Tailormade?
A study on the usability of Tails in India
By Chinmayi S K, Vasundhra Kaul

All text and images are available under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0) license unless stated otherwise.

For requesting waiver, email the authors at theteam@thebachchaoproject.org
About The Bachchao Project

The Bachchao Project is a techno-feminist collective that undertakes community-centric efforts to develop and support open source technologies and technical frameworks with the goals of mitigating gender-based violence and working towards equal rights for women, LGBTQIA people, and gender non-conforming groups. We conduct research and advocacy in all the above areas and guide communities in determining appropriate technological interventions for themselves.

Authors and Contributors

Chinmayi S K

Chinmayi is the founder of The Bachchao Project. She has a degree in computer science and has spent over a decade in technology for good and open technology communities.

She has experience building technology interventions, interdisciplinary research, designing training modules, growing and supporting open communities, designing and hosting events, and fundraising. Conducting interdisciplinary feminist research and creating spaces for dialogues is something she enjoys a lot.

Vasundhra Kaul

Vasundhra is interested in exploring ways the law interacts with vulnerable communities—including incarcerated persons, queer and LGBTQIA+ individuals and groups, and religious minorities.

They are cautiously optimistic about using technology as one tool for social change and enjoy helping communities and individuals find security solutions that work best for them. They are currently a member of The Bachchao Project.
Other Contributors

**Mythri Prabhakara**, Documentation  
**Ayesha Minhaz**, Editor  
**Supreeth**, Design Contributor

## Acknowledgements

This study was made possible by many individuals and groups, but we remain unable to credit them by name for security reasons. We hope they recognise themselves in this note and know that we are grateful to them.

The participants, who were open and honest throughout, helped us carry out the study the way we wanted to. They provided vital insights into how the functioning of Tails could be made better.

The lead volunteer from the participant group was an essential support for the everyday communication and coordination that usually follows a study of such size and structure.

Sajolida, from the Tails development team, was an essential part of this effort as well. He supported us throughout the process and helped make the study more effective.

Finally, this study was possible with the support of Internews and the Sarapis Foundation. We would like to thank them both for the opportunity and the support.
Abstract

With data breaches, surveillance, and censorship increasing in the recent past, digital privacy has become a concern for several sections of vulnerable populations in India. Even among ordinary citizens of the country, who were hitherto not as concerned about privacy-related issues, the inclination to function within a more secure online space is growing. In this context, studying the adaptability of Tails among non-technical users held a significant potential to understand the region-specific issues with the operating system and its shortcomings. While participants did adapt to Tails after some training and found the security reassuring, concerns such as boot-time issues, slow browsing speeds, failing Tor bridges, and troubleshooting difficulties were some hurdles encountered.

Keywords:
Tails, operating systems, digital privacy, data security, India, usability study
Contents

Part I: Introduction 1

Part II: Methodology 3
   Sampling
   Data Collection
   Anonymizations
   Security Considerations

Part III: Research Questions 7

Part IV: Process 8
   Preparation
   Learning Period
   Observation Period
   Post-observation Period

Part V: Findings 11
   Installation
   Booting Tails
   Image Corruption on USB
   Downloading Tails and Etcher
   Ease of use
   Connecting to the Internet
   Slow Browsing and Download
   Applications
   Onion Share
   Persistence Storage and Metadata Anonymization Toolkit
   Tor bridges
   Feeling of safety
   Troubleshooting
   Tails resources provided
   Tails documentation
   Accessibility
   Tails and India
Part VI: Recommendations

Part VII: Discussion
   Technical infrastructure
   Limitations
   Future Work

References
   Appendix: Glossary
I. Introduction

India has had a checkered history with respect to data privacy rights. In a groundbreaking judgement [1], the Supreme Court in 2017 ruled that the Indian Constitution guarantees a right to privacy. However, the largest democracy in the world still does not have a data protection act or a data protection agency[2]. Apprehensions about data security heightened ever since the government compiled the world’s largest biometric database, with over 1.3 billion records. In early 2018, there was news of a data leak of this database [3].

Understandably, such and similar data leaks have made ordinary citizens conscious of the need for additional security, and they have started thinking about privacy in more concrete terms. Several media persons, academics, and activists of this region have also highlighted the need for accessible tools and training that allow private and anonymous digital use. This need becomes more evident among those who use shared devices and want to keep their time on the device secure and private.

There are also other more vulnerable groups of persons. In India, 31.1% of married women between the ages of 15 and 49 reported experiencing spousal violence, according to a government survey conducted in 2015-16 [4]. According to the latest data from the National Crime Records Bureau [5], domestic violence against women topped the categories of violence against women in India. There are potentially far greater numbers that go unreported, especially in relationships outside of marriage. These persons, too, can benefit from having tools for anonymous and secure conversations, especially when sharing devices.

As it describes itself on its website, Tails is a “portable operating system that protects against surveillance and censorship [6]”. It is an accessible, free platform that can be used repeatedly – with multiple privacy and anonymity measures built into it.

Keeping in mind the varied needs that will arise from a multifaceted population, we decided to train a selected group of persons to use Tails for their work. While all of our study participants came from different backgrounds, there were a few unifying factors; they were all non-technical or casual digital users. The participants were
either currently engaged or had previously worked on human interest issues where privacy was a significant concern. Some were also undertaking field visits in areas with poor infrastructure, which meant greater dependence on public WiFi and computer cafes.

In this report, a mixed-methods approach was adopted, and both quantitative and qualitative methods were used. We modified the traditional usability study format after recognising that the participant group needed some basic initial training. Therefore, the study included elements of training and also exploration. These are recorded in the ‘Methodology’ section.

We also placed great emphasis on the security of the participants who participated in our study. A short note on aspects of ‘Security’ is followed by the section of an anonymised presentation of participant Demography.

Over four months, we familiarised participants with the basics of Tails and recorded their usage of the platform for their work. We found some issues with the platform, both technical and non-technical. Some of these have been recorded previously by the Tails team, and others are perhaps contextual to the local population we trained. Tails is a great platform for non-technical users in most instances and has significant potential for use in a country like India. However, adaptability will depend on how well Tails adjusts to the local circumstances. These are recorded under the ‘Findings’ and ‘Limitations’ chapters, respectively.

We have some specific recommendations for the Tails team that we hope they will consider incorporating in future releases. These are detailed in the ‘Recommendations’ chapter.

