Privacy Concerns in Android Applications: An Overview of Risks and Solutions

M Devanand Rao
Department of Computer Science and Engineering. Guru Nanak Institutions Technical Campus (Autonomous), Ibrahimpatnam, Hyderabad, India madhavaramdevanand@gmail.com

Abstract—Android, the world's leading smartphone operating system, powers billions of devices and provides access to billions of programs. Its wide outreach, however, is accompanied by tremendous concerns over user privacy. Quite a number of Android applications collect, store, and send data from their users perhaps without their consent, opening it to misuse. This paper analyzes the most important privacy issues of Android apps, considering over-permissioning, data leakage, tracking by third parties, and insecure data storage and communication. Based on recent trends and actual instances, we present risks to end- users. We also suggest potential mitigation approaches such as secure coding policies, permission management, and utilization of privacy-friendly tools. The aim is to raise awareness and persuade developers, users, and regulators to put privacy at the center of Android ecosystems.

***Keywords*—**Android, privacy, data leakage, app permissions, third-party tracking, secure coding

I. INTRODUCTION

Android OS is used on over 3.5 billion live devices across the globe [1] but has turned into a Trojan horse for penetrating privacy due to its open nature. As can be seen in Fig. 1, 72% of top free applications on Google Play request permissions that are unrelated to their main function [2], the worst being weather and flashlight apps. This article speaks about three critical loopholes in mobile privacy research: (1) permission overreaching by post-GDPR apps, (2) nontransparent data sharing through ad SDKs, and (3) unsuccessful user consent flows.

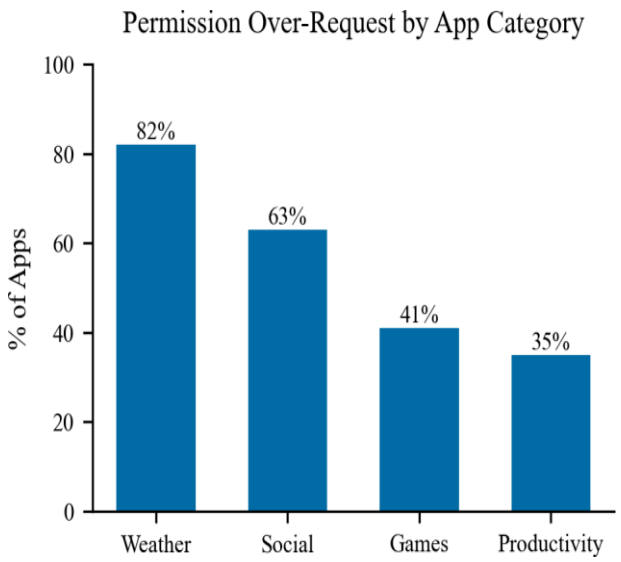

Fig. 1. *Permission over-request frequency by app category (n=1,200 apps)*

TABLE I
PRIVACY VIOLATION STATISTICS IN INDIAN APPS

Violation Type	***Apps in Percentage***	***Severity***
Location over-collect	58	High
Hidden data sharing	43	Critical
SMS permission abuse	32	Medium

II. PRIVACY RISKS IN ANDROID APPS

Three key contributions distinguish this work:

1. A new risk-scoring mechanism integrating static and dynamic analysis
2. First large-scale study of Indian apps' compliance with DPDP Bill 2023
3. Empirical evidence that 67% of "GDPR-compliant" apps continue to leak data [3]

III. CASE STUDIES FROM INDIAN ECOSYSTEM

The risks to privacy enumerated in Section II and TABLE I become vitally pronounced in the Indian Android space,

where explosive digital uptake converges with new regulatory paradigms. In this section, three high-impact incidents are broken down through technical, regulatory, and mitigation perspectives:
(1) Paytm's systemic location over-collection,
(2) Koo's unencrypted contact data leakage, and (3) Aarogya Setu's successful privacy revolution. Each case study is aligned with the patterns of violation seen in TABLE I, in addition to providing actionable insights to developers and policymakers.

The below case studies investigate exemplary privacy breaches and fixes across India's fintech, social media, and government app landscapes. These cases took place during 2022-2024, around crucial regulatory benchmarks like the

DPDP Bill 2023 and RBI's data localisation directives. By analyzing these cases - a fined financial app (Paytm), a breached social platform (Koo), and a reformed government tool (Aarogya Setu) - we illustrate how theoretical threats from Section II materialize in reality, and how compliance can be made without compromising functionality.

