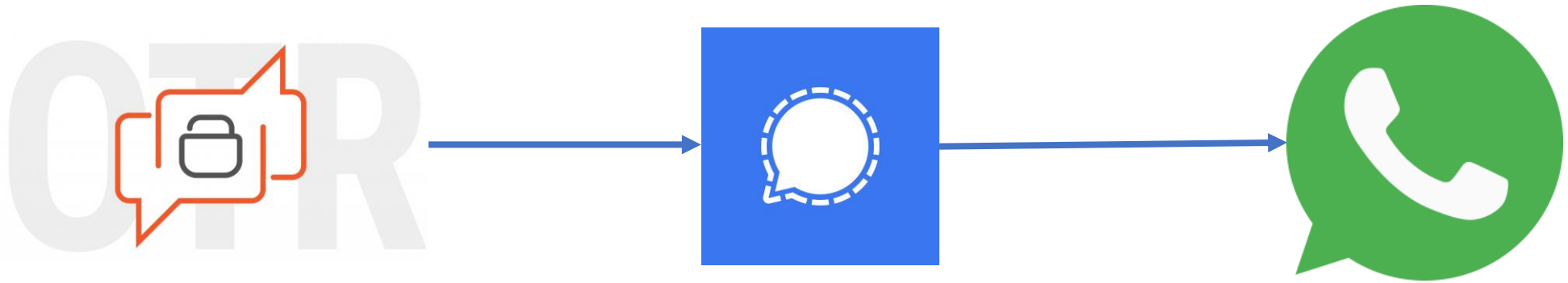
# **Cryptographic Deniability**: A Multi-perspective Study of User Perceptions and Expectations

**Tarun Kumar Yadav**, Devashish Gosain, Kent Seamons

BYU
BRIGHAM YOUNG
UNIVERSITY

KU LEUVEN

# Deniability in messaging apps



OTR

Signal
More than 40 million active users

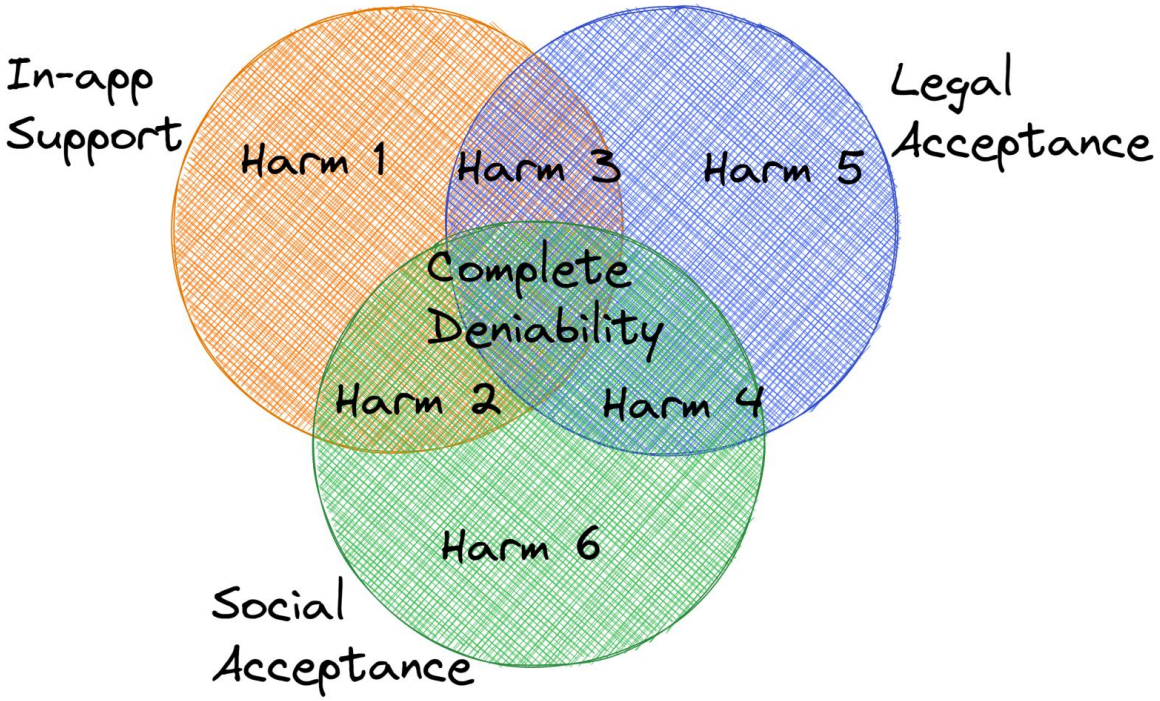
WhatsApp
More than **2 billion active users**

