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

Sophia Kununka, Nikolay Mehandjiev, Pedro Sampaio

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 prevalent use of mobile applications (apps) involves the dissemination of personally identifiable user data by apps in ways that could have adverse privacy implications for the apps' users. More so, even when privacy policies are provided as a safeguard to user privacy, apps' data handling practices may not comply with the apps' privacy commitments as stated in their privacy policies. We conducted an assessment of the extent to which apps' data practices matched their privacy policies. This study provides an exploratory comparison of Android and iOS apps' privacy compliance. Our findings show potential sensitive user data flows from apps in ways that do not match the apps' privacy policies and further, that neither Android nor iOS app data handling practices fully comply with their privacy policies.

Keywords. Mobile applications · Privacy policy ·Compliance

[a] Corresponding author. Tel.: +44(0)744 8223904.
E-mail addresses: Sophia.Kununka@postgrad.mbs.ac.uk (S.Kununka), P.Sampaio@manchester.ac.uk (P. Sampaio), N.Mehandjiev@manchester.ac.uk (N. Mehandjiev).

1 Introduction

Mobile applications (apps) handle unprecedented quantities of user data. App users offer or entrust diverse personal data to organizations and traders. The data provided by users may be sensitive such as personally identifiable information (personal data) which is data that can be linked back to the owner or source for example; user name, email, telephone number, gender, age, social security number, card number etc. [1]. In contrast, non-personal data is deemed unidentifiable data and can be aggregated for various purposes. User 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 research shows the fact that apps can communicate users' personal data to third parties without users' knowledge or consent [2].

While a range of approaches have been used in an endeavour to

address non-consented use of users' data, a key focus has been on the provision of privacy policies. 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 [3]. According the General Data Protection Regulation [4], privacy policies are a means for data controllers to inform data subjects (end users of the app) about what personal data will be collected and for what purpose and as such are a key element in ensuring informed consent. As such, they help to dispel users' anxieties about the revelation of personal data [5]. Further, privacy policies build user trust and enable app to achieve regulatory compliance. However, several studies [6] [7] [8] indicate that privacy policies have been found to be inadequate in their attempt to preserve user privacy. For instance, privacy policies have been critiqued for being "far too long and complex" [9]. Similarly, 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 an app's adherence or compliance to its own privacy policy.

Moreover, privacy related challenges have been identified in apps that run on both Android and iOS app platforms even while they rank top in popularity [10]. Android apps present users with a permission list, during installation, on a take-it-or-leave-it basis with no specific reason for its requirement unless if user consults the provided privacy policy. This could facilitates possible privacy abuse as apps seek to access as much user data as possible irrespective of whether or not it's required for the apps' functionality [11]. A study [12] found that in spite of a user's call history having no direct influence on the ads a user might want, there were Ad libraries that collected and conveyed this information to the internet. Further, Ad libraries have been observed to engage in permissions usage that could introduce privacy risks [13]. Efforts to address privacy abuse led to the development of Android's Marshmallow version [14] which operates on a similar principle to iOS. In both cases, requests for specific permissions are made as and when they are needed using a pop up message that allows users to either accept or deny the permissions [15].

Comparing how easy it is to understand the way permissions are on both platforms, it is observed that while Android is more informative in terms of detail, it uses more technical terminology than iOS which could impact on extent of user understanding [14]. Nonetheless, [16] argues that privacy risks arise because users often lack the full picture of information that could be collected and the possibilities of using it in ways that are unknown to them. Security-wise, the android apps present more risk while the iOS apps tend to be safer [17]. However, [16] stresses that there is reduced privacy awareness and fear among iOS users. Notwithstanding, iOS apps have been found to be vulnerable in some instances [18] [19] and the vetting process implemented by Apple to ensure that iOS apps are aligned with Apple's privacy critiqued for its lack of transparency [20].

