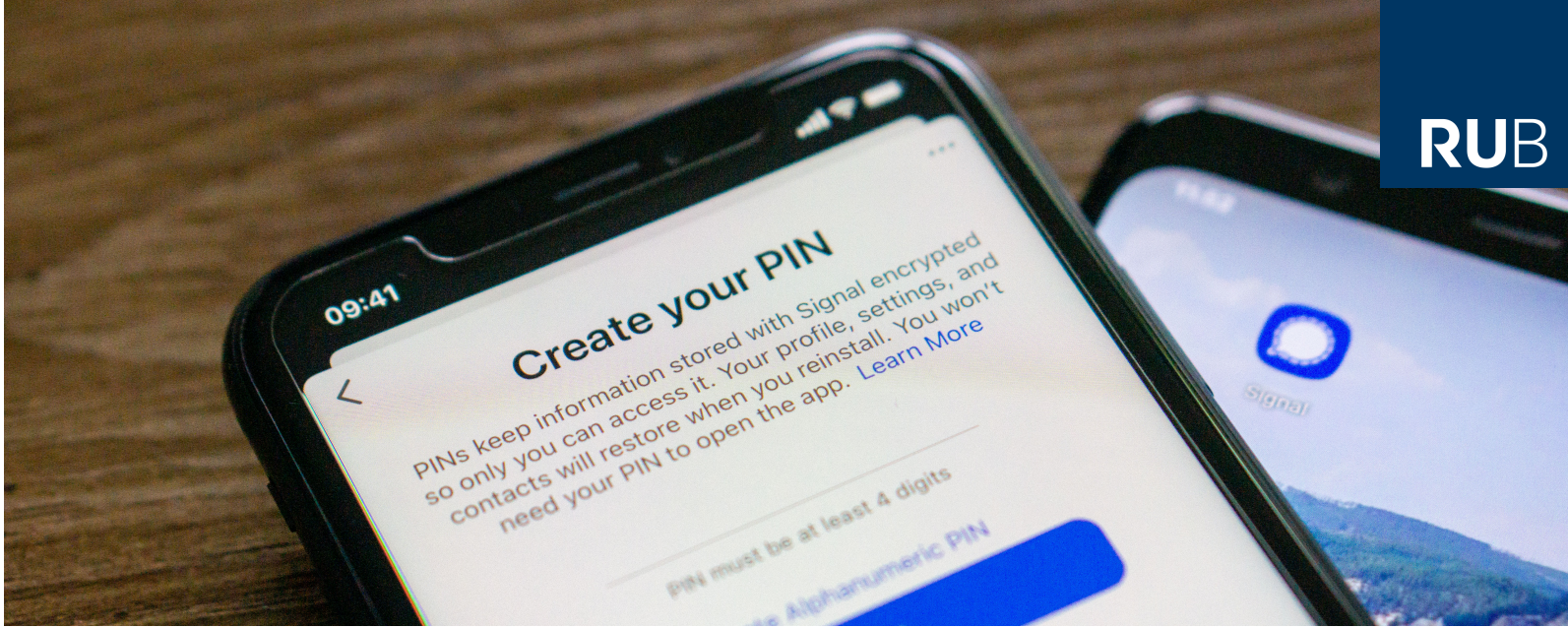



*"I Have No Idea What They're Trying to Accomplish:"*

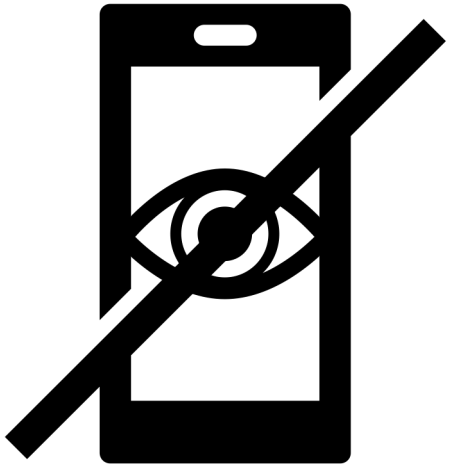
# Enthusiastic and Casual Signal Users' Understanding of Signal PINs

