Apps, Code, Culture, and Privacy Reform: Examining Influences on Android Permissions

Jonathan Schubauer*, David Argast, and L. Jean Camp

Indiana University Bloomington Center for Security and Privacy in Informatics, Computing, and Engineering (SPICE)

PRIVACYCON

Motivation

- What are the driving factors that influence Android permissions over time?

- How has the Android permission usages changed from recent privacy reforms?

- Are there any relationships between permissions requested by applications in their respective category?

- Do privacy laws and regulations influence permission usage among Android apps?

Google removed 700K apps violating policies
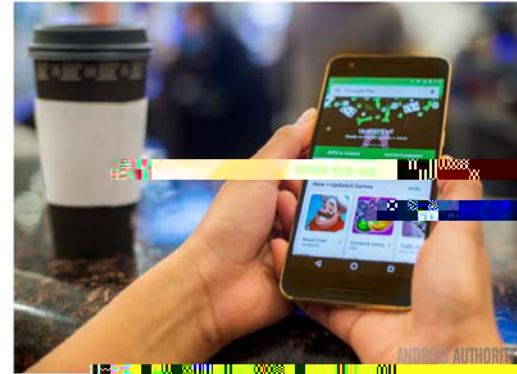
- Google removed 700,000 apps from the Play Store... policies.

PRIVACYCON

Case Study: MoChat

From Previous MoChat Privacy Policy:

"We do not collect user's personal information. User's personal information refers to <u>user's location,</u> age, address, phone, information stored in the device, and information used to identify the user or someone else when the user uses application, service or website."

But it does collect among other things:

Session Data: "connection request, server communication and data sharing and contains network test, quality of service, date, time and <u>location.</u> Please note that session and available data exclude any personal information."
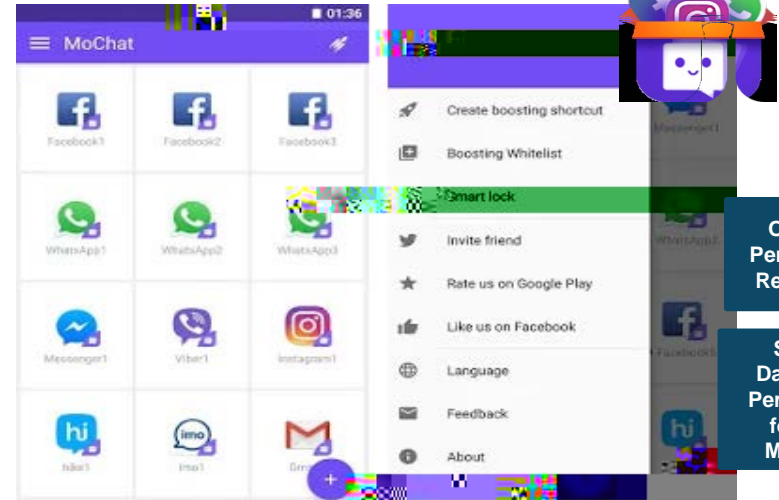
Over 400 Permissions Requested!

Several Dangerous Permissions found in Manifest!

And They Are Not Responsible In the Case of
1. **Hackers' attack**
2. Major impact caused by telecommunications operators;
3. Network or website closed due to government regulation;
4. **Virus attack**
5. Natural disasters, war and other events that can not be reasonably controlled, predicted or avoided even if they can be predicted

Methodology

Collecting and parsing app permission data
- ƒ 4623 Android Apps Pre-GDPR
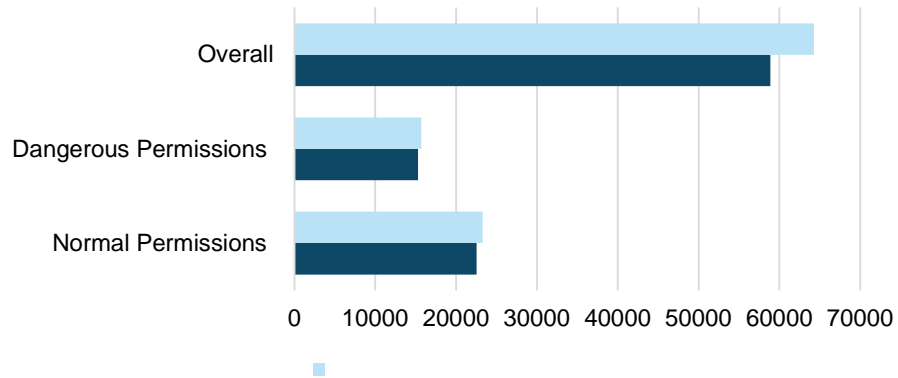- ƒ 4674 Android Apps Post-GDPR

