"You Have to Ignore the Dangers": User Perceptions of the Security and Privacy Benefits of WhatsApp Mods

Collins W. Munyendo*§, Kentrell Owens†§, Faith Strong$^{\diamondsuit}$,
Shaoqi Wang†, Adam J. Aviv*, Tadayoshi Kohno†, Franziska Roesner†
$\star$ *The George Washington University,* † *University of Washington,* $\diamondsuit$ *Austin College*

Abstract—**WhatsApp is the most popular social messaging platform, and modified versions (or "mods") of the official WhatsApp are increasingly popular. Mods advertise additional features and customization. However, some of these features, e.g., retaining deleted messages and statuses, enable mod users to subvert the privacy of others, and have the potential for serious security and privacy implications. In this study, we explore user perspectives of WhatsApp mods through an interview study (n=20) of mod users in Kenya, one of the countries with the highest WhatsApp mod usage. Many turned to WhatsApp mods for their "advanced" features to protect themselves (e.g., "anti-delete" for legal liability), while others admitted to using mod features to hide their behavior or to stalk others. To understand how users' expectations of WhatsApp mods align with the apps' behavior, we identify and analyze 13 instances of the most common mod (GB WhatsApp). While WhatsApp mods contained the features they claimed to offer, some participants incorrectly believed that features currently available in the official app only existed in mods. Additionally, several mods were significantly over-permissioned compared to the official WhatsApp, despite participants believing that they requested the same permissions as the official app. While almost half of participants indicated they trust mods more than the official WhatsApp, we found two mods contained malware. The use of WhatsApp mods poses risks to mod users and those they communicate with, but also empowers users in ways that the official app does not. We caution developers and mod users to do their due diligence before using or distributing mods.**

1. Introduction

Usable security and privacy (S&P) research has largely drawn participants from WEIRD (Western, Educated, Industrialized, Rich, and Democratic) populations [18], [24]. Given that the *majority* of technology users are not from WEIRD countries [19], an increasing number of usable S&P researchers have started to explore non-WEIRD populations, highlighting how differently people use technology around the world. For example, cultural expectations in South Asia dictate that women share their mobile phones with others in the household, forcing them to resort to techniques such as content deletion to protect their privacy [42].

This work focuses on one component of the broader non-WEIRD technology world: the modded WhatsApp ecosystem. While less common in the West, *modified versions* of the popular [48] WhatsApp client (a.k.a., "mods" or "modded WhatsApp") are becoming increasingly popular in Africa [12]. These mods claim to offer additional features and are interoperable with the official WhatsApp. However, they are not maintained by WhatsApp nor distributed through conventional mobile marketplaces, such as the Google Play Store. Further, the use of modded WhatsApps has serious potential S&P implications for the mod users and to those with whom they communicate. For example, mod users may have access to deleted messages (e.g., via an "anti-delete" feature) while also hiding information (e.g., by freezing their "last seen" time so that no one knows they are currently using the app). However, mod users risk installing software that is modified, downloaded from unscrupulous sources, and could potentially expose them to malware.

In this paper, we explore why and how people use modded WhatsApps, as well as how their expectations of these apps align with the mods' behavior. Specifically, we seek to answer the following four research questions:

RQ1: **Usage:** *Why and how do people use WhatsApp mods?*

RQ2: **Propagation:** *How do users describe learning about, acquiring, and updating WhatsApp mods?*

RQ3: **Perceptions:** *What are user concerns, practices, and mental models when using WhatsApp mods?*

RQ4: **Expectations:** *How do WhatsApp mods align (or misalign) with users' expectations or beliefs?*

To answer these research questions, we conducted in-depth, semi-structured interviews ($n = 20$) with WhatsApp mod users in Kenya. We focus our investigations on Kenya as it is one of the countries with the most WhatsApp mod users globally [25]. To contextualize participants' perspectives, we additionally conducted an analysis of common WhatsApp mods that participants reported using by reviewing the features they purport to offer, the permissions they require to access, as well as whether they contain malware.

We find that most participants turn to WhatsApp mods because of the "advanced" features that the mods offer, including an "anti-delete" feature that enables them to preserve messages or updates posted by others even when they are deleted. Other common reasons for using WhatsApp mods include an ability to save the time-limited status

§. Co-first authors; Collins and Kentrell contributed equally to this work.

updates of others and the additional themes and wallpapers that the mods offer. Most participants indicate learning about WhatsApp mods from their friends and family members, with a majority not considering any factors when installing the mods as they are more motivated to get the app.

We also find that WhatsApp mod users' security and privacy mental models seem to revolve around their social circles, i.e., their friends and colleagues, and not the mods themselves and the potential risks they pose to their users. We further observe tensions between modded WhatsApp users' desire for more control over their visibility when using WhatsApp while simultaneously wanting other users to *not* have the same level of control. While some participants told stories of others using the mods' additional features to spy or stalk on others or being a victim of this, one person admitted to carrying out the stalking themselves. We further surface misconceptions about which features are unique to WhatsApp mods; several participants were motivated to use mods by features that are also currently present in the official app. By investigating common mods used by participants, we find that these mods are systematically over-permissioned compared to the official WhatsApp, with some marked as outright malicious by VirusTotal [2].

Our results indicate that the use of modded WhatsApp poses various security and privacy risks, both to users and even non-users of these apps. Users of the mods may be inadvertently installing malware on their devices, while undermining the privacy of others, e.g., by retaining information that non-users have deleted. At the same time, some modded apps' features are useful, and some have been adopted by the official WhatsApp. In the end, we choose not to directly answer the question, *should people use WhatsApp mods?* Instead, we highlight the risks to both users and non-users of WhatsApp mods, the implications of using these mods, and how WhatsApp mods may empower and satisfy users in ways that the official WhatsApp does not.

2. Background and Motivation

Here, we provide a background on WhatsApp, modded Android apps, and WhatsApp mods and their features.

2.1. WhatsApp

WhatsApp is the world's most popular social messaging app [48] with over two billion users [56]. Messages and calls over WhatsApp have been end-to-end encrypted (E2EE) since 2016 [23], and recently, WhatsApp has introduced additional features related to security and privacy, e.g.,

- Chat lock: Allows users to hide specific chats behind a biometric or password (May/Nov 2023) [58], [59].
- Multiple accounts on one device (Oct 2023) [60].

As we will discuss more in Section 3, some participants in our user study described these features (and others) as reasons they used WhatsApp mods over the official WhatsApp (despite the features already being in the official WhatsApp).

Although we do not have insight into the origins of various features in the official WhatsApp, we note that features that have recently been implemented in the official app (e.g., chat lock and allowing multiple accounts on one device) were already present in some WhatsApp mods years before; one website advertised a mod with these features in 2021 [1]. WhatsApp may be implementing some mod features to discourage users from using WhatsApp mods; in its blog post for its new feature allowing multiple accounts to be used (a popular mod feature mentioned by participants in our study), the post ended with a statement encouraging users to *not* use mods to access this feature [60].

2.2. Modified Android Apps

Android apps are sometimes modified (or "repackaged") to incorporate preferred features into the apps (e.g., a new design for a social media app), to access premium features for free (assuming they are enforced client-side), or to impersonate an app and monetize its users [38], [67]. Several existing tools (including some built into Android Studio) allow decompiling APKs (i.e., Android Packages) to human-readable code to facilitate debugging, and a knowledgeable developer could decompile, modify, and repackage an app in minutes [13]. Using these tools, people decompile the apps, modify the code, and repackage them and sign them using their own digital certificates (i.e., the developer's public-private key pair and other metadata). While there are some benign reasons for modding an app, research has shown that modded apps are a vehicle for malware [8], with one study finding that about 86% of Android malware is from modded apps [68]. While we focus on Android apps, and particularly modified WhatsApps, given Apple's recent announcement regarding alternative app marketplaces in response to the EU's Digital Markets Act [3], we expect that modded apps may soon become widespread on iOS devices.

2.3. WhatsApp Mods

WhatsApp Mods are unofficial, modified versions of WhatsApp developed by third parties. These apps offer additional features beyond what is provided by the official versions of WhatsApp, e.g., the ability to disable incoming calls, and are interoperable with the official versions. We believe that these mods still support E2EE (due to their continued interoperability and some ad-hoc testing of WhatsApp's signature verification feature), but that does not mean that information is not extracted once messages are decrypted client-side. Although the early origins of these mods are not well-documented, they are believed to be descended from an open-source reverse engineering effort called "libwhatsapp" [14] that aimed to create a usable gateway to WhatsApp; this library has been archived and is currently read-only [12]. The original GB WhatsApp page (believed to have originated in Syria during its conflict) was taken down in response to legal threats from Meta (then Facebook) in August 2018 [12]. WhatsApp mods have become very popular in some places in Africa, e.g., Kenya [12]. At the same time, these apps pose potential security and privacy risks as they are mostly distributed through third-party websites or marketplaces or via sharing of the APKs directly (as confirmed by several participants in our interviews), evading app store security measures [41].

Modded app features. The WhatsApp mods in our study claimed to provide several features not offered by the official WhatsApp. In this paper, we explored a subset of the features that have clear security and privacy implications for *interpersonal communication*:

- **Anti-delete:** Often enabled by default, this feature preserves messages and statuses (ephemeral text or media updates that expire after 24 hours) posted by other users, even if they have been deleted globally.
- **Asymmetric hiding of read receipts:** This feature allows a WhatsApp mod user to receive messages and view messages without the sender being notified that the messages have been read while *the mod user is still notified about the sender reading their messages*. This differs from official WhatsApp where hiding read receipts is symmetric; in the official WhatsApp, either both users can see or both cannot see read receipts [63].
- **Hide status views:** Similar to the previous feature, this allows a WhatsApp mod user to view statuses without their name showing up in the list of status viewers.
- **Freeze "last seen":** WhatsApp mod users can freeze their "last seen" time (e.g., `11:57 am`) to conceal when they are actively using the app.
- **Disable incoming calls:** Mod users can reject incoming calls and *how* the call is rejected, e.g., they can make it appear as if they did not answer after several rings or that they do not have internet connection. In official WhatsApp, one can disable calls from unknown numbers and block calls from specific numbers [64] but not block calls from all numbers.

Several other mod features are available in the official WhatsApp. However, there exists some confusion among participants about which features are only available through the mods. We discuss these misconceptions in Section 3.2.

2.4. Threat Model

The potential security and privacy (S&P) risks from using WhatsApp mods motivate our investigation. In this work, we consider two primary threats to users (both WhatsApp mod and *non*-mod users):

Threats from mod developers. There is a security risk to WhatsApp mod users (and the people they communicate with) from malicious or careless developers. A malicious developer could use the mod to compromise users' devices–e.g., to install adware for financial purposes. A careless developer could also insecurely transmit or store users' data.

Threats from modded apps' users. People trust that data sharing in WhatsApp will be symmetrical: e.g., if I enable read receipts, someone that I send a message to can only see that I have read a message if they also have read receipts enabled. WhatsApp mods' claimed features break this trust.

TABLE 1: Demographics of participants.

		No.	**%**
Gender	Female	10	50.0
	Male	10	50.0
Age	18 - 24	9	45.0
	25 - 34	11	55.0
Education	High school	8	40.0
	Diploma*	5	25.0
	Bachelors	5	25.0
	Postgraduate	2	10.0
IT/CS Background	Yes	8	40.0
	No	12	60.0
Employment	Student	7	35.0
	Employed	12	60.0
	Self-employed	1	5.0

*In Kenya, diplomas focus on practical skills and vocational training and are usually completed in 1 to 2 years.

3. Usage, Propagation, and Perception of Mods

To understand why and how people use (**RQ1**), propagate (**RQ2**), and perceive (**RQ3**) modified WhatsApps, we first conducted in-depth, semi-structured interviews ($n = 20$) with participants that use modified WhatsApps in Kenya.