Daniel V. Bailey, Philipp Markert, and Adam J. Aviv

August 10, 2021 | 17th USENIX Symposium on Usable Privacy and Security (SOUPS)

# Signal is Privacy Focused

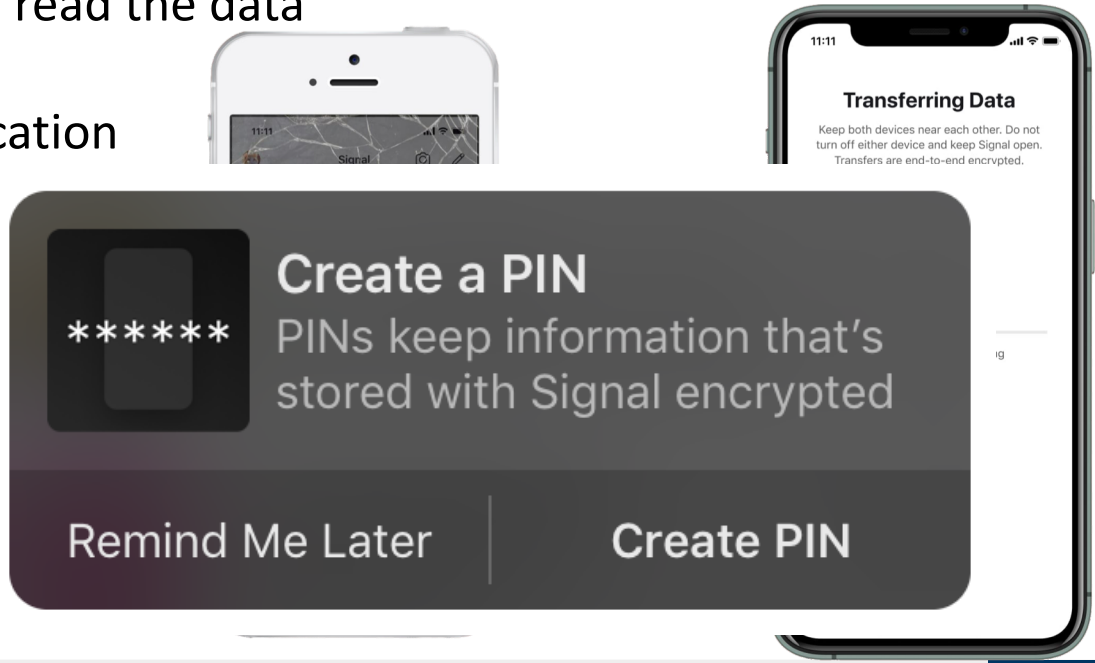
- Free from ads, trackers
- Contact list should be secret
  - No metadata mining
- **Signal should not be able to read your data**
  - New features should respect this rule



Signal

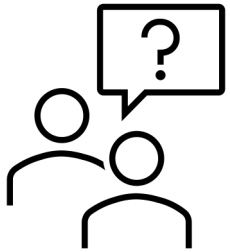
# Device Transfer

- Setting up a new device is much easier if Signal stores some data
  - But still don’t want Signal to read the data
- Phone number-based authentication
  - SIM-swap vulnerability

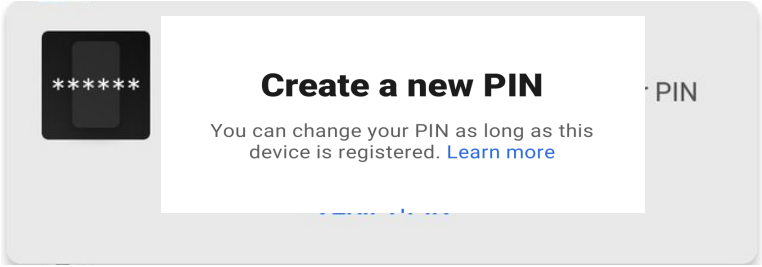


# Research Questions

- **RQ1:** Are participants aware of how and why in-app PINs are used in Signal?