Extracted permission data from APK files using Androguard

Analyzed relationships between app permissions requested from variables such as:
- o Location
- o Age
- o Popularity
- o Category
- o Rank
- o Size
- o IT Privacy Law
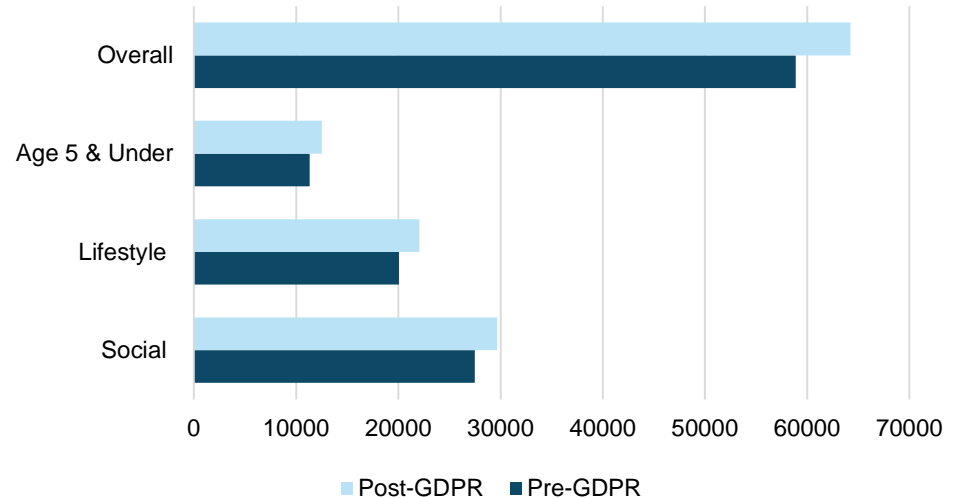
Android App Permissions Over Time

Permission Requests

Android App Permissions Over Time

- App Permissions Grow (+9%)
- Game Applications Stable (+2 P/YR)
- Social and Lifestyle Applications Grow Quickly (+4.4 P/YR)
- Statistical Analysis: P-Value < .001

Category Permission Requests

Post-GDPR   Pre-GDPR

PRIVACYCON

Dangerous App Permissions Over Time

Decreased dangerous permission requests
among all three countries:

- United States: **-14%**
- South Korea: **-26%**
-

Dangerous Permission Frequency

- Read and Write External mobile device storage remains most frequently requested.

- Location and audio access remain among top frequently occurring dangerous permission requests
  - 1358 total permissions requested to access precise location.
  - Over 800 total requests to access and record audio. **(+10% Post-GDPR)**

Top 10 Dangerous Permission Requests

Pre-GDPR   Post-GPDR
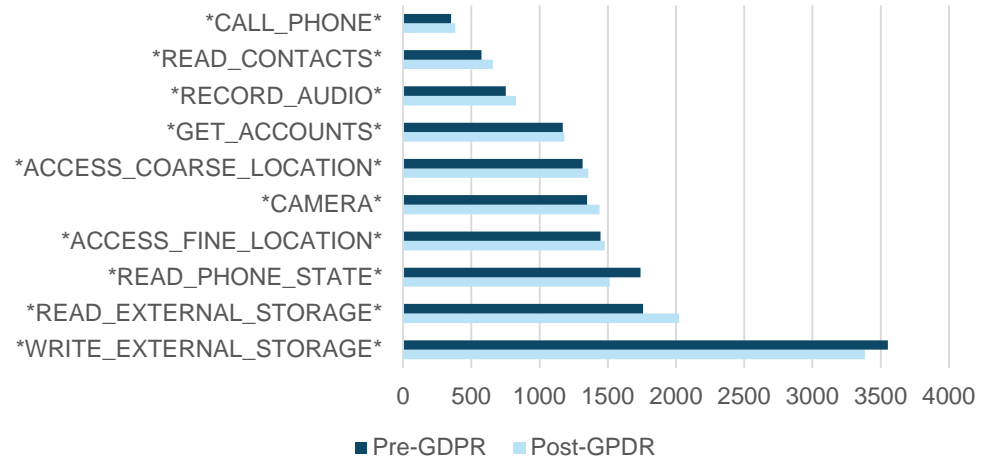
Aggregate Trends in Mobile Permissions

- Collectively both "Normal" and "Dangerous" permission requests are increasing over time.

- Frequency rates of dangerous permission requests decrease in certain categories and countries.

- Readable permission requests to access external storage and location data are increasing.

  READ_EXTERNAL_STORAGE: (**2021 requests**)

  ACCESS_FINE_LOCATION: (**1476 requests**)

Conclusion

- Limited evidence of regulatory impact
- More analysis may change conclusions
- Additional data compilation in progress
- Users should always be wary when giving access to sensitive PII as this can always end up in the wrong hands.