3.1. Methods

Recruitment and demographics. To recruit participants, we first employed the "anti-delete" feature (see section 2), one of the most common features of WhatsApp mods which is often enabled by default. One of the researchers, who is from Kenya, posted and immediately deleted an advertisement for the study on his WhatsApp status. Five users of WhatsApp mods were able to view and respond to this deleted update, and were recruited to the study. We also posted about the study in some local WhatsApp groups in Kenya. Afterward, we used snowballing [17] to recruit further participants, whereby participants recommended others to participate whom they know use WhatsApp mods. For all participants, we used the "anti-delete" feature to verify they were indeed using WhatsApp mods by sending them a code and immediately deleting it. Only participants that were still able to view and reply to this code were included.

To be eligible for the study, participants had to be 18 years of age or older, and current users of any WhatsApp mod. While we had an equal number of male and female participants, most participants were young (aged mostly between 25 to 34 years), with varying education levels. Table 1 has the full demographics of participants.

Interview procedure. We first asked participants to indicate all WhatsApps they currently use, as it is possible to use multiple WhatsApps and mods at the same time. We asked these participants to discuss only the most frequently-used mod. We then asked whether they were also aware of the official WhatsApp and, if so, the similarities and differences between their WhatsApp mod and the official WhatsApp. Subsequently, we inquired approximately when participants started using their WhatsApp mod and their primary motivation for doing so. We also asked participants how they learned about and installed their WhatsApp mod, as well as any factors they considered when doing so.

After asking participants about one thing they like and dislike the most about their WhatsApp mod, we asked whether they had recommended the app to any other people. Our next questions centered around trust in the modded and official WhatsApps, including factors that make participants to trust or not trust these apps as well as their developers or owners. We additionally inquired about any concerns that participants have in their WhatsApp mods.

We further asked about participants' update practices for their WhatsApp mods, including why and how they make these updates. We also asked about any challenges they had faced because of using mods. Lastly, we asked whether participants post on their WhatsApp status as well as any privacy controls they have around these updates. The full interview protocol is available in Appendix A.

Data collection. We first conducted two mock interviews with two qualitative researchers from our lab via Zoom. Based on their feedback, we added more probes and follow-ups to some questions, following best practices for qualitative work [10]. Afterward, we conducted three pilots with users of WhatsApp mods in Kenya. These interviews were conducted remotely through WhatsApp audio calls.

We conducted all interviews remotely via WhatsApp audio calls in November 2023. As our interview procedure was only slightly altered following the pilot interviews we included the three pilots in our final analysis, and so in total, we interviewed 20 participants, with interviews lasting 38 minutes on average. We took notes during the interviews, and stopped observing new themes after about 15 interviews; therefore, 20 interviews was likely sufficient for us to reach saturation. All interviews were audio-recorded and conducted in English, one of the official languages in Kenya [36]. Similar to recent studies in Kenya [34], [33], participants were compensated with either 125 minutes of call time or 2 GB worth of internet data. This was directly transferred to participants' phones after the interviews.

Data analysis. Using MAXQDA [30], we qualitatively analyzed the interview transcripts [10]. Two researchers began by collaboratively coding one transcript to develop an initial primary codebook, and then used this codebook to independently code three transcripts before meeting to resolve differences and update the codebook. The researchers repeated this process until all transcripts had been coded, regularly meeting to resolve differences, update the codebook, and discuss emerging themes. At the end of this process, the researchers revisited all transcripts to confirm everything had been accurately coded and all updates to the codebook were consistent across all the transcripts. Since the two researchers resolved differences across all the transcripts, there was no need to compute inter-rater reliability [31].

Limitations. This study has several limitations. Foremost, our investigations are only limited to Kenya. While Kenya is one of the countries with the highest adoption and usage of WhatsApp mods [25], future work is needed to explore how these apps are perceived and used in other countries and contexts. As is typical for qualitative studies, our sample size was relatively small and young. While we do not claim that our results generalize within Kenya, we took comprehensive notes during each interview and only ended data collection after we stopped noting new themes. Additionally, these apps are primarily used by young people, as mentioned by several participants in the study, and so we would expect a younger demographic in a sample of such users.

As is typical for paid studies, some participants tried to participate in the study for financial reasons despite not meeting the eligibility. We mitigated this by using the "anti-delete" feature of WhatsApp mods to ensure participants were actually using these apps before conducting interviews. One participant that had been recommended to participate was excluded this way. This study may also suffer from social desirability bias where interviewees try to look more favorable to the interviewer. We tried to mitigate this by telling participants that we were not testing them but only interested in their honest thoughts and practices. Most participants appeared honest, e.g., one admitting that they had used their WhatsApp mod to stalk their partner.

Ethical considerations. This study was reviewed and approved by two academic institutions' Institutional Review Boards (IRBs). Participation was voluntary and participants could withdraw from the study at any time without any consequences. We also encouraged participants not to respond to any questions they were not comfortable answering. To minimize any potential risks of unauthorized access of the study data, we did not collect any personally identifying information (PII) from participants during the interviews. Any PII captured or inadvertently disclosed by participants during the interviews was removed during transcription. In Section 6.2, we discuss our plans to disclose our findings to WhatsApp mod users and developers.

3.2. Qualitative Results (RQ1, RQ2, & RQ3)

To address **RQ1**, **RQ2**, and **RQ3** , we now present qualitative results from our interview study ($n = 20$) with WhatsApp mod users in Kenya. As counts and percentages could imply generalizability, we primarily use quantifiers such as most and few when presenting the results. For certain results where we do provide counts, we caution against drawing any generalized findings. Our fact-checking of participant sentiments in this section is derived from our feature analysis, described later in section 4.2.

3.2.1. Common Mods and Reasons for Their Use (RQ1).

In response to **RQ1**: *Why and how do people use WhatsApp mods?*, we detail the WhatsApp mods most commonly-used by participants as well as their reasons for using these apps.

TABLE 2: WhatsApps used by participants. Participants could indicate multiple, and the three participants using the official WhatsApp were predominantly using WhatsApp mods.

WhatsApp Name	App Type	No. of Part.
GB WhatsApp	Mod	18
Official WhatsApp	Official	3
WhatsApp for Business	Official	1
Yo WhatsApp	Mod	1
TM WhatsApp	Mod	1
GB WhatsApp Pro	Mod	1
FM WhatsApp	Mod	1

GB WhatsApp is the most commonly used mod by our study participants. Through our interviews with mod users in Kenya, we find GB WhatsApp to be the most commonly used WhatsApp mod among participants, with 18 out of the 20 participants indicating they use GB WhatsApp (see Table 2). Other WhatsApp mods mentioned by one participant were Yo WhatsApp, TM WhatsApp, GB WhatsApp Pro, and FM WhatsApp. Four participants indicated they use official versions of WhatsApp alongside their mods, and we discuss their reasons for doing so next.

Participants who use several WhatsApps mostly do so to seperate their professional and personal lives. When asked why they use several WhatsApps, participants mostly pointed to the need to separate their personal life from work. For instance, P12 said that they *"use the normal WhatsApp for my work-related number. Then the other one, I use [it] for my social number."* Other common reasons for using multiple WhatsApps were due to the unique features offered by WhatsApp mods as well as participants having multiple phone numbers. We note that it is common for people in Kenya to have multiple phone numbers for various reasons e.g., for internet access, calling etc. Further, WhatsApp now allows multiple accounts on the same phone, a feature that was announced shortly before our interview study [60].

WhatsApp mods' "advanced" features are the biggest motivation for their usage. When asked for their motivation for using the mods, almost all participants pointed to the "advanced" features offered by WhatsApp mods. Particularly, the most mentioned features were: (a) *anti-delete*: this feature preserves messages or updates posted by others even when deleted (b) *saving status*: this feature allows participants to directly download statuses posted by others (c) *additional themes and wallpapers*: mods usually have additional themes and wallpaper options beyond those offered by the official WhatsApp (d) *ability to lock app access*: allows participants to protect access to their WhatsApp application via a password, PIN, or biometric.

P2 started using their WhatsApp mod because *"you can be in a group and someone posts something, then deletes it. Maybe you were not online at that time . . . So GB WhatsApp will help you view or rather see those messages that were deleted."* P6, a lawyer, switched to GB WhatsApp because it has *"some features which makes the communication more secure . . . For example, if someone serves you a document, professionally. Once you read the document and there are [blue] ticks, then that person can screenshot that conversation and then file an affidavit in court saying that they sent you the document and you received it. But then they can delete it soon after you have just read, perhaps even before you download it."* This concern was recently echoed by a court ruling in Uganda stating that agreements made through WhatsApp are legally binding and can be used as evidence in court [26]. P11, on the other hand, stated that they *"like viewing the status of people and then . . . store them so that later I can even post them, as compared to the normal one where you cannot even store a status of somebody."*

Even though the official WhatsApp *currently* allows users to protect access to the app with a biometric [55] and chats using a password, PIN, or biometric [58], there was some confusion about this being a WhatsApp mod only feature. P4 noted that their main motivation for switching to GB WhatsApp: *"is the security features that you can put on the app itself. Let's say my chats, I consider them most secure on GB WhatsApp because I can lock my chats by creating a password or a pattern."* P17 pointed to *"the many themes"* offered by their WhatsApp mod as their main motivation for switching to the mod.

Other "advanced" features of mods mentioned by more than one participant were: (a) *freezing last seen*: allows participants to conceal when they are using the app (b) *restricting status viewership*: allows participants to control who can and cannot see their statuses (c) *hiding chats*: allows participants to hide specific chats (d) *hiding status views*: allows participants to view statuses without their name showing up in the list of status viewers. P5, for example, turned to mods to be able to hide certain chats because of *"situations where you'd give your friend [your WhatsApp] just to look at something. Next thing, they are in another conversation and you are wondering, why are you reading things that don't concern you?"* P10 *"wanted privacy and I think I got it with GB WhatsApp . . . You can hide, you can secure your chats, you can use fingerprints, you can hide a particular chat."* As we note in Section 2, this feature is also available in the official WhatsApp.

Besides WhatsApp mods' "advanced" features, several participants also switched to WhatsApp mods out of curiosity. For instance, P16 indicated that their WhatsApp mod *"was just trending. So like, people are talking about it. So you want.. out of curiosity, you go and get to use it. You get the experience."* After trying them, participants often stuck with the mods because of their features.

Most participants have shared some sensitive information using their WhatsApp mods. When asked if they had used their WhatsApp mod to share any sensitive information, more than half of participants were affirmative, using these apps to share passwords, images (sometimes sensitive e.g., nude photos), bank account details, and sensitive messages. Often, participants trusted the mods because of the "advanced" privacy features that the mods offer. For example, P1 described how you can send images that can only be viewed once: *"when I'm sending [a photo] to someone, and I want it to be that private, the person can view once, like the view once photo, you can't screenshot it, you can't do anything, you can't resend it."* While some of the passwords shared were for streaming sites such as Netflix, some of them were also work-related, as elaborated by P4: *"There was a time, I left the office, then you know, we use the same computer device at the office. So when I left, I indicated my own password and we had a certain madam who was not privy to the password. So when she asked me about the password to log in to the computer, I sent her the password through GB WhatsApp."* The official Whatsapp already allows users to set media messages as "view once" (with screenshot blocking) and supports disappearing messages [57], [62]. However, when we tested these two features on a WhatsApp mod, we discovered that the "anti-delete" feature nullifies both features; a "view once" image can be viewed more than once, a screenshot can be taken, and disappearing messages are retained.

RQ1 summary. In this section, we discussed the several "advanced" features that motivate people to use WhatsApp mods and found that several of them are also supported by the official WhatsApp. This could be due to misinformation on the modded apps' websites (i.e., checklists showing the features that the mods have that the official app does not [65]) or just a lack of knowledge, particularly about features recently added to the official WhatsApp. Whatever the cause, in the next section we discuss how this perception of certain mod features as unique leads participants to recommend mods to others in their social networks.