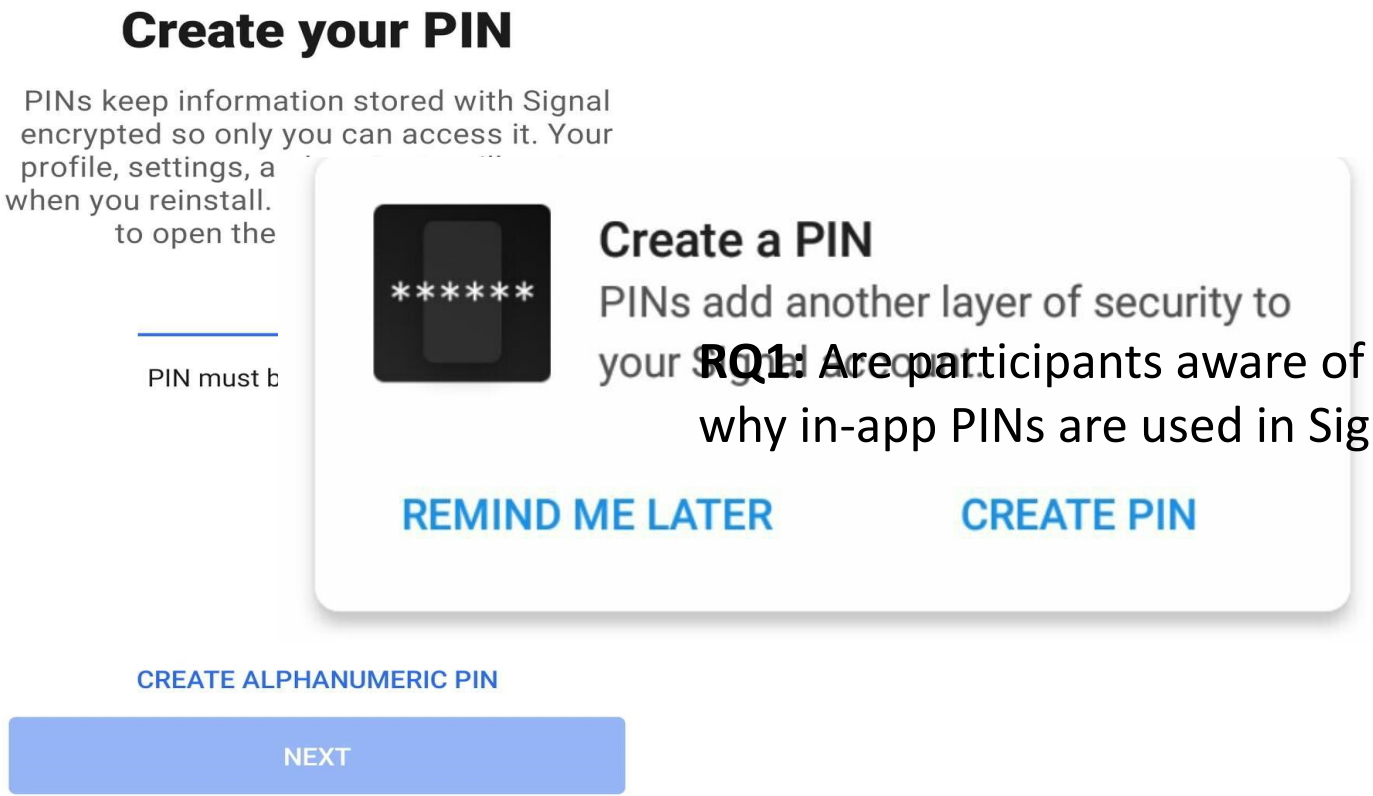



- **RQ2:** How effective are PIN reminders in assisting participants to remember PINs?



