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)
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?
What Factors May Influence the Mobile Permission Environment?

Apps
Application Characteristics: Google Rank, Category, Popularity

Code
Android Permissions: “Normal” or “Dangerous”

Culture
Privacy Attitudes: Location, Privacy Rights, etc.

Privacy Reform
Privacy Laws
Consumer Protections, Data Collection Practices, etc.

Why do we care?
• Over-Privileged Applications
• Advertisement Libraries
Case Study: MoChat

From Previous MoChat Privacy Policy:

“We do not collect user's personal information. User’s personal information refers to user’s location, 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 location. Please note that session and available data exclude any personal information.”

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
- 4623 Android Apps Pre-GDPR
- 4674 Android Apps Post-GDPR

Extracted permission data from APK files using Androguard
Analyzed relationships between app permissions requested from variables such as:
  - Location
  - Age
  - Popularity
  - Category
  - Rank
  - Size
  - IT Privacy Law
Privacy Legislation Evolution

2012
- Official Draft of GDPR Published - January
- Personal Information Protection Act (PIPA) (SK) Enacted - March

2014
- Location Information Act Amended
- European Parliament Approves Several Proposed Amendments to the GDPR - May

2016
- Judicial Redress Act Enacted - February
- GDPR Regulation Published in EU Official Journal - May
- Google Play revises Application Guidelines - June
- Google Play Updates Privacy and Security Protocols and User-Generated Content - July
- FCC Releases Rules to Protect Broadband Consumer Privacy - November
- Standard Data Protection Model - November
- Council of EU confirms agreement of GDPR terms - December

2018
- General Data Protection Regulation Effective - May

2011
- Network Act (EC) - July
- EC Proposes EU Data Protection Reform

2013
- PIPA Amendment Act No. 11560 - March
- Asia-Pacific Economic Cooperation endorses Privacy Framework - September
- Organization for Economic Co-operation and Development Revises Privacy Principles

2015
- Electronic Communications Privacy Act Amendments Act (355) - February
- FCC published the final rule on its new “Net Neutrality” regulations (Open Internet Order) - April
- Cloud Computing Act - September
- EU declares U.S. Safe Harbor Laws Invalid - October

2017
- German Data Protection Amendment Act (GDPR) Published in Federal Law Gazette - July
- EU-U.S. Privacy Shield adopted - November
- Privacy & Data Security Update - January
- FTC updates COPPA Compliance Plan for Businesses - June
- Google Play revises Application Guidelines - June

IT Privacy Legislation (2011-2018)
Android App Permissions Over Time

Permission Requests

Overall

Dangerous Permissions

Normal Permissions

Post-GDPR  Pre-GDPR

Facebook:
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
Decreased dangerous permission requests among all three countries:

- United States: -14%
- South Korea: -26%
- Germany: -10%

Overall decreased dangerous permission request frequency: -17%
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)
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.