# Why deniability needs to be studied?

- In theory we've solved deniability
- However, in practice…
  - Requires awareness of deniability by the sender
  - Requires acceptance of deniability by others
  - Requires acceptance of deniability by the legal system

If we don't address these issues there are tangible harms that users can experience

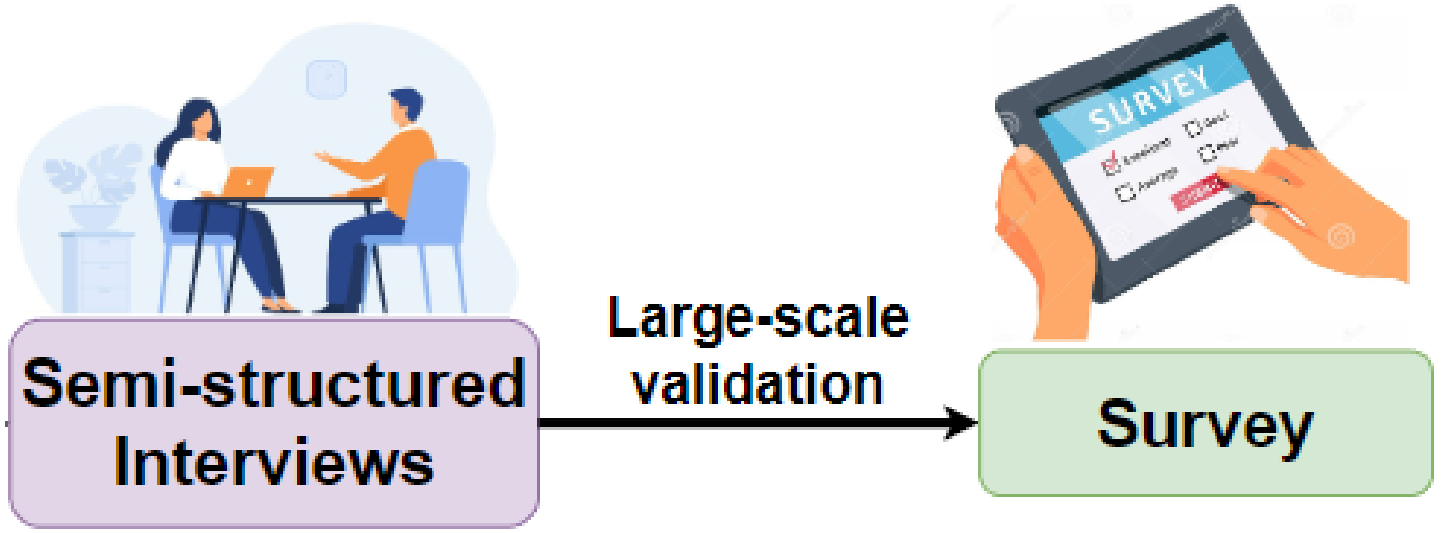
# Potential Harms




- Harm 1

- App offers deniability (messages cannot be used as evidence)
- Society is not aware of deniability (thinks they can use messages as evidence)
- Legal is not aware of deniability (thinks they can use messages as evidence)

# Study 1- Social acceptance



# Social acceptance – as a 3rd party

*Scenario*: Alice tells the participant that Bob said mean things about them

*Measures:* Trust score on Alice's claim

*Varying factors*:

- Participant's relationship w/ Alice
- Participant's relationship w/ Bob
- The medium through which Alice proves to the participant

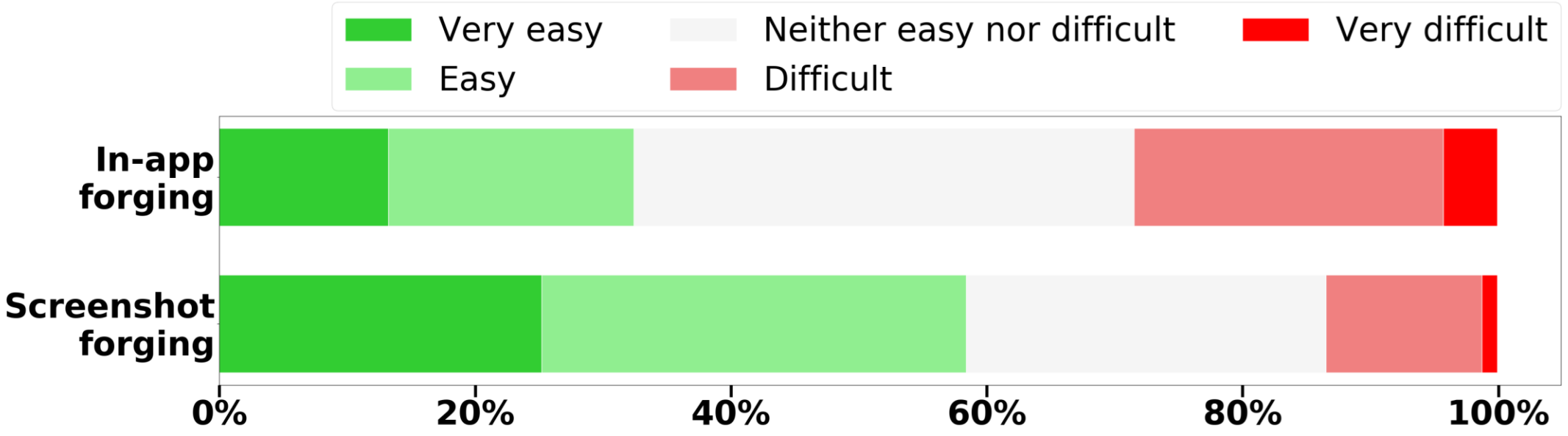
# Social acceptance – as a 3rd party

- *Finding 1*: Participants trust Alice's claim significantly more when shown in app as compared to oral claim
- *Finding 2*: Participants change in trust score from oral to in-app is significantly more when Alice is untrustworthy