3.2.2. Propagation of WhatsApp Mods (RQ2). In response to **RQ2**: *How do users describe learning about, acquiring, and updating WhatsApp mods?*, we describe how participants acquire, update, and distribute mods, as well as the considerations and tradeoffs they make when using them.

A majority of participants learn about WhatsApp mods from their friends and family members. When asked how they learned about their mod, more than half of participants indicated they had learned about them from their friends. For example, P2 detailed how they were in their *"class Whatsapp group and then people were posting funny clips and then I wasn't seeing them because they posted then delete[d]. So there is a friend of mine who told me that there is this guy who posted this, have you seen it? And I was like no, I can't see any video in that group. Then he was like, what WhatsApp are you using? I was like I am using the normal WhatsApp. He was like no, install GB WhatsApp. So that is what happened and that is why I started using GB WhatsApp."* Some participants also learned about the mods either personally through online searches or from family members. For instance, P18 indicated that they *"learned [about GB WhatsApp Pro] from my elder sister."*

Almost all participants have recommended their WhatsApp mods to friends, family members, and work colleagues. Similarly to learning about the mods from their friends, almost all participants indicated they had recommended the mods to others, mostly their friends and family members. This was mostly because of the mod features. P11 stated that they *"recommend to them because I find that my friends . . . Whenever I post some videos, they keep on asking me [to] send me the picture, send me the video, but . . . sending to them all the time was a problem and I told them that I have a certain app that can help you to do this. So I recommended them to use GB because you can easily save your status and share it to somebody easily."*

Several participants also indicated they had recommended their WhatsApp mods to their work colleagues. For example, P6 said that they have *"mostly recommended it to my professional friends because of the professional related benefits that I alluded to earlier. The anti-delete, then the control on when the blue ticks appear. Mostly that and then of course the restrictions on status sharing so that they can separate professional content and its audience and the personal and the normal WhatsApp."*

A majority of participants install and distribute WhatsApp mods by directly sharing the mods' APKs. When asked how they had installed their WhatsApp mod for the first time, more than half of participants said that the mod's APK had been shared with them by those that recommended the app, with P9 saying that *"the first way I installed the app was that [my friend] sent me the app through sender."* Some participants indicated the link to the mod was shared with them, while others searched online or from the Play Store. For example, P5 said that *"a friend who was using Yo WhatsApp . . . just told me there is a link, it has a couple of mods just look at the one you want."* P6 *"just searched [for it] after someone mentioned it"* while P20 *"downloaded it from the Play Store."* We note that WhatsApp mods are generally not available in the Google Play Store or are taken down after a short time. Further, installing APKs directly or from unverified websites leaves WhatsApp mod users susceptible to potentially installing malicious apps.

Half of participants did not report considering any specific factors when installing WhatsApp mods as they are motivated to get the app. When asked whether they considered any factors when installing their WhatsApp mod, half of participants indicated they did not as they were more motivated to get the app. For example, P16 *"never considered [anything]. I just installed it because I liked it. I never considered anything."* Interestingly, several participants considered or were worried about their security and privacy, but trusted their friends that shared these apps. For example, P1 *"thought of privacy. At first, I was curious about some viruses and whatever, but that friend assured me that it's okay."* P12 had heard of *"a lot of conversations around the security of the app. So I was scared, I won't lie. So the first thing I did was to uninstall my financial applications; that's bank mobile apps just to make sure that if someone is actually accessing this, somehow I won't be affected. And also, there were a lot of those.. the allow options. I was sort of scared about allowing the app to *access most of the options. But since I was benchmarking on someone, it was easier for me to make the decisions."* Despite being concerned, P3 indicated that ***"you have to ignore the dangers"*** if you want to use the mod.

We also asked participants whether permissions played any role in their decisions to install the mods. This was not the case, with participants often mentioning that these permissions must be granted to use the app, or these permissions are similar to those required by the official app. P11 said that *"when you want to install an app, you must have some permissions that must be granted so that you can be allowed to use the app."* P1 checked but the permissions were *"the same as [those required by the] normal WhatsApp"* while P2 *"didn't check because I knew they were normal permissions."* P6 tried *"to look at the reviews to the extent that they are available online. But of course, there are those applications which filter what reviews they show on their website. It's not a foolproof way of verifying if there are any complaints, but I looked at the reviews, and all I could see was the good reviews regarding some of the modifications that they had made on the original WhatsApp."* We note that most of the mods we explored were over-permissioned.

A majority of participants regularly update their WhatsApp mods to prevent the apps from expiring. Almost all participants regularly update their mods to prevent their apps from expiring, but also to get new features. P6 likened the update notifications to a *"a threat because they tell you that if you don't update within this number of days, then it will become outdated. When it does, you can't message. Once you open the app, the only information you will see is that this version of WhatsApp is outdated or expired and you are prompted to update."* P16 believed that if they are *"updating [the app], they have added other things. They have modified it again, maybe to our advantage."*

Regarding how these updates are made, most participants said that they usually receive prompts from the mods whenever there are updates to make. For example, P7 said that they *"usually get [a] notification [that] your WhatsApp is nearing to expire. So when I get that notification, I usually go and update WhatsApp."* Interestingly, several participants mentioned that they update their mods by redownloading the app. For instance, P4 stated that after *"you get a notification that you have to update your WhatsApp version, what I usually do, I check on my browser, which is Chrome then just type GB WhatsApp. So after it has downloaded, now in the process of installing is when I get rid of the old WhatsApp."*

RQ2 summary. Overall, we find that recommendations from friends, family, and work colleagues are the most common way in which participants learn about, install, and distribute WhatsApp mods. As most of these mods are not available on the Play Store, participants mostly install these apps from APKs directly shared with them, making them susceptible to installing potentially malicious apps. When installing these apps, most participants do not consider any specific factors as they are more motivated to get the app.

3.2.3. Challenges, Practices, and Mental Models (RQ3).

Here, we address responses to **RQ3** regarding WhatsApp mod users' concerns, challenges, and practices with mods as it relates to their security and privacy mental models.

Most concerns and challenges with WhatsApp mods center around difficulty obtaining or updating the mods, the frequency of the updates, and bans from using the official WhatsApp. While about half of participants had no concerns nor challenges with their mods, the other half experienced difficulty obtaining or installing the mods as there are often many versions of these apps online. For example, P4 described how *"it was really problematic for me to go on the web and download the GB WhatsApp version. Because when you write GB WhatsApp, it displays so many versions."* This was similarly the case for updates, with P3 stating that *"when it expires, I have to go back again and update and when you go to update, you might not find the same version of WhatsApp."* Several participants were unhappy with how frequent updates are, with P14 saying that it only *"take[s] like one month, [and] you have to update. What if you don't have [Internet] data?"* About half of participants complained about getting banned or suspended from using WhatsApp. P19 described how they were *"once banned from FM WhatsApp and I never knew the reason why I was banned, actually for 24 hours. I don't know. So I was so much worried."* It appears that the participant was banned from accessing their WhatsApp account (as can happen when you are detected to be using a WhatsApp mod [7]) and interpreted it as FM WhatsApp blocking them.

Some participants were worried about potential security and privacy issues with WhatsApp mods, as well as a potential crackdown on these apps as they are counterfeit. Often, they brushed these concerns off as nothing bad had happened yet. For example, during installation, P15 was warned that *"this app might harm your phone"* but still proceeded to install it. P3 described how they had been *"threatened by I don't know. We were told that the application was going to be shut at some point and that anyone who was using the application was in danger of not using even the normal application."*

While an overwhelming majority of participants have never encountered ads when using WhatsApp mods, the few who have encountered them found the ads to be useful. Only few participants indicated they had seen ads on their WhatsApp mods, with these ads mostly on ridesharing apps such as Bolt, gambling firms, food delivery apps, and mod features. This is somewhat surprising given that 4/5 apps we manually tested displayed ads. Interestingly, the three participants that saw ads perceived them to be useful, as elaborated by P4: *"there was one with Bolt, I think I went ahead and downloaded it and actually, it was impactful to me some other time, it saved me. I was in town, I was very late. I had to call the taxi via the app, and it was a good experience."* While ads are typically frowned upon by users in Western audiences, our findings about ads being useful for the few participants in Kenya that had seen them when using their WhatsApp mod match recent work among social media users in Bangladesh and India [45].

About half of participants are embarrassed or annoyed when their deleted statuses or messages are seen by others. As the *anti-delete* feature is one of the biggest motivations for switching to WhatsApp mods, we were curious about how participants felt when other people were still able to view a status update that they had deleted. About half of participants were not bothered, with some acknowledging that they reap similar benefits from using their mod. For instance, P2 said that *"it's okay, because I use the same WhatsApp so I wasn't even bothered."* Interestingly, another half of participants felt annoyed or embarrassed as elaborated by P4: *"I felt bad, I felt cringed, I felt insecure."* Despite feeling embarrassed, participants felt powerless or helpless about it. For example, P16 described feeling *"powerless, like what can I do for these people not to see this status? WhatsApp GB has ruined that privacy of like when you delete something and then people still see it."* Ironically, P16 and several other participants were drawn to WhatsApp mods because of features such as *anti-delete*. We discuss this, and other contradictions we observed next.

Some participants were unhappy when others used the "advanced" privacy controls offered by WhatsApp mods. Ironically, a few participants expressed concern with the mods' privacy features when they are used by others. For instance, P9 stated that *"the thing I do not like about it is the gray ticking, the single tick and gray tick . . . I would really like to know if someone has seen what I've sent. So whenever there is a gray tick, it really leaves me wondering; did the person see or did not see?"* P10 similarly indicated that *"if you find someone who is also using GB WhatsApp, he or she may ban you, or he may prevent you from calling him or her and yet he or she is online. Yeah, that is also a concern . . . someone may decide to be private to you now."*

Several participants detailed incidents where WhatsApp mods have been used to spy on or stalk others. Due to some privacy-subverting features of WhatsApp mods, we were curious if participants had any experiences or had heard of these apps being used to spy on or stalk others. Seven participants were affirmative, with one even admitting they had used their mod to stalk another person. For example, P19 said that *"a friend of mine was stalking her boyfriend"*. P18 and a few others described how you can use a mod to scan someone's WhatsApp QR code and be able to receive their messages: *"my friend's boyfriend scanned her [QR code] and he could technically see everything the girl was doing, the people she was talking to, how she used to reply [to] them."* This was echoed by P20: *"There is this friend of mine who, someone else was getting her messages so like, she came to find out that that person had scanned her code."* P10 even admitted that they had *"actually used [their mod] to stalk someone."* This ability arises from WhatsApp's recent support for having one account across multiple smartphones [61] and the ability to have multiple accounts on one phone. This has implications for intimate partner surveillance (IPS) [50], as someone seeking to surveil their partner can just add their partner's account to their device and switch between accounts to monitor their partner's messages.

Perceptions of trust in the official WhatsApp and mods vary. We were curious about the level of trust that mod users have in their mods in comparison to the official WhatsApp. Nine participants indicated they trust the official app more while eight participants trusted the mod more, with three having the same level of trust for both applications. Common reasons for trusting the official app included the app being original, its availability on the Play Store, its simplicity, and no past incidents. Reasons for the distrust of the official WhatsApp included the lack of privacy controls and privacy more generally as well as lack of advanced features compared to the mods. On the other hand, participants that trusted the mods more mostly pointed to lack of previous incidents, encryption, and the security and privacy controls offered by the mods. Common reasons for not trusting the mods included the potential for data misuse, the mods being counterfeit, frequent updates, and unavailability of the mods on the Play Store.