Companies that do not take user privacy concerns into consideration for instance when using personal data developing profiles that facilitate tailoring of Ads, are likely to counter public backlash [21]. Moreover, whereas regulation requires apps to provide privacy policies, the extent to which these policies are contractual is debatable as they change as

and when the firm decides. However, increased privacy confidence increases online success. Users want government involvement through means such as enacting laws that protect the privacy of personal information collected through apps. Regulatory bodies such as the Federal Trade Commission (FTC) in the US and the European Data Protection Regulation [4] demand that users are informed of the data gathered by apps, why it is collected and that opt out provisions are made for users [22]. Nonetheless, the existence of government regulation does not imply that companies comply with the requirement. This is underpinned by a recent study by several authors [23] in which a critical analysis of Facebook's revised policies and terms was conducted based on the EU Data Directive. The findings of the study indicate that Facebook engages in questionable privacy practices. As such, there is need to ascertain the extent of apps compliance to their privacy as a pointer to the extent to which users would have confidence in using the apps' service.

A study that examined the personal, behavioural and location data from 110 apps indicates that Android and iOS apps generally transmit sensitive data to 3.1 and 2.6 third party do-mains respectively [24]. Our work seeks to extend that study by exploring the apps data handling practices verses compliance of apps to their privacy policy. As such, our study conducts an investigation into whether the user data collected and disseminated by apps to third party domains is matches their privacy policies. The analysis was conducted based on a privacy compliance comparison between Android and iOS apps as these are the dominant app platforms, by exploring the extent to which apps adhere to their stated privacy policies and, the resulting effects of apps' data handling practices.

Our study seeks to answer the research question: Do mobile application privacy policies match their practices? To answer this question we consider mobile applications from the two dominant mobile application platforms i.e. Android and iOS. The remainder of the paper is organized as follows: related work is presented in section 2, followed by the research method in section 3, after which the findings of the study are presented in section 4. In section 5, a discussion on the findings is presented and Section 6 sums up the paper with conclusions and subsequent work.

2 Related Work

Related research conducted [25] has focused on availability, scope and transparency of mobile app privacy policy. That study found that two-thirds of the apps' contained content that was not directly related to the app. Further, information privacy practices were not clear. However, the study was limited to health. In another health privacy policy related study, [26] analysed website related vulnerabilities based on 23 website policies using goal mining techniques for the extraction of pre-requirements goals from post-requirements text artefacts from

which a taxonomy was developed. Research [27] argue that the permissions system should be more fine grained and develop an sought to enhance user understanding by providing a mechanism of equipping users with information required before application downloads. Further work [1] explored the practicability of combining permissions and app requests in advising using on whether the risk of installing an app outweighs the expected benefits.

More so, another study presented by [24], used 110 widely used Android and iOS apps to explore the different user data that apps conveyed to third parties. Using an iPhone 5 and a Samsung Galaxy S3, HTTP and HTTPS traffic from the apps was captured using a proxy and examined for personally identifiable data. As a control, push notifications were blocked so as not to allow apps to transmit data in background when not being used. However, by limiting the analysis to text matches within the HTTP and HTTPS traffic, potentially sensitive user data may have missed being observed in instances in which other protocols are used by the apps or, in cases where user data was hashed so as to obscure it.

3 Research Method

Our study is based on the findings presented by [24] discussed in related work above. As such, our study inherited the measurement errors made in [24], as mentioned above.

First, in our study, the selection of the apps was done on the basis of the number of third party domains that the apps conveyed sensitive data to. We found that in the Zang et al database, the number of third party domains associated with the apps ranged from none to 17. As such, we selected apps that conveyed sensitive data to two or more third party domains. This was 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 dissemination. As a result, the selection yielded two non-identical sets of 15 apps on each platform (see Table 1&2). The limited sample size facilitated a detailed analysis of the apps. The analysis of this sample size was feasible taking into consideration the effort and time required for an in depth analysis. The apps were from a cross range of categories such as; social, navigation, medical, business, games, health and fitness, lifestyle etc. Hence while the sample size was relatively small, the scope of representation was relatively spread. Due to a sample size limited because it was based on a predetermined database and the selection criteria, the results are not statistically significant. However, the significance of our findings are in that they serve as a preliminary indication of trends on how the Android and iOS apps data handling practices and compliance compare. This provides indicators of further research.

