# Anti-Privacy and Anti-Security Advice on TikTok:

## Case Studies of Technology-Enabled Surveillance and Control in Intimate Partner and Parent-Child Relationships

Miranda Wei, Eric Zeng, Tadayoshi Kohno, Franziska Roesner

*University of Washington*

Content warning: this talk discusses uses of technology for abuse in interpersonal relationships.

SOUPS 2022 | August 9, 2022 | Boston, USA


## “trends start here”

a social media platform on which users post short-form videos (“TikToks”)

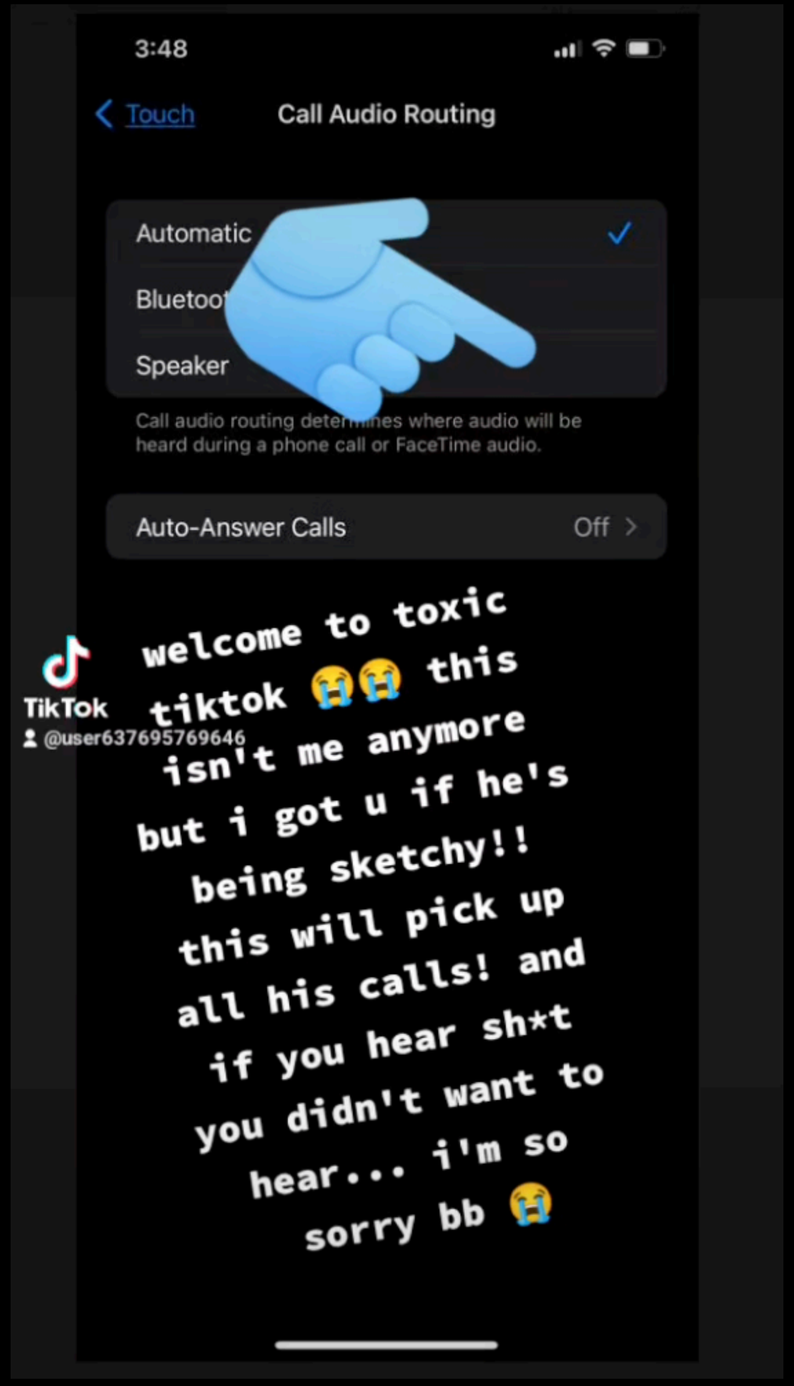
reached 1 billion monthly users in 2021

in early 2022, 28% of users were under 18, and 35% were between 19 and 29

numerous subcommunities: #egirl, #momtok, #fittok,  #relationship, #parenting

# how to eavesdrop

- step 1: set target's phone to pick up automatically
- step 2: call the target's phone
- step 3: eavesdrop on the target




this video is a recreation of a TikTok video from our dataset.

# anti-privacy and anti-security advice

techniques that involve violating privacy or breaking device and account security

videos are presented as guidance intended to be widely seen

# research questions

**RQ1:** **what information or systems** are being targeted in anti-privacy or anti-security advice on TikTok and **by whom**? **how** are these attacks carried out and for **what reasons**?

