A Comparative Study of Android and iOS Mobile Applications' Data Handling Practices versus Compliance to Privacy Policy

DOI:
10.1007/978-3-319-92925-5

Document Version
Submitted manuscript

A Comparative Study of Android and iOS Mobile Applications' Data Handling Practices versus Compliance to Privacy Policy

Sophia Kununka[1] (✉), Nikolay Mehandjiev [1] and Pedro Sampaio [1]

[1]Alliance Manchester Business School, The University of Manchester, UK

sophia.Kununka@postgrad.mbs.ac.uk,

{n.mehandjiev,p.sampaio}@manchester.ac.uk

Abstract. The exponential growth of the mobile application (app) industry has significant implications to user privacy. This can be attributed to the prevalent context of multiple apps use in which several privacy policies come into effect. More so, even in instances in which app policies are provided there is a possibility that app's data handling practice do not fully comply with the apps privacy commitments as stated in its privacy policy. We conducted an assessment of the extent to which apps' data practices matched their privacy policies. This study entails an in-depth comparison of Android and iOS apps' privacy compliance. Our findings show potential sensitive user data flows from apps against the apps' stated privacy commitments and further, that neither Android nor iOS app data handling practices fully comply with their privacy policies.

Keywords. Mobile applications · Privacy policy ·Compliance

1 Introduction

Digital platforms such as websites (web) [1], mobile applications (apps) [2] and, Internet of Things (IoT) [3] handle unprecedented quantities of user data. Users (end users) offer or entrust diverse personal data to organizations and traders including; geo-location information, credit card transactions, social security numbers, date of birth, list of friends, photos, Internet Protocol (IP) address etc. The data is provided with the confidence that users' data privacy (information privacy) will be maintained by limiting data utility to the specified purposes. Notwithstanding, gaps have been observed in privacy practices as user consent is not always sought before organizations engage user data for the organizations' benefits [4].

While a range of approaches have been used in an endeavour to address non-consented use of users' privacy data, a key focus has been on the provision of privacy policies. The major purpose of privacy policies is to dispel users' anxieties about the revelation of personal data or personally identifiable information (PII) [5]. A privacy policy is 'a set of rules, or statements that specify which processing and sharing practices are permitted for different types of data' collectable from the end user [6]. Privacy policies endeavour to guarantee data gathering and dissemination. Provision of app

policies builds user trust and enables app to achieve regulatory compliance. However, while provision of privacy policies are an important step in reinforcing user data privacy, the extent to which this endeavour is successful is largely dependent on the app's adherence or compliance to its own privacy policy.

As such, this study conducts an investigation into whether the user data collected and disseminated by apps to third party domains is reflected in their privacy policies. The analysis was conducted based a privacy compliance comparison between Android and iOS apps as they two form the dominant app platforms. A recent study that examined the personal, behavioral and location data from 110 apps indicates that Android and iOS apps generally transmit sensitive data to 3.1 and 2.6 third party domains respectively [7]. Our work follows up on a recommendation in the aforementioned study about the necessity to assess if privacy policies comply with the apps' information gathering and dissemination practices. As such, this study seeks to explore the extent to which apps adhere to their stated privacy policies and, the resulting effects of apps' data handling practices.

2 Research Method

Based on findings presented by [7], we extract two sets of data from their dataset. Firstly, we select apps that convey sensitive data to two or more third party domains based on the rationale that the greater the number of third party domains an app is linked to the higher the potential of user data dispersion. This yielded a total of thirty Android and iOS apps. Secondly, we sought to establish the data handling practices for each of the thirty apps by analyzing the types of data they convey to third parties in practice based on the finding of [7]. Having determined the apps' practical data handling practice, we compared the data apps relayed to third party domains against a checklist of 14 user data attributes which are; address, birthday, email, gender, name, password, phone number, zip code, employment, friends, medical info, search, username and location.

In the next phase of the study, using Nvivo, a qualitative analysis of the privacy policies from the aforementioned 30 apps was conducted. The qualitative analysis was used to establish apps' data handling practices as stated in their privacy policies, such as data collection, use and dissemination to third parties.