There is a dearth of literature on using Tails, and other security-focused platforms, especially in countries in the global south. We hope this report is the first of many on this subject.

[1] Puttaswamy V. India - Global Freedom Of Expression
[3] BBC News, 2018
II. Methodology

In this study, we looked at the usability of Tails for those Indian users who needed a secure and confidential platform for their work. The study did not use traditional usability methods, which simulated the use cases. Instead, it included training and exploration of the operating system. The study was thus based on participants self-reporting their experiences of the platform.

A mix of quantitative (questionnaires and surveys) and qualitative methods (interviews and focus group discussions) were employed to record responses from the participants.

The study was divided into four phases: the work period (June 1 to October 15), the learning period (June 15 to July 15), and the observation period (July 15 to October 11). Feedback was collected in the post-observation period. The details are recorded in subsequent sections.

1. Sampling

The participants for this usability study were selected based on a few criteria. They had to operate remotely from anywhere across the country and frequently use public computers for their work. Their primary needs included browsing capability and sharing of large files securely. Confidentiality had to be a crucial aspect of their work. Often, they had to undertake tasks related to research, editing, and organisation.

The following demographic information was recorded at the beginning of the study (decimals may be rounded up):

Gender
Most of the participants (61%) identified as women or as female, around 30% identified as male, and 9% (two participants) chose not to disclose their identity.

Age
Most of our participants belonged to the 21 - 24 age group (43%), followed by
26% and 22% participants who belonged to the 18 - 21 and 21 - 24 age group, respectively. The lowest representation was of people who were 27 and above (9%).

Region

All the participants were located in India for the duration of the study. For the purpose of this study, we divided the country based on several geographical indicators;

1. North India (Haryana, Himachal Pradesh, Jammu and Kashmir, Punjab, Rajasthan, Uttar Pradesh, Uttarakhand) :: 35% of the participants belonged to this region.

2. West India (Goa, Gujarat, Maharashtra) :: 26% of the participants belonged to this region.

3. South India (Karnataka, Andhra Pradesh, Tamil Nadu, Kerala, Telangana) :: 13% of the participants belonged to this region.

4. East India (Bihar, West Bengal, Orissa, Jharkhand) :: 13% of the participants belonged to this region.

5. Central India (Madhya Pradesh, Chhattisgarh) :: None of the participants belonged to this region.

6. North East India (Arunachal Pradesh, Assam, Manipur, Meghalaya, Mizoram, Nagaland, Sikkim, Tripura) :: 13% of the participants belonged to this region.

Minority status
Most of the participants did not belong to India’s religious or ethnic minority communities (78%). Most of the participants did not belong to a sexual minority either (91%).

2. Data Collection

KoBo Toolbox was used as a platform for all study-related surveys. Only necessary information was collected. Some demographic information was asked for, but no personally identifiable information was ever collected.
3. Anonymizations

Sharing of personally identifiable information was actively discouraged during the study. Any information that could identify the participants was discarded during documentation and analysis.

Participants sometimes accidentally revealed some identifying information about themselves and their work. It was redacted in transcripts, and they were informed of the same.

4. Security Considerations

This study was accomplished by taking utmost care regarding the security and risks faced by participants. Everyone who participated in this research was asked to choose a pseudonym separate from their real identities. The participants and the researchers were encouraged not to share any personal details during the study period.

Communication

The participants and researchers interacted through

(a.) Slack:
A Slack channel was created specifically for this study, and participants were asked to join it using pseudonyms. For enhancing anonymity, participants were encouraged to use a separate email ID for training-related Slack interactions. Further, the Slack channel is scheduled to be deleted after the documentation of the study.

The communication on the Slack channel was limited to the training sessions and subsequent usage of Tails. Participants shared their experiences and their frustrations through this medium. Slack was also used as a way for participants to share screenshots when they encountered issues.

(b.) Jitsi Meet Calls:
The training sessions were hosted on the Jitsi Meet server. The Jitsi calls were
protected with the lobby feature. The Jitsi call links were created right before the meetings, and invitations were shared on the participant Slack channel. These Jitsi Meet links were not reused to avoid any breaches. Here too, the participants were encouraged to join the calls with their respective pseudonyms. The participants were not required to share their screens or videos during these sessions. Some of these Jitsi Meet calls were recorded to ensure accurate transcription. Prior consent was obtained from participants, and all recordings were deleted post documentation.

**Tails OS**

The usage of Tails was restricted to this study and in the future for their work with their organisations. The researchers provided a verified Tails binary to the participants. The binary was also verified on the participants' end. The participants were briefed about Tails and its limitations, and security considerations for the participants, if any, were discussed.

It should be noted that all participants were given a copy of Tails 4.19 during their training period. A newer version of Tails was released near the end of their training, and we requested them not to update it till the training period had elapsed. This was done to ensure uniformity across reports.

Tor Bridges provided to the participants were directly obtained through the site https://bridges.torproject.org/ or through Tor employees.
III. Research Questions

1. Whether Tails is a user-friendly secure operating system for users in India who work on semi-public infrastructure:

   1.1. What is the experience of installation and setup?
   1.2. What is the experience of secure browsing and storage?
   1.3. What is the experience of secure file sharing?

2. What is the experience of working with Tails across varying and inconsistent internet speeds and bandwidths?

3. What are the needs of users doing research and community support with at-risk communities?

   3.1. What are the applications used most frequently (by participants) while using Tails?
   3.2. What applications or features are missing the most?
IV. Process

The study was divided into four phases: the preparation period, the training period, the observation period, and the post-observation period.

1. Preparation

During this period, first, the research questions for the study were finalised. Twenty participants with similar needs were shortlisted. The trainers prepared a consent form to initiate participants into the study. A pre-training questionnaire was also designed and sent to participants to understand their background and experience better. Based on all these, the sessions’ curriculum and timeline were decided upon, and resources were prepared accordingly.

A Slack channel was set up to facilitate the training sessions and to record quick feedback. All questionnaires and surveys were sent through the Kobo Toolbox application.

2. Learning Period

This period involved training the participants in the use of Tails and associated applications. The participants were given a copy of Tails and Etcher and instructed on how to burn a Tails image on their USB. The participants also received a glossary—prepared by the trainers—that they could refer to during their training (included in the appendix to this publication).