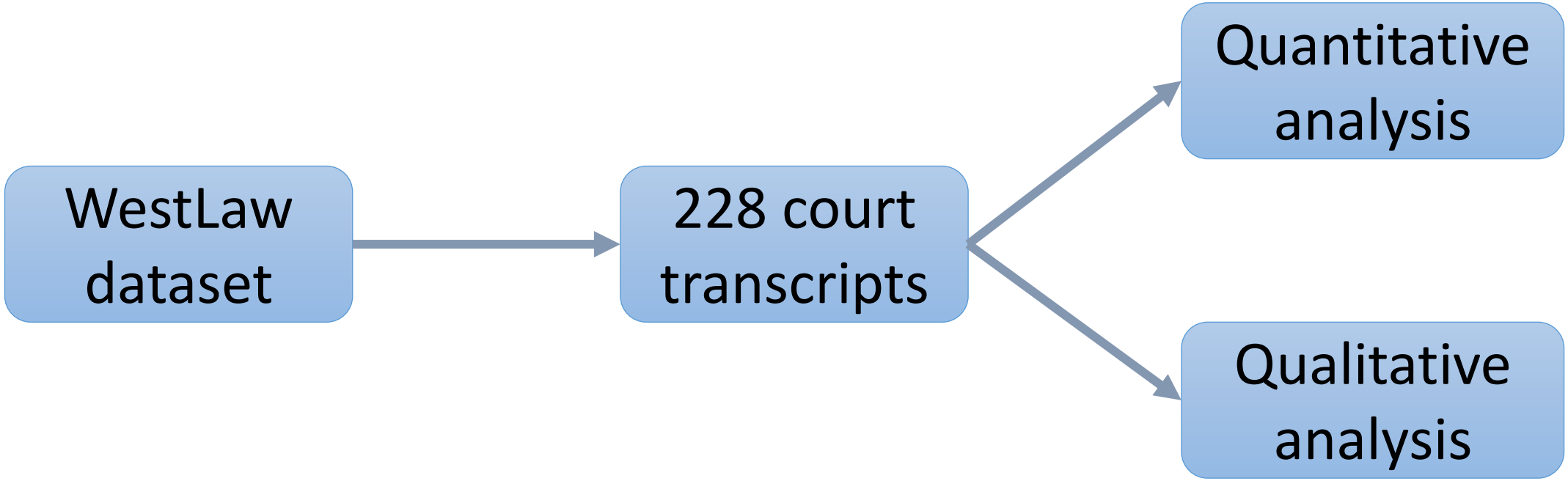
# Social acceptance – as a 3rd party

*"Even if friend A had a history of making stuff up, or not being the most trustworthy, she's showing me the texts on her phone what friend B said, then I'd be like, Okay this is legitimate."* - P6

# Social acceptance



# Study 2: Legal acceptance



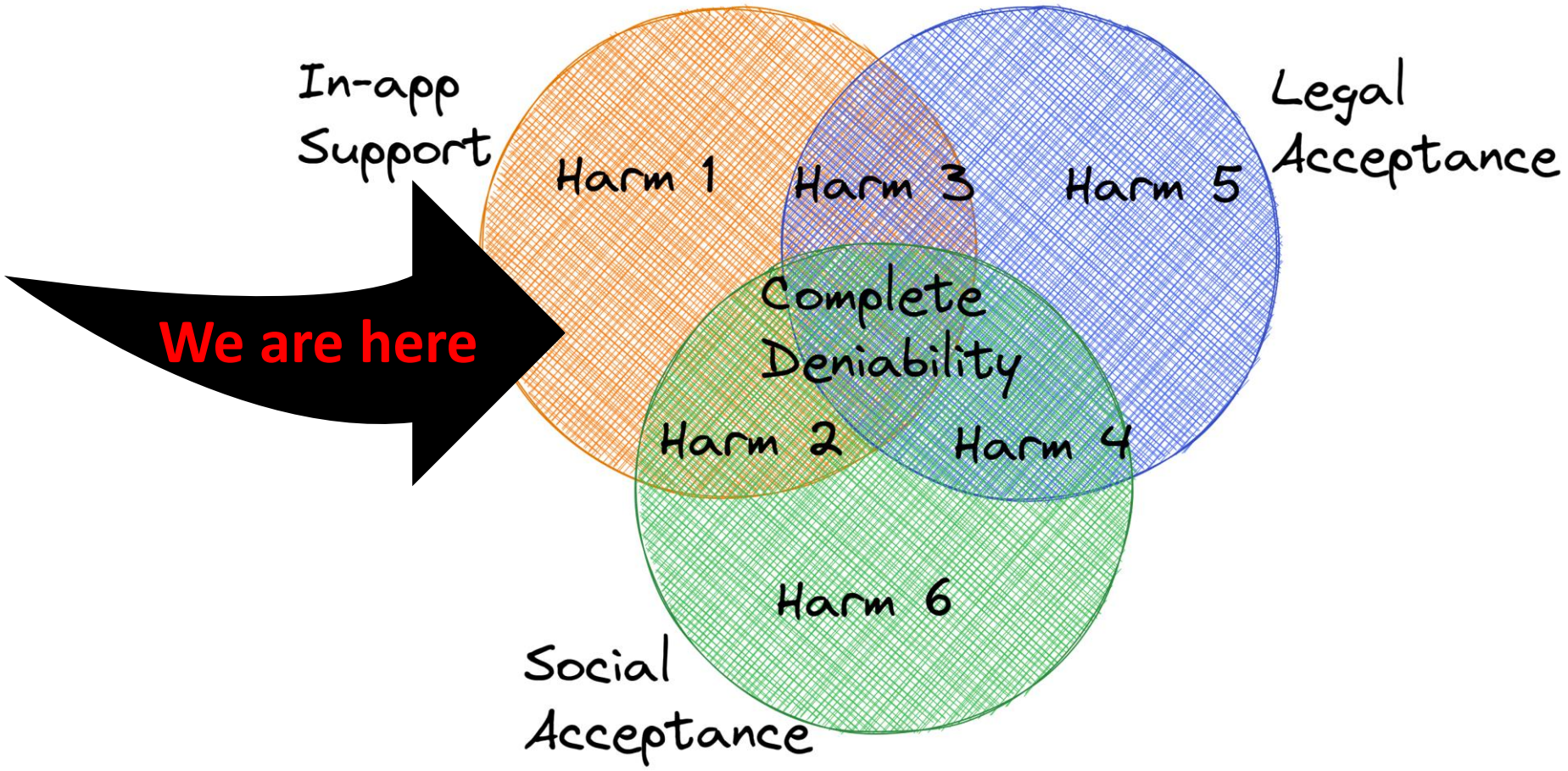
# Legal acceptance – quantitative analysis

