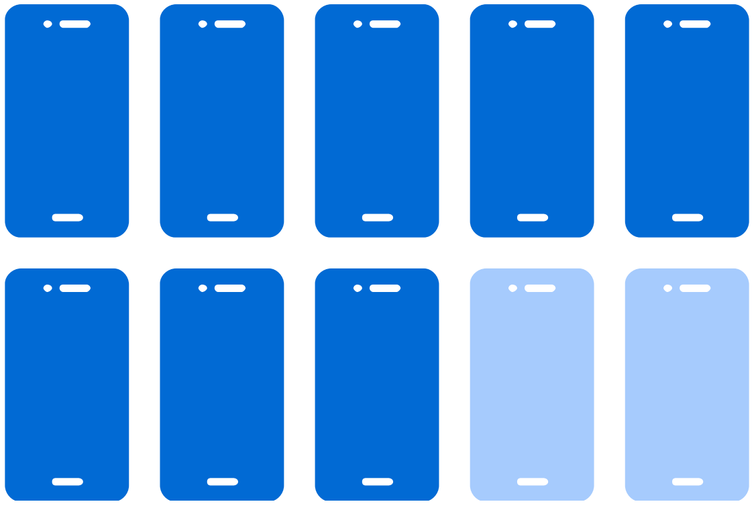
“Did They F***ing Consent to That?”: Safer Digital Intimacy via Proactive Protection Against Image-Based Sexual Abuse

Lucy Qin (Georgetown University), **Vaughn Hamilton** (Max Planck Institute for Software Systems), **Sharon Wang** (University of Washington)
Yigit Aydinalp (European Sex Workers Rights Alliance), **Marin Scarlett** (European Sex Workers Rights Alliance), **Elissa M. Redmiles** (Georgetown University)

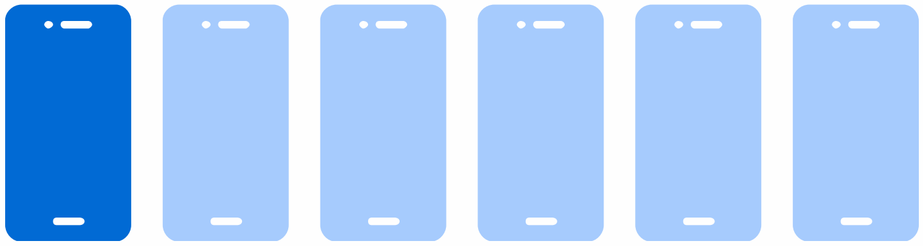


As Many As

8 IN 10

Adults in the U.S. Share Intimate Content*

*__Intimate content__ are images or videos that show a nude or semi-nude subject, contain intimate body parts, and/or intend to arouse.



1 IN 6

U.S. Adults in 2022 reported having their intimate content distributed without their consent

Non-consensual distribution of intimate imagery (NDII) is a form of sexual abuse.

and can lead to....

1

Mental health consequences

Similar mental health consequences to other forms of sexual abuse (PTSD, depression)

2

Doxxing & online harassment

Increased risk of doxxing
and other online hate and harassment. The risks are magnified for LGBTQ, women, and sex workers

Societal norms and lack of technological mitigations put people at risk

Societal norms and lack of technological mitigations put people at risk

This research focuses on proactive mitigation strategies against the nonconsensual distribution of intimate content (NDII)

Societal norms and lack of technological mitigations put people at risk

This research focuses on proactive mitigation strategies against the nonconsensual distribution of intimate content (NDII)