We prepared a set of training slides that discussed the topics we wanted to cover during the learning period. While these slides drew upon pre-existing Tails literature (mainly from the official Tails site), we broke down certain concepts and curated the content to make the resources more suitable for the participants we would be training. In doing so, we consciously chose to exclude certain features participants had not expressed interest in learning. Some features that may not have been part of the basic Tails run through were included.

Our primary method of instruction was to first send presentations and slides to
participants via Slack and then hold sessions over Jitsi. Additional resources were also shared via Slack. Participants reached out via Slack in case of difficulties. Following requests from the participants, additional training sessions were held as per mutual convenience. Each session had a corresponding presentation and take-home exercises. An adequate gap was maintained between sessions for participants to try out exercises independently and note any issues early on.

A total of six sessions were held during the training period. The applications for the training were shortlisted based on the participants' work requirements. While we anticipated sessions lasting up to 3 hours, we sometimes needed to spend up to one additional hour with participants to help them through the obstacles (documented in our findings). Barring the first session, all others began with a recap of the previous session and then moved on to that day's theory and hands-on practice. Participants were encouraged to voice concerns and actively take part in the discussions and exercises.

The participants informed us about the problems they had encountered in their use of Tails via the Slack platform. The Slack channel was also used to provide follow up support to participants. If participants requested additional support, sessions were set up to help them with specific aspects of training and troubleshooting. Additionally, office hours were held each week in case a participant required further support. After each session, a questionnaire was sent to the participants to collate their experiences of the tools used. All presentations and resources used in training were made available to all participants on the training day.

Details of the six sessions are recorded below:

(a.) Installation

The focus was on the initial set up and participants were walked through the boot menu options and briefed on what to expect. Before the session, copies of Tails 4.19 had been circulated to all participants via Google Drive. A link to download Etcher had also been sent. Detailed instructions (via Cryptpad) were provided on how to install and load Tails onto a USB. A glossary —of terms used in training— was shared, as many participants lacked prior technical knowledge.

Separate sessions were held for Windows and Mac users, owing to system similarities with boot options. Since the participants did not have technical knowledge about operating systems, concepts such as BIOS settings and
bootloader menu were explained. This session ended at the Home page of Tails. Participants were asked to explore some of the applications and controls as homework.

(b.) Browsing with Tor

This session focused on connecting to the internet and using the Tor browser for the first time.

A brief introduction was provided about Tor and how it operates. Participants were encouraged to view the Onion circuits their information was being routed through. They were provided onion addresses to popular sites to try out for themselves. Warnings about the Tor network and anonymity were also provided to the participants.

(c.) Persistence Storage (PS) and Metadata Anonymisation Toolkit (MAT)

This session involved background theory about how PS works in Tails and when it should be enabled. Participants were guided on how to set a secure password. Once participants enabled PSS, they were asked to download a picture from the internet and store it in Tails.

The participants then learnt about metadata and how to view it on their devices. The photos downloaded earlier during the session were used as samples to demonstrate the removal of metadata using MAT.

(d.) Mac Address Spoofing and Onionshare

Mac addresses were explained to the participants. After providing warnings about spoofing, all participants were walked through the process of disabling and enabling spoofing. Participants were also instructed in the use of Onionshare. They were then asked to share files with each other via the application after the removal of metadata.

(e.) Tails and Bridges

Participants were instructed on the purpose and use of Tor bridges and walked through the process. The participants were given bridges to try out and were asked to note whether they could make connections using them. The participants received information on when bridges are helpful, along with warnings about their use
in specific situations.

(f.) Winding up Tails

For the final session, participants shared any obstacles they had or were currently facing in their use of Tails. They had queries about applications and features that were not covered in training. Towards the end, we discussed the deletion of Tails from a USB and copying Tails from one USB to another.

After the last session, Focus Group Discussions were organised for the entire participant group. The motive of the focus group discussions was to collect experiential data and highlight specific obstacles the participants may have faced and how they overcame them. Two groups of participants—Windows users and Mac users—were invited to separate discussions.

3. Observation Period

Participants were encouraged to use Tails for their daily tasks and asked to record any errors they ran into and their general experience. During this period, we offered two office hours and were available over Slack if any questions arose. We did not hold any additional training sessions.

4. Post-observation Period

Feedback collection for this study was primarily done through focus group discussions and personal interviews. The participants were also asked to fill up a feedback survey.

The interviews followed a pre-decided script similar to the focus group discussions, so the questions were standardised. These discussions were recorded, and informed consent was taken to document them.

The recordings were temporarily stored on Dropbox before being downloaded to a trainer or documenter's system. After transcription and report writing, the recordings were destroyed.

The interviews were restricted to a total of eight people belonging to both groups. The transcripts of the sessions, focus group discussions, interviews and the Slack communications were consolidated for analysis and report writing.
V. Findings

1. Installation

Most participants found the installation process fairly straightforward. Participants who used Windows systems had more success with installation than those using macOS. Those participants who were unable to install Tails using the initial set of instructions were given additional support.

Most participants completed installations with the help of a walkthrough from the trainers. Six participants needed additional support for installations, and three participants failed to complete the installation process. Among those who failed to complete the installation process, two owned Apple laptops with M1 chips. The other participant had a Macbook Air Retina 2018. Security settings do not allow this Mac to use an external startup disk. While the Tails manual on the website was helpful, the trainers had to handhold this participant through the process. The participant was able to boot after changing these settings. However, the cursor pointer remained frozen after boot. Even blacklisting of trackpad hardware had no effect.

Gellhorn, who successfully installed Tails, said, “I mean the booting up itself is a fairly easy process, especially in Windows 10 it was right there in the menu. I am not sure about the technical parts of this, but the difficulty that most people would face is understanding how to load the Tails image onto the USB drive. I know it is fairly easy with Etcher software, but if that itself is like a longer [sic] process, then most people are used to it because most people are used to powering on their systems, and it is there. Maybe it is a one-time thing, but it is not that difficult. If something can be done to make the uploading of the image more accessible, that could be one thing that can help.”

Here, Gellhorn described the most commonly faced initial discomfort, the loading of the OS from the USB disk. Most people are used to the pre-installed OS on their laptops.

Though most participants successfully booted into Tails, some participants seemed hesitant or reluctant to explore the OS. At least two participants asked for information on how to shut down Tails—as they could not locate the power off
and restart Windows OS even after successfully booting into the Tails OS.