| | Major evidence | Minor evidence | Rejected as evidence |
|---|---|---|---|

# Legal acceptance – quantitative analysis

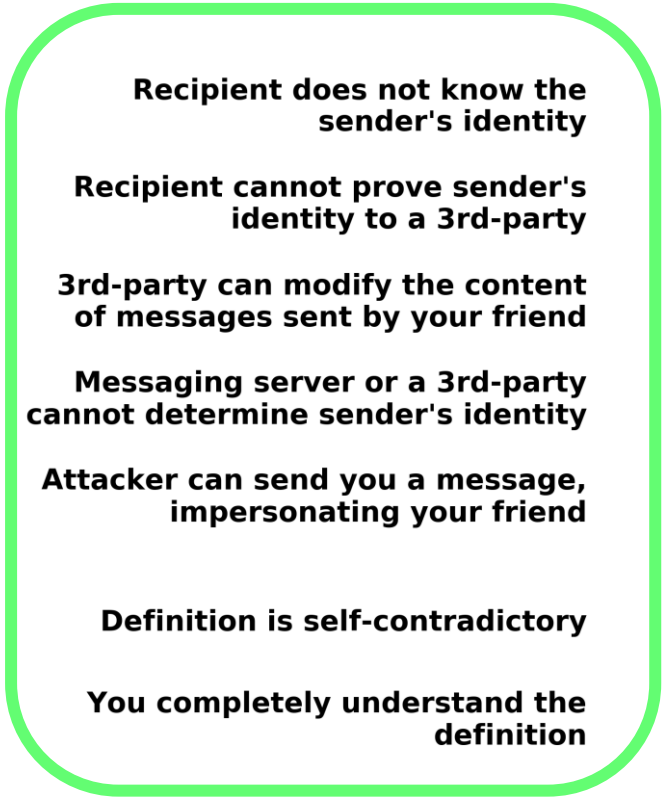
| Total cases | Major evidence | Minor evidence | Rejected as evidence |
|---|---|---|---|
| 228 | 34.6% | 33.6% | 0 |