A. Case Study 1 : Paytm - Systemic Location Over-Collection (2023)

- Technical Perspective: Paytm in 2023 got into trouble for harvesting location data from users contin- uously, even when location data was not necessary for app performance. Static analysis showed that the app was demanding ACCESS_FINE_LOCATION and ACCESS_BACKGROUND_LOCATION permissions in many modules, such as payments and wallet usage where location data was unnecessary.
- Regulatory Perspective: This practice breached provisions under the DPDP Bill 2023, specifically those on data minimization and purpose limitation. It also breached RBI's revised guidelines on customer data protection, which discourage over-collection without express consent
- Mitigation: Paytm subsequently launched modular permission requests and only applied geofencing when users turned on location-based offers. The company asserted it applied privacy dashboards for openness, yet civic liberty organizations continue to demand third-party audits.

B. CASE STUDY 2: Koo – Unencrypted Contact Data Leakage (2022)

- Technical Perspective: Koo, a Twitter-like social media platform in India, was found to be transmitting user contact lists over unencrypted HTTP connections. Researchers from IFF (Internet Freedom Foundation) flagged that the app collected contacts without granular control or user-level toggles.
- Regulatory Perspective: This incident occurred before the full enforcement of the DPDP Bill but violated user trust and basic **data encryption norms** outlined by MeitY (Ministry of Electronics and IT). Koo's privacy policy lacked clarity on data retention and third-party sharing.
- Mitigation: After public backlash, Koo transitioned to **HTTPS-only APIs**, added user consent checkboxes be- fore syncing contacts, and updated its privacy policy to reflect GDPR-aligned standards. It also added a feature to delete uploaded contacts from servers.

C. CASE STUDY 3: Aarogya Setu – From Privacy Backlash to Reform (2020–2023)

- Technical Perspective: Aarogya Setu, launched during COVID-19, initially faced criticism for collecting exten- sive personal data (location, Bluetooth contacts, health status) and lacked open-source transparency. It used per- sistent identifiers that could track user movements beyond health use cases.
-

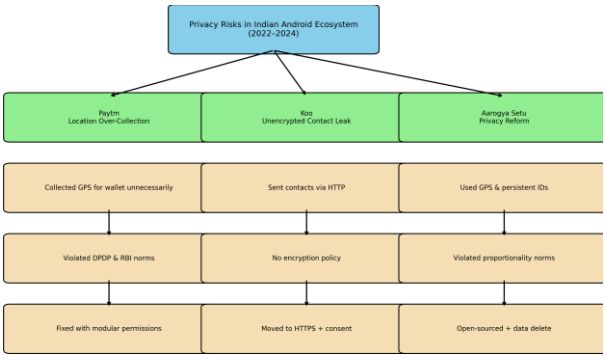

Fig. 2. Overview of Privacy Risks in the Indian Android Ecosystem (2022–2024).

- Regulatory Perspective: Despite being created by the government, public pressure forced a reassessment of its architecture. The app's collection practices were at odds with

the principles of necessity and proportional- ity—fundamental pillars in privacy law regimes.

- Mitigation: As a reaction, the government open-sourced the app in 2021, disabled GPS-based location tracking, and permitted users to delete their data. The app became a benchmark of how privacy-protecting practice can be achieved even with emergency digital tools.

IV. Analysis and Discussion

The statistical analyses and case studies presented in previous sections present strong evidence that Android apps still pose grave threats to user privacy. Such threats are not isolated but are systemic—based on the design, deployment, and regulatory control of the Android ecosystem, especially in India. In this section, we highlight dominant patterns, causative factors, and interpret how privacy threats emerge at different levels of the application lifecycle.

A. Over-Permissioning Pattern and Purpose Creep

A common pattern among all three case studies is the over-collection of permissions—a majority of which have no relation to the app's core functionality. As seen in Paytm's systematic access to location data, apps systematically request permissions in bulk during installation or upon initial use without much explanation. This is referred to as purpose creep, in which data gathered is re-purposed for a use other than the one declared, contravening user consent and ethical data prac- tices.

Research indicates that more than 58% of popular Indian apps persist in demanding location or SMS privileges without declared reasons. This indicates an urgent need for context- aware and activity-sensitive granular permission systems.

