UDC 004.056.53: 621.395.62

CYBERSECURITY ON YOUR SMARTPHONE: WHAT YOUR APPS ARE HIDING

Sevrukov K.I.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Likhtarovitch I. I. – Senior Lecturer at the Department of Foreign Languages

Annotation. This paper examines the cybersecurity implications of hidden data collection practices in mobile applications. By analyzing the economic incentives behind data monetization, technical permission-exploitation mechanisms, and resulting cybersecurity risks, the study argues that covert data collection constitutes a systemic vulnerability within the mobile ecosystem. Practical mitigation strategies for end users are also identified.

Keywords: mobile security, data privacy, application permissions, data monetization, digital hygiene, cyber risk.

***Introduction*.** Smartphones have become an integral part of daily life for billions of people worldwide. They provide access to contacts, bank accounts, social networks, and messengers. The convenience that makes a smartphone indispensable simultaneously makes it particularly vulnerable. The threat comes not only from malicious software, but also from applications that appear completely safe, whose data collection practices extend far beyond what is disclosed in their terms of service – agreements that are rarely read in practice.

The processing, transfer, and distribution of users' personal data to third parties leads to specific cyber threats, including theft of personal data, social engineering, and financial fraud. The purpose of this paper is to analyze the mechanisms by which mobile applications collect and transmit confidential user information without their knowledge, as well as the cybersecurity risks arising from these hidden practices.

Main part. Applications distributed as "free", such as social networks, VPN services, flashlight utilities and calculators, – are not free in the economic sense. Users pay with their personal data, which is collected by these applications. In some cases, this is necessary for correct operation, for example, precise geolocation for a navigation app. In other cases, it serves to understand development direction or to offer personalized advertising. However, applications frequently "leak" users' personal data to advertising networks and data brokers through third-party SDKs (Software Development Kits) – ready-made software libraries that include programs for data analytics, push notifications, or advertising content. Developers themselves often do not have a complete understanding of what data these libraries collect.

The result is a system of persistent digital profiling. Data from millions of users – their geolocations, interactions, and digital device traces – are correlated across services to form detailed behavioral profiles. This not only enables highly accurate personalized advertising, but also creates a vast repository of sensitive information that can compromise users in ways far beyond targeted marketing.

The iOS and Android operating systems implement a permission system based on the principle of least privilege: applications should request access only to data minimally necessary for correct functioning. In practice, this mechanism is bypassed through redundant permission requests. An illustrative example is the flashlight app – a utility whose sole purpose is to activate the camera flash, yet in numerous documented cases it has requested precise geolocation and device identification [1]. This serves no practical functionality for the app; it is done solely to collect data for the benefit of built-in advertising SDKs.

Beyond abusing permissions, applications employ additional data collection mechanisms. Metadata collection, including screen time, network status and device configuration, is gathered without the user's awareness or permission, as platforms classify such data as non-personal, despite

its significant value for profiling [2]. Background data transfer allows an application to continue exchanging information with remote servers even after the user has closed it, making ongoing data exfiltration difficult to detect or prevent.

The implications of covert data collection extend far beyond the informational domain. Detailed geolocation histories collected by advertising SDKs can accurately reveal a user's home address, workplace, medical clinic, and social circle – information that can be exploited for harassment, phishing attacks, and corporate espionage. Individually harmless data points, when combined across multiple applications sharing a common SDK, can produce a comprehensive profile sufficient to track a specific individual [3].

Public data networks present an additional threat vector. While TLS (Transport Layer Security) encryption is the standard for modern mobile traffic, its implementation frequently contains vulnerabilities: invalid certificate handling and outdated cryptographic protocols are not uncommon in production applications. Software obsolescence compounds this problem: a significant portion of applications run on versions released months or years prior, retaining unpatched security vulnerabilities that remain exploitable long after fixes have been published.

Users have access to a substantial set of protective measures. Permission management – reviewing granted permissions and disabling those not directly relevant to an application's core function – represents the most fundamental countermeasure. Applications requesting geolocation access should be configured to "during use only" mode. Microphone and contact access should be trusted only to applications whose purpose makes such access unambiguous. Regular updates to both applications and the operating system minimize exposure to known vulnerabilities.

Critical evaluation of "free" services is equally important: users who understand that advertising-model applications monetize their data are better equipped to assess the true cost of a given application before installing it [4]. The use of reputable VPN services may reduce the risk of traffic interception in environments where application-level encryption may be insufficient. Together, these practices constitute a coherent personal security posture that significantly reduces the attack surface presented by smartphone usage.

***Conclusion*.** The hidden data collection conducted by mobile applications is not an incidental phenomenon, but a structural consequence of the economic model underlying consumer software. The integration of advertising SDKs, abuse of the permission system, and background data transmission combine to create a pervasive surveillance infrastructure within applications that ordinary users perceive as simple utilities. The resulting cybersecurity threats – identity theft, behavioral profiling, network traffic interception, and vulnerability exploitation – are well-documented and growing in scale [5].

Countering these threats requires not only systemic regulatory measures, but also conscious behavior on the part of individual users. Permission management, consistent software updates and critical evaluation of free services represent a practical and accessible response to the problem. As smartphones have become the dominant computing device in everyday life, cybersecurity literacy is no longer optional – informed digital behavior is itself a necessary element of personal security in the modern information environment.

References

1. Android Permissions: User Attention, Comprehension, and Behavior [Electronic resource] / A. P. Felt [et al.] // Proceedings of SOUPS. – New York : ACM, 2012. – Mode of access : https://cups.cs.cmu.edu/soups/2012/proceedings/a3_Felt.pdf – Date of access : 03.03.2026.

2. Bug Fixes, Improvements, ... and Privacy Leaks [Electronic resource] / J. Ren [et al.] // Proceedings of NDSS 2018. – San Diego : Internet Society, 2018. – Mode of access : https://dspace.networks.imdea.org/handle/20.500.12761/506 – Date of access : 03.03.2026.

3. Exposing the Invisible Web: Third-Party HTTP Requests on 1 Million Websites [Electronic resource] / T. Libert // International Journal of Communication. – 2015. – Vol. 9. – P. 3544–3561. – Mode of access : https://ijoc.org/index.php/ijoc/article/view/3646/1503 – Date of access : 03.03.2026.

4. The Age of Surveillance Capitalism [Electronic resource] / S. Zuboff. – New York : PublicAffairs, 2019. – Mode of access : https://www.hbs.edu/faculty/Pages/item.aspx?num=56791 – Date of access : 03.03.2026.

5. Number of Smartphone Users Worldwide from 2016 to 2029 [Electronic resource] / Statista Research Department. – Hamburg : Statista, 2024. – Mode of access : https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/ – Date of access : 03.03.2026.