# Potential Harms



# Do users understand deniability?

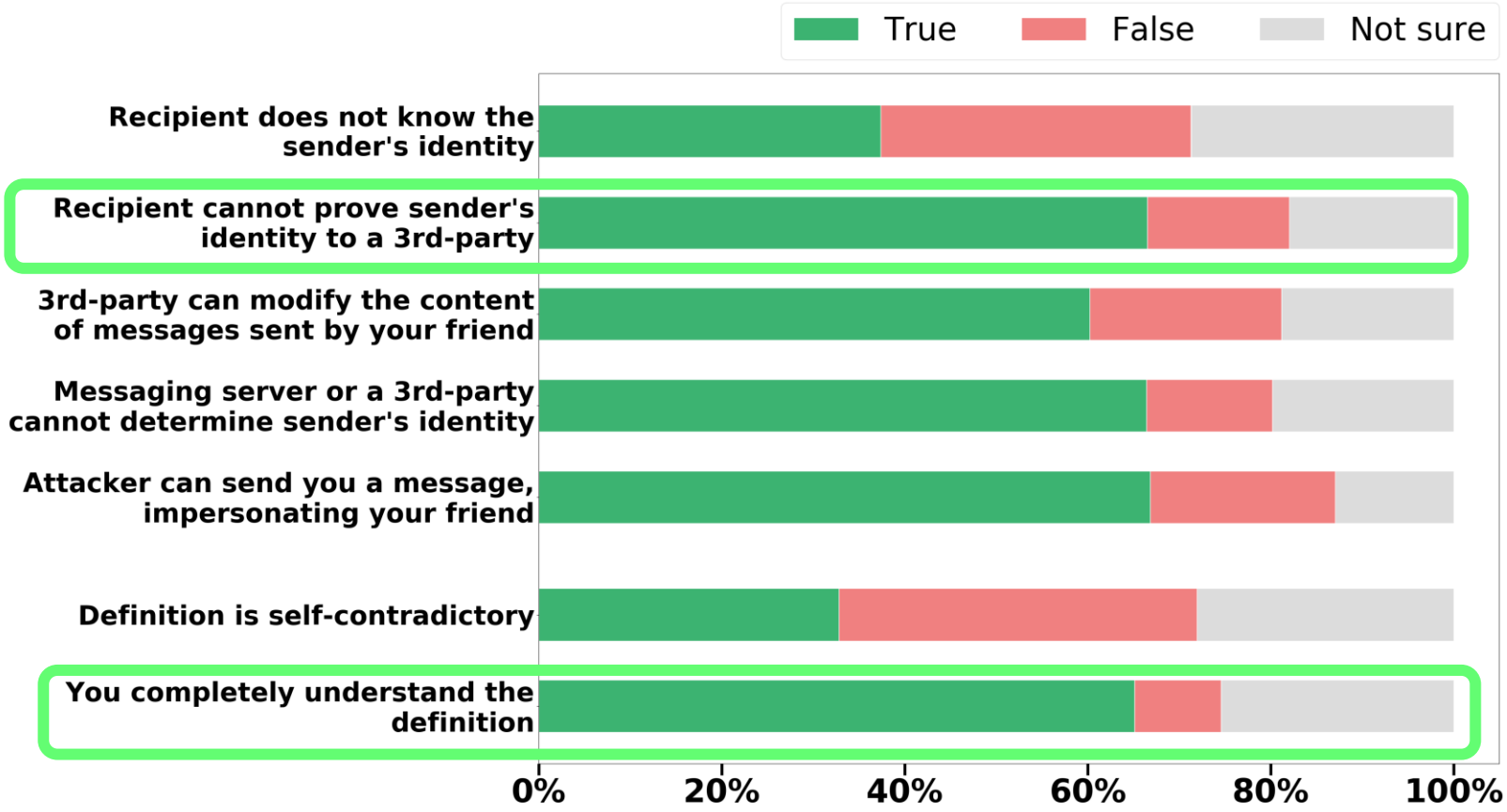
**Deniability definition**: "*The messages you send do not have digital signatures that are checkable by a third party. Anyone can forge messages after a conversation to make them look like they came from you. However, during a conversation, your correspondent is assured the messages he sees are authentic and unmodified.*"



