IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, May 2025
Impact Factor: 7.67

Privacy Under Siege: Data Leakage and Tracking in Mobile Applications

Ms. Priyanka Kanire and Ms. Sadhana Vishwakarma
Research Students
Dr. Ambedkar Institute of Management Studies and Research, Nagpur, India
jayantgondane27@gmail.com

Abstract: *Today mobile has become integral part of human life. The increasing usage of mobile applications has provided the great convenience and personalization in fact it has transform the relation of human with technology. However, this revolution in mobile applications and related technology introduced new complications such as breaches of data privacy, user trekking. Mobile apps often gather, send, and keep sensitive information for users without adequate transparency or consent. This research examines the phenomenon of data leakage and tracking in mobile applications by analyzing the technologies that enable them, stakeholder motivations, and the adequacies of legal and technological remedial mechanisms. Based on case studies and thorough literature review, this work attempts to fill the gap in the existing privacy frameworks by suggesting an integrated approach of balance between policy and enforcement, technology, and user self-education. This research focuses on the mobile ecosystem to privacy-centric systems that allow users to have control over their data, following the principles of minimalism, reduction, ethical practices of software.*

Keywords: Mobile privacy, data leakage, user tracking, mobile applications, third-party SDKs, privacy regulation, data security

I. INTRODUCTION

The ubiquity of mobile applications today has facilitated communication, banking and performing health-related functions. With billions of mobile applications available on platforms like Google Play and Apple App Store, users are more engaged with mobile technology than ever before. However, constant digital presence poses significant privacy issues such as data leakage and user tracking, resulting in the loss of privacy. This paper analyses mobile applications in depth with respect to privacy issues and attempts to document the flow of data within mobile ecosystems, the components therein, and the fallout from lax data controls.

II. BACKGROUND AND MOTIVATION

According to Cohen (2019), data leakage is the unauthorized data transmission from a user's device, while tracking consists of monitoring user behavior across applications and services. Both activities are frequently executed covertly, and they can be used for ad campaigning, behavioural profiling, or other nefarious purposes. The incorporation of mobile applications into sensitive fields such as medicine, finance, and education enhanced the risk enormously. The contribution of this document is to analyze the technological, moral, and legal ramifications of these activities and advocate for the construction of a mobile infrastructure that prioritizes user privacy.

III. LITERATURE REVIEW

Recent studies capture the breadth of the data harvested by mobile applications and the advanced methods employed to monitor users. Zang et al. (2015) conducted a thorough review of mobile apps, noting the rampant invisibility of data sharing practices among well-known app vendors. Likewise, Reardon et al. (2019) revealed the ways in which applications leak sensitive user information through covert channels that bypass Android's permission granting system.

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, May 2025
Impact Factor: 7.67

Papageorgiou et al. (2018) reported on the use of advertising third party SDKs, which are pervasive in user-facing applications and possess the ability to collect a plethora of information about the users. Such SDKs often transmit data without permission to advertising networks that have an established infrastructure for meticulously profiling users. Li et al. (2019) cited empirical studies arguing that a significant number of applications do not adequately protect user privacy and instead expose them to considerable risks, even when limited access is granted to application controls.

In addition, Exodus Privacy and AppCensus have shown to be useful in the analysis of application behaviour evaluation. For instance, AppCensus showed that over 70% of the applications that were sampled in their study sent private data to be monitored (AppCensus, 2023). All of these works strengthen the claim that the phenomenon of mobile data leakage is not only rampant, but is also backed with a system of concealment that is readily available to users.

Compliance measures like the GDPR and CCPA have tried to establish legal limits concerning the harvesting of data. The compliance with such regulations is, however, not uniform as laws fail in keeping pace with evolving technologies (European Commission, 2018; CCPA, 2018).

IV. MECHANISMS OF DATA LEAKAGE AND TRACKING

4.1 Permissions and APIs

Apps typically ask for access to sensitive information through permissions such as: location, contacts, and camera data. Subsequent to being given the permissions, apps can then use the platform APIs to fetch and send the relevant data. Many permission request patterns not essential to the app's functionality have been shown in previous research which suggests some underlying motive relating to data collection (Li et al. 2019).

