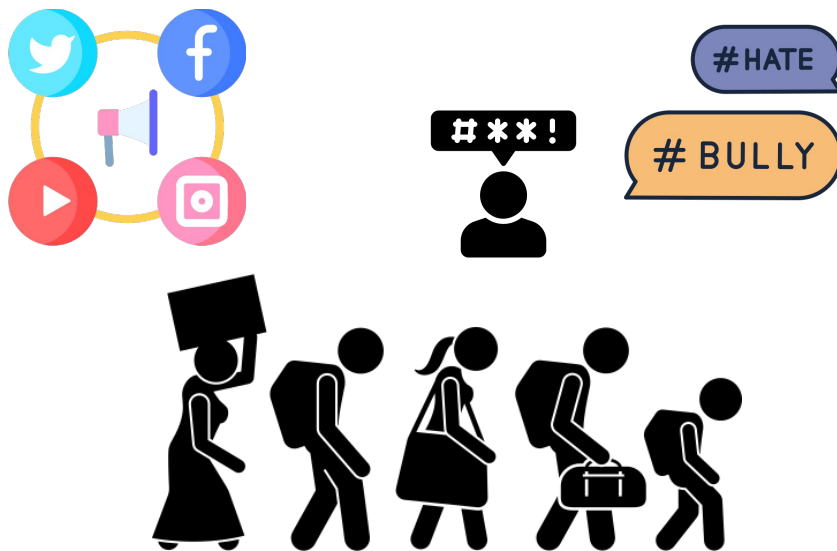# Research Portfolio

by Arjun Arunasalam

Overview

➔ These slides showcase my expertise in conducting user-centric methodologies in two projects

◆ Research Project 1: **Understanding the Security and Privacy Implications of Online Toxic Content on Refugees**

◆ Research Project 2: **ATTention Please! An Investigation of the App Tracking Transparency Permission**

➔ ***Both*** these research projects have been accepted and are set to appear in Usenix Security 2024, a top tier computer science venue

Understanding the Security and Privacy Implications of Online Toxic Content on Refugees

Research project by **Arjun Arunasalam**, Habiba Farrukh, Eliz Tekcan, Z. Berkay Celik
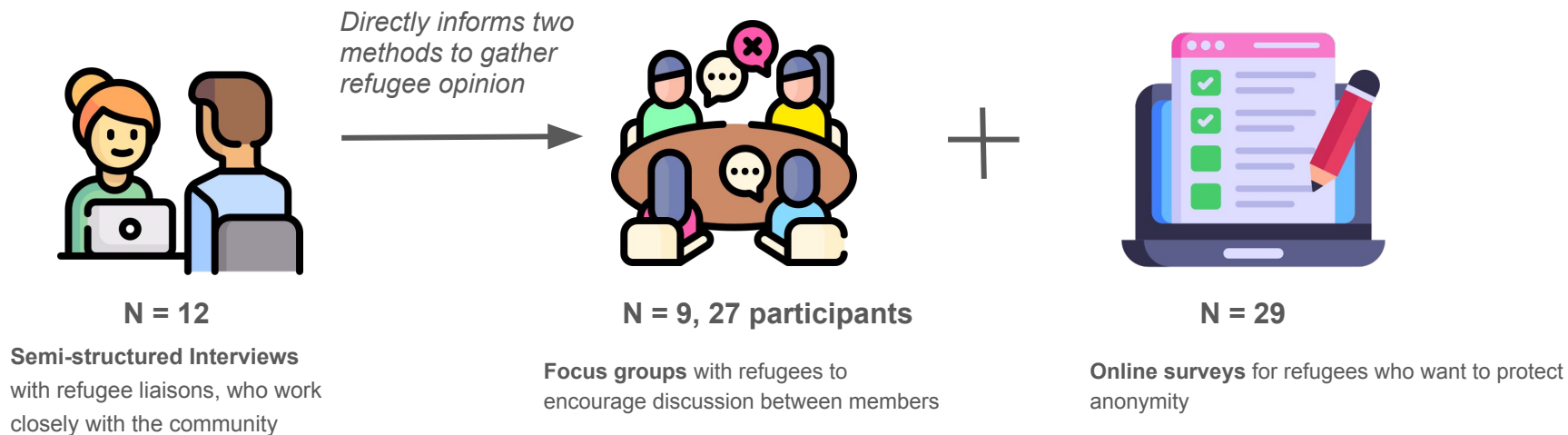
Problem: How are refugees online security and privacy actions impacted by toxic content?

