5RIGHTS FOUNDATION

Preliminary Findings on Walkie Talkie – All Talk Safety Concerns

Walkie Talkie connects minors in unmoderated chats, raising serious concerns over privacy, safety, and exposure to harmful content. Stricter safeguards are urgently needed.

Walkie Talkie - All Talk presents itself as a fun and social platform for Gen Z to connect in real-time. However, beneath its playful exterior, the app lacks essential safeguards, putting minors at significant risk. Our initial findings reveal **weakly implemented age verification, random 'chat roulette' pairings with strangers, and inadequate moderation**. As a result, children are exposed to **inappropriate conversations, bullying, and potential exploitation**. Policymakers, child safety advocates, and tech experts must recognise this as yet another example of an app failing to prioritise child protection in its design.

How Walkie Talkie Works

The app allows users to communicate through live voice chats, with three main modes:

- **Public Mode**: Users join live conversations on open frequencies, where they can speak with anyone. There are no safeguards to prevent minors from engaging with adults or being exposed to harmful content.
- **Duo Mode**: Users are randomly paired with others for one-on-one voice chats (similarly to Omegle), with limited filtering options.
- **Groups Mode**: Users can create private group chats with friends or meet new people, with minimal privacy controls.

Additionally, the app algorithmically suggests new 'friends' and enables private messaging, making it easy for users to stay connected beyond initial conversations.

Major Safety Concerns

1. **Weak Age Verification & Privacy Risks**

Walkie Talkie asks users to input their date of birth but does not enforce robust verification. This means anyone can enter a false age and access conversations with children. While it claims to be for users aged 12-17, there are no real measures to prevent adults from joining or interacting with minors.

Furthermore, the app collects personal data, including phone numbers and optional details like gender identity. Without strong security measures, this poses serious privacy risks for young users. There is also the question of whether it is truly necessary to collect some of this personal data.

2. Exposure to Harmful or Inappropriate Content

The app's design means that users can encounter a wide range of inappropriate conversations, including:

- Bullying, harassment, and hate speech.
- Discussions that glorify sensitive topics like mental health struggles or self-harm.
- Inappropriate adult-themed content.

A recent internal test conducted by 5Rights revealed instances where minors were openly discussing distressing personal experiences with bullying, with no intervention or signposting support from moderators. We struggled to find any option to report the conversation to a safeguarding team.

We also encountered instances of children making disparaging comments to one another around skin colour and sexuality but again struggled to find any option to report this.

Additionally, a recent update allows users to send photos in chats, described on the app's store page as a way to "spice up your chats," which raises further safety concerns.

3. Unregulated Stranger Interactions and Recommender System

The random pairing system in Duo Mode and Public Mode means minors could be matched with anyone. There are no visible safeguards to prevent predatory behaviours, making it dangerously easy for bad actors to engage with young users.

The app also algorithmically suggests a list of "friends" to minor users. A recent update allows users to create group chats, advertised as a way to avoid muting random strangers in Public Mode. However, this also enables potential bad actors to gather selected individuals into unmoderated conversations, increasing the risk of harmful interactions.

4. Premium Features & In-App Purchases that Worsen Risks

For a fee, users can unlock additional features, including:

- The ability to create up to 100 private groups.
- Photo-sharing in chats.
- Voice filters to disguise identity.
- An in-app shop offering extra features.

These features, while marketed as fun extras, can be exploited by those looking to manipulate or deceive users.

5. Constant Notifications that Pull Kids Back

Walkie Talkie bombards young users with notifications, **constantly prompting them to return to the app**. These notifications create a sense of urgency and **FOMO (fear of missing out)**, encouraging excessive screen time and making it harder for children to disengage. The app's design fosters habitual use, keeping kids connected even when they might want or need a break.

What Needs to Change?

To make Walkie Talkie a safer platform for children, the following measures must be implemented:

- **More Robust Age Verification**: Implement more robust age verification to ensure users are who they claim to be.
- **Effective and More Visible Content Moderation**.
- **Safer User Controls**: Allow users and parents to set stricter privacy controls, including blocking unknown contacts, filtering topics, and restricting access to public chats.
- **Reduce Harmful Notifications**: The app should limit excessive notifications and provide users with clear options to manage or disable them.

If platforms like Walkie Talkie do not take responsibility alone, **policymakers must step in and enforce regulatory measures to protect children and teens online**.

The Urgent Need for Regulatory Action

Walkie Talkie is just one of many apps that prioritise engagement over safety. Without intervention, children will continue to be exposed to serious risks in unmoderated digital spaces. **Policymakers, tech leaders, and child protection advocates must work together to push for stronger online safety regulations that hold platforms accountable**.