Almost all participants believe that WhatsApp mods offer them more control over their data compared to the official app. Between the official WhatsApp and the mods, almost all participants indicated that their mod gives them more control over their personal data. For example, P4 said that with mods, *"I have got total control of my chats, total control of information. Everything is under my control other than the normal WhatsApp whereby the platform, it is what it is just the way it is. You can't have any control over it."* This was echoed by P7 who said that with GB WhatsApp, *"you can completely hide your chats from the normal chats where only you can access, you can use either your fingerprint to lock it, you can use a password or a passcode. But with the normal WhatsApp, you can't do that. You see, with GB you have more power than this one. So that's why I will prefer that one."* As we note above, hiding chats is possible in the official WhatsApp [58]. We also note that this belief in more control may extend to participants' interpersonal communication, but does not extend to control over their data with respect to developers or third-party libraries.

WhatsApp mod users' security and privacy mental models revolve around their friends and others in their circles, but not on the technology platform itself. One overaching theme from our study is how WhatsApp mod users' mental models of security and privacy center around their friends, and not the technology platform or developers. Notably, when participants think about their security and privacy when using mods, they are mostly concerned about what other people such as their friends can see (or what they can see from their friends), and not the platform itself or any security and privacy issues it might have, similar to Facebook users in South Africa [40]. Thus, they perceive the mods to be more secure than the official WhatsApp since the mods provide more security and privacy controls, at times breaking the security and privacy of others. For instance, P18 said that they *"prefer the WhatsApp [GB Pro] because of the security stuff. Like I can get any information I want, whether you try to delete it."* P7 mentioned that they prefer using GB WhatsApp because they *"like privacy. It has more features for privacy. So I prefer using it because I can hide my chats, but [with] the normal WhatsApp you can't do that."* P16 was more trusting of their mod *"because you have a password to access your WhatsApp. So that's privacy enough."* As discussed in Section 2.1, individual chats can be hidden in the official WhatsApp [58], and the ability to lock down the entire smartphone app behind a biometric has been available on the official WhatsApp since 2019 [55].

RQ3 summary. Overall, we find that many participants struggle with obtaining as well as updating their WhatsApp mods due to the absence of these apps on the Play Store. We also find some contradiction in participants' practices and expecations when using the mods, with participants often motivated by the mod features such as *anti-delete* but at times displeased when others equally use these features "against" them. Further, several participants detail experiences where the participants themselves or others they know have used WhatsApp mods to either spy on, or stalk others.

4. Contextualizing Users' Perceptions of Mods

Throughout the user study, participants made several claims about the mods' behavior. While some of these claims can evaluated with a quick online search (e.g., does the official WhatsApp offer a specific feature), broader claims about the mods' unique features, permissions requested, and trustworthiness demand a broader, more systemic evaluation. Specifically, participants believed that (1) WhatsApp mods offer unique S&P features that hide information from the person with whom they are communicating, (2) WhatsApp mods request similar permissions as the official WhatsApp, and (3) WhatsApp mods are more trustworthy than the official app; almost half of participants expressed this final sentiment.

To investigate how participants' expectations of WhatsApp mods either align or misalign with the apps' actual behavior, we analyzed common WhatsApp mods, particularly those most frequently used by participants in the user study (see Section 3). For a subset of the WhatsApp mods, we conducted a *feature* analysis and manually validated that they offered the features they claimed. Additionally, we analyzed the output of VirusTotal [2]—an online software security analysis platform—to understand the permissions these apps requested and if they contained malware.

4.1. Methods

Identifying and selecting WhatsApp mods. As WhatsApp mods are generally not available on the Play Store, it is challenging to find the "official" source for these apps. We chose to focus on "GB WhatsApp" because this name is associated with the most popular mod [25], and almost all participants in our interview study (described in Section 3) used it. A cursory search for "GB WhatsApp" will yield numerous websites that all claim to have GB WhatsApp for download on their pages. We saved the top ten search results and downloaded their APKs to our local machine in December 2023 (shortly after we conducted the interviews).

For the purposes of our study, we wanted to understand the *popularity* of WhatsApp mods we downloaded. Given the difficulty of both quantifying and trusting the number of downloads outside of official app marketplaces, we decided to use the Chrome User Experience Report (CrUX) [16]—an internet measurement report that among other metrics outputs a *popularity* metric for domains that surpass an undisclosed minimum threshold of unique visits. We used CrUX for internet traffic in Kenya during the month of December 2023 to determine the popularity of websites that we found hosting WhatsApp mods. Using this approach, we found that multiple websites hosting WhatsApp mods (e.g., https://gbapps.org.pk) were in the top 1000 of websites visited in Kenya during the time of our study. In total we collected 14 APKs (ten from the WhatsApp mods we downloaded, three from these apps' updates, and the official WhatsApp from the Google Play Store), shown in Table 3.

Feature analysis. To test whether the features described in Section 2.3 and by participants functioned as described, we developed a *testing procedure* that we walked through for five mods in our corpus and the official WhatsApp (see Appendix C for the full procedure). This procedure involved a series of steps on a *test phone* (a Google Pixel 5a with the target app installed) and a non-test phone (with the official WhatsApp installed). For example, when the "anti-delete" feature was enabled, we deleted a message on the non-test phone and observed the test phone to ensure the message was still visible. We initially chose to use the top five mods in our search results (MODs 1-5). We attempted to use MOD5, but the app was blocked by Google Play Protect when we attempted to sideload it using ADB (for reasons that we discuss in Section 4.2). To simulate actions that a typical user would likely take (i.e., *not* disabling Google Play Protect), we proceeded to use MOD6a instead of MOD5 for our analysis. We went through the procedure manually twice for each of the five apps. During this procedure, we also collected network traffic from the test phones to examine the advertising and tracking domains contacted by the WhatsApp mods and their usage of TLS compared the official WhatsApp.

VirusTotal reports. To understand (1) the permissions that WhatsApp mods requested relative to the official WhatsApp and (2) whether WhatsApp mods exhibit malicious or undesired behavior, we uploaded the apps to VirusTotal. VirusTotal is a comprehensive, multi-tool scanning device widely used in industry and research [20], [49], [69] and maintained by Google Cloud's Chronicle Security Operations [11]. VirusTotal aggregates several anti-virus (AV) engines. Prior work [4] has shown that AV engines may be unreliable; we follow the approach used by Wang et al. [52]

TABLE 3: Metadata of the GB WhatsApps we collected. The thumbprint is the SHA1 hash of the digital certificate used to sign the APK. A CrUX rank of 'N' indicates that a website was in the Top N websites during December 2023 in Kenya.

App ID	Package Name	Thumbprint	SDK	APK SHA256	CrUX Rank	Source
MOD1	com.gbwhatsapp	61ed377e...	33	50769499...	1000	https://gbapps.org.pk
MOD2	com.universe.messenger	c8df88cd...	33	ea37bf76...	5000	https://www.gbwhatsapp.chat
MOD3	com.universe.messenger	c8df88cd...	33	e5827f17...	5000	https://www.gbwhatsapp.download
MOD4a	online.whatsticker	bea2d1d9...	33	e71a72cb...	5000	https://allwapk.com
MOD4b	online.whatsticker	bea2d1d9...	33	f1203e04...	5000	https://allwapk.com
MOD4c	com.aerowtsapp	bea2d1d9...	33	278c1435...	5000	https://allwapk.com
MOD5	com.gbwhatsapp.sofid	e07080ed...	33	512958b7...	1000	https://gbapps.net
MOD6a	com.universe.messenger	c8df88cd...	33	ea37bf76...	50000	https://www.whatspro.org/
MOD6b	com.universe.messenger	c8df88cd...	33	d6551b78...	50000	https://www.whatspro.org/
MOD7	com.gbwhatsapp	61ed377e...	33	50769499...	1000	https://androidwaves.com
MOD8	com.gbwhatsapp	e509c3c1...	33	fbed8a41...	1000	https://gbwasap.com/
MOD9	online.whatsticker	bea2d1d9...	33	f1203e04...	50000	https://gbwhatsapp.en.malavida.com
MOD10	com.gbwhatsapp	61ed377e...	29	352ae77c...	50000	https://gbwatsapp.download/
Official	com.whatsapp	38a0f7d5...	33	2976510d...	N/A	Google Play Store

and consider apps as *malicious* if at least 10 AV engines (a number found to be a robust threshold [4], [21], [66]) classify them as such. VirusTotal also outputs information about APKs using Androguard (e.g., permissions).

4.2. Results (RQ4)

The WhatsApp mod ecosystem changes rapidly and is at times unreliable, with several apps 1) not working or 2) requiring an update within a short period of time. For example, nine days after we initially downloaded MOD4a, the app would not function and required an update. After following the links provided by the app, we downloaded MOD4b and ran it through our procedure (Section 4.1). When running a second procedure with MOD4b 11 days later, we were prompted to install another update; since this update was not mandatory like the previous one, we simply ignored it and installed the app (MOD4c) after we finished the procedure. This experience mirrors complaints we observed from participants in the interview study about the difficulty and frequency of updates; we were prompted to manually update the app twice in 20 days.

For the S&P features we tested, we found that all of the WhatsApps mods supported them. The S&P features claimed by WhatsApp mods that we focused on were: anti-delete, hide message read receipts, hide status views, freeze "last seen," and disable incoming calls.[1] As described in Section 4.1, we designed a procedure to verify that these features functioned as they were advertised, and for the features we tested, we found that all the WhatsApp mods indeed supported them. Disabling incoming calls caused the modded WhatsApp to receive a notification of a missed phone call but the phone did not ring. Hiding read receipts and hiding status views also functioned properly and as expected, but the features varied in the amount of information they revealed to the WhatsApp mod user.

For example, when we tested the "anti-delete" feature, we observed that after a message was deleted from the official WhatsApp, the message was still visible in the WhatsApp mod, and the message had a symbol (⊘) added to its display indicating that it had been deleted. However, when we observed a status on the test phone after it had been deleted on the non-test phone, we did not observe any visual indicators. This may explain how people using mods accidentally leak that they are using a mod—by responding to a deleted status that they are not aware was deleted.

Freezing "last seen" time also functioned properly but with a surprising side-effect: the mod user is unable to view other users' "last seen" time. This may be due to the way the feature is implemented, and it introduces a tradeoff for the WhatsApp mod user—by hiding information (your activity) from other users, you also lose information about others.

Although the majority of the permissions are similar, WhatsApp mods requested permissions that allow them to take privileged actions, such as editing system settings or drawing on top of other apps. Some participants described not being concerned about permissions requested by the WhatsApp mods because they were the same as or similar to the offical WhatsApp. However, there were seven permissions requested by WhatsApp mods that were not requested by the official WhatsApp, including one dangerous permission (`ACTIVITY_RECOGNITION`), one permission that is ignored for third-party apps (`MOUNT_UNMOUNT_FILESYSTEMS`), two normal permissions (`QUERY_ALL_PACKAGES`, `EXPAND_STATUS_BAR`), and three *signature* permissions that have a distinct approval flow (in Android API level 23+) and navigate the user to a separate screen (`WRITE_SETTINGS, SYSTEM_ALERT_WINDOW, MANAGE_EXTERNAL_STORAGE`). Respectively, these three permissions could enable a mod to change device settings to conceal its behavior, to allow the app to appear on top of other apps and change the way other apps appear, or to read, change, or delete files in storage. We present a list of extra permissions for each mod in Table 4.

Two WhatsApp mods were malicious (AV-count $>$ 10), and were classified as trojans. As presented in Table 5, two of the apps (MOD5 and MOD8) contained the Triada Trojan [46], a trojan that collects data from devices, downloads malicious payloads, and is known to be distributed via

[1] As we discuss in Section 2.3, the ability to hide read receipts and hide status views in mods is *non-reciprocal*, unlike in the official WhatsApp.

TABLE 4: Mod permissions that are not requested by the official WhatsApp.