“The wariness that I faced in exploring different areas of Tails is because I did not know what application was what. I did not want to do something that was not what I was supposed to do. That sort of unfamiliarity was still there in Tails, and that sort of made me wary of exploring it.” [Gellhorn]

2. Booting Tails

Participants shared that booting the Tails OS takes more time than booting other operating systems. Sometimes the OS also gets stuck during this process.

“Tails does not boot at once and takes two or three tries, Sometimes [sic] Tails gets stuck and has to reboot. Takes [sic] 15-20 minutes to boot up.” [Captain Holt]

“Yeah, it took a bit of time to adjust because it is privacy oriented. Doing basic tasks like searching and everything [sic], took more time, it took more time to boot up, going to Tor was more difficult than google chrome.” [Popeye]

3. Image Corruption on USBs

One participant experienced frequent image corruption. This was rectified by rewriting the image. We were unable to figure out why this issue occurred.

“I think, the only frustrating part of it, I would not say it was frustrating particularly, but it was just a little bit tedious was having to upload the image to the USB drive again because I think once or twice when I was trying to boot up the OS, it just showed an error message. I think I alerted the team about this also. I formatted the drive and uploaded the image again but [sic] I had to do it a few times. I think that was the only tedious part, I do not know if that will continue, I hope it does not but [sic] that was the only difficulty that I faced.” [Gellhorn]
4. Downloading Tails and Etcher

Many participants expressed that they faced difficulty in downloading and creating images through Etcher. Still, everyone apart from the three participants — using the macOS ecosystem — could complete the task using the initial instructions. The participant group had no previous experience of installing a new OS or burning an ISO image. They expressed that this process was new and quite unusual for them.

Three participants found the task of downloading Etcher and the initial image to be particularly challenging. One participant downloaded incomplete binaries of Etcher and encountered errors while running it. One participant had downloaded an incomplete binary or not burnt the ISO image properly, which was solved upon formatting and recreating the image on the disk.

One participant, Sherlock Holmes, took nearly four hours to download Etcher and the Tails image due to the slow mobile network speeds. They described the process as considerably frustrating.

“When I tried to download Tails, it took me approximately 3 to 4 hours. Whenever my laptop goes to sleep automatically, I have to restart it again and again. I have done this at least 3 to 4 times. So it became quite frustrating.”

[Sherlock Holmes]

The process of creating a bootable Disk was not intuitive for all.

Almost all participants were worried about not being able to locate the USB in the finder/file viewer after they had finished copying the image to the USB through Etcher.

5. Ease of Use

Most of the participants we spoke to during the interviews said that Tails was an easy to use OS. They said there was a steep learning curve to using Tails, but eventually, one gets used to the OS. The understanding of the OS was not limited to the technically skilled user and could be used by all.
“My overall impression, if I am just talking in a very holistic way, then I would say that, barring a few impediments, Tails is pretty easy to use, considering that it is a completely new OS and it works very different from the general ones we use [sic], so I would say that it is a very [sic] easy to use OS, especially for people who consider privacy to be important to their work, which is something that I have been wondering about for quite some time now so, I think I definitely do feel safer searching on Tails, basically working with tails.” [Rashford]

“Tails is user-friendly, that is it [sic] is easy to use for people who are not tech-savvy, for instance, I am not a very tech-savvy person, but I found Tails to be fairly simple to use.” [Meduvada]

“Initially, as I said before, it is a steep learning curve, it is not intuitive, it takes time to learn it, in that sense it is not very accessible, but once you get the hang of it, it becomes very easy to use, very accessible to use.” [Popeye]

The participants mentioned that the categorisation of applications was very helpful to navigate and made the OS simple to use.

“But otherwise in terms of readability, in terms of simplest things that one would access, like how to switch off and switch on tails, where the Wifi icon is, [sic] screen brightness, language, and the different kinds of applications, that was fairly easy for me to navigate and to get a sense of where things were. I did not have to ask where a particular app is because it was pretty clear how to find them. And the categorizations into accessories, graphics, internet, office etc., that was pretty simple.” [Eno]

Learning Tails also included learning new habits and unlearning old habits for some participants.

Eno says, “In particular, for our activities and getting used to the whole routine of remembering your passphrase, opening persistent volume, using Tor browser etc., and making sure that I am not signinig [sic] on to any identifying ID’s but once I had established at the outset why we should not do that, it was just about keeping that at the back of my mind while using Tails. While using it itself, it went really
smoothly for me. Including booting it up each time, I have never had any trouble booting it on my system.”

To one participant, this was a frustrating experience. It also discouraged the participant to continue using Tails beyond their work requirement.

“I would say that it has been, because everything is so different than what I am used to. It has taken some time to get used to. Because of that I guess, because of how frequently, I use my laptop in general, it has been frustrating, those roadblock [sic] have taken longer than necessary for me to this thing, Initially, during those roadblocks [sic] I was thinking I would not use this…”

“Yeah, I would not unless my work requires me to. It is very useful for a certain type of work generally as a software, but I do not think I would use it because of the booting time and just everything else, in terms of like, when I do research for stuffs [sic], there are lot [sic] of tabs open, and sometimes I just shut my laptop and go to bed and stuff, when I wake up I do not want to remember what I was doing, it will become difficult with such a system, just like general things, YouTube suggestions, like Youtube suggests what you generally watch, that won’t happen.

If you consider it like security and privacy-wise, it is obviously the opposite of what Tails so, but I have got so used to my laptop always just having everything on there. Because Tails requires us to switch off everything and switch on [sic] again. So I think I would only use it if I must, if my work requires me to use it for a very specific purpose.” [Norbu Choden]

6. Connecting to the Internet

If not automatically connected at boot, the process of connecting to the internet meant that trainers had to provide additional support. The troubleshooting required someone with a technical understanding of how networks could filter, the hardware of the machine, and the mobile operating system. This made it complicated for the end-user.
Six participants—three MacOS users and three Windows users—reported that they could not connect to the internet on their own and that the WiFi symbol did not appear upon booting. One of the five participants resolved the issues with subsequent reboots. The other two participants used USB tethering to connect to the internet. One of the participants shared that they could only connect to networks with the option provided while booting the OS.

Two participants could not connect to the internet. These two tried connecting to the internet through:

- Enabling MAC spoofing
- Creating WiFi Hotspots from their mobile devices
- USB Tethering

One of the participants owned a MacBook Air (1.8 GHz Dual-Core Intel Core i5), and the other used an Asus Laptop. Both participants were connected to the Airtel Network.

