Understanding How Third-Party Libraries in Mobile Apps Affect Responses to Subject Access Requests

7th Workshop on Technology and Consumer Protection (ConPro ’23)

May 25, 2023

Nikita Samarin and Primal Wijesekera

UC Berkeley and ICSI

Third-party libraries (TPLs) simplify software development but decrease visibility over software components

```
// Base class for receiving messages from Firebase Cloud Messaging.
import com.google.firebase.messaging.FirebaseMessagingService;
import com.google.firebase.messaging.RemoteMessage;

1 usage
public class MyFirebaseMessagingService extends FirebaseMessagingService {
    @Override
    public void onMessageReceived(@NonNull RemoteMessage remoteMessage) {
```

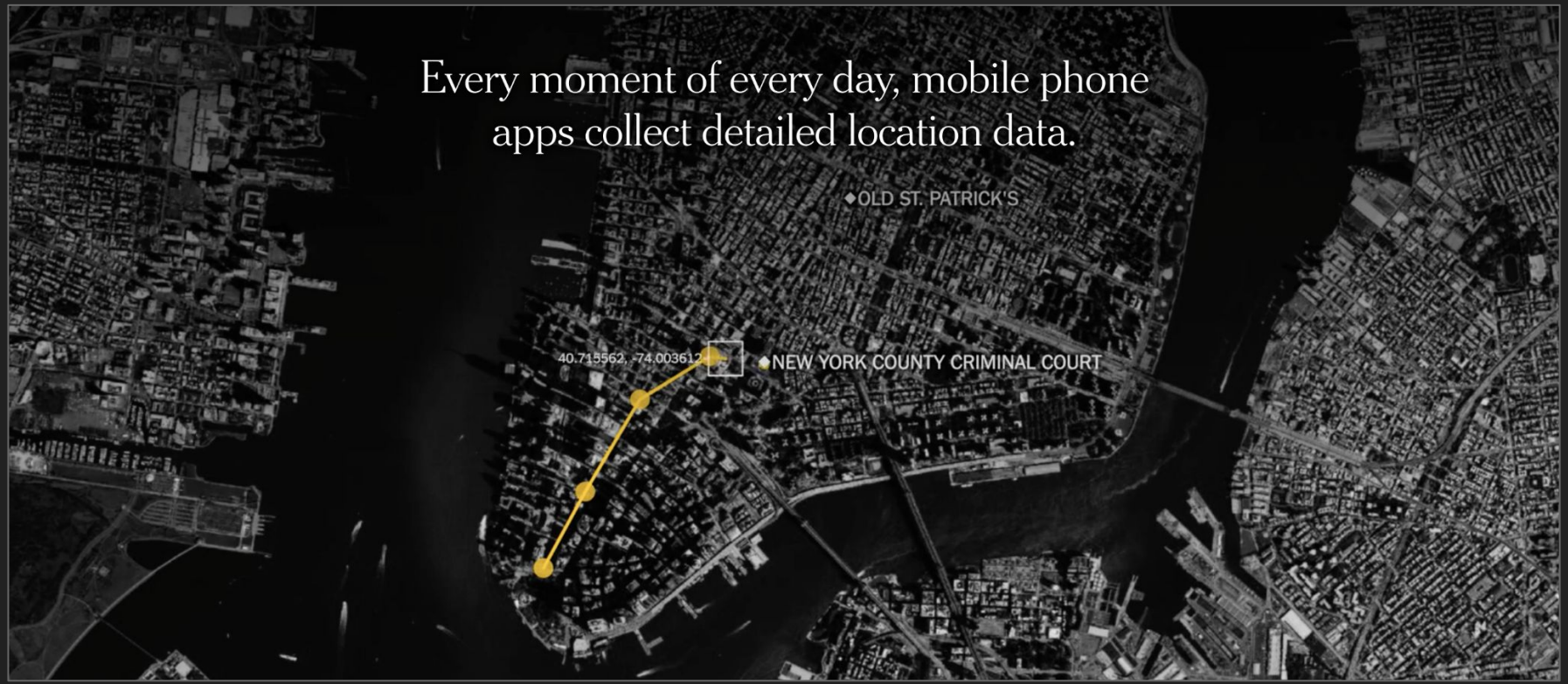
The opaqueness of TPLs and other third-party code contributes to security, privacy, and compliance risks