Permissions	ACTIVITY_RECOGNITION	EXPAND_STATUS_BAR	MANAGE_EXTERNAL_STORAGE	MOUNT_UNMOUNT_FILESYSTEMS	QUERY_ALL_PACKAGES	SYSTEM_ALERT_WINDOW	WRITE_SETTINGS
MOD1						X	
MOD2	X	X	X	X	X	X	X
MOD3	X	X	X	X	X	X	X
MOD4a						X	
MOD4b						X	
MOD4c			X			X	
MOD5						X	
MOD6a	X	X	X	X	X	X	X
MOD6b	X	X	X	X	X	X	X
MOD7						X	
MOD8						X	
MOD9						X	
MOD10			X			X	

WhatsApp mods [6], [32]. Several other WhatsApp mods were considered adware by some AV engines, but there was not enough consensus to consider them malicious.

Domain analysis. Modded apps contact several domains that the official app does not, including tracking and advertising domains. For all the apps we analysed, there were 52 total domains visited, with the apps visiting between zero (only the official WhatsApp) and 40 advertising/tracking domains as determined by uBlock Origin's ad/tracker list [29]. Within these 40 domains, the most common domains contacted by the mods were `flurry.com` (MODs 2,3,4b,6a), `vungle.com` ((MODs 2,3,4b,6a), and `doubleclick.net` (MODs 2,3,6a). While carrying out the procedure, we observed ads in 4/5 of the modded apps that we manually tested (MOD2, MOD3, MOD4b, and MOD6a), as might be expected from the advertising/tracking domains observed in their network traffic. On some occasions, these ads had fake 'X' buttons that would redirect the user to the Google Play Store rather than closing the ad.

TLS utilization. Similarly to official WhatsApp, almost all (98-100%) of the captured network traffic in mods is encrypted via TLS. The few requests using HTTP were GET requests to app-specific domains (e.g., alexmods.com) for HTML pages with recent app updates.

TABLE 5: Malware classificiation. Note: AV-count is the number of anti-virus engines classifying an application as malicious.

App ID	AV-count	VirusTotal Label
MOD1	6	andr/wamod
MOD2	5	adware.hiddenad
MOD3	4	adware.hiddenad
MOD4a	0	none
MOD4b	2	none
MOD4c	3	none
MOD5	14	trojan.triada/bankbot
MOD6a	5	adware.hiddenad
MOD6b	3	none
MOD7	6	andr/wamod
MOD8	12	trojan.triada/frtr
MOD9	2	none
MOD10	6	pua
Official WhatsApp	0	none

RQ4 summary. Our analysis of the mods mirrors participants' frustration with the ephemerality of the mods and confirms that features such as "anti-delete" mentioned by most participants function as described. However, common WhatsApp mods used by participants pose various risks, with all mods requesting more permissions than the official app and two mods classified as malicious by VirusTotal. These findings are troubling, given that some participants trust WhatsApp mods more than the official WhatsApp.

5. Related Work

Understudied, marginalized, and vulnerable populations. Usable security and privacy researchers have moved beyond the idea of a "typical user" to focus on specific, previously-understudied or marginalized populations [43], [51], [53], [54]. In an interview study closely-related to this work, Naveed et al. explored the privacy behaviors of 40 low-literate and low-income users in Pakistan [35]. The researchers found that some of their participants (17.4% of women and 35.3% of men) used WhatsApp mods (GB and FM WhatsApp), and some described leveraging the modded app features to preserve their privacy. For example, one participant reported freezing her "last seen" time so that her brother would not come in and scold her for being online at night. Among their participants, most people learned about the modded apps from friends or co-workers, something we also observe in our user study in Kenya. The authors recommend that *non*-modded app users should be notified by WhatsApp when they are communicating with modded app users, so that they can choose to block the person or communicate with them. In the current mods landscape, if WhatsApp detects that people are using modded apps, they will block the user's account [7]; some of our participants mentioned getting blocked while using a modded app. Given that mods are constantly pushing updates to avoid their users being blocked and the ease of acquiring disposable phone numbers to use with mods, we do not believe that WhatsApp will choose to allow modded app users (if they are able to detect them) to continue using their platform.

Security and privacy (S&P) perceptions around the world. As S&P perceptions and practices tend to vary across countries and cultures [5], [9], [22], [40], [44], an increasing body of work has started to explore populations beyond just the United States and Western Europe. For instance, Munyendo et al. [33] found that mobile loan app users' privacy concerns in Kenya are often outweighed by their need to procure loans, while many users of cybercafes struggle with password management and account creation, leading to cybercafe managers to advise them to use memorable passwords e.g., their names or national ID numbers [34]. This directly contradicts password advice recommended in the West. In South Asia, women are culturally expected to share their mobile phones with others in the household, making it difficult to protect their privaacy [42]. In South Africa and similar to mod users from our study, Reichel et al. [40] found that Facebook users are more worried about interpersonal privacy, rather than risks posed by platforms. All these studies emphasize the need to explore other populations' security and privacy challenges and needs to better protect and support them.

Android security research. There is a growing body of work focusing on specific classes of Android apps and their impact on users, particularly understudied populations. Some examples of these apps are consumer spyware apps [28], parental control apps [15], mobile loan apps [33], branchless banking apps [39], [47], and electronic monitoring apps [37]. We build on this work by focusing on modified versions of WhatsApp, the perceptions of users of these mods from Kenya, and as well as how participants' expectations align or misalign with the mods' behaviour.

Repackaged Android apps. In their literature review on detecting repackaged Android apps, Li et al. found that determining repackaged app provenance is challenging [27]. Given a pair of repackaged apps, there is no straightforward way to determine which app was the "original" app. This means that given a corpus of WhatsApp mods (as we have collected in this study), it is challenging to determine which modded app is the "official" GB WhatsApp and which apps are mods of mods. In a study of six third-party marketplaces, Zhou et al. developed a system (DroidMOSS) to detect repackaged apps at scale [67]. For the aproximately 23,000 apps they collected from third-party marketplaces in the US, China, and East Europe, they randomly sampled 200 apps and compared them to another corpus of apps they had from the offical Android Market (i.e., Google Play Store). They found that 5-13% of the apps were repackaged, and the rest were either redistributed from the Android Market or were only available in third-party marketplaces. In our study, we find that popular WhatsApp mods in Kenya are hosted on individual websites rather than third-party marketplaces, potentially posing a lot of security and privacy risks to users.

6. Discussion and Conclusion

In this section, we reflect on our findings and contextualize the risks posed by WhatsApp mods. We also provide some recommendations for relevant stakeholders.

6.1. Mod Implications and Takeaways

Mod users' security and privacy (S&P) mental models center around other people, and not developers. Throughout our study in Kenya, we observed that WhatsApp mod users' S&P mental models revolved around their social circles i.e., their friends and family, and not the developers of the mods. Similar to Facebook users in South Africa [40], most WhatsApp mod users were more worried about what they could see from their friends, including deleted content as well as what their friends could see about them; and not the mods and their potential security and privacy issues. In fact, most participants believed the mods are more secure than the official WhatsApp because of the level of control around their privacy that the mods afford them. Even those that had concerns about the mods were willing to overlook these concerns to have the privacy controls from the mods. At the same time, we found that these apps pose various S&P risks, with some of them containing malware.

Due to the risks posed by the mods, we suggest that official WhatsApp should prioritize feature updates that give users more control e.g., by allowing them to disable calls, to dissuade users from using the mods. In fact, several participants indicated they would prefer to use the official app if it afforded them more privacy controls. WhatsApp could pay close attention to the mods and implement some of their favourable privacy controls (and may already do so, albeit slowly), and/or elicit feedback from users. However, we caution against incorporating adversarial features such as "anti-delete" as they ultimately harm users' privacy, e.g., when they accidentally share or post sensitive information.

Security advocacy is a promising way of teaching good security and privacy practices. While WhatsApp mods are often not on official app market places, they have still managed to grow in popularity. For instance, GB WhatsApp is the second most used social messaging application in Africa, behind only the official WhatsApp [25] and ahead of Facebook Messenger. In our study, we found that most mod users learn about and distribute these apps through their social circles of friends, family members, and work colleagues, similar to WhatsApp mod users in Pakistan [35]. There is perhaps an opportunity to leverage these social connections and contacts to spread good security and privacy practices through security advocacy. As prior work in Kenya [34] notes that people often get S&P advice from "local experts" such as managers at public computing facilities such as cybercafes, targeting and teaching these "experts" good security and privacy practices could have widespread impact. Exploring the efficacy and feasibility of such initiatives is a promising direction of future research.

Some participants have ambivalent attitudes when using WhatsApp mods. Ironically, we noticed some contradictions between some participants' preferences for their own S&P in comparison to others. While most participants were drawn to mods because of features such as "anti-delete," several expressed frustration and anger when others were able to view things they had deleted. Some even admitted that the mods have ruined privacy. Similar to the "privacy paradox", it might be interesting to explore the prevalence and root causes of such seemingly contradictory attitudes, especially for chat applications such as WhatsApp where settings are often symmetrical, i.e., you can see other peoples' read receipts *only* if you enable your own read receipts.

The use of WhatsApp mods poses various security and privacy (S&P) risks, both to mod users and non-users. As our results show, people who use mods are potentially exposing themselves to malware by installing them. Two of the WhatsApp mods were clearly malicious with several other mods displaying dubious behaviors. Even if the apps are not malicious at install-time, because of the frequent and dynamic nature of their updates, users cannot be sure that a later version of a WhatsApp mod will not include a malicious payload. Beyond the more serious malware risk, there is a broader privacy risk from the advertising/tracking the apps do; these could ostensibly monetize users by sharing data about them with advertisers and analytics companies. Therefore, we caution users do their due diligence before choosing to use mods. One simple way to do this could be assessing the mod's APK via VirusTotal before installing it.

Non-users of WhatsApp mods, on the other hand, are placed in a difficult situtation. By using the safer, official WhatsApp downloaded from the Google Play Store, they are at an informational disadvantage. If they are aware of the existence of modded apps and their features, they know that they cannot trust read receipts or "last seen" times, and they know that there is a risk that anything they send and later delete could be retained by a modded app user. If they are not aware of others' usage of modded apps, there is more severe informational asymmetry. WhatsApp mod users may deceive or manipulate them using the modded app features, and the non-users will trust everything WhatsApp's UI tells them. In that way, non-users who are not aware of mods may be more susceptible to deception and scams. One potential remedy to this could be WhatsApp informing non-mod users whenever they are communicating with a mod user [35], alongside the potential implications of that.

6.2. Responsible Disclosure

Websites hosting WhatsApp mods. By reviewing common WhatsApp mods via Virus Total, we found two of them to be malicious and containing malware. There is a chance that the websites hosting these WhatsApp mods took the APKs from other sites not in our study and repackaged them (unaware that they contained malicious components). However, there is also a chance that these websites knowingly host malicious apps. At the very least, we assume the people behind these websites know that they are impersonating the official WhatsApp and in some cases monetizing users. Nevertheless, we reached out to the two websites hosting modded APKs classified as malicious and notified them of our findings. We recommended that they remove all malicious APKs from their websites and upload any new APKs to VirusTotal before hosting them.

Participants using WhatsApp mods. While we conducted data collection for the interviews and the app analysis simultaneously, we did not analyze the mods until after the interviews were completed. This means that we did not get the chance to tell participants that these apps potentially contained malware. Moreover, because we could not know the specific APKs that the participants had on their devices, we would not have been able to immediately confirm if *their* modded app contained malware.[2] In the end, we drafted a message to all participants summarizing our findings, and suggesting that they upload their APKs to VirusTotal if they want to check if their mods are malicious. Working with our IRBs, we have appropriately re-contacted all participants.

6.3. Recommendations and Conclusion

Lessons and recommendations. Our results are directly useful to various stakeholders, including end-users, developers, WhatsApp, and application markets. For WhatsApp mod users and other users generally, we caution against using modded apps without doing due diligence, as some of these apps are potentially malicious and may share users' personal information with advertisers and other third parties. For developers hosting these apps, especially mods of other mods, we also emphasize the need for due diligence; copying or downloading other mods directly without closely inspecting their codebase could lead to developers unintentionally hosting and sharing potentially harmful applications. For WhatsApp, we believe there is an opportunity to stay up to date and incorporate some of the favourable mod features into the official WhatsApp. After all, several participants indicated they would prefer to use the official app if it afforded them more privacy controls. For third-party marketplaces, it might be useful to regularly scan their stores with the goal of detecting and removing apps that are potentially malicious.