Participants who had issues connecting to the internet found the connectivity issues and troubleshooting process rather frustrating.

“The internet, the fact that I could not find the icon, and the fact that we had to keep understanding various parts, maybe it is the system’s problem, maybe it is the software system’s problem, maybe it is the internet connection’s problem, figuring out why the internet was causing the problem was frustrating.” [Meduvada]

“No. I mean, I think I won’t rank them but not being [sic] able to connect to the internet initially, because most of the work we do would be on the internet only, right? We had to share stuff and all the exercises you were doing, like in terms of, are you able to like open Tor and stuff, that was the most frustrating.” [Norbu Choden]

At least 2 participants stated their confusion about not seeing the WiFi symbol in the drop-down menu when connecting to WiFi.
“I tried connecting to the WiFi again. I did not choose my network preference while starting up TAILS. But I still don’t have the option to connect with WiFi in the right corner drop-down menu.” [Vidar]

7. Slow Browsing and Download

The speed of the browser was a common topic of discussion during our sessions. Participants found it very hard to browse the websites when they used mobile internet. This is especially necessary for participants who were connecting to the internet through tethering.

“Yeah [using the browser], that was actually very difficult, when I had wifi and [sic] my WiFi was regular, it was not a problem. I think with 4G on my phone, it was impossible, it was [sic] taking a lot of time.” [Norbu Choden]

Some participants expressed that the slow browsing speeds did not bother them once they started using Tails more.

“[..], except that it was very slow [to browse], I mean that was brought up a few times during the training(s) but other than that, nothing else. I would not say that it being slow is an impediment to using Tails because when we were training, the trainers were quite obvious of the fact that it is not going to be as fast as our usual search engines. Initially, that was an issue, but now I would not say it is as much.” [Rashford]

8. Applications

At least three participants expressed that they did not know the existence of the applications preloaded on Tails. One participant was not aware of the existence of Tails before this study.
Gellhorn said, “I think the unsafe browser and Tor as well— I had never used Tor before. I wished I had known how to access it before because it is just something very interesting to see. Tor I think [sic] would be the main thing, which is very very interesting.

Norbu Choden said, “I think it [Tails] is very new. I did not know something like this existed before we actually started training.”

One participant recommended that a general note on the programs could help in building familiarity with them.

Gellhorn said, “Yeah. Just a sort of thing which you know, when you click the drop down [sic] menu to the top left, there is a large list of programs and everything. If we could get a short note on what everything is, what each of the program [sic] does, I understand that that kind of unfamiliarity come [sic] to a lot of people with the kind of programs that come built in in [sic] windows and mac OS also, but specifically for Tails, if the aim is to use tails, practice makes perfect, if you want to get people to practice Tails itself, I think that kind of thing will help people reassure them that this is something that anyone can use and it is not just for the experts [sic]. So I think that will be helpful with the useability.”

Otherwise, the participants expressed that the categorisation of applications in the OS was familiar to them and made the transition easier.

> “Otherwise, I do think that the categorization of applications etc is fairly intuitive and corresponds to other OS's so people won’t have to spend a lot of time looking for a particular application...” [Eno]

At least 2 participants stated their confusion about not seeing the WiFi symbol in the drop-down menu when connecting to WiFi.

9. **Onion Share**

Participants felt that Onion Share was a very useful feature. Almost all participants found it easy to use and easy to understand. The participants used this to send documents to their colleagues and friends during the training period. Three other participants who could not connect to the internet or run Tails were unable to complete this activity.
“Like I had mentioned in our previous conversations as well, transmitting information through Tails is something I have been using predominantly, so if I am specifically talking about privacy, of course, the onion site and the functions relating to those have also been pretty useful, so I would say those are two of the most important parts, I mean there are others as well but in my regular use, I think these are the two things that have, you know, really been useful for me in terms of privacy...” [Rashford]

At least 2 participants stated their confusion about not seeing the WiFi symbol in the drop-down menu when connecting to WiFi.

10. Persistence Storage and Metadata Anonymization Toolkit

Persistence Storage was a new concept for most participants. Most of them welcomed the idea (of persistence storage) since this supported their need. Participants said that it was one of the features that added to the feeling of safety when using the Tails OS.

“Yeah. Definitely. I think it will. Metadata anonymization [sic], using persistent storage, using Tor for browsing because it connects to multiple nodes, all of these are safety features which I feel make Tails safe.” [Popeye]

Most participants considered the Metadata Anonymization toolkit as vital to their work and their idea of safety.

“The Metadata anonymization is very handy, also the tor browser is something that can be easily accessed which can’t be done through other software, this ensures that activities on the internet are not susceptible to incursion so that is why it has been nice.” [Popeye]

Issues

Five participants mentioned that they faced difficulties when trying to enable persistence storage, and two participants were unable to enable it. One participant
did not enable it from the welcome screen and had to be asked to follow the instructions again. Three other participants who could not connect to the internet or run Tails also were unable to complete this activity.

After enabling persistence, all participants except one who could not run Tails were able to create the persistent volume without any issues.

One participant observed that with persistent storage:

“‘The odd thing where I was setting up my Persistent storage and it automatically had a [sic] “x” size depending on the device that this OS was booted on...’” [Eno]

Three participants reported that they had difficulties while trying to remove metadata using the toolkit. Three other participants who could not connect to the internet or run Tails also were unable to complete this activity.

Two participants reported that their systems crashed when trying to remove Metadata from their files, and at least one participant reported that they received an error.

“‘.. There are only two issues I faced. When I was undertaking my data anonymization, a lot of times it failed. You had to try again and again for it to succeed. And secondly, sometimes I am not able to connect to the bridge for the Tor browser.’” [Popeye]

“I think it was while using the metadata, it somehow it just crashed twice, and the third or fourth time it could happen, I really do not know why that happened but that was how it went about, that was like very very annoying for me.” [Captain Holt]

11. Tor Bridges

Connecting through Tor bridges to the internet found very little success despite multiple attempts to obtain a bridge and connect. In this case, Tails would fail to work for most people if the Tor network is blocked or censored in India.
The participants were asked to obtain Tor bridges from https://bridges.torproject.org/, and the team also obtained a set of pre-tested bridges from the Tor developers. However, almost all the participants faced difficulties while connecting to the internet via a bridge. Only one participant was able to connect to the internet in this manner, but eventually, they were unable to connect on subsequent attempts.