**RQ2:** how do anti-privacy and anti-security advice videos relate to a **broader societal context**?

# methods

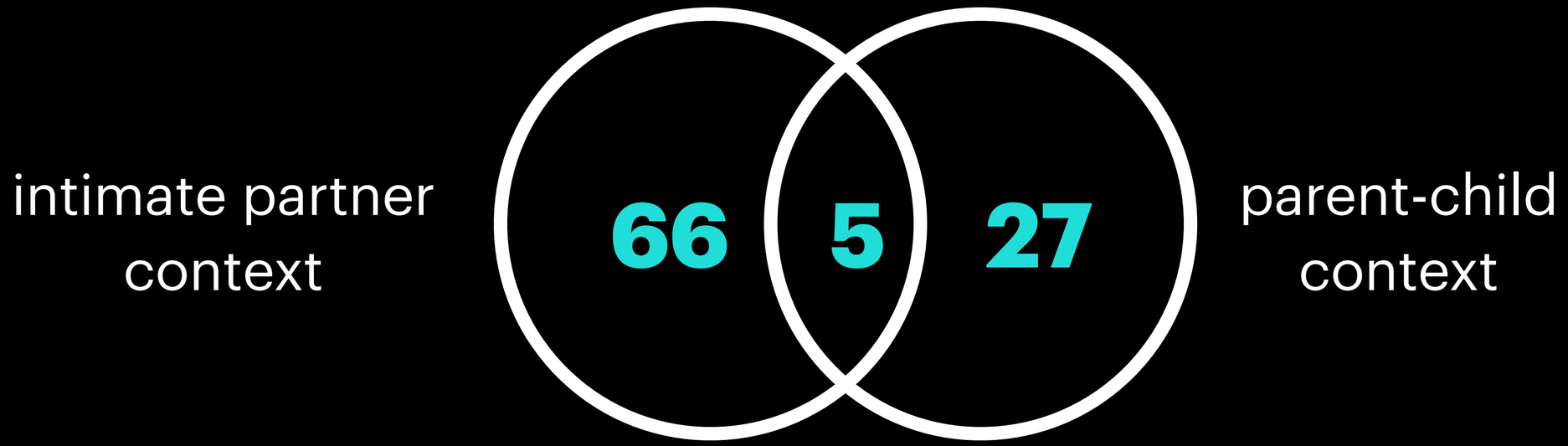
# case study methodology

- progressive focusing: select research questions and cases concurrently

  > *“The aim is to thoroughly understand [the case]. If early [research] questions are not working, if new issues become apparent, the design is changed.” [The Art of Case Study Research, Stake 1995]*

- selected cases: intimate partner and parent-child relationships
- iteratively surfaced relevant videos, mainly using keywords and hashtags
  - e.g., “toxic” “relationships” “parental controls” “kid tracking”

# final dataset: 98 TikToks




- 60 minutes and 14 seconds of audio-visual content
- over 16 million likes across all videos

# data analysis

## deductive thematic analysis

use codebook approach to apply a security threat modeling framework

- what information or systems are being targeted?
- by whom?
- using which techniques?
- for what reasons?

## inductive thematic analysis

generate themes from our high-level observations* of the videos and their context

- what social factors contextualize the anti-privacy and anti-security advice we collected?

** our analyses and interpretations result from our particular social, cultural, disciplinary, and ideological positionings*

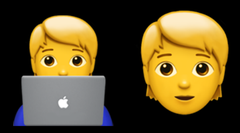
# ethical considerations

- we study public data —> IRB exempt
  - but does public = allowed for research purposes?
  - we recreated all content and paraphrase all quotes
- we surface complicated social ethics questions
  - is surveillance and control permissible in consensual intimate partner relationships or trusting familial relationships?

# results

# overview of case studies

| | intimate partner | | parent-child | |
|---|---|---|---|---|
| actors |  instigator |  target |  parent |  child |
| motivations | detect cheating<br>arbitrary surveillance<br>exert control | | *(parent perspective)*<br>child safety<br>exert control | |
| techniques | exploit data downloads<br>check recently used emojis<br>takeover Snapchat account<br>create fake accounts on dating app<br>... (24 total) | | hide AirTag in bag, clothing, or car<br>install tracking app (e.g., Life360)<br>Sync iCloud messages<br>use text forwarding<br>... (7 total) | |