We want to understand the impact of TPLs on app developers' ability to comply with privacy regulations

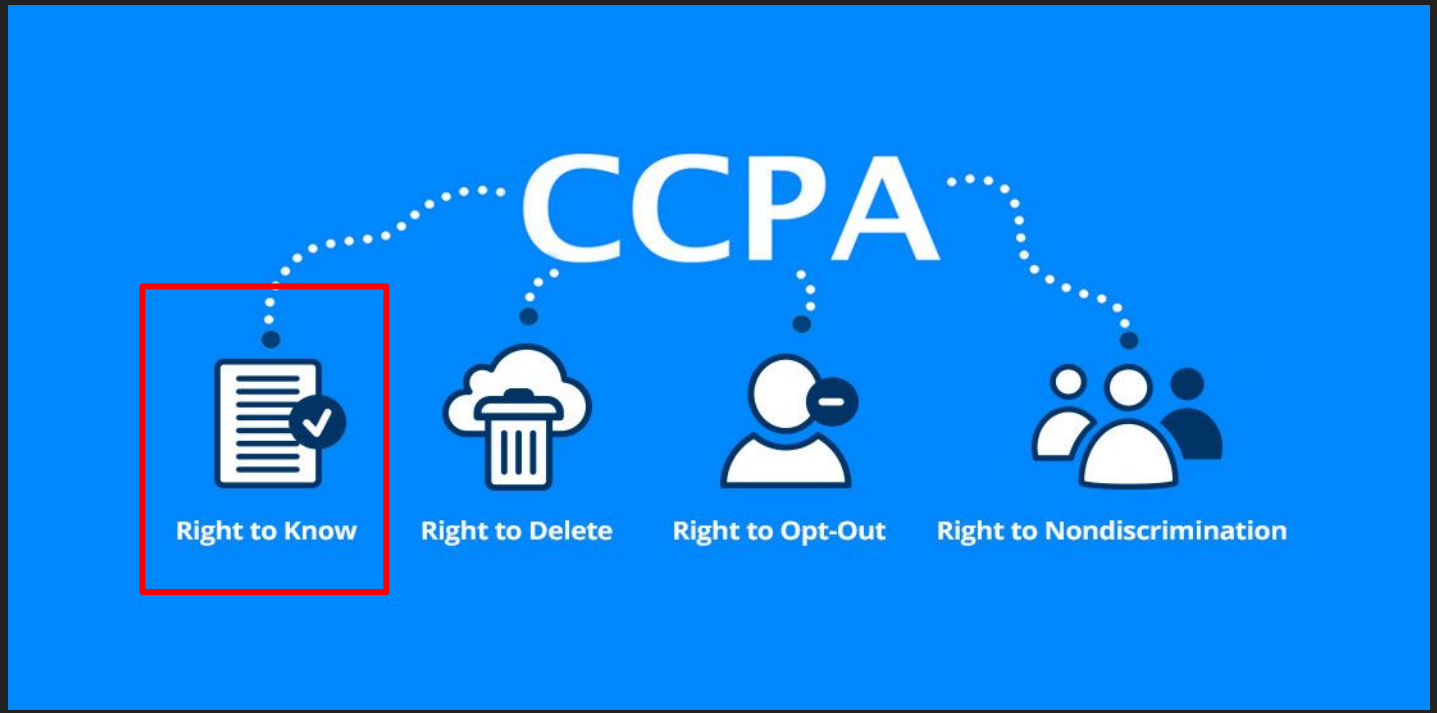
We examine the impact of TPLs on two tasks relevant to privacy compliance:

1. Compliance with the "right to know" under the California Consumer Privacy Act (CCPA) — this proposal
2. Disclosing data sharing with third parties via cloud push messaging — ongoing work

We focus on the mobile app ecosystem



1) Compliance with data subject access requests (DSAR)



*CCPA, as amended, has introduced new rights in addition to these four.