“Yeah, I was able to do it the first time I tried it. Today I tried the bridge thing again and it did not work.”

“When I was trying to connect to the bridge, the progress bar was static, it was not moving forward, and I have shared the bridge, so that was an issue I faced.” [Popeye]

12. Feeling of safety

Most participants felt that Tails added to their feeling of safety. The pluggability of the OS was a significant factor in this.

The pluggability of the OS helped primarily in helping the participants feel safe.

“... the OS is not located on my primary device. It is not a drive that I have to manually plug. Which [sic] is otherwise unidentified. A random person would not be able to distinguish between this USB and all the other USB’s that I have. So that portability, even if I do not have my personal device with me but I can still use this OS on any other device if I have to do the work of my organization, I think that is its biggest advantage [sic]. Because otherwise all my work is so tethered to the particular device I am using and all my personal devices and having secure channels for communication that I can have, even on other devices, outside of my personal device is the biggest asset that Tails gives [sic] us.” [Eno]

The Tails OS provided tools that by default supported the principles of anonymity. The tools supported most functions necessary to research and communicate anonymously online; users did not have to worry about data trackers or surveillance. The participants appreciated this.
“I think the one thing that makes me feel safest about Tails is the level of anonymity that goes with it. So that was definitely one thing that I appreciated. Besides the anonymity, another thing that I appreciated was that you could actually do a majority of the work that you are doing over the internet anonymously, so that was very new to me [sic]. Until then anonymity was an abstract concept.” [Meduvada]

Some participants attributed their feeling of safety to the amount of control they had over their data storage, and they said this reduces the anxiety about vulnerability in today’s climate of trackers.

“Yes. I think it will be quite a bit. Just in the booting up itself of the software, it already feels there are many different layers of security in knowing that your program is safe. And even when operating, you know, the fact that you have control over everything, where everything gets stored and you can delete everything, I think that kind of useability does not exist in Operating systems, at least not that the lay person [sic] is aware of. That exists in operating systems like windows, mac or Linux. I have not used much so I do not know about that [sic]. But using mac and windows [sic] I can sense that there is a lot of control over things. I think that is the entire protection around communication, that itself would be a great benefit especially right now when everyone is sort of a little anxious about how their communication is vulnerable to being viewed by others.” [Gellhorn]

13. Troubleshooting

One significant concern shared by a participant was that if a user is from a non-technical background, it would be difficult to troubleshoot when something goes wrong. As trainers, we agree with this. After every session we conducted, additional troubleshooting and support had to be provided. Some of this meant understanding how different hardware works, how the internet works, and how Linux works. There were also some gaps in the Tails documentation around troubleshooting.
“I mean, like, what was technical for me was, how, like when I was having roadblocks, like the solutions for the roadblocks were not normal, nobody would think of doing that, like for example, for my internet, so I had to restart it and then do the mac spoofing thing, if somebody else is using, how would they know, like this is the cause for the problem. I was just following what you were saying, if you guys were not there and I was just using it on my own, how to solve and find shortcuts, know my way around, that was very technical in nature.” [Norbu Choden]

14. Tails resources provided

Almost all the participants we interacted with found the materials prepared by the trainers to be comprehensive and easy to follow.

“I actually went over the PPTs that were shared by the team and one [sic] they were all fairly easy to navigate. I knew that, for instance, the moment I had OnionShare, I would know what to do. I though [sic] OnionShare was quite simple, easy to understand, easy to use.” [Meuvada]

“I think the documents that were provided by the team were very, very helpful because they explained things in a very succinct manner, it was very easy to comprehend what was given, and it was not too much you had to read to be able to understand what was going on. So it was a very good fundamental user manual of sorts.” [Gellhorn]

Gellhorn, Rashford, and Meuvada expressed a need for a foundational theory manual for participants who wanted to learn more about the background of some of the applications they used during the study. Meuvada also brought up the possibility of doing preliminary sessions. These could be in addition to the resources we had already provided and not mandatory.
“I, for one, did not even know that Tails existed. But when I downloaded it, plugged it in, and booted up the system, there was a great deal that I did not know how to access the internet at that time. I knew that the Tor browser existed, but I did not know how it operates, does it operate differently than Mozilla, chrome, opera, anything of that sort. I did not know much about that, so there is a need to, there [sic] is a lack of know-how. I think that is the thing that can be addressed.” [Gellhorn]

“One thing that I did not understand when I started was what Tails really was. I just knew it was something to help against surveillance and to protect our privacy and our data [...] I had no idea that Tails was an entirely alternative software [...]. [...] Preliminary sessions would have been good. In the sense that, when Tails training started, initially, I felt like I had just jumped into the deep end of the pool. I felt like I was being a little slow. After the session was over, I would just go back to the presentations just to see if I had gotten it right but a few preliminary sessions, I think, not because I could not operate tails, but simply because I think it is interesting to know and just understand the framework.”

After the initial few sessions, the trainers started sending presentations and exercises while holding open hours in case of difficulties. It was done after discussing with the participants. However, at least one participant mentioned that one-on-one conversation was the most useful when they needed additional support for troubleshooting. The participant preferred screen recordings over an additional manual.

“I think both the PPT’s and taking it step-by-step helped me because I really needed somebody to be there at each point. Because it was completely new and it became much easier when somebody was on the other end, telling me exactly what to do. [...] Usually, I would have more problems, and I would have to stay back, and those were most useful. Live sessions, I think that it is useful if your laptop is working, and everybody else’s is, and you are going at a pace. But then, once you go off track, you have to wait till the end. I think one on one was most useful for me.” [Norbu Choden]

Captain Holt found the presentations and office hours system the best to follow and did not have significant difficulty running Tails. Popeye found training sessions the easiest, at least for the initial few weeks.
Overall, those who needed little to no troubleshooting preferred having the presentations sent over the Slack channels. The need for continuous interaction grew for participants who found themselves facing technical difficulties.

15. Tails documentation

We provided training materials to all participants with follow-up support and resources, including an introduction to the Tails website. While most participants did not browse the website during their training or observation period, a few did.

Gellhorn visited the Tails official documentation when they had trouble booting Tails. They said, "I think the Tails website made it easy to understand how to do it. Which for a person who is not very familiar with, [...] how to format disks, etc. [sic]."