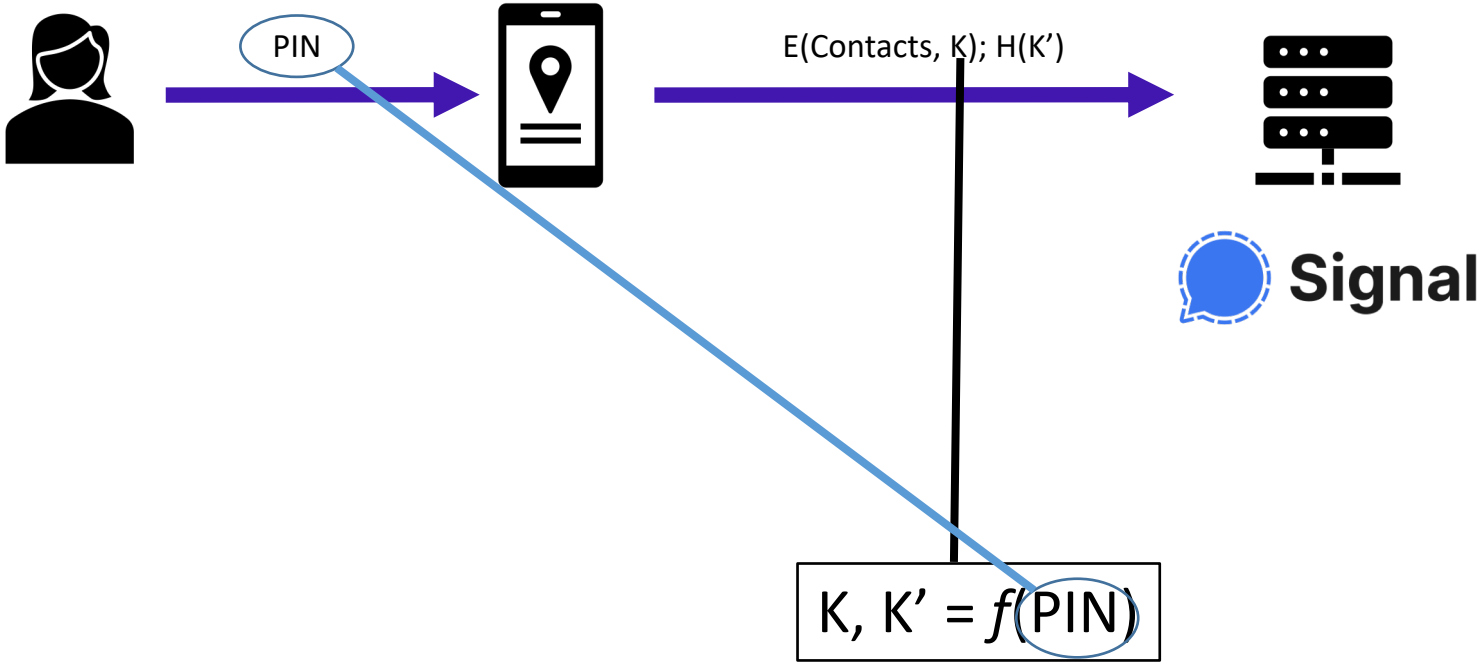

- **RQ3:** How do participants choose an and does their understanding of how these PINs are used affect that choice?