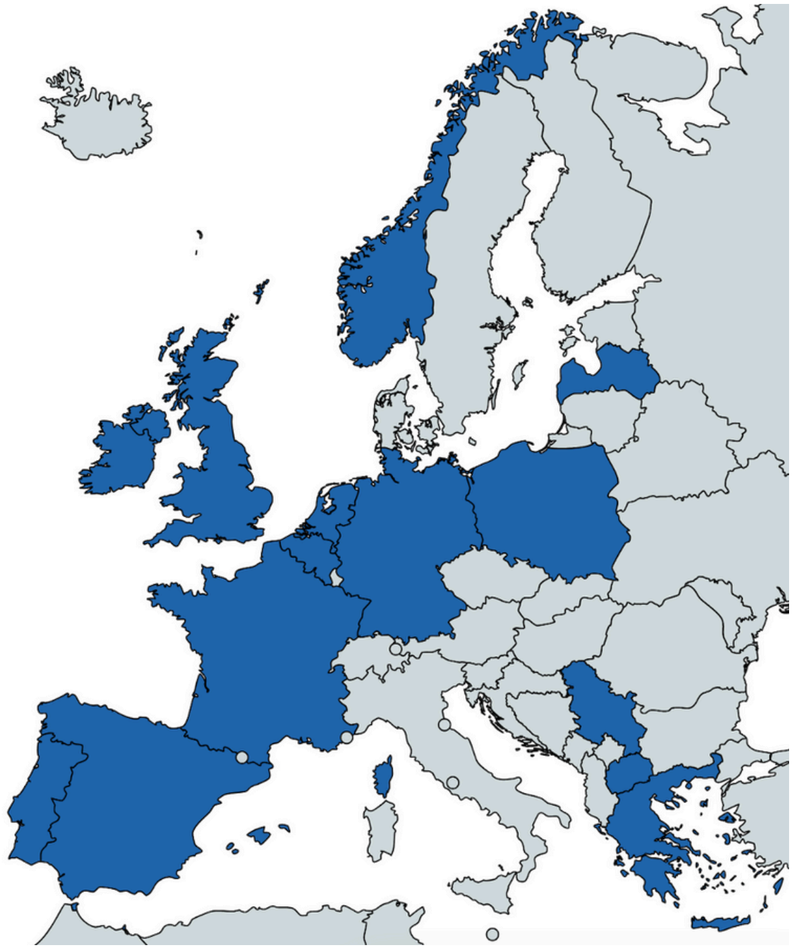
We investigated:

The contexts, technologies, threat models, and defensive strategies of intimate content sharing

Method: Semi-structured interviews

52 adults living in European countries who share intimate content

- 28 who shared for recreational purposes, 24 shared for commercial purposes
- 22 victim-survivors of NDII (includes participants from both of above groups)



Overview of Findings

People share intimate content with...

Strangers
(e.g., body positivity group on social media)

New relationships
(e.g., someone on a dating app)

Established
relationships
(e.g., dating, marriage)

Commercial Platforms
(OnlyFans, etc.)

People share intimate content with...

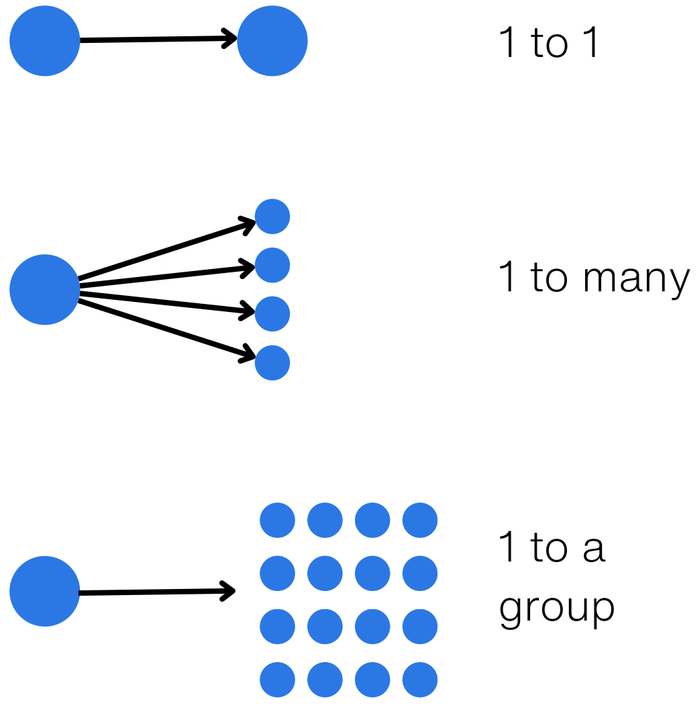
Strangers
(e.g., body positivity group on social media)

New relationships
(e.g., someone on a dating app)

Established
relationships
(e.g., dating, marriage)

Commercial Platforms
(OnlyFans, etc.)

In different structures



“I’ve shared them with a lot of people. I’ve shared them with romantic partners, I’ve sent them to strangers on the internet, like, on [social media], I sometimes search for people looking for [intimate content], and then just send them”

-P3

Participants used
40+ platforms

Any platform that can create, share or store visual content **is likely used for intimate content**

Messaging
(apps and SMS)

Social Media Platforms

Hookup/ Dating Apps

Adult Content Platforms

File Share Platforms

Email

“...I’ve got like Telegram, I’ve got Signal, I’ve got WhatsApp, I’ve got Kik, you name it, I’ve got it... occasionally, if there’s something really large, that requires drop boxes and that sort of thing. And I’ll do that”

-P12

What are people concerned about when sharing intimate content?