Thereafter, the apps' data handling practices as stated in their policies was assessed against their actual practical data handling practices in order to ascertain the extent to which app comply to their own policies.

3 Findings and Discussion

Our results indicated that Android apps handle 64% of the types of data attributes examined while iOS handles 50%. Moreover, out of the user data attributes gathered and disseminated by Android, 68% were found to comply with the respective apps' privacy policies while 32% did not match the app privacy policies. Similarly, of the

user data attributes handled by iOS, 60% were found to reflect the apps' privacy policy commitments while 26% did not comply with their policies. Interestingly, further 14% of the iOS attributes were found to be gathered and disseminated with no privacy policy available.

Moreover, confirming findings by [7] that found that iOS apps had a lower potential of spreading personally identifiable information, when we compared the Android and iOS data handling practices against their privacy policies, we found that Android had an 18% potential of sharing PII outside the limits of its policy while iOS' potential was 17 %. However, the probability of iOS sharing PII in a manner non-compliant to it policy further increases to 23% when apps that did not have privacy policies yet transmitted data are considered.

The most non-policy compliant data handled by both platforms were the username and address data attributes which are both PII. These trends indicate the immense interest that apps have in PII data and hence the necessity of ensuring that users are granted adequate controls and protection so as to enhance their privacy. These sensitive data flows could have privacy implications for users.

Inferring from our findings, we argue that one of the criticisms of current practice is that an app may request a user to grant access to personal data on the premise that its need for the app's functionality. However, often there is no facilitate through which the user can confirm that the data requested for by the app is in line with the stated privacy policy. A further complication to user comprehension of potential privacy implications occurs in contexts that involve multiple privacy policies' interactions. Multiple privacy policies come into effect in scenarios that involve for instance data exchange or dependencies in multiple app contexts which are difficult for the user to understand and are potential sources of privacy breaches.

4 Contributions

Drawing from our findings, we recommend the necessity of enhancing app platforms such that data collection is not merely checked against the app's request to use data, but that this process is enhanced by cross checking apps' data handling practices against the apps' privacy commitments to app users as stipulated within their privacy policies. This would automate enforcement of privacy policy and also eliminate the transfer of data from apps that do not have privacy policies. In hindsight, a technological solution could prove the most feasible solution to this challenge through the development of a real-time graphical visual aid that depicts apps' compliance to their policies and, as well as provide automated opt-out options for users in cases of non-compliance. In addition to building user confidence in apps' commitment to preserve user data privacy, it would also be of value to privacy compliance bodies by automating compliance to stated privacy policies.

References

1. Selvadurai, N.: Protecting online information privacy in a converged digital environment – the merits of the new Australian privacy principles. Information & Communications Technology Law 22(3), 299-314 (2013)
2. Enck, W., Gilbert, P., Chun, B., Cox, L., Jung, J., McDaniel, P., Sheth, A.: Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones. ACM Transactions on Computer Systems, 1 (2014)
3. Hvistendahl, M.: Information technology. China pushes the 'Internet of Things'. Science (New York, N.Y.), 1223 (2012)
4. Anderson, B.: The Difference Between Data Privacy and Data Security. In: The Situation Room. (Accessed September 9, 2013) Available at: http://blog.eiqnetworks.com/blog/bid/313892/The-Difference-Between-Data-Privacy-and-Data-Security.
5. Westin, A.: Privacy and Freedom. Atheneum Publishers, New York (1967)
6. Papanikolaou, N., Creese, S., Goldsmith, M.: Refinement checking for privacy policies. Science of Computer Programming, 1198-1209 (2012)
7. Zang, J., Dummit, K., Graves, J., Lisker, P., Sweeney, L.: Who Knows What About Me? A Survey of Behind the Scenes Personal Data Sharing to Third Parties by Mobile Apps. Technology Science (2015)
8. Egele, M., Kruegel, C., Kirda, E., Vigna, G.: PiOS: Detecting Privacy Leaks in iOS Applications., p.NDSS (2011)