# Signal PIN




**RQ1:** Are participants aware of how and why in-app PINs are used in Signal?

# Signal PIN Usage




*Hard to explain to users!*

# Methodology Discussion

## Recruitment

- *n* = 235 Signal users
- From
  - r/samplesize
  - r/signal
  - Signal Community Forum
  - Snowballing
  - Prolific, paid

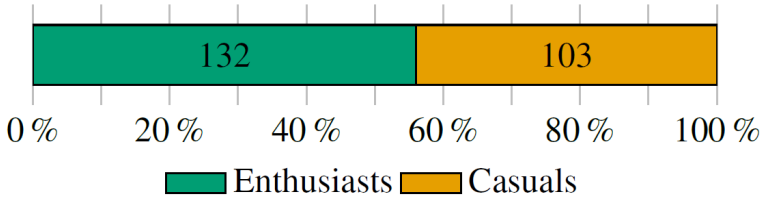
## Instrument

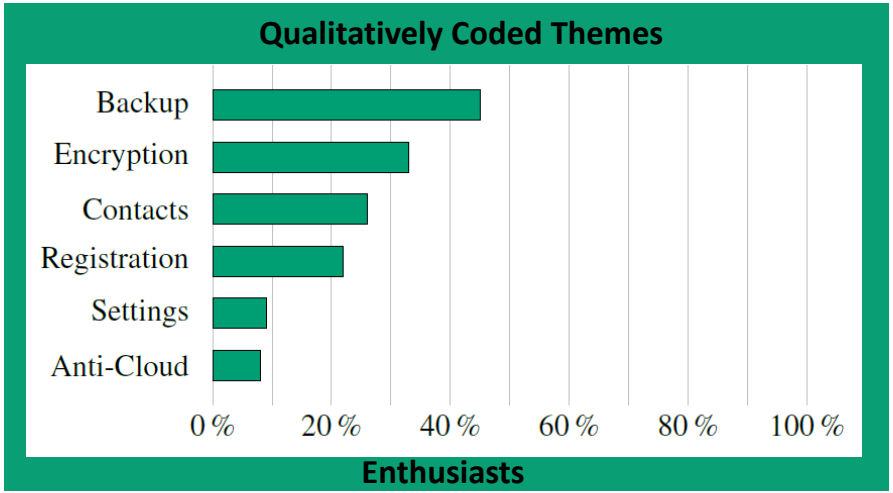
- Survey on Qualtrics
- 7 minutes
- All procedures in line with typical IRB-approved studies in our field
- Mix of qualitative and quantitative questions

## Analysis

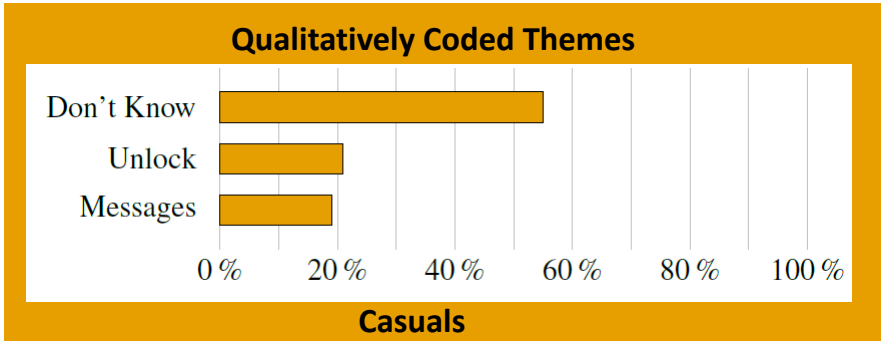
- Coder A produced a codebook
- Coders A+B used the codebook to code
- Coders A+B met and compared codes until they agreed

# RQ1: Understanding Signal PINs




- To gauge Signal PIN comprehension, we asked:
  *"In your own words, please explain how PINs are used by Signal."*
- Participants classified into two groups:
  - Enthusiasts 56%
  - Casuals 44%