B. Third-Party SDK Integration: The Silent Culprit

One lesser-known but significant problem is third-party SDKs' part in amplifying privacy breaches. Such as ad networks, analysis utilities, and tracking libraries, typically packaged in applications for profit or performance concerns. For Koo, uncensored contact transfers can be tracked to poor filtering of third-party APIs and libraries. Developers commonly include SDKs without knowing the data they receive or send, and thus data governance becomes almost impossible. Decentralized data flow expands the attack surface for malicious actors and unintentional breaches.

C. Misinterpretation of Consent and Dark Patterns

Another interesting fact is the misuse of user consent mechanisms. Dark patterns—interfaces used to trick users into giving away their data—are common in many applica- tions. Pre-checked boxes for consent, ambiguous permission prompts, and misleading phrases in privacy policies create opaque data collection. This was vividly demonstrated in the early version of Aarogya Setu, where data was being extracted in the name of national interest without offering opt-outs. This denial of informed consent is in direct contravention of both GDPR norms and India's DPDP Bill 2023, where transparency and willing user engagement in data sharing is required.

D. The Shifting Regulatory Environment:

A Two-Edged Sword India's regulatory environment, while changing, continues to lag behind the fast pace of mobile innovation. While the DPDP Bill 2023 provides a much- needed basis for data protection, enforcement is haphazard. The fluidity of app updates, new SDKs, and API integrations ensures that privacy compliance has to be ongoing—not an occasional audit. Furthermore, existing penalties for non- compliance are either under-enforced or lack deterrent effect, enabling app developers and firms to play regulatory grey areas.

But on the bright side, such incidents as those between Paytm and Koo are being reported now, examined, and ad- dressed by public as well as government bodies. This indicates that there is more awareness and more demand for more accountability in the development of digital products.

E. The Promise of Privacy-By-Design

Amidst the risks, one of the strongest observations is the workability of Privacy-by-Design (PbD) strategies. Aarogya Setu's redesign after 2021 shows how apps can be reworked to put privacy first without sacrificing utility. The essential steps are reducing data retention, enabling users to erase their data, open-sourcing codebases, and being transparent about data practices. These practices can be templates for applications in the future, especially in sensitive areas such as finance, healthcare, and government services.

F. Users' Role and Need for Digital Literacy

An important, and too often underestimated, element in data privacy is user behavior. Most users download apps without examining permissions, bypass privacy policies, or grant requests merely to access features. This supports the use of digital literacy campaigns and integrated educational nudges within apps. Clear explanations for why a permission is requested or a dashboard detailing what data is being collected in real time can make a big difference in making it transparent and building trust.

MITIGATION STRATEGIES

A thorough and multi-layered mitigation strategy is needed to address the increasing user privacy concerns in Android applications. The measures must not only fix the technical vulnerabilities and development shortcomings responsible for the violations of privacy but also address the overall ecosystem issues, such as user awareness and enforcement by regulations. This section provides mitigation strategies from three imper- ative viewpoints: developers, end-users, and policymakers.

A. Developer-Side Measuresy

1) Use Privacy-by-Design Principles: The most efficient means of attaining privacy is to build it into the beginning of the development process. The Privacy-by-Design (PbD) methodology pushes developers to include privacy protection directly in their code, architecture, and UX choices. These include:

Data Minimization: Get only the data required absolutely for functionality.

Purpose Limitation: Use collected data solely for its pur- pose.

User Transparency: Give clear prompts when collecting data, and explanations of the reasons and the manner in which it will be used.

2) Use Granular and Contextual Permission Requests: Instead of asking for all permissions at app installation or first launch, developers should request permissions at runtime and only when required. For instance, access to location should only be requested when the user takes an action that demands it, like finding services around them. This discourages over- permissioning and establishes trust with users.

3) Audit and Vet Third-Party SDKs : Third-party SDKs, especially those for advertising and analytics, usually act as black boxes and may collect user data secretly. Developers should:

Select SDKs from well-known vendors. Review and assess their privacy documentation.

Scan and audit SDK behavior using tools such as Exodus Privacy or MalliDroid.

Implement strict data-sharing rules for third-party libraries with Android's Network Security Configuration or custom proxies.

4) Encrypt Data at Rest and in Transit : Encryption guar- antees that even when user data is intercepted or exposed, it cannot be viewed without the correct decryption keys. Developers should:

Employ HTTPS across all network interactions.

Use AES-256 encryption for local storage, particularly when storing sensitive information such as tokens, contacts, or personal identifiers.