Second, after determining the apps to be used in the study, we planned to analyse the apps through the following steps; (a) establishing the practical data handling practices for each of the thirty apps, (b) determining the apps' privacy commitments to users on data

handling as stated in their privacy policies and, (c) establishing the extent of compliance by apps to their own privacy policies.

To establish the practical data handling practices for each of the thirty apps, we analysed the types of user data they convey to third parties in practice based on the finding of [24]. In particular, 14 types of user data were found: address, birthday, email, gender, name, password, phone number, zip code, employment, friends, medical info, search, username and location.

Table 1: Android apps and number of associated third parties

App	Third Parties
American Well	4
Drugs.com	7
Expedia	4
Kayak	3
MapQuest	5
Priceline	4
Glide	8
Jobsearch	4
Snagajob	3
Monster Lengend	5
Myfitnesspal	4
Runkeeper	3
Pinger Text Free	11
Tango	4
Pinrest	4

Table 2: iOS apps and number of associated third parties

App	Third Parties
Fruit Ninja	4
Piano Tiles	3
Instagram	2
Instasize	2
Leafly	3
Ovia Fertility	2
Urgent Care	4
MapMyRun	4
Nike	4
TimeShop	3
Walgreens	5
Groupon	3
Inrix	2
Local Scope	17
Phone Tracker	2

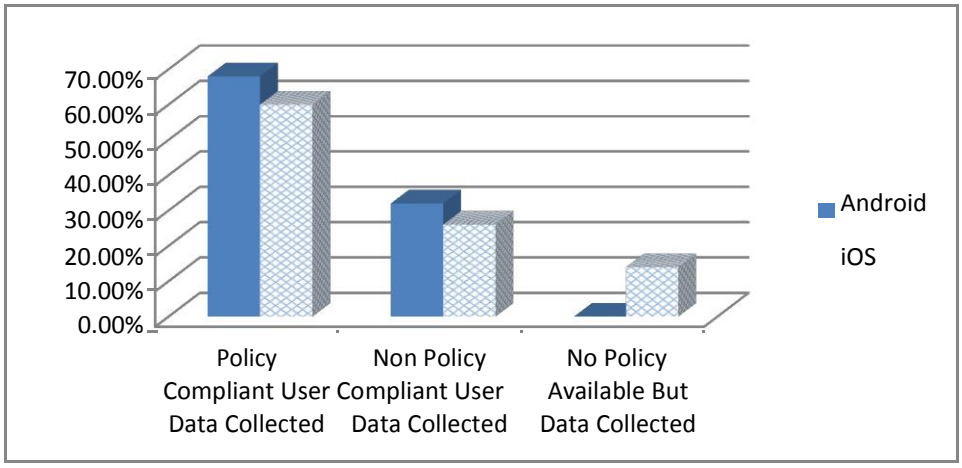
Next, we sought to establish the apps' privacy commitments to users on data handling as stated in their privacy policies. The apps' privacy policies were sourced online using the privacy policy' link provided through each app. The privacy policies were source between September to December 2015 and as such should substantially correspond to the specific version of apps that were used in [24]'s study to extract the traces of sensitive data dissemination from apps. These privacy policies were uploaded into Nvivo software [28] to facilitate a qualitative analysis of their content. The process of content coding involved the review of privacy policies in order to establish a fundamental understanding of the policies. This was followed by coding using thematic analysis to identify content on data collection, use and dissemination to third parties etc., that were of particular interest to our study. The mechanism of coding and data interpretation was validated by two researchers so as to ensure substantial agreement on data interpretation and results. A study found that when six senior researchers individually coded a focus group, the results of their coding while showing major similarities in findings, also had elements of disagreement [29].

In the final stage, we determine the extent of compliance by apps to their own privacy policies. We systematically assessed the results from the apps' privacy commitments as stated in their policies, against their practical data handling practices involving the 14 user data types that were earlier identified. The analysis was restricted to the collected and transmitted data from the app and does not include what happens on the receiving entities. The results are presented in the next section.