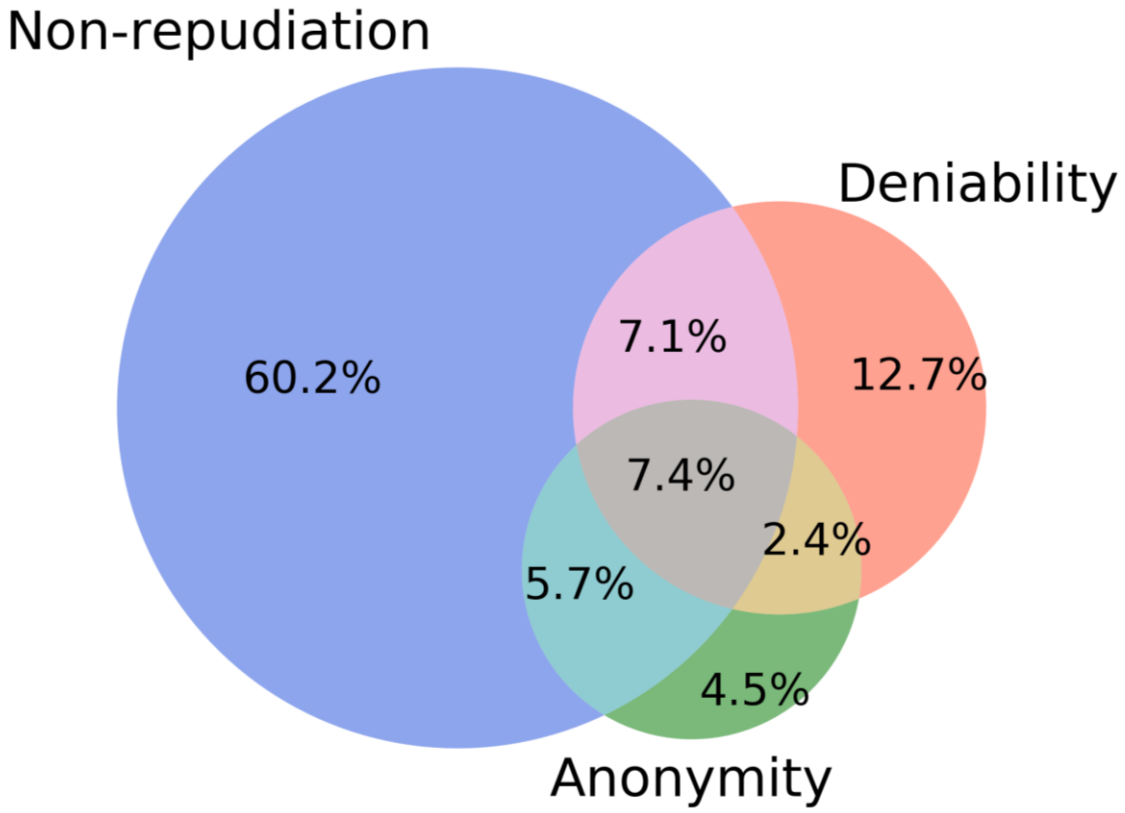
# Do users understand deniability?

*"Well, none of it makes sense" – P3*

**Deniability definition**: "*The messages you send do not have digital signatures that are checkable by a third party. Anyone can forge messages after a conversation to make them look like they came from you. However, during a conversation, your correspondent is assured the messages he sees are authentic and unmodified.*"



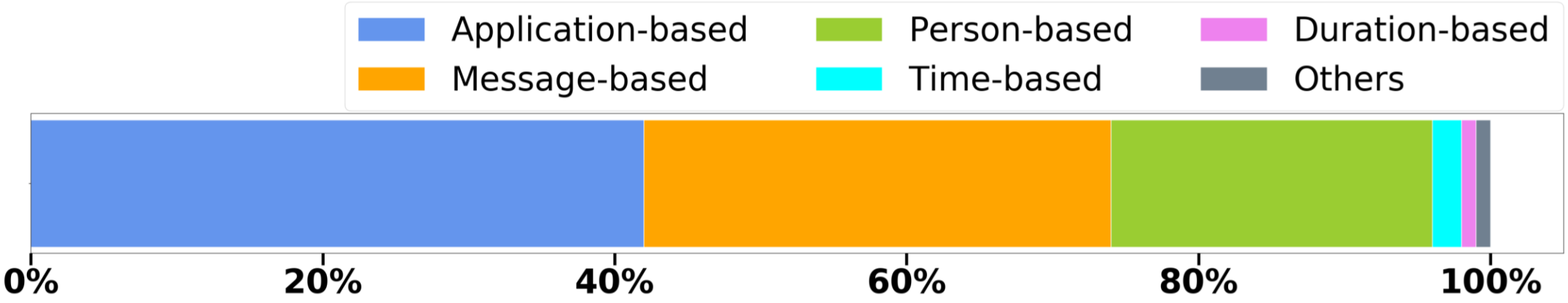
# What do users prefer?