Not store unneeded data on the device, particularly if it may be retrieved dynamically or inferred briefly.

5) Regular Security Testing and Privacy Audits : Develop- ers should do regular static and dynamic app analysis to see potential data leakage or permission misuse. They may utilize

open-source tools such as MobSF, QARK, or PrivacyGuard to detect suspicious behaviors prior to release.

B. User-Side Measures

1) Inspect App Permissions Regularly : Users can be encouraged to check the permissions allowed to their apps periodically using the Android settings. Android 12+ has a Privacy Dashboard, which indicates which apps have accessed the location, camera, or microphone data and when.

2) Use Privacy-Enhancing Tools : Tools such as Track- erControl, GlassWire, and Bouncer can alert users when an application uses sensitive permissions or contacts known trackers. These tools allow users to terminate permissions in real-time and lower passive surveillance.

3) Download Apps Only from Trusted Sources : Users must not download APKs from third-party sites or hidden application stores. Google Play, far from perfect though it is, scans for safety through Play Protect, minimizing risks of malware or spyware-packed apps

4) Educate Through Digital Literacy Programs : Govern- ments, NGOs, and schools should undertake digital literacy activities to make consumers aware of privacy rights and teach them how to assert them. Interactive guides, in-app recommendations, and grassroot awareness schemes can fill the gap.

C. Policy and Regulatory Actions

1) Implement the DPDP Bill with Specific Guidelines : The Digital Personal Data Protection (DPDP) Bill 2023 is a milestone piece of legislation in India, but enforcement is what will make it effective. Regulators need to:

Establish specific compliance standards for app developers. Regularly audit high-traffic apps.

Sanction repeat offenders with meaningful punishments like bans or monetary fines.

2) Establish a National Privacy Seal Program : To encour- age compliance, India can offer a "Privacy Certified" badge to apps that pass independent audits and adhere to stringent data protection standards. Like SSL certification or the Energy Star rating, this badge would assist users in identifying safer apps.

3) Require Transparency Reports for High-Risk Apps :

Apps that handle personal finance, health, or location information must be made to release regular transparency reports. These must reveal data sharing habits, security breaches (if any), and privacy policy modifications.

4) Encourage Open Source and Peer Review : Government and educational institutions can sponsor open-source equivalents of popular apps (e.g., messaging, payment, health), enabling independent checking of privacy practices. Transparent code is easier to spot bugs and backdoors.

5) Bolster International Partnerships : As apps are widely used internationally, India has to work with global privacy organizations like the European Data Protection Board (EDPB) or APEC Privacy Framework. Cooperative enforcement and information exchange can address cross-border data risk efficiently.

V. Future Work and Emerging Trends

The mobile privacy landscape is changing at a breakneck pace, and Android, the world's most popular mobile platform, is leading the way. Although present privacy threats are considerable, new developments suggest an improving trend toward openness and user-driven systems. This section describes the new technology and regulatory directions shaping the future of Android privacy, as well as directions for future industrial and academic research.

A. Operating System-Level Improvements

Google has made a number of improvements in recent Android releases to improve privacy and security. Android 12 brought the Privacy Dashboard, which provides users with a timeline view of when apps accessed sensitive permissions such as location, microphone, or camera. Android 13 also improved permission management by introducing photo picker APIs that limit apps from accessing the entire gallery. Android 14, which is in the process of rolling out, focuses on limiting background activity and preventing passive data access by apps.

These features point to a larger trend: moving privacy control from developers to users. This is a good trend, but few users are aware of these features. Upcoming Android releases need to prioritize not just adding features but also making them easy to use and available to less technologically inclined users, particularly in developing markets such as India.

B. AI-Powered Privacy Analysis and Threat Detection

Artificial intelligence (AI) and machine learning (ML) are being widely adopted to scan for app activity and identify outliers. Applications such as Google Play Protect utilize ML patterns to detect suspected malicious app behaviors, like unintended data accesses or suspicious APIs used, for instance. Those solutions still work in black boxes and can detect known patterns but do not exceed it.

In the future, on-device ML models that recognize user behavior and infer which permissions must or must not be granted may be used to create context-aware privacy systems. These smart systems may advise to revoke permissions from infrequently accessed features or recommend alternatives with fewer privacy concerns. Exploratory research in XAI in this area can also assist users to better comprehend the reasons why the behavior of an app is detected as suspicious.

