Investigating the Compliance of Android App Developers with the CCPA

Nikita Samarin*, Shayna Kothari*, Zaina Siyed†, Primal Wijesekera*‡, Jordan Fischer§,
Chris Hoofnagle§¶, and Serge Egelman*‡
*Electrical Engineering and Computer Sciences, †College of Letters and Science, §School of Information, ¶School of Law
University of California, Berkeley and ‡International Computer Science Institute
Email: {nsamarin, shayna.kothari, zainasiyed, primal, jordan.fischer, choofnagle, egelman}@berkeley.edu

***Abstract*—The California Consumer Privacy Act (CCPA) provides California residents with a range of enhanced privacy protections and rights. Our proposed project aims to investigate the extent to which Android app developers comply with the provisions of the California Consumer Privacy Act (CCPA) that require them to provide consumers with accurate privacy notices and respond to consumers' "request to know" by disclosing personal information that they have collected, used or shared about them for a business or commercial purpose. In doing so, we aim to understand whether the information provided by developers in privacy notices and in response to "right to know" requests is complete and accurate, and whether the response accurately explains how this data has been collected, used, and shared.**

I. Introduction and Background

The United States lacks a comprehensive federal privacy regulation and instead relies on industry- or state-specific discrete privacy laws. On the state level, the California Consumer Privacy Act (CCPA) was recently enacted to provide enhanced privacy protections and rights for California residents, including the ability to request information about how a business collects, uses, and discloses their personal data [1], [2]. This "right to know" is designed to allow consumers to access information that belongs to them and ensure that businesses subject to the CCPA do not violate disclosed data practices in their privacy notices.[1]

Previous studies have identified issues with similar privacy laws enacted earlier, most notably GDPR in Europe [3], [4]. For instance, Kröger et al. sent subject access requests to vendors of 225 mobile apps and found that at least 19% of the vendors were unreachable, with requests being fulfilled in less than 53% of the cases [5]. Other authors have also examined the shortcomings of the CCPA, such as the difficulty of exercising requests to opt-out of the sale of their personal information [6]. Our proposed study will complement these findings by focusing specifically on the process of submitting verifiable consumer requests under the CCPA and comparing the responses from app developers with the actual privacy practices that we identify through app and network analysis. We believe that our work, therefore, is crucial in evaluating the overall efficacy of CCPA and its utility to mobile app users.

[1]A statewide proposition to amend the CCPA was passed in November 2020, however, it will not take effect until 2023.

II. Preliminary Work

Our research group developed an infrastructure enabling us to analyze how Android apps collect and transfer personal data. An extensive instrumentation framework in the custom OS provides a holistic view of Android applications' runtime behavior. We can observe sensitive resource usage, data access, and sharing patterns over the network of any given Android application without any modification to the application. Our instrumentation is resilient to most of the anti-analysis and anti-debugging techniques currently deployed by apps.

We focus on 160 Android mobile apps that are developed by companies that fall or can be reasonably inferred to fall under the CCPA definition of a "business", which we downloaded together with their privacy policies in November 2020. Similar to [7], we have also generated fictitious values for different types of personal information covered by CCPA to facilitate the subsequent search for this data in the logs produced by app testing and generated aliases that we will use to submit verifiable consumer requests to developers. Figure 1 illustrates the data flow that we observed at runtime after testing a sample of our selected apps using our instrumentation.

III. Proposed Study

We aim to uncover any existing contradictions between:

1) personal information that we record being collected and transmitted by an app using dynamic and static analysis, and network traffic measurement;
2) personal information that the app developer discloses to us in response to the "right to know" request after we perform the analysis of their mobile app; and
3) personal information that the app developer claims to collect in the privacy policy of their mobile app.

For (1), we will manually test each selected app with our instrumented version of the Android operating system. We will search for predefined data values within the resulting test logs, as well as perform an open-ended search to see if the app transmits other unexpected personal data.

After running the tests, we will submit verifiable consumer requests to developers (for (2)) and analyze the privacy notices (for (3)). We aim to obtain all types of information that a business has to provide under the CCPA, allowing us to compare these three data viewpoints to quantify the accuracy and completeness of the information disclosed by the developer.

ACKNOWLEDGMENTS

We acknowledge the financial support provided to us by the Center for Long-Term Cybersecurity at UC Berkeley.

REFERENCES

[1] California Consumer Privacy Act (CCPA), 2018 Cal. Legis. Serv. Ch. 55 (A.B. 375).

[2] California Consumer Privacy Act Regulations., 2020. Title 11, Division 1, Chapter 20.

[3] Zimmeck, S., Story, P., Smullen, D., Ravichander, A., Wang, Z., Reidenberg, J., Russell, N.C. and Sadeh, N., 2019. MAPS: Scaling privacy compliance analysis to a million apps. Proceedings on Privacy Enhancing Technologies, 2019(3), pp.66-86.