To use or not to use ... that is the question. We decline to answer the question: *should people use WhatsApp mods?* Instead we attempt to elucidate the good, the bad, and the ugly of mods, from the users' perspective. Mod users gain features that they value that the official WhatsApp does not offer. For example, the ability to download statuses allows for media portability, and the ability to block all incoming calls (while also controlling how the caller perceives the blocking) could be considered an anti-spam or an anti-harassment feature. While other features (e.g., freezing "last seen") facilitate information asymmetry, this is not necessarily a bad thing—particularly if the asymmetry benefits someone with less power (e.g., the example from Naveed et al. [35] in Section 5). While there are risks that, without security checks in place, this ecosystem can facilitate the spread of malware, WhatsApp mods also have clear utility (and sometimes privacy and safety) benefits for end-users.

[2] Two apps with identical package names cannot be installed on a device. The Google Play Store does not contain apps with identical package names, so they are often used as identifiers for apps. However, since modded apps are sideloaded, their package names can conflict with those of existing apps. Due to these factors, unless participants sent us a hash of their APK, we could not identify which specific mod they were using.

Acknowledgments

We would like to thank the members of the University of Washington's Security and Privacy Research Lab (specifically Yael Eiger, Rachel McAmis, and Michael Flanders) and the George Washington University's GWUSEC Lab (including Lucy Simko, Jan Tolsdorf, Adryana Hutchinson, Neal Keating, Monica Kodwani, and Elena Korkes) for their amazing suggestions and feedback. We are also grateful to all the anonymous reviewers and shepherd for their thoughtful comments and feedback, as well as all our participants for their time and invaluable insights. This material is based upon work supported in part by the National Science Foundation under Grant Numbers 1845300 and 2205171.

References

[1] GB WhatsApp Pro v14.0.0 Apk Download for Android (Official) — web.archive.org. https://web.archive.org/web/20211221152909/https://gbwhatspro.com/, 2021.

[2] Virustotal. https://www.virustotal.com/gui/home/upload, 2024.

[3] Peter Ajemian. Apple announces changes to iOS, Safari, and the App Store in the European Union — apple.com. https://www.apple.com/newsroom/2024/01/apple-announces-changes-to-ios-safari-and-the-app-store-in-the-european-union/, 2024.

[4] Daniel Arp, Michael Spreitzenbarth, Malte Hubner, Hugo Gascon, Konrad Rieck, and CERT Siemens. Drebin: Effective and explainable detection of android malware in your pocket. In *Proc. NDSS*, 2014.

[5] Steven Bellman, Eric J. Johnson, Stephen J. Kobrin, and Gerald L. Lohse. International Differences in Information Privacy Concerns: A Global Survey of Consumers. *The Information Society*, 20(5):313–324, 2004.

[6] David Bisson. Triada trojan conceals itself in whatsapp mod. https://securityintelligence.com/news/triada-trojan-conceals-itself-whatsapp-mod/, October 2021.

[7] WhatsApp Help Center. About unofficial apps. https://faq.whatsapp.com/1217634902127718?helpref=faq_content.

[8] Kai Chen, Peng Wang, Yeonjoon Lee, XiaoFeng Wang, Nan Zhang, Heqing Huang, Wei Zou, and Peng Liu. Finding unknown malice in 10 seconds: mass vetting for new threats at the google-play scale. In *Proc. USENIX Security*, 2015.

[9] Hichang Cho, Milagros Rivera-Sánchez, and Sun Sun Lim. A multinational study on online privacy: global concerns and local responses. *New Media & Society*, 11(3):395–416, 2009.

[10] Deborah Cohen and Benjamin Crabtree. Qualitative research guidelines project, Jul 2006. http://www.qualres.org/.

[11] Chris Corde and Nimmy Reichenberg. Introducing the unified Chronicle Security Operations platform — Google Cloud Blog — cloud.google.com. https://cloud.google.com/blog/products/identity-security/introducing-the-unified-chronicle-security-operations-platform, September 2023.

[12] Cory Doctorow. African WhatsApp Modders are the Masters of Worldwide Adversarial Interoperability. https://www.eff.org/deeplinks/2020/03/african-whatsapp-modders-are-masters-worldwide-adversarial-interoperability, 2020.

[13] Max Eddy. Rsac: Reverse-engineering an android app in five minutes. https://www.pcmag.com/news/rsac-reverse-engineering-an-android-app-in-five-minutes, February 2014.

[14] Enrico204. whatsapp-decoding/libwhatsapp at master · Enrico204/whatsapp-decoding — github.com. https://github.com/Enrico204/whatsapp-decoding/tree/master/libwhatsapp, 2017.

[15] Álvaro Feal, Paolo Calciati, Narseo Vallina-Rodriguez, Carmela Troncoso, Alessandra Gorla, et al. Angel or devil? a privacy study of mobile parental control apps. In *Proc. PETS*, 2020.

[16] Chrome for Developers. https://developer.chrome.com/docs/crux/about/, June 2022.

[17] Benjamin Gardner. Incentivised snowballing. *The Psychologist*, 22(9):768–769, 2009.

[18] Ayako A Hasegawa, Daisuke Inoue, and Mitsuaki Akiyama. A Survey on the Geographic Diversity of Usable Privacy and Security Research. *arXiv preprint arXiv:2305.05004*, 2023.

[19] Joseph Henrich, Steven J Heine, and Ara Norenzayan. Most people are not WEIRD. *Nature*, 466(7302):29–29, 2010.

[20] Colin C. Ife, Yun Shen, Steven J. Murdoch, and Gianluca Stringhini. Marked for Disruption: Tracing the Evolution of Malware Delivery Operations Targeted for Takedown. In *Proc. RAID*, 2021.

[21] Muhammad Ikram, Narseo Vallina-Rodriguez, Suranga Seneviratne, Mohamed Ali Kaafar, and Vern Paxson. An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps. In *Proc. IMC*, 2016.

[22] Margaret C. Jack, Pang Sovannaroth, and Nicola Dell. "Privacy is Not a Concept, but a Way of Dealing with Life": Localization of Transnational Technology Platforms and Liminal Privacy Practices in Cambodia. *Proc. ACM Hum.-Comput. Interact.*, 3(CSCW), 2019.

[23] Jan and Brian. end-to-end encryption — blog.whatsapp.com. https://blog.whatsapp.com/end-to-end-encryption?lang=en_US, April 2016.

[24] Mannat Kaur, Michel van Eeten, Marijn Janssen, Kevin Borgolte, and Tobias Fiebig. Human Factors in Security Research: Lessons Learned from 2008-2018. *arXiv preprint arXiv:2103.13287*, 2021.

[25] Yomi Kazeem. WhatsApp is so popular in Africa, even knock-off versions are used more often than Facebook. https://qz.com/africa/1804859/fake-whatsapp-app-more-popular-than-facebook-instagram-in-africa, 2020.

[26] Juliet Kigongo. Whatsapp messages form binding contract, court rules. https://www.monitor.co.ug/uganda/news/national/whatsapp-messages-form-binding-contract-court-rules-4513586, 2024.

[27] Li Li, Tegawendé F. Bissyandé, and Jacques Klein. Rebooting Research on Detecting Repackaged Android Apps: Literature Review and Benchmark. In *Proc. IEEE TSE*, 2021.

[28] Enze Liu, Sumanth Rao, Sam Havron, Grant Ho, Stefan Savage, Geoffrey M Voelker, and Damon McCoy. No Privacy Among Spies: Assessing the Functionality and Insecurity of Consumer Android Spyware Apps. In *Proc. PETS*, 2023.

[29] Peter Lowe. Peter lowe's ad and tracking server list. https://pgl.yoyo.org/adservers/serverlist.php?hostformat=hosts&showintro=1&mimetype=plaintext, January 2024.

[30] MAXQDA. https://www.maxqda.com/, 2024.

[31] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and Inter-Rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proc. ACM Human-Computer Interaction*, 3(CSCW), 2019.

[32] Tomas Meskauskas. Triada trojan (android). https://www.pcrisk.com/removal-guides/24926-triada-trojan-android, November 2023.

[33] Collins W. Munyendo, Yasemin Acar, and Adam J. Aviv. "Desperate Times Call for Desperate Measures": User Concerns with Mobile Loan Apps in Kenya. In *Proc. IEEE S&P*, 2022.

[34] Collins W. Munyendo, Yasemin Acar, and Adam J. Aviv. "In Eighty Percent of the Cases, I Select the Password for Them": Security and Privacy Challenges, Advice, and Opportunities at Cybercafes in Kenya. In *Proc. IEEE S&P*, 2023.

[35] Sheza Naveed, Hamza Naveed, Mobin Javed, and Maryam Mustafa. “Ask This from the Person Who Has Private Stuff”: Privacy Perceptions, Behaviours and Beliefs Beyond W.E.I.R.D. In *Proc. CHI*, 2022.

[36] Nathan Oyori Ogechi. On language rights in Kenya. *Nordic Journal of African Studies*, 12(3):19–19, 2003.

[37] Kentrell Owens, Anita Alem, Franziska Roesner, and Tadayoshi Kohno. Electronic Monitoring Smartphone Apps: An Analysis of Risks from Technical, Human-Centered, and Legal Perspectives. In *Proc. USENIX Security*, 2022.

[38] Alok Rai. #20 Amazing Android Modded Apps to use in 2023 - Today’s Tech World — todaystechworld.com. https://todaystechworld.com/top-android-modded-apps/, January 2023.

[39] Bradley Reaves, Jasmine Bowers, Nolen Scaife, Adam Bates, Arnav Bhartiya, Patrick Traynor, and Kevin R. B. Butler. Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications. *ACM Trans. Priv. Secur.*, 20(3), Aug 2017.

[40] Jake Reichel, Fleming Peck, Mikako Inaba, Bisrat Moges, Brahmnoor Singh Chawla, and Marshini Chetty. ‘I have too much respect for my elders’: Understanding South African Mobile Users’ Perceptions of Privacy and Current Behaviors on Facebook and WhatsApp. In *Proc. USENIX Security*, 2020.

[41] Pedro Domínguez Rojas. That cool whatsapp mod you’ve installed comes with a surprise, and not a good one. https://en.softonic.com/articles/that-whatsapp-mod-so-cool-that-you-installed-comes-with-a-surprise-and-not-the-good-kind, 2023.

[42] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. “Privacy is not for me, it’s for those rich women”: Performative Privacy Practices on Mobile Phones by Women in South Asia. In *Proc. SOUPS*, 2018.

[43] Shruti Sannon and Andrea Forte. Privacy research with marginalized groups: What we know, what’s needed, and what’s next. *Proc. ACM Hum.-Comput. Interact.*, 6(CSCW2), nov 2022.

[44] Yukiko Sawaya, Mahmood Sharif, Nicolas Christin, Ayumu Kubota, Akihiro Nakarai, and Akira Yamada. Self-Confidence Trumps Knowledge: A Cross-Cultural Study of Security Behavior. In *Proc. CHI*, 2017.

[45] Tanusree Sharma, Smirity Kaushik, Yaman Yu, Syed Ishtiaque Ahmed, and Yang Wang. User Perceptions and Experiences of Targeted Ads on Social Media Platforms: Learning from Bangladesh and India. In *Proc. CHI*, 2023.

[46] Lukasz Siewierski and Android Security & Privacy Team. Pha family highlights: Triada, June 2019.