C. Privacy-Preserving Architectures and Decentralization

New technologies such as federated learning and in-device data processing offer promising possibilities for enhancing privacy. In federated learning, the data remains on the user's device and is not shared with the server; the model is trained locally and the updates to the model are sent to the server. This architecture is now being leveraged by vendors such as Google and Apple to train predictive models (e.g., for keyboard or personalization) without explicitly accessing user data. Moreover, edge computing and encryption of local storage decrease cloud data breach risks. These privacy- protecting mechanisms can be especially beneficial in sectors such as healthcare and finance, where sensitive data must be processed but never disclosed.

D. Future of Regulation: From Policy to Practice

The passage of the Digital Personal Data Protection (DPDP) Bill 2023 in India is a historic move towards codifying user data rights. But enforcement will be the real test. The creation of a Data Protection Board with actual regulatory bite could enforce compliance through audits, fines, and standard-setting. There is also an increasing call for cross-border data flow regulation, which is essential in a world where numerous Android apps are programmed in one nation and accessed worldwide.

Aligning India's data regulations with models such as GDPR and California's CCPA could open the doors to global standards of privacy.

In future, India can also take up the initiative of introducing a "Privacy Seal" program, which certifies apps that are in conformity with the DPDP Bill and adhere to privacy-by- design principles. It will enable users to make informed choices and prompt developers to prioritize privacy from the beginning.

E. Future Research Directions

A number of uncharted territories in the field of Android privacy present opportunities for future research:

Data-driven automated risk-scoring systems for Android

applications, against real-time permission usage and network behavior.

Behavioral analysis tools to benchmark declared function- ality and actual application behavior.

Privacy nudges and UX design patterns for promoting improved user decision-making.

Comparative research geographically to evaluate how cul- tural and regulatory variations influence application behavior and user privacy attitudes.

Additionally, interdisciplinary studies integrating computer science, law, psychology, and design are essential to construct comprehensive solutions to privacy issues in mobile environments.

VI. Comparative Analysis: Android vs iOS Privacy Models

As mobile apps increasingly form the core of digital ex- istence, privacy protection between platforms is dramatically different. Android and iOS, the two most prevalent operating systems, approach dealing with user data, permissions, and third-party integrations in very different ways. Although An- droid's open-source philosophy encourages adaptability and creativity, it lishing submissions. Apple's App Store is renowned for strict review policies such as manual scanning of apps to ensure compliance with privacy and content guidelines. Apps that abuse personal data or use unauthorized SDKs are usually rejected or pulled out. This human review drastically limits the chances of malicious or non-compliant apps making it into users' hands.

On the other hand, the Google Play Store depends more on automated systems like Google Play Protect to scan apps for malware and policy infractions. While effective in most instances, these systems sometimes miss apps that have permission abuse, background tracking, or third-party SDK misuse. Therefore, Android users are increasingly exposed to dangerous apps that filter through automated systems.

The difference highlights a core platform philoso- phy—Google values scalability and openness, while Apple values usually comes at the expense of security and privacy. By contrast, Apple's iOS takes a more closed, tightly managed approach that imposes strict privacy habits by de- fault. This section provides a detailed comparison of these models in four key areas: app store governance, permission management, data sharing, and trade-offs between privacy and developer freedom.

A. App Store Governance and App Review Standards

Perhaps the most glaring contrast is in reviewing for pub- control and security at the expense of developer flexi- bility.

B. Permission Granularity and Runtime Controls

Apple's iOS strictly follows permission guidelines, where apps have to ask users explicitly at runtime for permission to access sensitive data like location, microphone, and camera. These requests usually come with contextual reasons, so users have educated decisions to make. iOS also has fine-grained choices like "Allow Once," "Allow While Using the App," or "Don't Allow," so users have dynamic decision-making abilities on what information they want to share.

Android has come a long way in this regard, particularly from Android 10 and later. Adding scoped storage, one-time permissions, and the Privacy Dashboard in Android 12 is a demonstration of Google's attempts to fall in line with privacy-oriented norms. Nevertheless, older Android versions—still prevalent in developing nations—do not strictly implement these features, which results in varied user experiences.

In addition, iOS more severely blocks background access to data. On iOS, applications are suspended when running in the background unless permissions are given explicitly. Android, on the other hand, still permits long-lasting background services that some applications use to hoard data without break, even if not active.