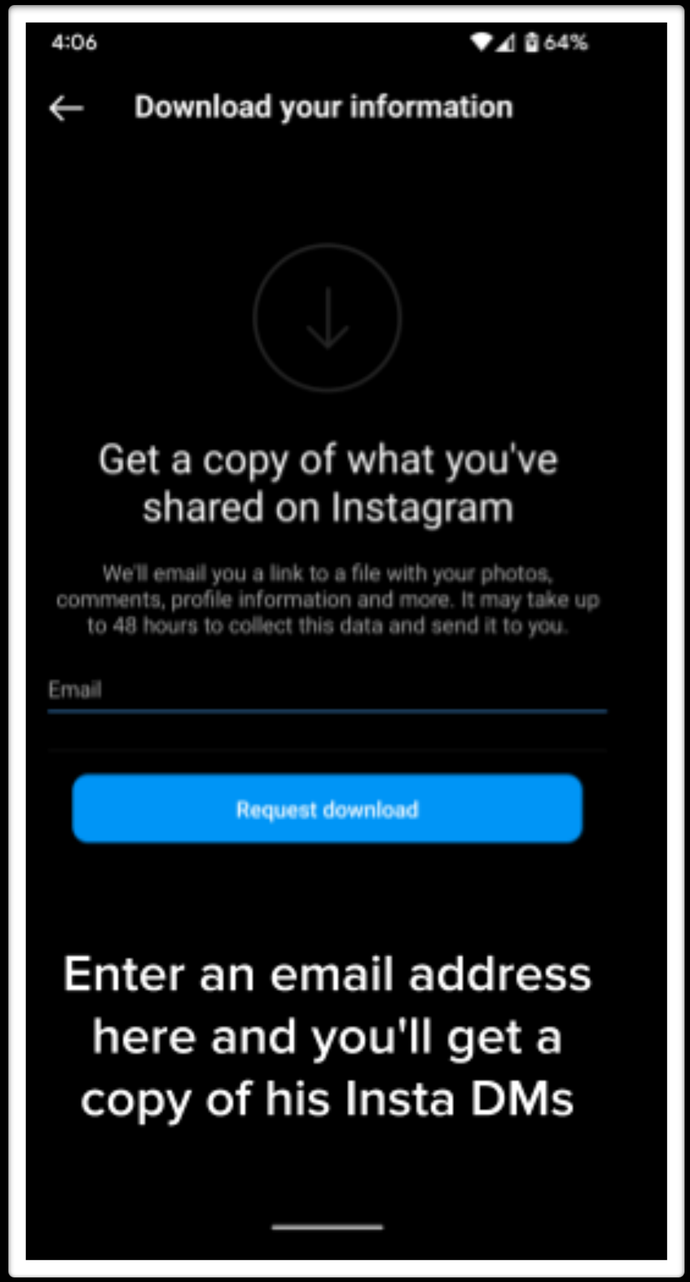


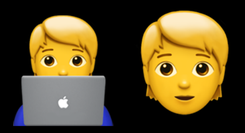
intimate partner context

# goal: surveil digital communications

## technique: exploit data downloads

- data downloads: privacy feature made common by the EU General Data Protection Regulation (GDPR)
- physical access is assumed in intimate relationships: “go on his Instagram”





intimate partner context

# goal: surveil digital communications

## technique: emoji side channel

- exploit smartphone UI: often possible to view keyboard without unlocking
- look for emojis like 🍆 🍑 💦 in the recently used section, infer content of target's messages to others

*"i have personally used this before to confirm or deny my suspicions... just casually ask for his phone and find a way to type something with the keyboard."*