# Enthusiast Quote

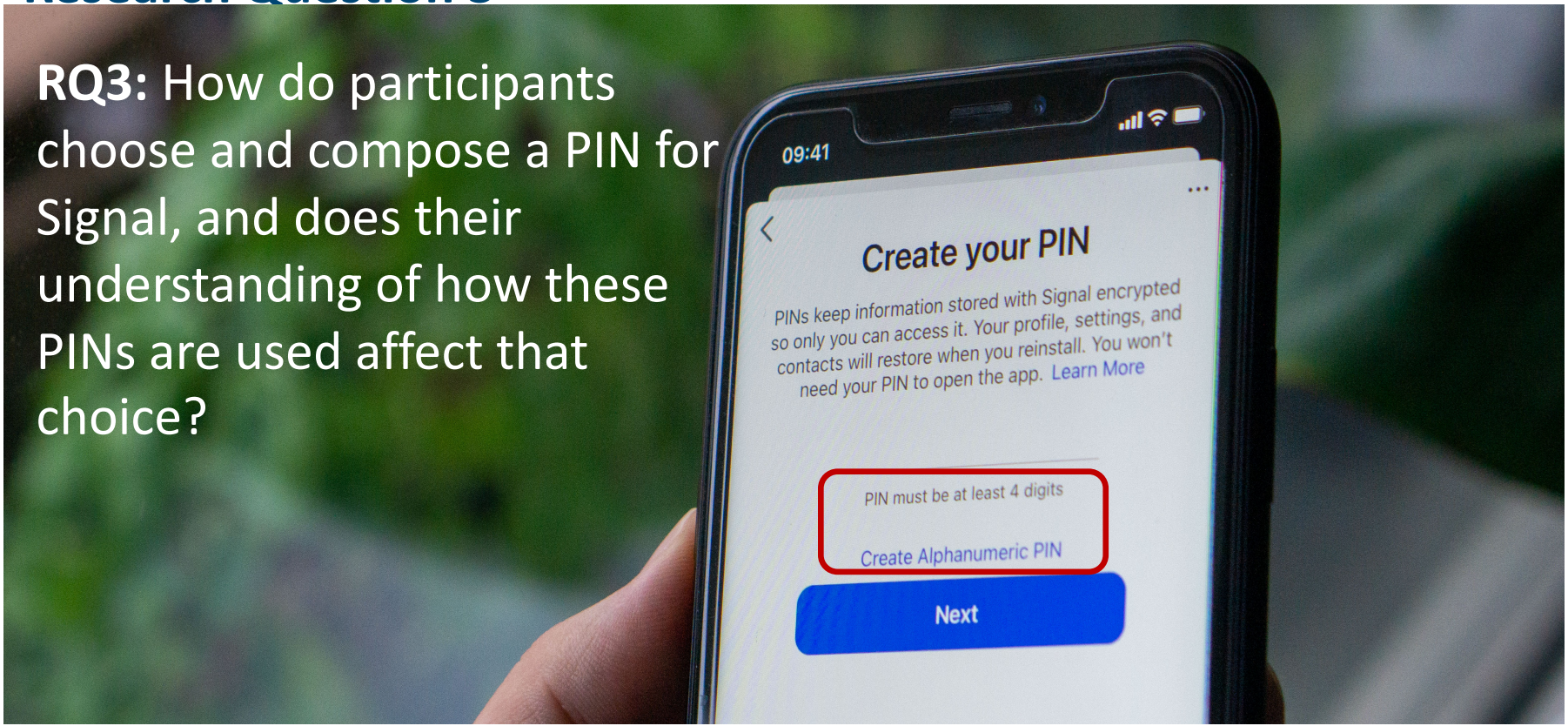
**P10:** “It protects data like settings and group membership and signal [sic] contacts that will be **stored on Signal’s servers using SVR**. Previously this was … lost upon … getting a new device unless a full backup was made on Android.”

# Casual Quote

**P47:** “I don't understand their purpose very well. I thought that they might be using the PIN system to verify the identity of the person using signal (if for instance someone unauthorized gained access to the phone), but the way that pin entry is optionally offered every few weeks doesn't align with such a purpose. as such, **I have no idea what they're trying to accomplish**.”