4 Findings

Our results indicated that Android apps handle 64% of the types of the users' data examined while iOS handles 50%. Moreover, out of the types of user data gathered and disseminated by Android, 32% did not match the app privacy policies. Similarly, of the user data handled by iOS, 26% did not comply with their policies. Interestingly 14% of the iOS user data were found to be gathered and disseminated with no privacy policy available as shown in Figure 1.

Figure 1: A comparison of Android and iOS apps data practice verses privacy policy.



Most collected user data. Considering the overall figures of user data handled by the Android and iOS apps, the data attributes most collected and disseminated by Android were; address (15), email (15) and name (15) i.e. these three user data attribute were collected by all the Android apps in our study since the study involved fifteen Android apps. On the other hand, iOS' highest were; location (14), email (12) and name (12) i.e. none of iOS highest user attributes were collected by all the fifteen iOS attributes in the study.

Extent of compliance between policy and data dissemination. Compliance was considered as per data type. Taking into account the extent to which the apps' policies match their data handling practices, Android's most compliant users' data were; email (12), name (12) and location (10); whereas iOS had email (9), location (9) and, name and friends both (6). It appears that apart from iOS collecting friends, the other compliant user data attributes were the same for both platforms.

In contrast, considering non-compliance between the apps' policies and their data handling practices, Android's most non-compliant user data were; username (6), gender (5) and address (5) while for iOS the list comprised of; password (5), address (4), username and name both at (3) as shown Figures 2&3. In both iOS and Android, the similarities in non-compliance was that the *username* and *address*

user data was collected and disseminated outside the privacy policy agreement, while the differences in the data handled outside the policy was that Android collected *gender* user data attribute while iOS collected the *name* user data attribute.

Further, iOS apps were found to handle users' data without privacy policies. The affected user data included; name (3), friend (2) and search (2) as shown in Figure 1.

Figure 2 - iOS apps data practice versus privacy policy statements

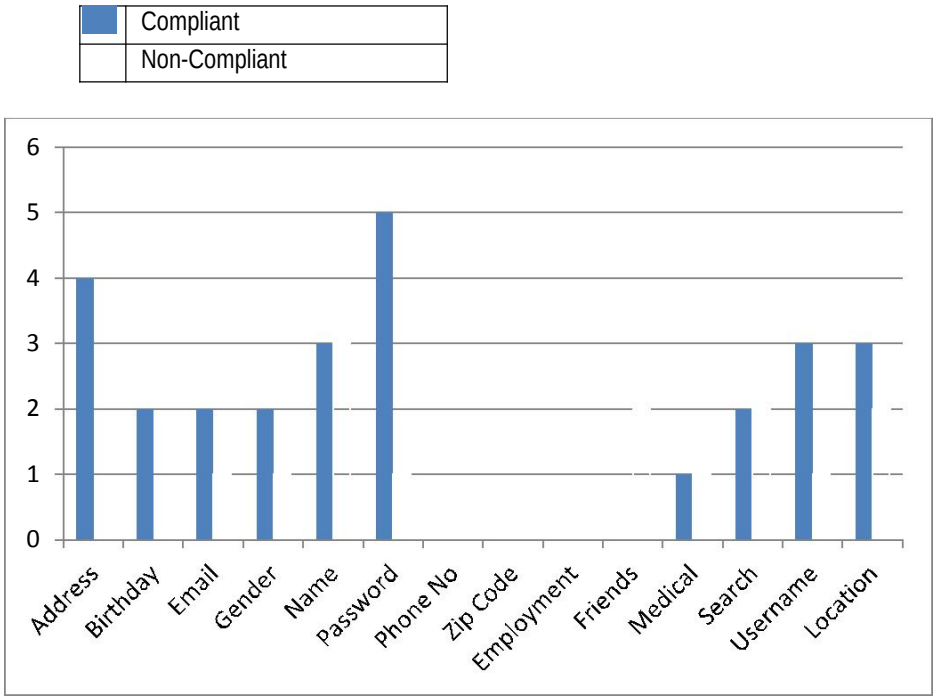
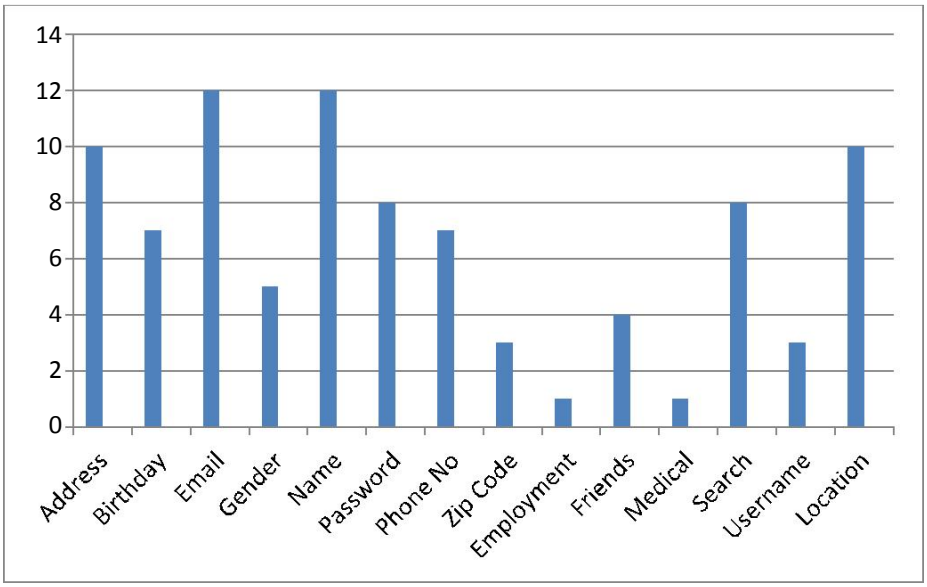


