The Invisible Threat: Exploring Mobile Privacy Concerns

Nishant Aggarwal*, Wesley Tan*, Konrad Kollnig^, Sebastian Zimmeck*
*Department of Mathematics and Computer Science, Wesleyan University
^Law and Tech Lab, Maastricht University

Introduction

Our research addresses the growing concern over third-party tracking practices on Android devices, where various applications collect personal data and sell it to data brokers, compromising user privacy. Despite legal provisions such as the California Consumer Protection Act (CCPA) and General Data Protection Regulation (GDPR)**, the process of opting out of data sales remains cumbersome and time-consuming for consumers**. In response, to enhance user accessibility to their privacy rights we want to implement the Global Privacy Control (GPC) signal on Android.

The GPC signal is designed to simplify the exercise of legal privacy rights under CCPA by enabling users to opt out of third-party tracking through a single step. Our research revolves around the development of a mobile application that seamlessly integrates the GPC functionality, empowering users to effortlessly exercise their right to protect their personal information.

By implementing GPC on Android devices, we aim to provide a user-friendly and efficient means for individuals to assert control over the collection and sale of their data. The proposed app ensures that users can easily navigate through the complexities of privacy policies and in-app mechanisms, streamlining the opt-out process from third-party tracking.

Exploration

This section outlines the diverse technological avenues explored to implement Global Privacy Control (GPC) on Android devices. We investigate three primary approaches: AdId Integration, GPC Signal via Header, and Integration with Third-Party Libraries.

Approaches Explored:

1. AdId Integration: Leveraging Android Advertising Identifier for seamless GPC implementation.
2. GPC Signal via Header: Embedding GPC signal directly into communication headers.
3. Integration with Third-Party Libraries: Integrating GPC functionalities with widely used libraries.

Each approach's advantages and limitations were evaluated, leading us to select the AdId Integration method for its potential to streamline GPC implementation while minimizing user experience disruption. Our next steps involve a comprehensive exploration of the technical and legal aspects for AdId's compatibility with GPC. This includes conducting a large-scale app analysis to assess the feasibility and adherence to privacy standards.

Data Analysis

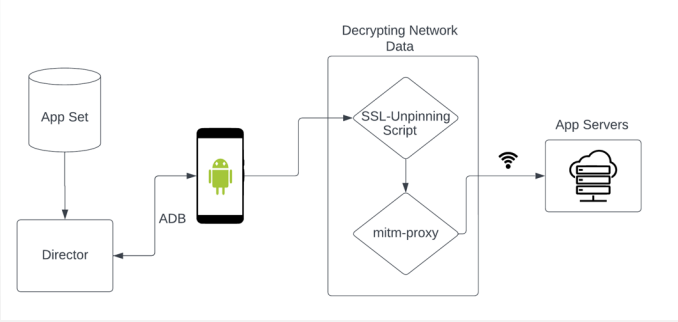

Fig 1: App Analysis Pipeline

In order to ascertain the practical effectiveness of AdId deletion, a thorough investigation of network communications between the applications and servers will be conducted through a large-scale data analysis. **This analysis aims to shed light on the degree of enforcement of GPC signal and AdId deletion and the extent to which AdId aligns with GPC principles.**

Our methodology involved installing the app on a Google Pixel 6A device running Android 13 (Build TQ2A.23.05.05.002) using adb. Subsequently, we used the mitmproxy and employed the SSL-unpinning script to **decrypt and collect network data during network captures for each of the six different settings which include various combinations of AdId deletion, GPC signal, and granting apps permissions to various PII (Personally identifying information) including location.**

To access network traffic using mitmproxy, we rooted the phone with Magisk and installed the mitmproxy certificate in the system store using the MagiskTrustUserCert Module. Additionally, to bypass Chrome Certificate Transparency, we integrated the MagiskBypassCertificateTransparencyError Module. SSL pinning was circumvented by deploying a Frida server on the phone and executing an SSL-unpinning script for each app.

To ensure the reliability of our network captures and minimize background traffic interference, we implemented specific adjustments in the system settings. We disabled "private DNS" to prevent potential conflicts with our proxy and enabled "Data Saver" to reduce background traffic, thereby capturing network data solely for the app under scrutiny.

We plan to collect and analyze the data within the next month!

GPC App

Figure 2 displays the first version of the **GPC Android App**. The app has two main buttons at the top, which **direct users to browsers with built-in GPC features**. There's also a button at the bottom, **allowing users to access the AdId settings and giving them the option to delete their AdId**. This version of the app is primarily for testing its functionality, rather than focusing on the usability. In the future, we plan to redesign the app to make it more user-friendly and easier to understand and use.

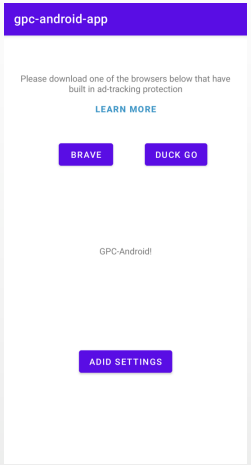

Fig 2: GPC App

Future Work

The findings of our research have the potential to shed light on the compliance level of apps with Google's AdId and the GPC specification, potentially prompting Google and CCPA to consider stricter enforcement of regulations.

Considering the broader implications, **future efforts may focus on developing comprehensive privacy frameworks that address the evolving landscape of mobile applications and data sharing**. This could involve collaborations between industry stakeholders, policymakers, and privacy advocates to establish unified standards that safeguard user data and promote transparency.

Acknowledgements

We are grateful to the National Science Foundation (Award #2055196), the Alfred P. Sloan Foundation (Grant G-2021016874), Wesleyan University, and the Anil Fernando Endowment for their support of this research. Conclusions reached or positions taken are our own and not necessarily those of our supporters, its trustees, officers, or staff.