# Research Question 3

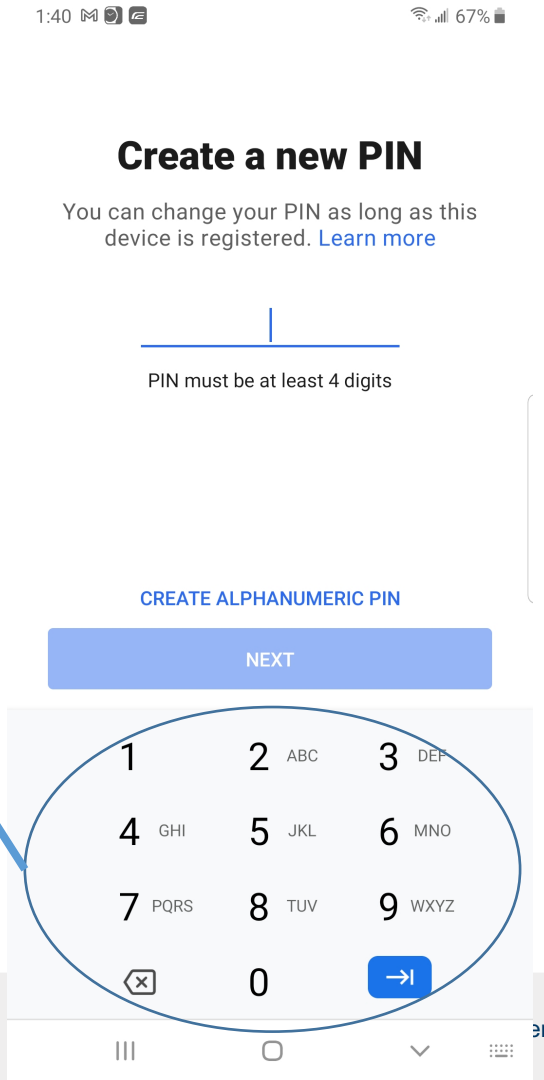
**RQ3:** How do participants choose and compose a PIN for Signal, and does their understanding of how these PINs are used affect that choice?



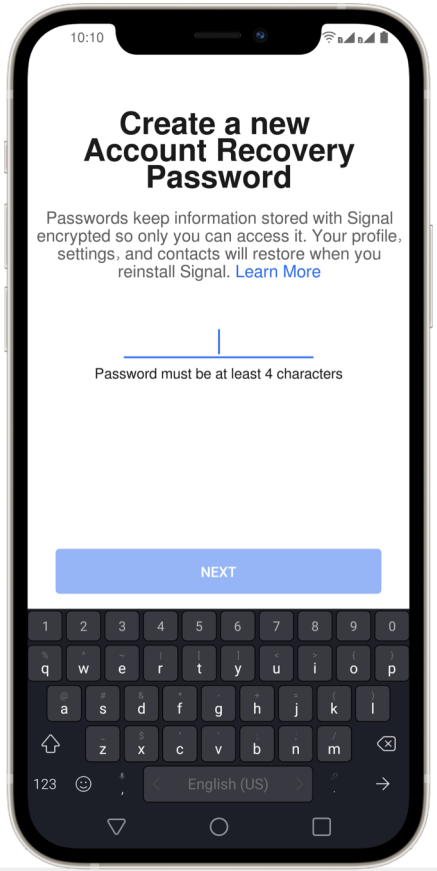
# RQ3: PIN Composition

Enthusiasts pick long alphanumeric passwords

Casuals pick a numeric PIN



# Conclusions: Toward Better Signal PINs




- Encryption only as good as the PIN
- Better communication about Signal PIN and its purpose
- Calling it “Account Recovery Password” might encourage longer and better passwords


Casual Signal users
confused about Signal PIN

Casual Signal users
need better communication

Casual Signal users
need help to pick better PINs

Scan here
for paper link!

RUB

# “I have no idea what they're trying to accomplish:” Enthusiastic and Casual Signal Users' Understanding of Signal PINs

Daniel V. Bailey, Philipp Markert
Ruhr University Bochum

Adam J. Aviv
The George Washington University