Meduvada explored the documentation to know more about the history of Tails and for examples of its use. They did not use it for any resources or reference materials.

16. Accessibility

One participant reported having a physical disability that made it difficult for them to use Tails overall. They requested extra time for the exercises and mentioned the same in their interview as well.

A large majority of participants did not feel they would be best placed to talk about how accessible Tails was since they were non-disabled.

One of the participants who responded, Sherlock Holmes, believed that all software required a certain amount of technical knowledge and adaptability to technology and that Tails was no exception

“It depends on the nature of disability a person has, are there people surrounding him or her to assist them with Tails, it totally depends. There is not straightforward answer to it.” [Sherlock Holmes]
17. Tails and India

Most of the participants spoke about the usefulness of Tails in India with respect to the security options it provides. It holds especially true for those who are human rights defenders or journalists. Meduvada explains further:

“I do not think Tails is just about protecting privacy against the state. I think it is also about protecting privacy between people, between legal entities, other persons, other corporations, etc. It definitely has use for almost everyone that uses the internet.”

There is a growing concern about monitoring and surveillance from third parties, and as we explained the uses of Tails, many participants expressed interest in the amnesiac nature of the tool. Gellhorn summed it up with,

“I think it is especially useful in the Indian context. Not just because you know people are handling sensitive information but because privacy is a serious concern and [...] India does not have much regulation of government monitoring and surveillance [sic]. The privacy laws are very thinly veiled, so I think for India especially, it is very, very useful for any work you are doing. Especially because it just brings a lot of reassurance. For example [...] there was a big controversy over WhatsApp’s privacy policy that was being implemented. Everyone started flocking to signal, to telegram. I think that is indicative of the fact that people want privacy. I think it will be a very useful tool for anyone in India, especially in this day and age.”

For this reason, some participants described the use of Tails as a preventive measure, especially when handling sensitive information. It makes them feel more secure than the operating systems they use.

Participants also brought up certain limitations they felt Tails had for the broader Indian population. Eno looks forward to seeing support for additional Indian languages. They also felt that the use of Tails in low bandwidth areas might present a problem since a large portion of the population lives and works in rural areas. We encountered this issue, especially among participants not residing in major cities.
Problems owing to poor internet infrastructure, adverse weather conditions and power cuts contributed to certain participants being unable to carry out activities in time or attend sessions.
VI. Recommendations

1. Chipset Support

Two participants were unable to perform the initial installation of Tails, owing to the M1 chips in their Apple laptops. This signalled the beginning of significant concern as almost half of the participants used Apple laptops to run Tails, and the company is introducing these chips across newer product lines.

Tails needs to be compatible with these newer Apple processors to ensure it does not alienate a chunk of its potential user base. We understand from the Tails documentation that currently, Tails is only available on the x86_64 architecture and does not work on ARM architecture so far [7]. However, we believe that general support should exist for all ARM-based devices.

2. WiFi problems with some systems

Multiple participants faced problems while connecting to the internet. Of these, two were unable to connect to the internet at all and could not see the WiFi symbol appear on the Tails home screen. According to documentation [8], this seems to be a problem common to some Tails users. Other participants had trouble connecting via the WiFi option and used mobile or Bluetooth tethering instead. The missing WiFi symbol made the participants feel unfamiliar with the OS. If the symbol had appeared with an indication of not being connected to the internet, it would help put participants at ease.

3. Search feature to look up files more easily

Participants reported finding it generally easy to navigate the operating system. However, some felt that a search bar to find applications and files more quickly could be helpful. A search bar is something they found useful while using other operating systems and hoped could be added to Tails too.
4. Add more keyboard shortcuts (common to other OSs)

Early in the training sessions, we shared Tails-compatible keyboard shortcuts [9] with the participants as an assistive measure [list taken from]. The participants requested more shortcuts that are commonly found in other operating systems. These included the option to cut, copy, paste, undo, redo, switch between applications, select all, etc.

5. Add a glossary or basic technical information to the Tails documentation (preliminary sessions)

A major concern multiple participants flagged was that Tails had a steep learning curve, at least on initial viewing. Since our participants were non-technical users, we attempted to address this by providing a glossary of technical terms before the training. The training presentations were also kept relatively jargon-free. Despite this, we got feedback requesting a separate session to go over basic concepts before the actual training began or for additional resources for reference.

It would be helpful to add a manual with basic terms to the trainer resources so that participants wishing to learn more about Tails or learn basic computing terms could easily refer to it.

6. Verified Tor Bridges

There is a need for more verified bridges for this region. The bridges obtained from https://bridges.torproject.org/ failed to connect on Tails Platform. The research team then obtained bridges from the Tor Team for the study participants, which also failed to connect. If the expectation for people working in surveilled and censored regions is to use bridges, this issue certainly requires further work in terms of verification. Furthermore, the documentation on the usage of Tor Bridges is non-existent on the Tails website.

7. Video conferencing or chat support

Across the participant group, several spoke about the need for having a chat platform (Signal as an example) and videoconferencing support.
This shows how participants are taking to Tails as a platform for secure communication outside of emails.

8. Graphics

Almost all the participants reported finding the current look of Tails 'aged'. Participants compared it to old Windows home screens and several described the 'feel' of Tails as the most different thing to get used to, at first glance. Aesthetics aside, there was a persistent concern that using Tails on a public computer would make the user stand out as it looks considerably different from current operating systems. There is ample documentation discussing why developers use the GNOME desktop [10], but we hope the concerns mentioned above will also be factored into the design decisions.

9. Startup tutorial

All the participants we spoke to indicated that the training materials provided to them helped in setting up Tails and running it. While circulating such material is a possibility, some participants wondered if it would be possible to have a tutorial option on the screen. This tutorial could take the user through some of the features we covered in the training sessions and make the initial use of Tails less intimidating.

“I think it is especially useful in the Indian context. Not just because you know people are handling sensitive information but because privacy is a serious concern and [...] India does not have much regulation of government monitoring and surveillance [sic]. The privacy laws are very thinly veiled, so I think for India especially, it is very, very useful for any work you are doing. Especially because it just brings a lot of reassurance. For example [...] there was a big controversy over WhatsApp’s privacy policy that was being implemented. Everyone started flocking to signal, to telegram. I think that is indicative of the fact that people want privacy. I think it will be a very useful tool for anyone in India, especially in this day and age.” [Eno]

10. Localization

Currently, Tails is not available in any commonly spoken Indian languages [11].
While all the participants of this particular study were fluent in English, many pointed out that not all potential Tails users in India would be. Additional translation for at least five commonly spoken Indian languages would be a good start to introducing Tails to more regional users.