4.2 Third-Party SDKs

Third-party Software Development Kits (SDKs) incorporated into applications can create new avenues for data harvesting without the consent or knowledge of the consumer, and sometimes, the developer. These SDKs are developed for advertisement, analysis, and even social media, allowing auction of the application without the developer's consent. SDKs allocated for such purposes may forward the obtained user information to different countries, exaggerating the ease of legal control (Papageorgiou et al. 2019).

4.3 Network Traffic Analysis

Reckless configuration of network protocols combined with data that has not been secured can give rise to unintended data breaches. For example, analyzing packets and the data that is transmitted between certain locations can uncover sensitive details like; login details, the history of an individual's location, and their preferences. Research has shown that a hefty amount of mobile applications fail to use HTTPS or try to use it partially which results in man-in-the-middle attacks (Reardon et al. 2019).

4.4 Quad Four: Device Fingerprinting

Collecting a set of distinct device identifiers, including both hardware and software components, to recognize a device is referred to as device fingerprinting. Fingerprinting is far harder to manage and safeguard against than tracking devices using cookies. As a result, it is a more powerful method of tracking devices over an extended period of time.

V. STAKEHOLDERS AND THEIR MOTIVATIONS

5.1 Developers

Despite the fact that some developers focus on user experience and functionality, others monetize their applications by employing sophisticated advertising and analytics systems that capture users' personal information. Freemium and ad-supported apps generally operate with aggressive data harvesting business models.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, May 2025
Impact Factor: 7.67

5.2 Advertisers

User profiling is critical to targeted advertising. Data granularity is paramount for personalized advertising to increase user engagement and interaction with the advertisements. There is a growing demand for data which sustains a complex network of data brokers and ad exchanges (Papageorgiou et al., 2018).

5.3 Users

Most users do not possess the requisite knowledge or the understanding of privacy issues and therefore, unknowingly provide permissions that endanger their sensitive information. Users' informed consent is often hindered by the complexity and hidden nature of privacy policies.

5.4 Regulators

The GDPR and CCPA are examples of legislative measures initiated by the European Union and the state of California, respectively which seek to safeguard privacy. However, enforcement and compliance poses difficulties within the context of a universal digital marketplace. The diversity of national laws creates double burdens for the profiteering data subjects to exploit (European Commission, 2018; CCPA, 2018).

VI. CASE STUDIES AND EMPIRICAL ANALYSIS

6.1 Facebook and Cambridge Analytica

The incident of Cambridge Analytica secretly collecting data from millions of Facebook users is an example of how the information obtained from mobile applications can be used to influence elections. This scandal jumpstarted the public and political discourse regarding privacy in the digital age.

6.2 TikTok and National Security Concerns

the controversy regarding the management of user data and privacy has brought scrutiny and bans from governments across multiple countries. These actions also reveal more of the global concern over data privacy. Charges have been made regarding the misuse of data and action is being taken towards dealing with the required policies for data governance.

6.3 Empirical Study on Data Leakage

Some recent studies have shown that many mobile applications are more than willing to collect and transmit sensitive materials without the awareness of the user, highlighting the current state of violated personal privacy. For example, AppCensus discovered that more than 70% of the applications they tested used third-party trackers to relay information about the users (AppCensus, 2023).

VII. PRIVACY-PRESERVING MEASURES

7.1 Technical Solutions

- **Differential Privacy:** Adds statistical noise to datasets, preserving individual privacy while allowing aggregate data analysis.
- **End-to-end Encryption:** Ensures data is encrypted throughout transmission, minimizing interception risk.
- **App Sandboxing:** Isolates apps from one another to prevent unauthorized data access.
- **Permission Granularity:** Allows users to grant permissions selectively and revoke them dynamically.

