we could distinguish if participants had written stories from Val or Ash's perspective. One thing that was notable was how stories assigned blame.
When stories were told from Ash's perspective, blame was placed on Val's character:
"Val is the controlling type"
"Val is possessive"
"Val is a lunatic"

Self-serving sensemaking

"Val is the **controlling type**" - P2

"Val is quite **possessive**" - P5

"Val is a **lunatic**" - P69

"Val has a mind which works in a suspicious manner" - P40

"**Val caught Ash** in their bedroom talking on telephone at 3AM" - P53

"**Val was worried** because Ash received many texts in the last days" - P101

"Val started to think about how Ash had seemed distant lately" - P37

Ash

Val

But when stories were told from Val's perspective, the explanations were more situational. There was some context that made Val's actions justified:
"Val caught Ash in their bedroom talking on telephone at 3AM"
"Val was worried because Ash received many texts in the last days"
This attribution pattern was very stark. And it tells us something about how people experience these incidents. It tells us that these experiences were personally significant, because otherwise people would just relay the facts, and not center their reflections around themselves not being guilty.

What are incidents of unauthorized physical **access** to smartphones involving people known to each other like?

To conclude. We started with this question: What are incidents of unauthorized access like? We hope our analysis gives some sense about what happens in incidents, and how people experience them.

So far, we have mostly refrained from being very prescriptive about what others should take from our analysis. But there are two very practical ideas that may be useful for designing user-facing security technologies.

When considering user-facing security technologies:

Model for the possibility of non-stranger access

One is to give consideration to non-strangers in threat models. This is absolutely not a new idea, but some of the details in our analysis can be useful to develop scenarios which are easier to digest.
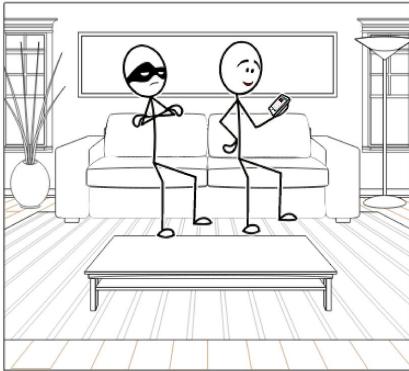
A "showertime attack"

For instance, taking the codes we found more frequently in stories, we could define a "showertime attack". A shower-time attack would be an instance of a person learning a lock code from someone close to them, and then accessing the device without permission while they were briefly away, and then maybe going through records of written communications. It may be easier to work with a specific scenario like this than to think about unauthorized access and non-stranger as abstractions.
[Storyboard created with StoryboardThat]

When considering user-facing security technologies:

Account for the possibility of non-stranger access

Ask: how can this be used to signal trust?

Another practical thing to do when designing user-facing security technologies is to ask this question: can this be used to signal trust? This is an important question, because if being trusted requires displaying vulnerability, that may very well undermine the security model we were aiming for. For instance, as we saw, we would be wrong to assume that lock codes are only known to device owners. And we can think how this principle applies to other security technologies. For instance, are people sharing their master password for their password manager in order to display trust? Are people setting up each other's fingerprints on their phones to display trust? The answer may be "no, people are not doing that", but, even so, it seems prudent to at least ask the question -- how can this be used to signal trust?

Vulnerability & Blame:
Making Sense of Unauthorized Access to Smartphones

We explored:

- What happens in incidents of unauthorized access to smartphones
- How people's conceptions of interpersonal trust interacts with security

When thinking about user-facing security technologies:

- Build threat models accounting for non-stranger access
- Ask: how can this be used to signal trust?

Diogo Marques

Tiago Guerreiro

Luís Carriço

Ivan Beschastnikh

Konstantin Beznosov

@ CHI 2019

@ CHI 2019

@ CHI 2019

U LISBOA | UNIVERSIDADE DE LISBOA

UBC THE UNIVERSITY OF BRITISH COLUMBIA