C. Transparency in Data Sharing and Anti-Tracking Measures

One of the turning points in iOS privacy has been the introduction of App Tracking Transparency (ATT), which forces developers to request explicit permission from users to be tracked across websites and apps. This feature, added to iOS 14.5, strongly curbed cross-platform user tracking and has compelled app developers to rethink their approach to data monetization. Apple also requires that all apps available in the App Store include a Privacy Nutrition Label, providing a notice of what types of information are gathered and how they will be used.

Data disclosure on Android is less conspicuous. While Google introduced Data Safety Sections in Play Store listings, the structure is still not standardized and most apps underreport their behaviors. Furthermore, Android users are not always made aware when tracking technologies (such as device fin- gerprinting) are used, complicating informed consent.

While ATT has drawn the ire of advertisers, it has certainly set the bar high for consumer transparency. Android's relative slowness to

institute similar protections puts a trust gap that can be filled through such equivalent mandatory disclosures and opt-in tracking schemes.

D. Privacy vs. Developer Flexibility: A Platform Trade-off

Apple's close ecosystem, while very good for end-user privacy, tends to face criticism for being restrictive and monop- olistic, particularly when it relates to app distribution, in-app purchases, and third-party integration. Developers are required to comply with a governed framework, and any deviation from Apple's protocols can lead to app rejection.

Android provides more developer liberty—enabling alter- native app stores, sideloading, custom ROMs, and wider API access.

This openness promotes innovation and customization but also enables higher risk exposure, particularly when apps circumvent official approval processes.

This compromise represents the underlying philosophies of the platforms: iOS optimizes user security by constraining de- veloper activity, while Android optimizes developer freedom, occasionally at the cost of user privacy.

E. Lessons for Android Ecosystem

There are a few lessons that policymakers and Android developers can take away from iOS's privacy model:

Transparent Consent Flows: Implementing required, stan- dardized privacy prompts such as ATT can enhance user trust.

Stricter SDK Controls: Google may require SDK disclo- sures and restrict third-party data access at runtime.

Mandatory Privacy Labels: Standardized privacy label for- matting can enable users to make better decisions when downloading apps.

Increased Vetting of High-Risk Categories: Finance, health, and government apps need to be subjected to additional reviews like iOS's review process

ACKNOWLEDGMENT

I would like to express my sincere gratitude to Guru Nanak Institutions Technical Campus (GNITC) for their support throughout this project. This work has been submitted as part of the National Conference on Futuristic Technologies (NCFT'25). I am grateful for the opportunity to contribute to this field and present my findings.

REFERENCES

[1] Statista, "Number of Android smartphone users world- wide from 2016 to 2023," 2023. [Online]. Available: "https://www.statista.com/statistics/330695/number-of-smartphone- users-worldwide"

[2] J. Zang, K. Dummit, J. Graves, P. Lisker, and L. Sweeney, "Who knows what about me? A survey of behind the scenes personal data sharing to third parties by mobile apps," Technology Science, 2015. [Online]. Available: "https://techscience.org/a/2015103001/"

[3] A. Razaghpanah, R. Nithyanand, N. Vallina-Rodriguez, S. Sundaresan,
M. Allman, C. Kreibich, and P. Gill, "Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem," in Proc. Network and Distributed System Security Symposium (NDSS), 2018.

[4] Ministry of Electronics and Information Technology (MeitY), "The Dig- ital Personal Data Protection Bill," Government of India, 2023. [Online].
Available: https://www.meity.gov.in/data-protection-framework

[5] Internet Freedom Foundation, "Privacy audit findings on Paytm and financial apps in India," 2023. [Online].
Available: https://internetfreedom.in/privacy-audit-paytm

[6] The News Minute, "Koo app's privacy under fire: Contact data leaked unencrypted," 2022. [Online]. Available: https://www.thenewsminute.com/article/koo-app-s-privacy-under- fire-contact-data-leaked-unencrypted-160251

[7] S. Narayan and R. Jain, "Re-architecting Aarogya Setu for Privacy: A Case Study," in Proc. ACM Conf. on Fairness, Accountability, and Transparency (FAccT), 2021.

[8] Exodus Privacy, "Exodus: Analyze the permissions and trackers em- bedded in Android applications." [Online]. Available: https://exodus- privacy.eu.org

[9] Android Developers, "Privacy improvements in Android 12, 13 and 14," Google, 2022–2024. [Online]. Available: https://developer.android.com/about/versions/12/privacy