Figure 3 - Android apps data practice versus privacy policy Statements



5 Discussion

According to [30], there is an increase in fear regarding illicit exposure of personally identifiable information due to increasing identity theft. Personally identifiable information (PII) is sensitive and focal to privacy law [31]. As such, access to users' data should be aligned with the privacy policy of online social media. Laws and regulations such as the California law [32, 33]; the UK the Data Protection Act 1998 [34], EU Data Protection Directive [35] etc. also require that user are provided with privacy policies before app download. However, our findings show that while the Android apps in the study were found to have policies, 14% of the iOS user data handled was from apps without policies. Similarly, [36] study of health apps found that iOS had a 61.7% likelihood of not having privacy policies as compared to Android at 77.3%. Differences in our results may arise from the fact that we considered fewer apps (30) with more categories while [36] considered 600 app limited to health apps. These findings highlight the fact that while the law demands for the provision of policies, major app platform are not fully complying. This is also an indicator that even when laws are enacted to protect user privacy, there is need for more effective mechanisms of enforcing these laws.

However, specifically considering compliance of apps' data handling practices their privacy policies, Android had an 18% likelihood of sharing personally identifiable information outside the limits of its

policy whereas iOS' ranked slightly lower at 17 %. While our study investigated the extent of compliance between the Android and iOS apps' data dissemination against their privacy policies, a related study by [24], compared Android and iOS likelihood to disseminate users' personally identifiable information in a manner not reflected by the permissions request at the apps' download, they found that Android was more likely to disseminate personal data in a way a way that breached the requested permissions.

However, taking into account the iOS apps found without privacy policies in our study, the probability of iOS sharing personally identifiable information in a non-policy compliant manner further increase from 17% to 23%, making it higher than Android (18%). Users' ability protect their personal data necessitates that they are aware of such leakages [30]. Moreover, our findings also contradict a general user perception that apps with user textual reviews are safer [16]. This is evidenced by the fact that the apps in our study had user reviews yet our findings show that some had no privacy policies.

Specifically in both Android and iOS apps studied, mismatches between the policies and the data handled were most observed involving the *username* and *address* user data which are both classified as personally identified information. Further, our findings indicated that the similarities in the most collected user data in both Android and iOS was that both collected *name* and *email* user data which are both personally identified information. Nonetheless our results also showed that these two types of user data were also among the leading policy compliant user data. Our results show that in both cases of compliance and non-compliance with the apps' policies, the user data involved is personally identified information. These trends indicate the immense interest that apps have in personally identifiable information data and hence the necessity of ensuring adequate and effective user privacy preservation measures.