7.2 Regulatory Measures

- **Stricter Enforcement of GDPR and CCPA:** Regular audits and substantial penalties for non-compliance.
- **Mandatory Transparency in Data Collection Practices:** Clear and accessible privacy notices with real-time consent mechanisms.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, May 2025
Impact Factor: 7.67

- **Global Data Protection Standards:** International treaties and coordination to bridge regulatory gaps across jurisdictions.

7.3 User Empowerment

- **Educating Users on Privacy Settings:** Public awareness campaigns and in-app tutorials.
- **Promoting Privacy-Centric Apps:** Incentives for developers to build apps with privacy by design.
- **Enhancing App Store Scrutiny and Labeling:** Privacy scores and labels to inform users about data practices before installation.

VIII. FUTURE DIRECTIONS

Continuing work in the future will need to look at the application of privacy integrating technologies into development processes as unparalleled challenges regarding privacy emerge. The application of AI in the protection of data, emerging self sovereign identity frameworks, and the autonomy of blockchain networks in guaranteeing open access to information support data managing systems creates novel opportunities. Moreover, new forms of cooperation between public authorities, privat e actors, and civil society actively needed to strengthen absent innovations while ensuring user privacy.

IX. CONCLUSION

The need to maintain user privacy is an increasingly complex concern due to the extraordinary proliferation of mobile applications. The erosion of user trust is aggravated by numerous privacy threats, from tracking user movements to identity theft and other malicious uses. While the existing literature is silent on the enabling factors regarding privacy violations, this paper has described the primary privacy violators, particularly their self-interests, degree of examined negligence, and available countermeasures.

While some regulations and technical measures attempt to address the problem, they fundamentally lack comprehensive global frameworks and collaboration from all relevant parties. A combination of advanced privacy-preserving technologies, strong legal policies, and an educated user population will reshape the mobile application marketplace into one that fundamentally views user data as sensitive and requires adequate protective measures. Only through this type of collaboration will it be possible to restore user trust and maintain digital dignity in a highly interconnected world.

REFERENCES

[1]. Almuhimedi, H., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., Cranor, L., & Agarwal, Y. (2015). Your location has been shared 5,398 times! A field study on mobile app privacy nudging. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 787–796.

[2]. AppCensus. (2023). Retrieved from https://www.appcensus.io

[3]. Binns, R., Veale, M., Van Kleek, M., & Shadbolt, N. (2018). 'I'm being profiled, and I don't even know it': Automated decision-making in mobile advertising. *Technology in Society, 54*, 1–13.

[4]. California Consumer Privacy Act (CCPA), Cal. Civ. Code §§ 1798.100 et seq. (2018).

[5]. European Commission. (2018). General Data Protection Regulation (GDPR). Retrieved from https://gdpr.eu/

[6]. Exodus Privacy. (n.d.). Retrieved from https://exodus-privacy.eu.org

[7]. Li, L., Li, D., Liu, Z., Zhu, H., Zhang, T., & Jin, H. (2019). An Empirical Study of the Privacy Risks of Android Apps. *ACM Transactions on Privacy and Security, 22*(1), 1–30.

[8]. Papageorgiou, O., Beresford, A. R., & Stringhini, G. (2018). Tracking and advertising in mobile apps: Threats and mitigation. In *Proceedings of the 11th ACM Conference on Security and Privacy in Wireless and Mobile Networks*.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, May 2025
Impact Factor: 7.67

[9]. Reardon, J., Feal, A., Wijesekera, P., Egelman, S., & Vallina-Rodriguez, N. (2019). 50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System. In *28th USENIX Security Symposium*.

[10]. Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society, 12*(2), 197–208.

[11]. Wang, Y., & Liu, L. (2020). Privacy risks in mobile applications: A review and future directions. *Computers & Security, 92*, 101740.

[12]. Zang, J., Dummit, K., Graves, J., Lisker, P., & Sweeney, L. (2015). Who knows what about me? A survey of behind the scenes personal data sharing to third parties by mobile apps. *Technology Science*.