We focused on **109 apps** with **CCPA disclosures** in their privacy policies

Microsoft | Privacy Privacy dashboard Privacy report Privacy resources Privacy Statement

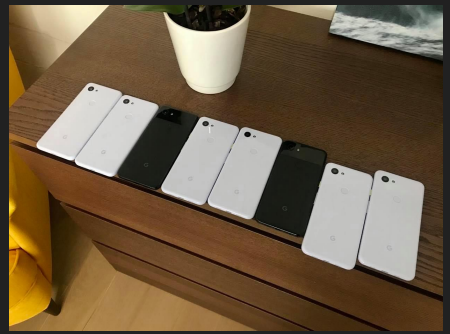
California Consumer Privacy Act (CCPA) Notice for California Consumers

Last Updated: June 2021

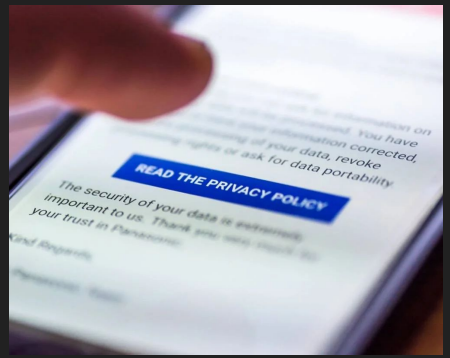
Overview

The California Consumer Privacy Act of 2018 ("CCPA") becomes effective on January 1, 2020 and creates a variety of privacy rights for California consumers.

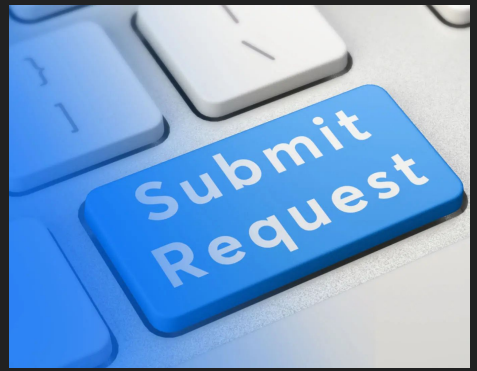
We compared the ***disclosed*** and ***actual*** data practices



==



==



?

*For more information about our results and methods, please see our full paper: https://petsymposium.org/popets/2023/popets-2023-0072.pdf