Our results ascertained that neither Android nor iOS apps' data handling practices fully comply with the apps' privacy policy statements. These results are restricted to the observation of data collection and transmission at app level. They do not include whatever happens on the receiving servers. In addition, the measurement errors made in [24] were inherited, as mentioned above. Overall, taking into account both personal and non-personal user data analysed in the study, Android data handling practices are more compliant to policy than that of iOS with compliance figures of 68% and 40% respectively. Policies claim to limit the user data conveyed to third parties to non-personal data [30]. However, [37] state that metadata has the potential danger of re-identification of users or sources, stressing that it is still possible to expose specific users even from non-personal data. This is underpinned [30], asserting that certain third party servers have the ability to trace and combine different pieces of user data from which a user profile can be formed. According to a study [38], a combination of the zip code, gender and birthday is able to facilitate the identification of up to 87% of Americans.

Based on the finding of this study, which in tandem built on the results from [24], we argue that in the preservation and protection of app user privacy a number of aspects must be considered i.e. regulation, permissions requested at apps' download, privacy policies provided and, the dissemination of user data by the apps to other apps or third parties. The relevant regulations determine the privacy requirements or best practices that must be taken into consideration by apps in order to safe guard user privacy. As such, the apps permissions, policy and dissemination of user data should be aligned to regulation. This study established that there are instances in which user data was disseminated with no policy to guide the process. For cases in which no policy is provided, users could opt not to download such apps. However, this may be unlikely [39] and may depend on a users' level of privacy awareness, keenness and the personal reasons for which they require the apps service.

Further, this study shows that the dissemination of data by apps through their data handling practices does not always comply with their stated privacy policies, even in cases where potentially sensitive user data is involved. This is of concern since a study by [40] found that 72% of the participants assume that the provision of a policy implies that app providers comply with the policy and necessary regulation to safeguard their privacy. We further argue that one of the criticisms of current practice is that an app may request a user to grant access to personal data which is not required for its app's functionality. This excess data may have been stated in the privacy policies, in which case it would appear as acceptable. However, it may violate the minimize principle in some regulatory frameworks [4] but not necessarily the privacy policy. There is a user expectation that regulators will protect their privacy [40]. As such, this emphasizes the need for more effective mechanism of validation of apps' data handling practices against their policies.

Validation could be effected through more rigorous regulatory enforcement to monitor that apps comply to their policy. Another form of validation could take shape in form of automation of the validation process. An automated solution could function at platform level i.e. Android and iOS. At platform level, the solution could be developed first to check that and app indeed has a privacy policy before its acceptance onto the platform. Second, the automation could be used to validate compliance between apps policies and against their data dissemination practices. In a way, it would be similar to the Apple vetting process that validates that app comply with the license agreement before digital signing and uptake onto the iTunes store.

In addition to ensuring the provision of privacy policies and the validation of apps data handling practices against their policies either by regulators or through automation, several other solutions may be considered. These efforts have been geared improving policy representations in a bid to encourage or facilitate greater policy readability and user comprehension in order to encourage user reading of privacy policies so as to support informed decisions [41] [42] [43].

6 Conclusion and future work

Our results show that neither Android nor iOS apps' data handling practices meet the full requirements of their privacy policies even in cases of potentially sensitive user data. Further, instances in which iOS apps continue to disseminate user data in the absence of privacy policies were found. This is further complicated by the fact that there is no facility through which the users can confirm that the way their data is disseminated by apps matches the permissions requested by apps at download and their privacy policies. 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. As such, future research could explore ways of automating enforcement of privacy policies by drawing on privacy policy specification languages such as the Platform for Privacy Preferences (P3P) and the Enterprise Privacy Authorization Language (EPAL). This would 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. Taking into account considerations of the privacy requirements stipulated by regulatory frameworks such as the European General Data Protection

Regulation would assist in enhancing and protecting users' privacy. In addition to building user confidence in apps' commitment to preserve user data privacy, it would also be of value to privacy regulatory bodies by automating compliance to stated privacy policies.