⭐ Accepted in **USENIX Security 2024** (top-tier Computer Science venue*) ⭐

* Top-tier computer science venue per <u>csrankings.org</u> and <u>conferenceranks.com</u>

images: Flaticon.com

Understanding the Security and Privacy Implications of Online Toxic Content on Refugees

Method & Design: Mixed-methods approach - semi-structured interviews, focus groups, surveys

Directly informs two methods to gather refugee opinion

N = 12

Semi-structured Interviews with refugee liaisons, who work closely with the community

N = 9, 27 participants

Focus groups with refugees to encourage discussion between members

N = 29

Online surveys for refugees who want to protect anonymity

images: Flaticon.com

Understanding the Security and Privacy Implications of Online Toxic Content on Refugees

Insights:

- Through **(1)** mixed-methods, we characterize refugees' **(2)** social media use, **(3)** exposure to toxic content, **(4)** the security and privacy actions they take in response.
- We also showcase **(5)** barriers: how existing features fail to meet user needs.
- Finally, we understand **(6)** refugees' opinions on platform involvement and their ideal features to combat toxic content.
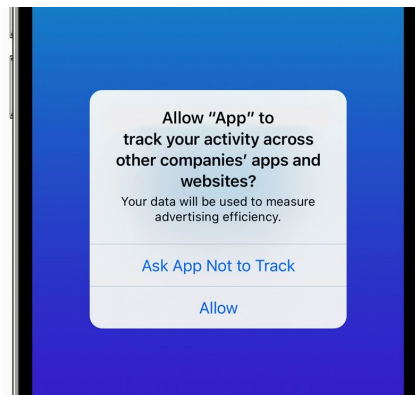

images: Flaticon.com
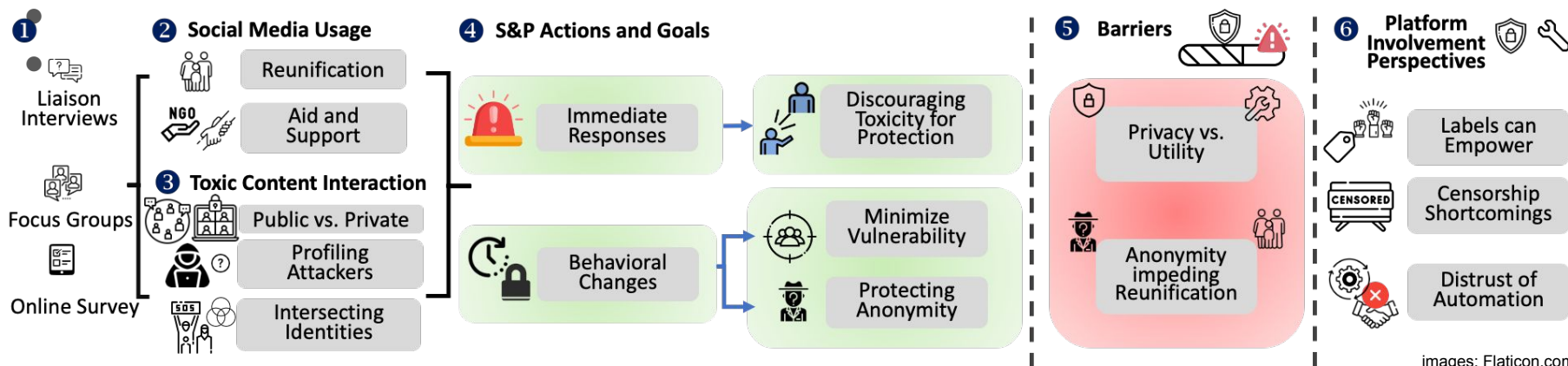
ATTention Please! An Investigation of the App Tracking Transparency Permission

Research project by Reham Aburas, **Arjun Arunasalam**, Habiba Farrukh, Jason Tong, Antonio Bianchi, Z. Berkay Celik*

Problem: How do mobile end users perceive Apple's App Tracking Transparency Permission Alerts and can deceiving patterns impact users?