Recipient Threats

Non-consensual distribution of intimate imagery

What are people concerned about when sharing intimate content?

Recipient Threats

Non-consensual distribution of intimate imagery

Non-recipient Threats

Device Sharing: someone sharing device accidentally finds content

Shoulder Surfing: someone looking over a recipient's shoulder in public accidentally sees content

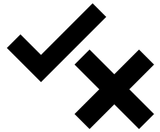
Hacking: breach of the platform databases storing content

Insider Threat: company employee viewing content illicitly

To protect themselves, participants used technological strategies when available and interpersonal strategies to fill in the gaps

Defending against recipient resharing

Before Sharing

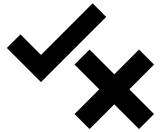


Rule Setting

Screening/ Vetting

Defending against recipient resharing

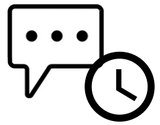
Before Sharing



Rule Setting

Screening/ Vetting

While Sharing

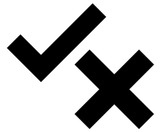


Expiring Messages

Screenshot Notifications

Defending against recipient resharing

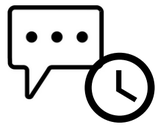
Before Sharing



Rule Setting

Screening/ Vetting

While Sharing



Expiring Messages

Screenshot Notifications

After Sharing

Deletion Request

Message Unsend

Defending Against Recipient Resharing

Before Sharing

Rule Setting

Screening/ Vetting

While Sharing

Expiring Messages

Screenshot Notifications

After Sharing

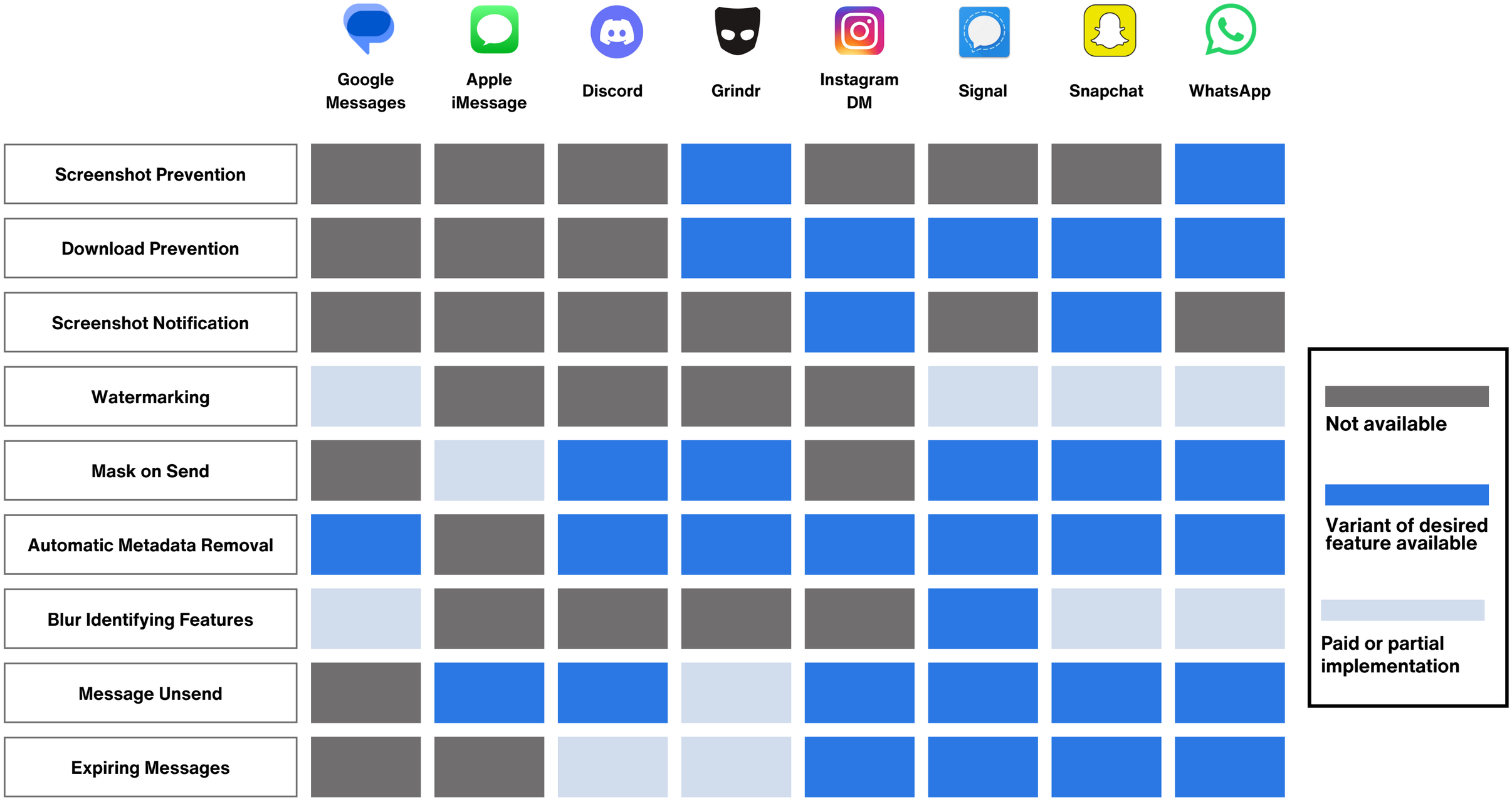
Deletion Request

Message Unsend

Defending against identification

Removing Identifying Features

Metadata Removal


Google Messages
Apple iMessage
Discord
Grindr
Instagram DM
Signal
Snapchat
WhatsApp
Screenshot Prevention
Download Prevention
Screenshot Notification
Watermarking
Mask on Send
Automatic Metadata Removal
Blur Identifying Features
Message Unsend
Expiring Messages
Not available
Variant of desired feature available
Paid or partial implementation

Technological Recommendations

Using protective strategies is time consuming and difficult

“I spend more time scrubbing personal info off my pictures, putting them in private folders, etc., than actually taking said pictures. The learning curve is steep.” (P33)

Friction matters

Safety features can reduce harm

“No matter how much features people put into safety, there’s always always always going to be a risk...[but] as long as the features and the way you’re doing it has the minimum level of safety, that will [stop] most people.”