References

1. Sarma, B., Li, N., Gates, C., Potharaju, R., Nita-Rotaru, C., Molloy: Android permissions: a perspective combining risks and benefits. In : 17th ACM symposium on access control models and technologies, pp.13-22 (2012)
2. Thurm, S., Kane, Y.: Your Apps Are Watching You. In: Wall Street Journal. (Accessed 2010) Available at: http://online.wsj.com/news/articles/SB10001424052748704694004576020083703574602?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052748704694004576020083703574602.html
3. Papanikolaou, N., Creese, S., Goldsmith, M.: Refinement checking for privacy policies. Science of Computer Programming, 1198-1209 (2012)
4. Directive, E. U.: EUR-Lex. In: Access to European Union Law. (Accessed 2017) Available at: http://eur-lex.europa.eu/search.html?qid=1516438784094&text=GDPR&scope=EURLEX&type=quick&lang=en
5. Westin, A.: Privacy and Freedom. Atheneum Publishers, New York (1967)
6. AI Anton, J., Reese, A.: Analyzing Web site privacy requirements using a privacy goal taxonomy. In : IEEE Joint Requirements Engineering Conference, Essen, vol. 9, pp.23–31 (2001)

7. Jensen, C., Potts, C., Jensen, C.: Privacy Practices of Internet Users: Self-Report Versus Observed Behavior. International Journal of Human Computer Studies 63(1-2), 203-27 (2005)
8. Sadeh, N., Hong, J., Cranor, L., Fette, I., Kelley, P., Prabaker, M., Rao, J.: Understanding and capturing people's privacy policies in a mobile social networking application. Personal and Ubiquitous Computing, 401-412 (2009)
9. Cellan-Jones, R.: BBC. (Accessed 2014) Available at: http://www.bbc.co.uk/news/technology-30234789
10. Liu, R., Cao, J., Yang, L.: Smartphone privacy in mobile computing: Issues, methods and systems. Information and Media Technologies 10(2), 281-293 (2015)
11. Wei, X., Gomez, L., Neamtiu, I., Faloutsos, M.: Permission evolution in the Android ecosystem. In : ACSAC '12 Proceedings of the 28th Annual Computer Security Applications Conference, Florida, pp.31- 40 (2012)
12. Grace, M., Zhou, W., Jiang, X., Sadeghi, A.: Unsafe Exposure Analysis of Mobile In-App Advertisements. In : ACM, Arizona (2012)
13. Book, T., Pridgen, A., Wallach, D.: Longitudinal Analysis of Android Ad Library. (2013)
14. Ashnis: noeticforce. (Accessed 2016) Available at: http://noeticforce.com/app-permissions-android-vs-ios
15. Hoffman, C.: How -To Geek. (Accessed 2013) Available at: https://www.howtogeek.com/177711/ios-has-app-permissions-too-and-theyre-arguably-better-than-androids/
16. Benenson, Z., Gassmann, F., Reinfelder, L.: Android and iOS users' differences concerning security and privacy. In : Human Factors in Computing Systems, pp.817-822 (2013)
17. Felt, A. P., Finifter, M., Chin, E., Hanna, S., Wagner, D.: A survey of mobile malware in the wild. SPSM (2011)
18. Seriot, N.: iPhone Privacy., Black Hat, USA (2010)
19. Bonnington, C.: First Instance of iOS App Store Malware Detected. (Accessed 2012) Available at: http://www.wired.com
20. Egele, M., Kruegel, C., Kirda, E., Vigna, G.: PiOS: Detecting Privacy Leaks in iOS Applications. NDSS, 177-183) (2011)
21. Liu, C., Arnett, K. P.: An Examination of Privacy Policies in Fortune 500 Web Sites. American Journal of Business 17(1), 13 - 22 (2002)
22. Wetherall, D., Choffnes, D., Greenstein, B., Han, S., Hornyack, P., Jung, J., Schechter, S., Wang, X.: Privacy revelations for web and mobile apps. In : HotOS, vol. HotOS XIII (2011)
23. Van-Alsenoy, B., Verdoodt, V., Heyman, R., Wauters, E., Ausloos, J., Acar, G. (Accessed 2015) Available at: https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-2.pdf
24. 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. In : Technology Science (2015)
25. Sunyaev, A., Dehling, T., Taylor, P., Mandl, K.: Availability and quality of mobile health app privacy policies. ournal of the American Medical Informatics Association 22e1, e28-e33 (2015)
26. Antón, A. I., Earp, J. B.: A requirements taxonomy for reducing Web site privacy vulnerabilities. Requirements Engineering 9(3), 169-185 (2004)
27. Rosen, S., Qian, Z., Mao, Z. M.: Approfiler: a flexible method of exposing privacy-related behavior in android applicaitons to end users. In : 32 annual ACM