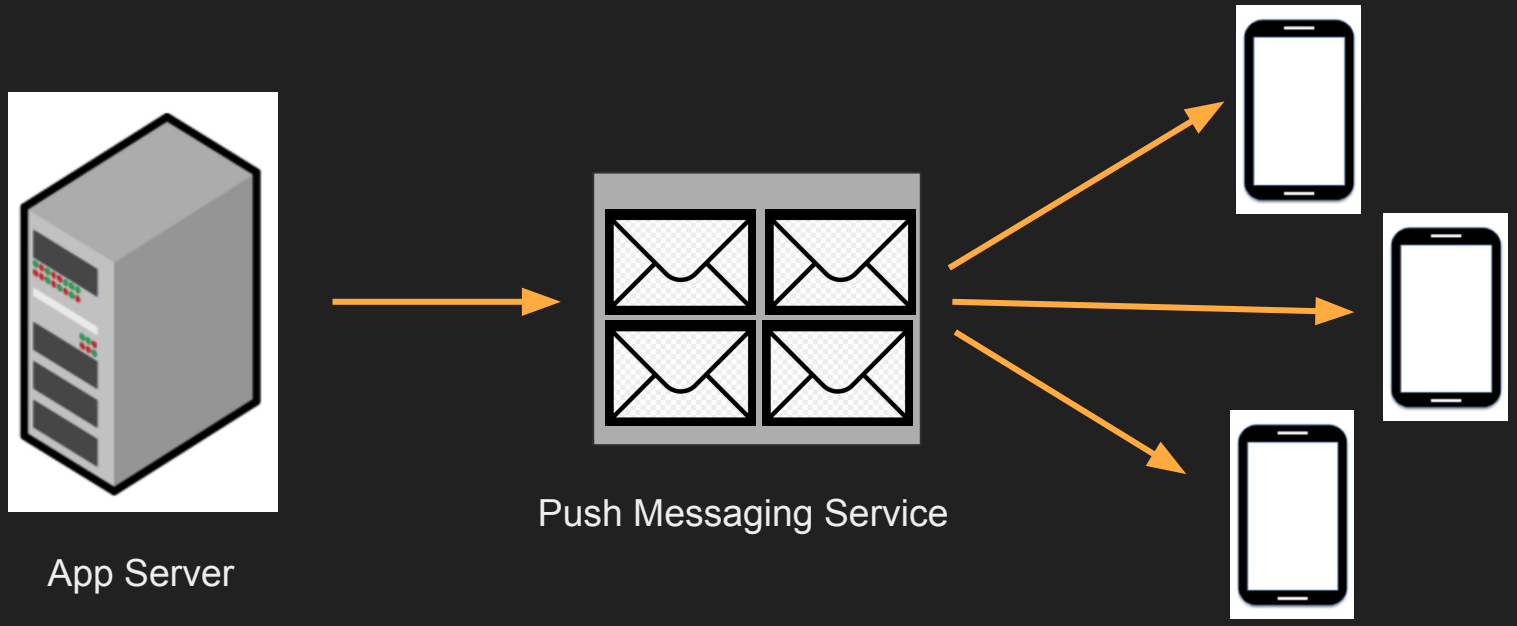
Key Findings

We observed a total of 582 unique flows of personal information from the 80 apps that completed our DSAR:

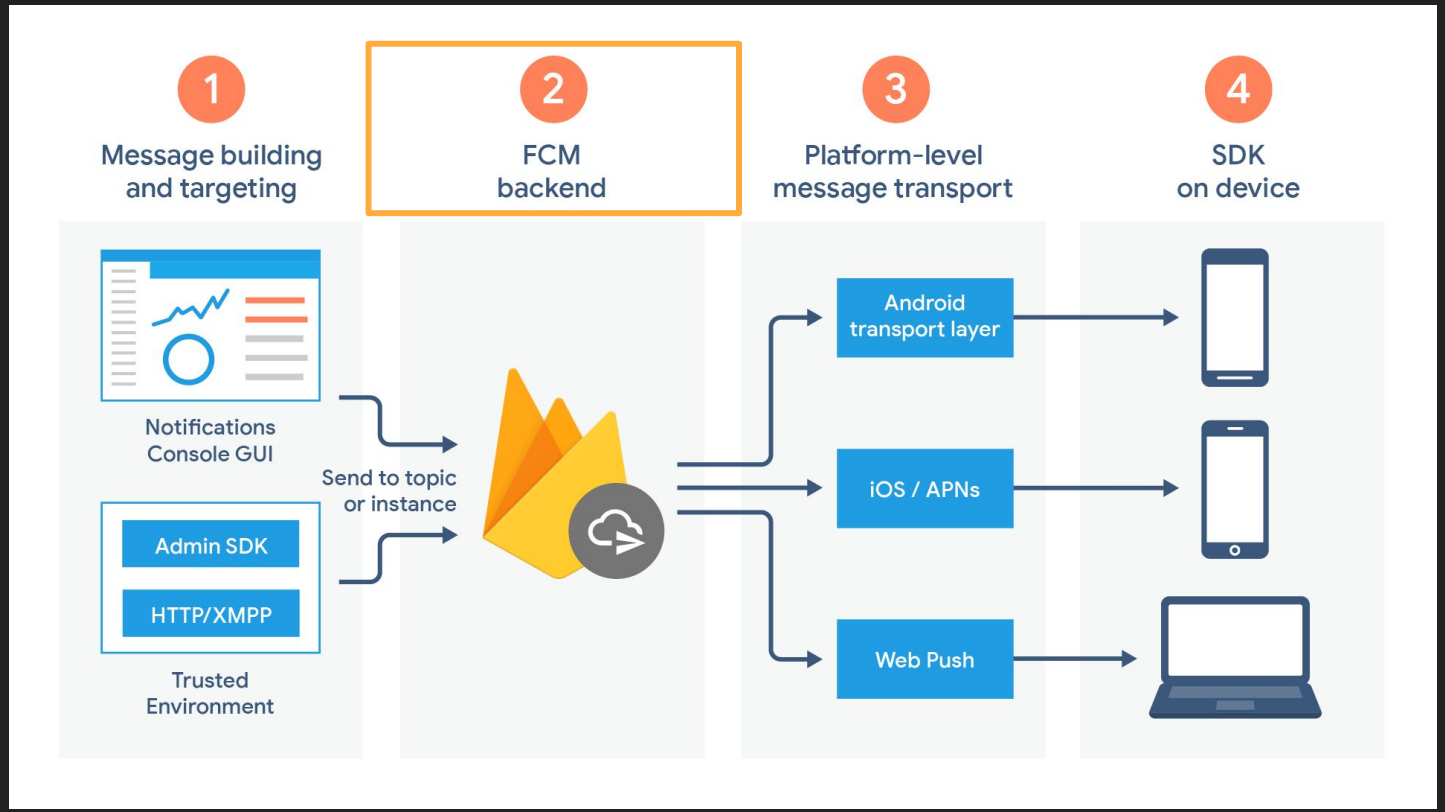
- 178 flows to third-party domains, of which only 20 (11%) were disclosed
- 404 flows to first-party* domains, of which 266 (66%) were disclosed
- The difference between these proportions was statistically highly significant ($p < 0.001$)