[9] https://tails.boum.org/doc/first_steps/accessibility/index.en.html#index2h1
VII. Discussion

1. Technical infrastructure

Internet

When asked if they would use WiFi or mobile data to connect to the internet, 65% of participants said they used WiFi exclusively, 17% said they used mobile data exclusively, and 18% said they relied upon a combination of the two.

There was a near-even split between Windows users and Mac users, with the former having a larger share (57% and 43%, respectively).

Technical Knowledge

Most of the participants (96%) had not undergone any specialised training in computers or computer systems. The one participant who responded in the affirmative had studied Computer Applications while in high school.

Despite this disadvantage, we observed a base level of technical competence among the participants. A majority of them (87%) were able to update their operating systems. A little over half (52%) had explored their system settings, while less than half (48%) had familiarity with operating systems other than the ones they currently used.

A significant share of the participants (65%*) had never installed an operating system on their own in the past. Nearly 91%* had previously not used a Linux-based operating system, and 96% were not equipped in running a virtual machine. Only one of the study participants knew BIOS settings and had modified them, but around 87% had no understanding of it. Formatting of external hard drive or USB was known to 57% of participants.

Application experience

Even as 65% of the participants understood VPN usage, 83% of the total
participants had never used a Tor browser before. A vast majority (91%) had never heard of Metadata Anonymisation Toolkit, and none had ever used it before.

2. Limitations

Slack as a medium

It was hard to drive participant engagement and encourage people to share on the slack channel.

The Slack channel was set up exclusively for communication concerning the project, and conversations between the participants were restricted to the study at hand. This meant that the participants would only log into the channel when there was a need to access resources, ask doubts or provide inputs.

It was further complicated by using a separate email ID to access this channel as the slack notifications went unnoticed unless someone logged into their email id at regular intervals.

As a result, we had to obtain additional support from one of the team members for the purpose of communication. This team member notified the participants of any tasks and reminded them to respond promptly to scheduling and surveys.

Research Online

One of the disadvantages of conducting research online is that participants are engaged in other activities apart from the project. The participants had to juggle several responsibilities, including work and academics, which meant their consistent availability was an issue. As a workaround, we planned activities that participants could complete offline and share inputs with us later. However, this still required a fair bit of communication and management.

Internet Access

The participants joined us from different parts of the country, and therefore we faced the issue of unequal internet infrastructure. We did ensure that everyone subscribed to internet plans that were adequate to meet the requirements of this study. However, poor infrastructure maintenance and upkeep led to some participants not having as efficient an internet access as others.
In turn, this affected some of the study tasks. Nonetheless, these circumstances gave us an insight into the reliability of Tails under such conditions.

**Bias**

The findings of this study include the experience of users who were trained using the material curated by the team. Also, the participants have an incentive to use the platform.

One of the metrics determining the usability of a tool is the ability of users to figure out how to perform any given task on the tool successfully. During the study, the users received curated material instead of just using the user manual available on the website. Thus, the effectiveness of the Tails user manual or the raw learning associated with exploring the Tails Platform is excluded in our considerations.

**3. Future Work**

The researchers plan to submit the recommendations and findings to the Tails team. Some of these recommendations will also be submitted as feature requests or bugs. A preliminary copy of this report has been shared with a member of the Tails team. Most of the issues faced by the participants of this study are relevant to all Tails users, and further testing is required to determine potential solutions.

This study examined one platform that supports the privacy and security of individuals and communities, and we found that there are some issues —both technical and experiential— with real-time use. There is significant potential for Tails and similar applications across India. However, efforts must be made to address the concerns and adequately build the applications for the Indian conditions.
References


Appendix

Glossary

**Prepared with the help of:**
https://ooni.org/support/glossary
https://tails.boum.org/contribute/glossary/

**Bandwidth:** It is the total capacity of data transfer for your internet network. Internet Service Providers advertise these on their plans in the form of Bits Per Minute.

**BIOS:** Basic Input/Output System.
It is the software stored on a small memory chip on the motherboard, which is the first software to run when a computer starts up.

**Checksums:**
They are blocks of data often used to verify data integrity but not relied upon to verify data authenticity. While running checksums, the user will be able to see if the data they are downloading has been altered in any way on its journey. However, this is not sufficient to tell if the data is from the source it says it is.

**ISP: Internet Service Provider.**
This is an organisation that provides services for accessing and using the internet. ISPs can be state-owned, commercial, community-owned, non-profit, or otherwise privately owned.

**Mozilla Thunderbird:**
Mozilla Thunderbird is a free and open-source cross-platform email client, personal information manager, news client, RSS, and chat client developed by the Mozilla Foundation.

**OS: Operating system.**
An operating system is the primary software that manages all the hardware and other software on a computer. The operating system, also known as an “OS,” interfaces with the computer’s hardware and provides services that applications can use.
Privacy Extensions:
These are browser add ons that assist users in getting control over their privacy online through various ways.

Processor:
This is an electronic component of the system where the data processing logic and control are included.

Tor:
The Tor network —which is free and open-source— provides its users with online anonymity, privacy, and censorship circumvention. Tor’s design bounces communications around a distributed network of relays run by volunteers located around the world. This facilitates the hiding of users' IP addresses and enables them to circumvent online tracking and internet censorship.

Virtual machine:
The virtual machine is a complete operating system on its own, running within a program window separate from the host machine.

VPN:
A Virtual Private Network (VPN) is software that creates an encrypted connection (commonly called “tunnel”) from your device to a server (run by a VPN provider). When you browse the internet through this “tunnel,” websites and other online services will receive requests from the IP address of that server rather than from your actual IP address.

Veracrypt:
VeraCrypt is a free, open-source disk encryption software for Windows, Mac OS X, and Linux.

VPNs can therefore be used to circumvent internet censorship.

WiFi: Wireless Fidelity.

WiFi is a wireless networking technology that allows devices such as computers, mobile devices, and other equipment to interface with the Internet. It allows these devices to exchange information with one another, creating a network.