conference on Human factors in computing systems., pp.2347-2356 (2014)

28. QSR: What is NVivo? (Accessed 2017) Available at: http://www.qsrinternational.com/what-is-nvivo
29. Armstrong, D., Gosling, A., Weinman, J., Marteau, T.: The place of inter-rater reliability in qualitative research: an empirical study. Sociology 31, 597–606 (1997)
30. Krishnamurthy, B., Wills, C. E.: On the leakage of personally identifiable information via online social networks. In : 2nd ACM workshop on Online social networks, pp.7-12 (2009)
31. Schwartz, P., Solove, D.: PII Problem: Privacy and a New Concept of Personally Identifiable Information. NYUL Rev 86(1814) (2011)
32. Harris, K.: Privacy on the go., FTC (2013)
33. CalOPPA: California Online Privacy Protection Act (CalOPPA). In: http://consumercal.org. (Accessed 2015) Available at: http://consumercal.org/about-cfc/cfc-education-foundation-2014/what-should-i-know-about-privacy-policies/california-online-privacy-protection-act-caloppa/
34. TermsFeed: Privacy Policies are Mandatory by Law. (Accessed 2017) Available at: https://termsfeed.com/blog/privacy-policy-mandatory-law/
35. Directive, E. U.: EUR-Lex. In: Access to European Union Law. (Accessed 2017) Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046
36. Sunyaev, A., Dehling, T., Taylor, P. L., Mandl, K. D.: Availability and quality of mobile health app privacy policies. Journal of the American Medical Informatics Association 22(e1), e28-33 (2014)
37. Montjoye, Y., Radaelli, L., Singh, V., A, P.: Unique in the shopping mall: On the reidentifiability of credit card metadata. Science 347(6221) (2015)
38. Malin, B.: Betrayed by my shadow: Learning data identify via trail matching. Journal of Privacy Technology (2005)
39. Janger, E. J., Schwartz, P. M.: The Gramm-Leach-Bliley Act, Information privacy and the limits of default rules. Minnesota Law Review 86, 1219−1230 (2002)
40. Yue, L.: User control of personal information concerning mobile-app: Notice and consent? Computer Law & Security Review 30(5), 521-529 (2014)
41. Earp, J. B., Vail, M., Anton, A. I.: Privacy policy representation in web-based healthcare. In : 40th Annual Hawaii International Conference, p.138 (2007)
42. Cranor, L., Kelley, P. G., Cesca, L., Bresee, J.: Standardizing privacy notices: an online study of the nutrition label approach. In : SIGCHI Conference, pp.1573– 1582 (2010)
43. Kununka, S., Mehandjiev, N., Sampaio, P., Vassilopoulou, K.: End User Comprehension of Privacy Policy. In : International Symposium on End User Development , Eindhoven, pp.135-149 (2017)
44. Wei, T. E., Jeng, A. B., Lee, H. M., Chen, C. H., Tien, C. W.: Android privacy. Machine Learning and Cybernetics (ICMLC),. 1830-1837 (2012)
45. Van-Alsenoy B, V. (Accessed 2015)
46. Schwartz, P. M., Solove, D.: Notice and Choice. In : The Second NPLAN/BMSG Meeting on Digital Media and Marketing to Children (2009)
47. Sunyaev, A., Dehling, T., Taylor, P., Mandl, K.: Availability and quality of mobile health app privacy policies. Journal of the American Medical Informatics Association 22(1), 22-33 (2014)