[47] Karen Sowon, Edith Luhanga, Lorrie Faith Cranor, Giulia Fanti, Conrad Tucker, and Assane Gueye. The Role of User-Agent Interactions on Mobile Money Practices in Kenya and Tanzania. In *Proc. IEEE S&P*, 2024.

[48] Statista. Most popular messaging apps 2024 — Statista — statista.com. https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/, 2024.

[49] Guillermo Suarez-Tangil and Gianluca Stringhini. Eight years of rider measurement in the android malware ecosystem. *IEEE Transactions on Dependable and Secure Computing*, 19(1):107–118, 2022.

[50] Emily Tseng, Rosanna Bellini, Nora McDonald, Matan Danos, Rachel Greenstadt, Damon McCoy, Nicola Dell, and Thomas Ristenpart. The Tools and Tactics Used in Intimate Partner Surveillance: An Analysis of Online Infidelity Forums. In *Proc. USENIX Security*, 2020.

[51] Ashley Marie Walker, Yaxing Yao, Christine Geeng, Roberto Hoyle, and Pamela Wisniewski. Moving beyond’one size fits all’ research considerations for working with vulnerable populations. *Interactions*, 26(6):34–39, 2019.

[52] Haoyu Wang, Zhe Liu, Jingyue Liang, Narseo Vallina-Rodriguez, Yao Guo, Li Li, Juan Tapiador, Jingcun Cao, and Guoai Xu. Beyond Google Play: A Large-Scale Comparative Study of Chinese Android App Markets. In *Proc. IMC*, 2018.

[53] Yang Wang. Inclusive security and privacy. *IEEE Security & Privacy*, 16(4):82–87, 2018.

[54] Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L. Mazurek, Manya Sleeper, and Kurt Thomas. SoK: A Framework for Unifying At-Risk User Research. In *Proc. IEEE S&P*, 2022.

[55] WhatsApp. Introducing Fingerprint Lock for Android — blog.whatsapp.com. https://blog.whatsapp.com/introducing-fingerprint-lock-for-android/, October 2019.

[56] WhatsApp. Two Billion Users – Connecting the World Privately — blog.whatsapp.com. https://blog.whatsapp.com/two-billion-users-connecting-the-world-privately, Feb 2020.

[57] WhatsApp. New Features for More Privacy, More Protection, More Control — blog.whatsapp.com. https://blog.whatsapp.com/new-features-for-more-privacy-more-protection-more-control, August 2022.

[58] WhatsApp. Chat Lock: Making your most intimate conversations even more private — blog.whatsapp.com. https://blog.whatsapp.com/chat-lock-making-your-most-intimate-conversations-even-more-private, May 2023.

[59] WhatsApp. Introducing Secret Code for Chat Lock — blog.whatsapp.com. https://blog.whatsapp.com/introducing-secret-code-for-chat-lock, November 2023.

[60] WhatsApp. Multiple Accounts Coming to WhatsApp — blog.whatsapp.com. https://blog.whatsapp.com/multiple-accounts-coming-to-whatsapp, October 2023.

[61] WhatsApp. One WhatsApp account, now across multiple phones — blog.whatsapp.com. https://blog.whatsapp.com/one-whatsapp-account-now-across-multiple-phones, April 2023.

[62] WhatsApp. About disappearing messages — WhatsApp Help Center — faq.whatsapp.com. https://faq.whatsapp.com/673193694148537, 2024.

[63] WhatsApp. How to check read receipts. https://faq.whatsapp.com/665923838265756/?cms_platform=android, 2024.

[64] WhatsApp. How to silence unknown callers — WhatsApp Help Center — faq.whatsapp.com. https://faq.whatsapp.com/1238612517047244, 2024.

[65] GB WhatsApp. GBWhatsApp Pro APK V17.60 Download For Android (2024) — gbwhatspro.com. https://gbwhatspro.com/, 2024.

[66] Min Zheng, Patrick PC Lee, and John CS Lui. ADAM: An Automatic and Extensible Platform to Stress Test Android Anti-virus Systems. In *Proc. DIMVA*, 2012.

[67] Wu Zhou, Yajin Zhou, Xuxian Jiang, and Peng Ning. Detecting Repackaged Smartphone Applications in Third-Party Android Marketplaces. In *Proc. CODASPY*, 2012.

[68] Yajin Zhou and Xuxian Jiang. Dissecting Android Malware: Characterization and Evolution. In *Proc. IEEE S&P*, 2012.

[69] Shuofei Zhu, Ziyi Zhang, Limin Yang, Linhai Song, and Gang Wang. Benchmarking Label Dynamics of VirusTotal Engines. In *Proc. CCS*, 2020.

Appendix A. Interview Protocol

Main Study

Q1 What WhatsApp or WhatsApp(s) are you currently using? List all.
If multiple:

a) Why do you use several WhatsApps?
b) Which one do you most frequently use or prefer, and why?

We will focus on your most used modded app for this interview.

Q2 Are you aware of the official WhatsApp?

a) What do you think are the similarities between *your modded app* and the official WhatsApp?
b) What do you think are the differences between *your modded app* and the official WhatsApp?

Q3 Approximately when did you start using *your modded app*?
Q4 On what platforms do you use *your modded app*?
Q5 What motivated you to start using *your modded app*?

a) How did you learn about *your modded app*?
b) Do you remember where you got the app from or how you installed it? Please elaborate.
c) Did you consider any factors when installing the app?
   i) How did you decide which website to download from?
   ii) Did you check the permissions? Why or why not?
   iii) Did you look at any guidance?

Q6 What do you like the most about *your modded app*?

a) Is there a particular feature you like the most? Why?

Q7 What do you like the least about *your modded app*?

a) Is there a feature you like the least? Why?

Q8 Has anything about *your modded app* surprised you?
Q9 Have you recommended *your modded app* to other people?
If yes:

a) Who did you recommend *your modded app* to, and why?
b) Did you provide them any guidance on how to install the app?
c) Are they using the app you recommended now? Why or why not?

If no:

a) Are there any reasons why you have not recommended *your modded app* to others?
b) Are there any people you would recommend *your modded app* to? Why or why not?
c) Are there people you would not recommend *your modded app* to? Why or why not?

Q10 Have you used *your modded app* to share any sensitive information?

a) Prompts: banking information, passwords, sensitive images etc. Please elaborate.

Q11 How much trust do you have in *your modded app*?

a) What factors make you trust (or distrust) *your modded app*?
b) Do you trust the developer, owner, or company behind *your modded app*? Why or why not?

Q12 How much trust do you have in the official WhatsApp? Elaborate.

a) What factors make you trust (or distrust) the official WhatsApp?
b) Do you trust the developer, owner, or company behind the official WhatsApp? Why or why not?

Q13 By comparing *your modded app* and the official WhatsApp, which one do you feel gives you more control over your data? Elaborate.
Q14 Do you have any concerns with *your modded app*?
If yes:

a) What concerns? Why?
b) Any concerns related to security or privacy?

If no:

a) Are there any reasons why you are not concerned?
b) Is there anything that would make you concerned about *your modded app*? Elaborate.

Q15 Do you think or know about other people using *your modded app* or similar versions of WhatsApp?

a) What do you think are the benefits other people get (or might) get from using these apps?
b) What concerns do you have from others using these apps?
c) Can you tell when someone is using a modified version of WhatsApp? Please elaborate.

Q16 Have you used any other WhatsApp or WhatsApp(s) in the past?

a) What WhatsApps were you previously using?
b) Have you ever used the official WhatsApp?
c) Have you ever used WhatsApp for Business?
d) Why did you stop using them?
e) Did you remove them from your phone? Why or why not?

Q17 Have you ever updated *your modded app*?
If yes:

a) Why did you update it?
b) How did you make the update?
c) How often do you update *your modded app*?

If no:

a) Why have you not updated *your modded app*?
b) Are there any reasons that would make you update *your modded app*? Please elaborate.

Q18 Have you encountered any challenges or issues because of using *your modded app*? What issues? e.g. getting banned from WhatsApp.
If yes:

a) How did you navigate these challenges?

If no:

a) Why do you think you have not faced any challenges or issues when using *your modded app*?

Q19 What permissions are required by *your modded app*? (help participants to find them if they cannot).

a) Are you surprised by any of the permissions required by *your modded app*? What permissions and why, or why not?
b) What permission would you say is the most concerning? Why?
c) What permission would you say is the least concerning? Why?

Q20 Have you seen any advertisements when using *your modded app*?
If yes:

a) What advertisements have you seen?
b) Thinking about the last advertisement you saw when using *your modded app*, how do you feel about it?

If no:

a) Why do you think you have not seen any advertisements when using *your modded app*?

Q21 We have heard of people using mods to {spy on others, just stalking them, avoiding others knowing when they are online...}. Is this something you have also heard of or are aware about?
Q22 Have you ever posted on WhatsApp status updates?
If yes:

a) What are some of the things you post about (or posted about)?
b) Are these updates viewed by everyone in your contacts? Why?
c) Have you posted something and deleted it? What did you post?
d) Do you know if people were still able to view it after you deleted it? How did you feel about it?

If no:

a) Are there reasons why you do not post on WhatsApp status? Please elaborate.
b) Are there reasons that would make you post? Why or why not?

Q23 Is there anything else you would like to share about *your modded app*, other modified versions of WhatsApp or the official WhatsApp?
Q24 Is there anything you will do differently with these app(s) as a result of this interview?

Demographics

D1 What is your age range?
D2 What is your gender?
D3 What is the highest degree or level of education you have attained?
D4 Which of the following best describes your background?

a) I have an education in, or work in, the field of computer science, computer engineering or IT.
b) I do not have an education in, nor do I work in, the field of computer science, computer engineering or IT.
c) Prefer not to say.

D5 How do you earn your living?