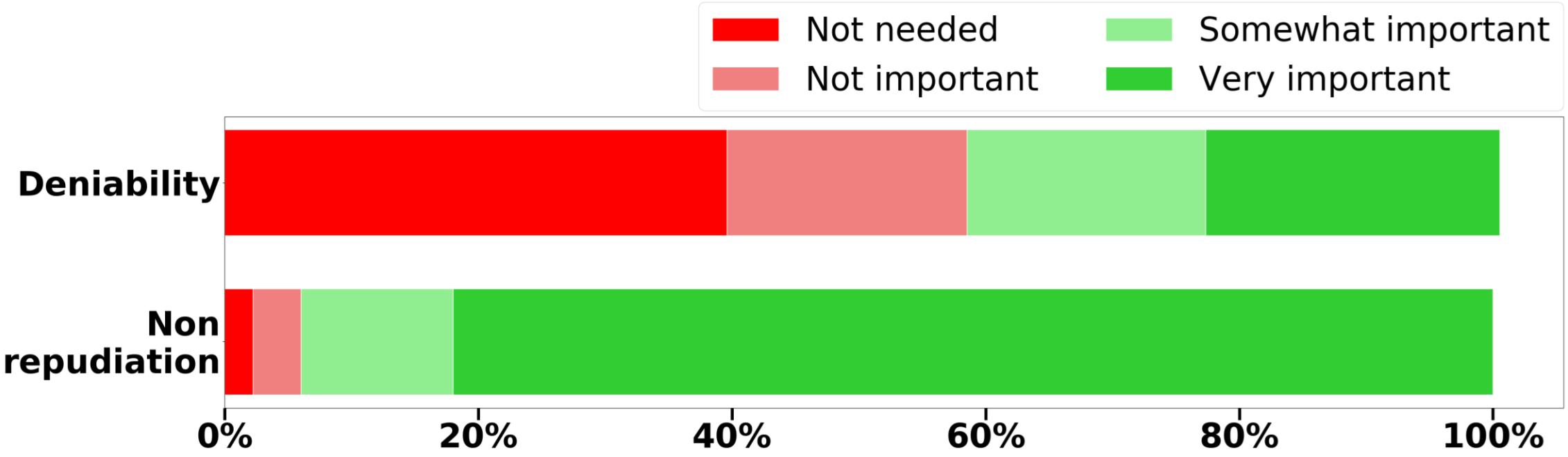

*"... I feel like a lot of where this country is, it's partially because of the lack of any control and any fact-checking online. So I would go with non-repudiation to help combat this problem..."*

- P12

# What do users prefer?



# What do users need?



# Key Takeaways

Deniability is ineffective for vulnerable groups

# Key Takeaways

Deniability is ineffective for vulnerable groups

Users are vulnerable to social engineering attacks due to unawareness of deniability

# Key Takeaways

Deniability is ineffective for vulnerable groups

Users are vulnerable to social engineering attacks due to unawareness of deniability

Deniability should not be provided by default for non-experts

# Key Takeaways

Deniability is ineffective for vulnerable groups

Users are vulnerable to social engineering attacks due to unawareness of deniability

Deniability should not be provided by default

Deniability has a bad reputation

# Key Takeaways

Deniability is ineffective for vulnerable groups

Users are vulnerable to social engineering attacks due to unawareness of deniability

Deniability should not be provided by default

Deniability has a bad reputation

Deniability definition needs improvement

# Any questions?