[4] Di Martino, M., Robyns, P., Weyts, W., Quax, P., Lamotte, W. and Andries, K., 2019. Personal Information Leakage by Abusing the GDPR 'Right of Access'. In Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019).

[5] Kröger, J.L., Lindemann, J. and Herrmann, D., 2020, August. How do app vendors respond to subject access requests? A longitudinal privacy study on iOS and Android Apps. In Proceedings of the 15th International Conference on Availability, Reliability and Security (pp. 1-10).

[6] Mahoney, M., 2020. California Consumer Privacy Act: Are Consumers' Digital Rights Protected?

[7] Zang, J., Dummit, K., Graves, J., Lisker, P. and 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, 30.

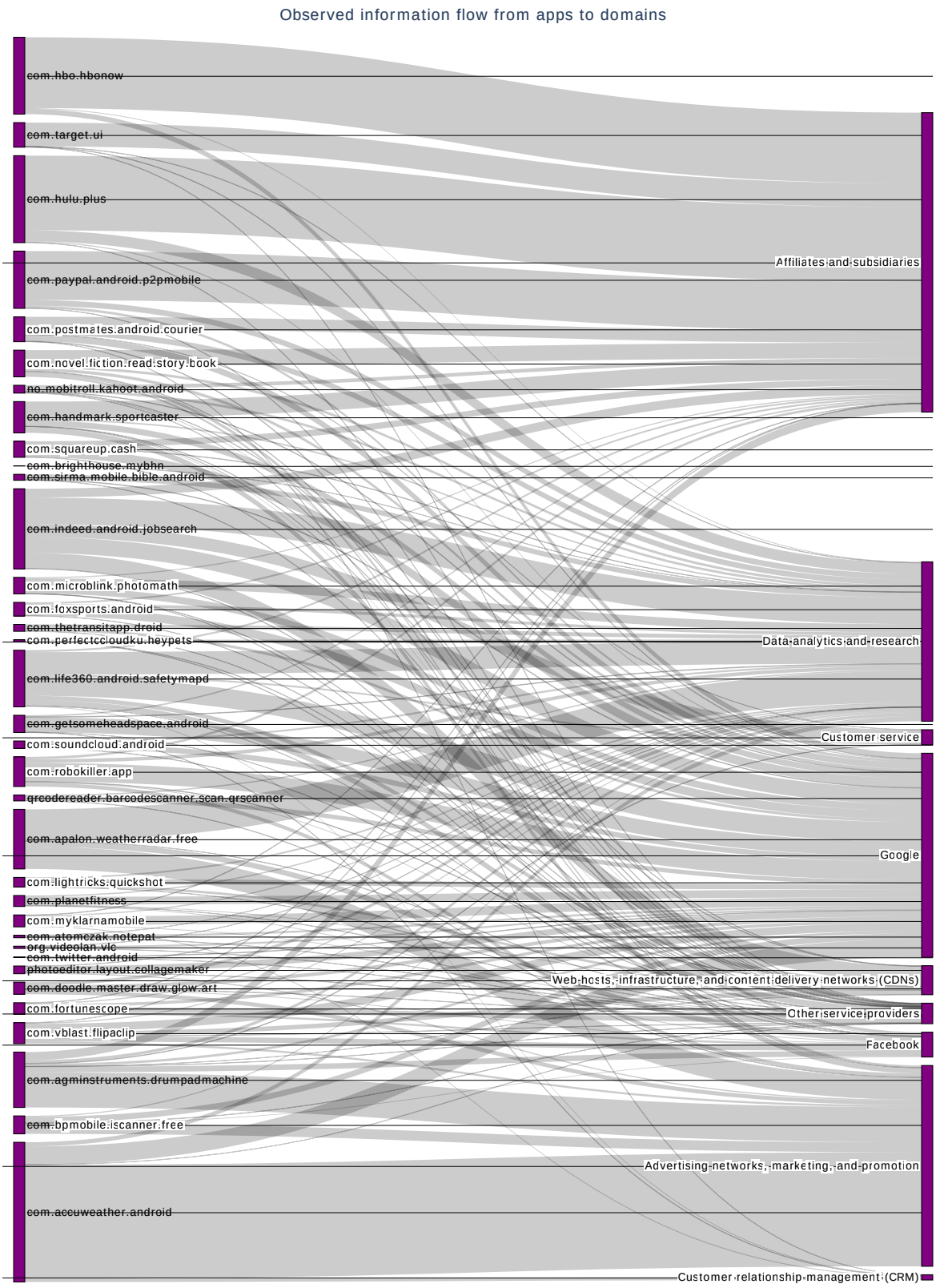

Fig. 1. Observed information flow from a sample of apps to domains (categorized according to our taxonomy). Thicker lines represent more data being transmitted from a specific app.