Appendix B. Qualitative Codes

- **previous-whatsapps (31)**
  official-app (14), whatsapp-for-business (6), fm-whatsapp (5), tm-whatsapp (3), yo-whatsapp (2), gb-whatsapp (1)
- **current-whatsapps (26)**
  gb-whatsapp (18), official-app (3), yo-whatsapp (1), whatsapp-for-business (1), tm-whatsapp (1), gb-whatsapp-pro (1), fm-whatsapp (1)
- **duration-of-using-mods (19)**
  1-2-years (12), 3-4-years (4), less-than-a-year (2), over-4-years (1)
- **devices-for-mods (25)**
  phone (20), laptop (4), tablet (1)
- **reasons-for-multiple-whatsapps (18)**
  work-personal-life-separation (6)
  features (5): *privacy (2), anti-delete (1)*
  multiple-phone-numbers (3), curiosity (1), backup (1), communication (1), compatibility-issues (1)
- **similarities-between-mods-and-official (28)**
  texting/chat-format (7), call-features (4), status-features (4), same-functions (3), voice-notes (2), group-features/controls (2), hide-online-status (2), certain-settings (1), same-interface (1), save-photos-to-gallery (1), encryption (1)
- **differences-between-mods-and-official (50)**
  save-status-on-mods (6), hide-status-view-on-mods (5), additional-themes/wallpapers-on-mods (4), advanced-features-on-mods (4), more-privacy-on-mods (4), anti-delete-on-mods (4), longer-video-status-on-mods (3), hide-blue-ticks-on-mods (3), restrict-status-viewership-on-mods (3), freeze-last-seen-on-mods (2), more-fonts-on-mods (2), groups-and-chats-seperation-on-mods (2), hide-chats-on-mods (2), restrict-profile-picture-viewership-on-mods (2), channels-on-official-app (1), online-notifications-on-mods (1), better-media-quality-on-mods (1), restrict-group-addition-on-mods (1)
- **motivation-for-using-mod (43)**
  additional-features (34): *anti-delete (5), save-status (5), themes/wallpapers (5), lock-chat-access (4), freeze-last-seen (2), restrict-status-viewership (2), hide-chats (2), hide-status-views (2), ability-to-delete-for-all (1), emojis/stickers (1), improved-media-quality (1), show-blue-ticks-after-replying (1)*
  curiosity (6), more-privacy (2), familiar-developer (1)
- **learning-of-mods (22)**
  friends (12), family (4), personally (4), partner (1), someone (1)
- **initial-mod-installation (21)**
  apk-shared (12), link-shared (3), searched-online (3), playstore (3)
- **mod-installation-considerations (40)**
  none (10): *needed-app (5)*
  security/privacy (7), permissions-must-be-granted (7), trusted-person-that-shared (6), permissions-similar-to-official (4), initially-apprehensive-of-permissions (2), gathered-background-info (1), app-reviews (1), removed-sensitive-apps (1), tried-several-links (1)
- **mod-likes (44)**
  anti-delete (7), themes (6), save-status (5)
  control (5): *restrict-profile-picture-viewership (2), restrict-status-viewership (2), restrict-group-addition (1)*
  hide-chats/conversations (4), hide-status-views (3), lock-app-access (2), freeze-last-seen (2), hide-blue-ticks (2), privacy (2), accurate-status-view-count (1), know-others-online-status (1), flight-mode (1), message-backup (1), media-quality (1), communities (1)
- **mod-dislikes (24)**
  frequent-updates-to-app/interface (9): *app-expiring (2), insufficient-data (1), no-changes (1)*
  none (5), hanging/crashing (3), privacy-controls-used-by-others (2), bans/suspensions (2), ads (1), backup-issues (1), wrong-recipient (1)
- **mod-surprises (20)**
  no (11)
  yes (9): *additional-feat. (3), security/privacy-controls (2), mods-not-having-channels (1), bans (1), see-ghost-viewers (1), qr-linking (1)*
- **recommended-mod (20)**
  yes (18), no (2)
- **who-participants-recommended-mod-to (29)**
  friends (12), family (10), work-colleagues (6), neighbor (1)
- **guidance-after-recommendation (29)**
  apk-shared (12): *app-expired (2), avoid-malicious-links (1)*
  link-shared (6): *app-needs-update (1)*
  none (4), downloaded/installed-app-for-them (2), communicated-dangers (1), pointed-them-to-social-channel (1)
- **shared-sensitive-info-with-mods (20)**
  yes (13), no (7)
- **sensitive-info-shared (27)**
  sensitive-images (6): *nude-photos (1)*
  banking/financial-info (5), passwords (5), sensitive-messages (4), work-related-documents (3), academic-certificates (2), insurance-documents (1), government-issued-documents (1)
- **mod-concerns (21)**
  none (9): *safe/secure (2), no-incidents (2), app-works (2), familiar-with-app (1) potential-security/privacy-issues (3), app-crackdown (2), app-requires-extra-perms (1), unknown-dev (1), app/data-compromise (1), potential-copyright-issues (1), unsure-of-app-intention (1), can't-make-mistakes (1), qr-message-linking (1)*
- **mod-challenges (40)**
  bans (11): *no-idea (4), violated-terms (2), many-status-updates (1)*
  none (10): *respectful (4), follow-terms (2), update-regularly (1), keep-settings-simple (1)*
  difficulty-updating (9)
  difficulty-obtaining-app (7): *mod-not-on-playstore (3)*
  message-delay (1), delayed-app-opening (1), unintended-exposure (1)
- **know-when-others-use-mods (20)**
  yes (17): *mod-features (17)*
  no (3)
- **reasons-for-ditching-whatsapps (17)**
  simple (5), curiosity (2), boredom (2), app-failure (2), not-secure (2), can't-use-same-phone-no (2), app-expired (1), business-closure (1)
- **update-mods (23)**
  yes (22): *avoid-app-expiring (13), new-features (4), mods-synced-to-official-app (1), avoid-mod-crashing (1)*
  no (1)
- **update-frequency (16)**
  2-3-months (8), 1-month (6), 7-12-months (2)
- **update-mechanism (20)**
  app-prompts (13), app-redownloading (5), apk-shared (1), social-media-channel (1)
- **permission-surpise (20)**
  yes (4): *don't-see-need (1), perm-not-on-official-app (1)*
  no (16): *perms-similar-to-other-apps (8), perms-necessary (7)*
- **ads-on-mods (25)**
  yes (7): *ridesharing-apps (2), mod-features (2), gambling (1), food-delivery (1)*
  no (15)
- **ad-perceptions-for-those-that-saw-ads (3)**
  useful (3)
- **whatsapp-status-updates (20)**
  yes (20)
- **status-updates (42)**
  memes/funny-posts (9), videos (8), photos (7), work-related (4), quotes (3), events (3), music (3), news (2), mood (2), sports (1)
- **restricted-status-viewership (20)**
  yes (17), no (3)
- **feeling-about-viewable-deleted-update (19)**
  no-problem/not-bothered (9), bad/embarrassed/annoyed (7), powerless/helpless (3)
- **comparison-of-trust-for-apps (20)**
  official-app-trusted-more (9), mod-trusted-more (8), same-level-of-trust-for-mods-and-official (3)
- **comparison-of-trust-for-app-owners (20)**
  official-app-owners-trusted-more (10), mod-owners-trusted-more (6), same-level-of-trust-for-owners-of-mods-and-official (4)

- **reasons-for-trusting-mod (19)**
  no-incidents (5), encryption (3), security/privacy-features (3), can-lock-chat-access (2), can-restrict-status-viewership (1), can-restrict-group-addition (1), more-themes/wallpapers (1), mods-faster-than-official-app (1), mods-similar-to-other-apps (1), mods-familiar (1)
- **reasons-for-distrusting-mod (12)**
  potential-for-data-misuse (3), counterfeit (2), frequent-updates (2), not-on-playstore (2), potential-security/privacy-issues (1), anti-delete-feature (1), crashing/app-failure (1)
- **reasons-for-trusting-mod-owners (12)**
  no-incidents (7), unique-features (3), skilled-team (2)
- **reasons-for-distrusting-mod-owners (17)**
  don't-know-owners (5), devs-very-capable (4), counterfeit (3), original-did-most-work (2), profit-incentives (1), potential-for-data-misuse (1), devs-human (1)
- **reasons-for-trusting-official-app (14)**
  on-playstore (4), original (4), no-incidents (2), simple (2), privacy-restrictions (2)
- **reasons-for-distrusting-official-app (9)**
  no-group/status-restrictions (3), not-as-advanced-as-mods (3), no-privacy/security (2), potential-for-data-misuse (1)
- **reasons-for-trusting-official-app-owners (10)**
  no-incidents (3), owners-known (2), restrictions/confidentiality (2), popularity (1), skilled-team (1), pioneers (1)
- **reasons-for-distrusting-official-app-owners (7)**
  no-security/privacy-features (4), no-advanced-features (2), devs-human (1)
- **app-with-more-control-over-personal-info (14)**
  mods (16): *privacy/security-controls (10), familiar (2), features (2), no-incidents (1)*
  both-mods-and-official (3): *no-incidents (2), privacy/security-controls (1)*
  official-app (1): *restrictions (1)*
- **security/privacy-mental-models (12)**
  mods-provide-security/privacy (12)
- **spying/stalking-with-mods (7)**
  by-others (6), by-participant (1)
- **older-adults-struggle-with-mods/tech (3))**

Appendix C. Testing Procedure

Below we outline our testing procedure for validating the mod features. We recorded the screens of the test phone and the normal phone using a third, recording phone placed on a camera stand.

C.1. Set-up

- Factory reset the test phone.
- Set the screen timeout to 30 minutes on all phones.
- Set-up the camera stand and the recording phone.
- Install Google Drive, Google Docs on the test phone.
- Install the target app onto the test phone: via ADB for modded apps (after enabling "USB debugging" in developer mode), and from Google Play for the official app.

C.2. Main procedure

- Start video recording.
- Open the target app and login.
- Enable settings related to the following features. If these settings are enabled by default or do not exist, make note of that.
  - Anti-Delete feature for messages
  - Anti-Delete feature for stories
  - Hide read receipts for messages
  - Hide read receipts for stories
  - Freeze "Last Seen"
  - Disable incoming calls

Message read receipt test

- Start the test.
- Test phone sends: 'Hi, test begins.'
- Normal phone reads the message;
- Test phone leaves chat and goes to main screen listing all chats
- Normal phone sends: 'Test received.';
- Test phone reads the message;
- Normal phone leaves chat and goes the main screen listing all chats
  - (Modded App Only) At this point, the normal phone should not have received a read receipt. If the result is different, note that.
- Test phone takes an image and sends it;
- Normal phone views the message and opens the image;
- Test phone leaves chat and goes to main screen listing all chats
- Normal phone takes an image and sends it;
- Test phone reads the message and opens the image;
  - (Modded App Only) At this point, the normal phone should not have received a read receipt. If the result is different, note that.

Status read receipt test

- Start the test;
- Test phone posts a status with an image;
- Normal phone checks the status;
  - Verify that normal phone's status view is visible on test phone.
- Test phone reads the message and opens the image;
  - (Modded App Only) At this point, the normal phone should not be able to see that the test phone viewed the status. If the result is different, note that.

Anti-deletion test (message, image, status)

- The conversation between the normal and test phone should be open on both devices
- Normal phone deletes a message "For Everyone";
  - (Modded App Only) We should still be able to see the message on the test phone. If not, note that.
- Normal phone deletes an image;
  - (Modded App Only) We should still be able to see the image on the test phone. If not, note that.
- Normal phone deletes status;
  - (Modded App Only) We should still be able to see the status on the test phone. If not, note that.
- Test phone deletes status;
- Test phone deletes message;
- Test phone deletes image;

Freeze "Last Seen" test

- Note down last seen time observed on test phone for normal phone:
- Close the app on the normal phone;
- Wait five minutes
- Note down last seen time observed on test phone for normal phone:
- Reopen app on normal phone and go to the chat with the test phone;
- Note down last seen time observed on test phone for normal phone:
- Note down last seen time observed on normal phone for test phone:
- Close the app on the test phone;
- Wait five minutes
- Note last seen time observed on the normal phone for test phone:
- Reopen app on test phone and go to chat with the normal phone;
- Note last seen time observed on normal phone for the test phone:

Disable Incoming Calls test

- Start test;
- Test phone calls the normal phone;
- Normal phone answers and hangs up;
- Normal phone calls the test phone;
- Test phone answers and hangs up;
  - (Modded App Only) The test phone should never receive this call. If it does then note this below.
- The procedure ends.

Appendix D. Meta-Review

The following meta-review was prepared by the program committee for the 2025 IEEE Symposium on Security and Privacy (S&P) as part of the review process as detailed in the call for papers.

D.1. Summary

This interview study explored users' perceptions of modified versions of WhatsApp ("mods") in Kenya. The study investigated the motivations behind using WhatsApp mods, particularly their additional privacy features. The paper highlighted the dangers of using WhatsApp mods, such as excessive permissions and malware.

D.2. Scientific Contributions

- Provides a valuable step forward in an established field.
- Addresses a long-known issue.
- Expands the scope of security and privacy (S&P) research to understudied populations.

D.3. Reasons for Acceptance

1) The paper provides a valuable step forward in an established field. It provides novel insights into WhatsApp mod users' perceptions, exploring their practices, and mental models about the related security and privacy implications.
2) The paper addresses the long-known issue of security and privacy risks of modded apps. The paper proposes recommendations for improving the security and privacy of WhatsApp (mods).
3) The paper encourages the exploration of non-WEIRD (Western, Educated, Industrialized, Rich, Democratic) populations in S&P research. While there are a lot of privacy perception studies of Western users, this study provides novel insights into Kenyan users.

D.4. Noteworthy Concerns

1) The authors do not compare perspectives of WhatsApp mod users with those who do not use mods.

Appendix E. Response to the Meta-Review

The reviewers note that we did not compare perspectives of WhatsApp mod users with those who do not use mods. While interesting, this was unfortunately outside the scope of our study. We leave this investigation to future work.