⭐ Accepted in **USENIX Security 2024** (top-tier Computer Science venue) ⭐

Allow "App" to
track your activity across
other companies' apps and
websites?
Your data will be used to measure
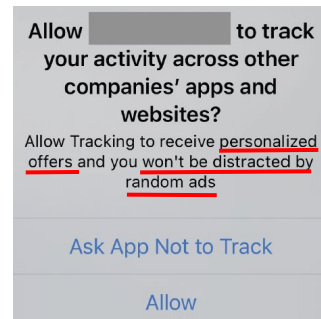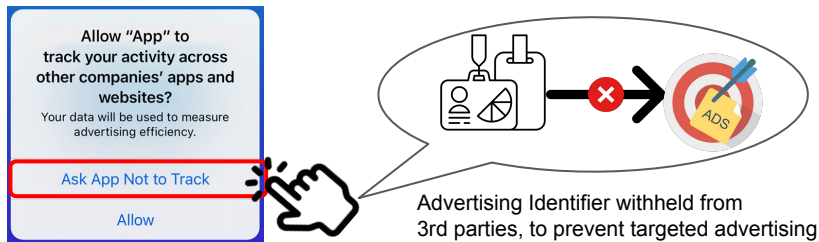advertising efficiency.

Ask App Not to Track

Allow

* Second author. This project comprises many additional components (e.g., static, dynamic analysis of apps, machine learning). I was primarily involved in designing the user study portion.

ATTention Please! An Investigation of the App Tracking Transparency Permission

Background:

(1) App Tracking Transparency refers to the alert which requests permission to access user data for tracking a user or device.

(2) Denying this permission prevents the users' IDFA (advertising identifier) from being shared with other parties.

(3) The text in the permission is designed by developers who can customize to deceive/trick users into granting permission to track.

Allow "App" to
track your activity across
other companies' apps and
websites?
Your data will be used to measure
advertising efficiency.

Ask App Not to Track

Allow

Advertising Identifier withheld from
3rd parties, to prevent targeted advertising

Allow ▮▮▮▮▮▮ to track
your activity across other
companies' apps and
websites?
Allow Tracking to receive personalized
offers and you won't be distracted by
random ads

Ask App Not to Track

Allow

Deceptive patterns (e.g.,
granting permission does not
provide offers)

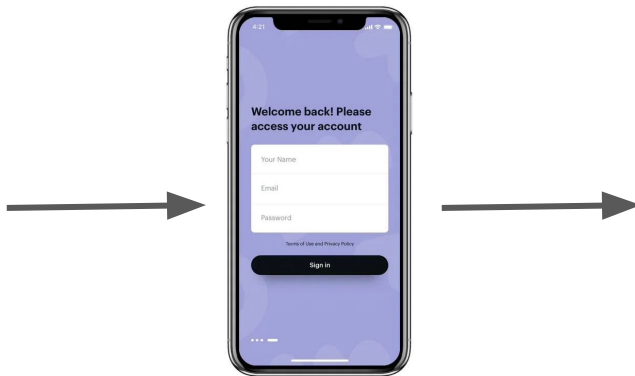## How are users impacted by this?

images: Flaticon.com

ATTention Please! An Investigation of the App Tracking Transparency Permission

Method & Design:

Between subjects user study with N=114 participants to understand (1) how users perceive the permission alert and (2) the impact of deceptive alerts.
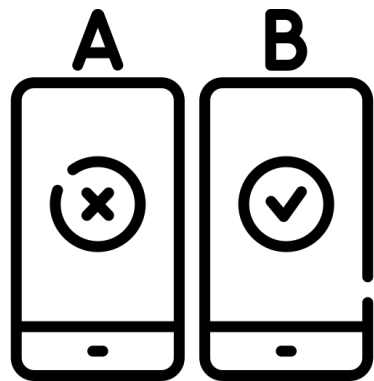
Between-subjects online survey with 114 participants.
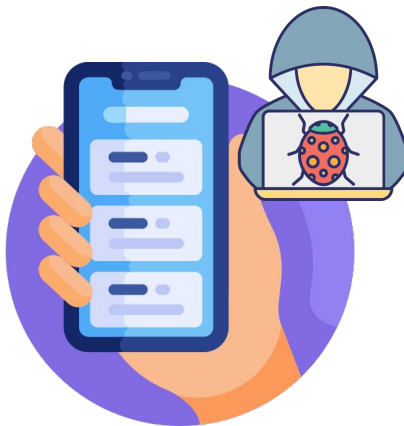
Leveraging **interactive app prototypes**

Measuring **user perceptions and impact of alerts** using **inferential statistics**

images: Flaticon.com
marvelapp.com

ATTention Please! An Investigation of the App Tracking Transparency Permission

Insights:

Users incorrectly believe that selecting "Not track" protects various data types beyond Advertising ID

Users incorrectly believe they will receive rewards/better app features if they allow tracking

Users are often confused about the text in permission alerts

images: Flaticon.com

Thank you!

Please take a look at preprints of these papers for more information

Email: aarunasa@purdue.edu for questions