👦👧 parent-child context

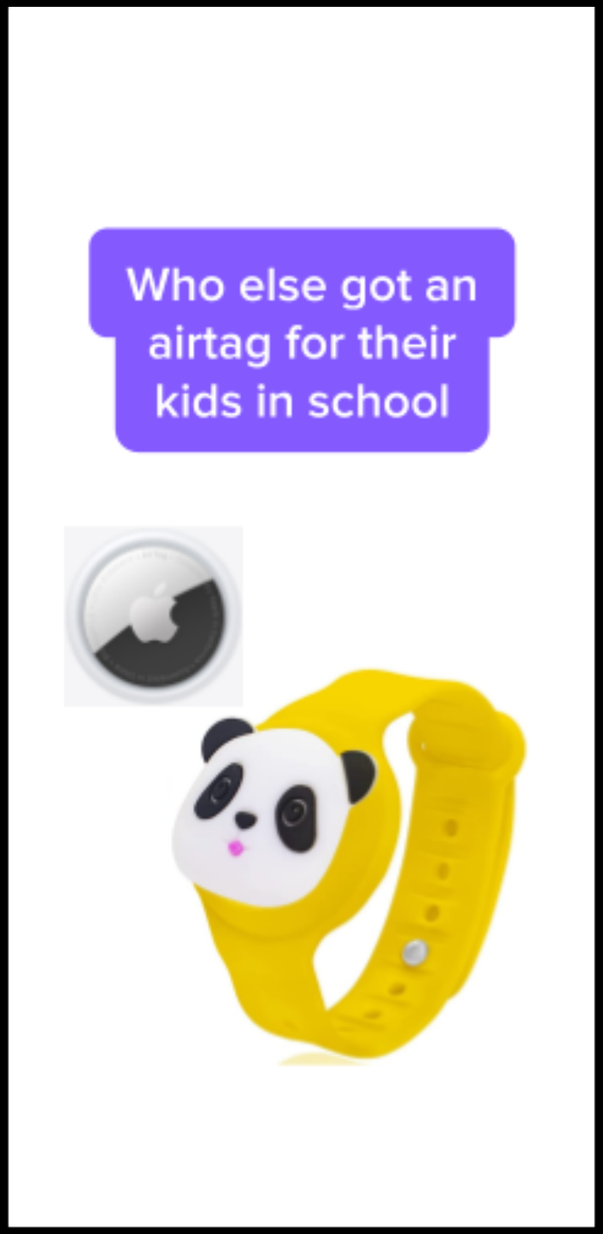
# goal: surveil physical location

## technique: location tracking with AirTags

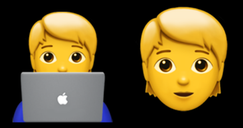
- especially for younger children

## technique: location tracking with apps

- especially for older children
- family surveillance apps, e.g., Life360, Bark

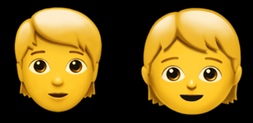


# social context: social acceptability

 intimate partner context

## covert framing

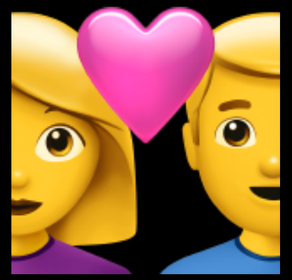
- “disclaimer: these videos are only for entertainment purposes”
- #toxic, #stalker, #crazygirlfriend
- performative self-awareness that surveilling and controlling adults oversteps social and legal norms

 parent-child context

## overt framing

- “i really recommend this if you have a kid going to school”
- #MomHacks, #parenting
- social and legal norms dictate that parents are responsible for the care of their children

# social context: gender



intimate partner context

- assumed female audience with male partners
- *“ladies, the goal is to manipulate the algorithm, basically how men manipulate us”*
- women’s emotional labor in heterosexual relationships

parent-child context

- assumed mom with children
- *“#SaveOurChildren #MomHack #MomsOfTikTok”*
- women’s domestic labor in family relationships


the round pegs in the square holes.
The ones who see things differently.
They're not fond of rules. And they
have no respect for the status quo.
You can quote them, disagree with
them, glorify or vilify them. About
the only thing you can't do is ignore

# conclusion

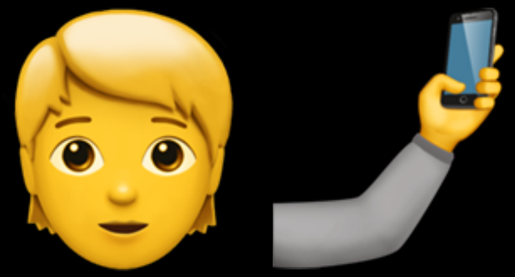
# anti-privacy and anti-security advice on TikTok is surveillance and control made fun and easy

information is easy to find

techniques are easy to execute

designed to go viral

# classic security assumptions are outdated



beyond one person, one device:
need to design for interpersonal adversaries with physical access

deeply personal motivations for anti-privacy and anti-security advice calls for socio-technical solutions

# TikTok as a data source for security and privacy

## benefits

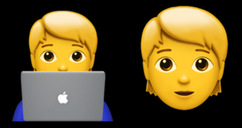
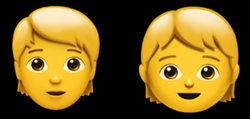
- distinctive openness that counteracts social desirability bias in security and privacy
- uniquely young user and creator base

## challenges

- ethical considerations of gathering public data
- platform limitations to gathering relevant data
- highly contextualized data

# Anti-Privacy and Anti-Security Advice on TikTok:

## Case Studies of Technology-Enabled Surveillance and Control

in intimate partner  and parent-child  relationships


✨ **Miranda Wei**
*weimf@cs.washington.edu*

🏂 **Eric Zeng**
*ericzeng@cmu.edu*

🤦 **Tadayoshi Kohno**
*yoshi@cs.washington.edu*

😻 **Franziska Roesner**
*franzi@cs.washington.edu*


- collected 98 TikTok videos showcasing anti-privacy and anti-security advice
- surfaced creative techniques used for deeply social motivations
- classic security assumptions are outdated
- TikToks are a valuable data source for user research on security and privacy