-P16

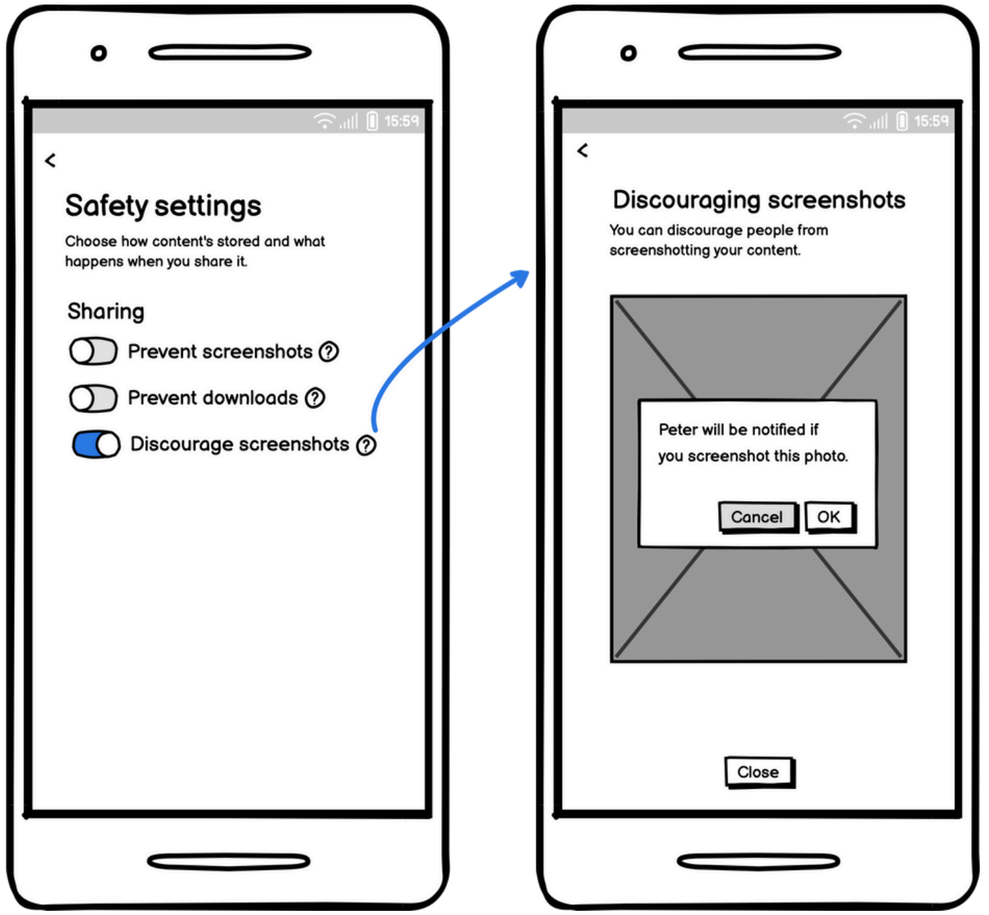
Technological recommendations

Technological recommendations

- Increase availability & visibility of existing features

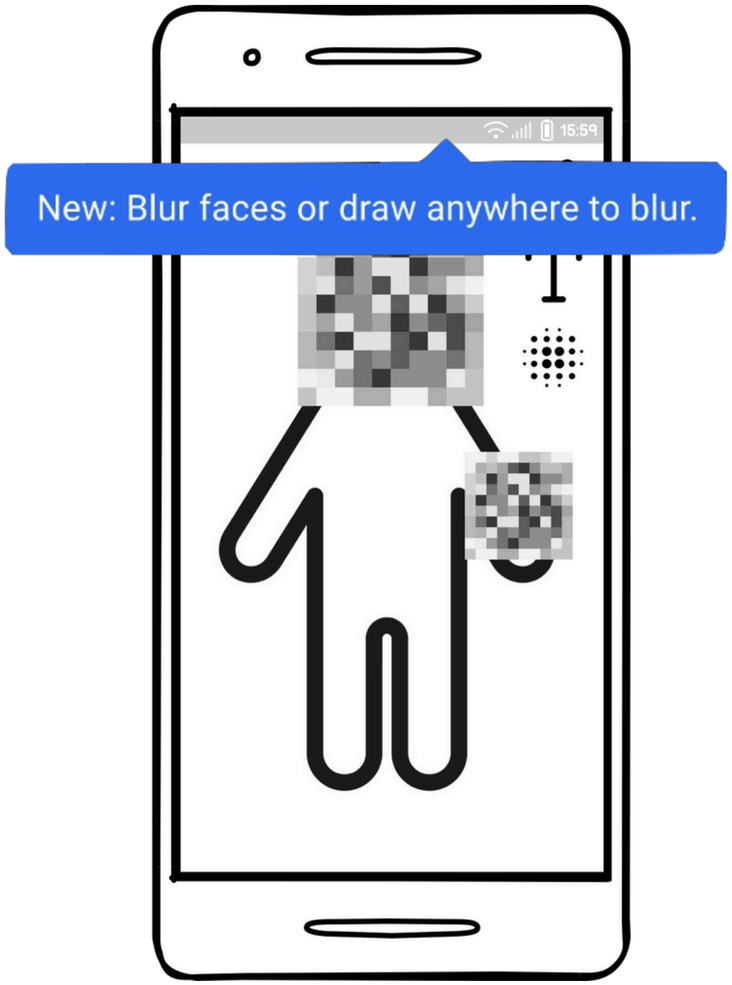
Technological recommendations

- Increase availability & visibility of existing features
- Offer content-level data control and presets



Technological recommendations

- Increase availability & visibility of existing features
- Offer content-level data control and presets
- Support manual strategies



Research Directions

Can safety features incentivize the behaviors they seek to prevent?

“[Expiring messages] sort of invite people trying to screenshot... [because] it almost creates this environment of, oh, this is secret, which sort of invites people to be like, Oh, I’m going to try and hold on to it”

-P31

How do we build and evalute the risks of tools used for proactively discovering NDII?

There’s a need to further investigate the security/privacy risks and reduce false positives

“What if [a hash] could be traced back to me?”

-P10

How can we balance content control with harm documentation?

New design ideas should be explored to resolve the desire for features such as ephemerality while allowing senders to maintain documentation in case of harm

Victim-blaming enacted by the absence of protective technological design

It is critical to reallocate responsibility from individuals to platforms and technologists

“Everyone does it... it’s a part of how we sort of sexually express ourselves, or make money... If something does happen, and it does go badly, then you feel like, 'Oh, well, everyone’s just saying, I shouldn’t have done it.’ So somehow, it’s my fault even though it’s obviously not.”

-P31

Learn more about this work

Personas, wireframes

Paper