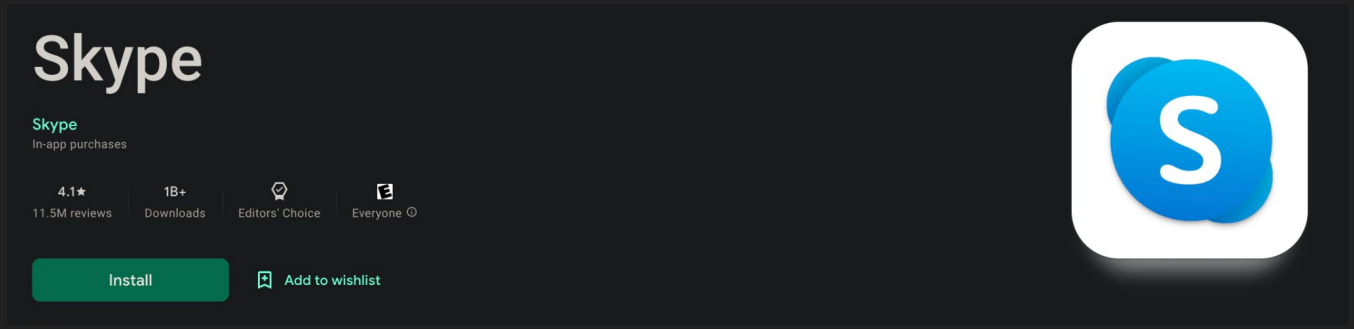
* Flows of the same personal information both to first- and third-party domains counted as a flow to first-party domain only

2) Indirect data sharing via push messaging



Google’s Firebase Cloud Messaging (FCM)






```
firebase:message:10717:START:{
  google.delivered_priority=high,
  conversationId=8:spectrens,
  google.sent_time=1666823124165,
  google.ttl=2419200,
  senderId=spectrens,
  rawPayload={
    "version":"1666823124122",
    "content":"Hey Sharon, how are you doing?",
    "contenttype":"text",
    "imdisplayname":"Nikita Samarin",
    "conversationLink":"https:\/\/azeus1-client-s.gateway.messenger.live.com\/v1\/users\/ME\/conversations\/8:spectrens",
    "composetime":"2022-10-26T22:25:24.046Z",
    "from":"https:\/\/azeus1-client-s.gateway.messenger.live.com\/v1\/users\/ME\/contacts\/8:spectrens",
    "id":"1666823124122",
    "threadtopic":"live:.cid.dd0405d0...",
    },
  recipientId=live:.cid.dd0405d0e1fdcc54
}:END:
```

28 days timeout

Takeaways

- Third-party libraries (TPLs) simplify software development but decrease visibility over software components
- The opaqueness of TPLs and other third-party code contributes to security, privacy, and compliance risks
- When it comes to responding to DSARs, developers disclosed 66% of information sent to first-party domains but only 11% sent to third-party ones
- Developers relying on push messaging services expose themselves to unanticipated third-party data sharing

Please reach out! nsamarin@berkeley.edu | @nsamarin | linkedin.com/in/nikitasamarin/