Data Protection in Mobile Apps

EUI DPO Meeting in Florence, 7 November 2019

Dr Robert RIEMANN, EDPS IT Policy Unit
Daily Internet Time spent per Capita by Device

Source: Zenith
© Statista 2019

Additional Information: Worldwide; Zenith; 2011 to 2018
Teardown of Samsung Galaxy Note 10

- Accelerometer
- Gyroscope
- Barometer
- Light Sensor
- Compass
- Microphone
- Cameras
- Fingerprint Sensor
- GPS
Development of Mobile Apps

- every mobile app is developed on top of many building blocks
- building blocks offer simple API to carry out complex tasks:
  - Sensor API to take photos, record audio, get geo localisation, etc.
  - Software Development Kit (SDK) to e.g. authenticate against Facebook using cryptography
- most apps use building blocks provided by third parties

(Source: android.com)
Privacy of Mobile Phone Users at Stake

Top Travel Apps Fail The Privacy And Security Test

Davey Winder  Senior Contributor
Cybersecurity
I report and analyse breaking cybersecurity and privacy stories

No Body's Business But Mine: How Menstruation Apps Are Sharing Your Data

Monday, September 9, 2019

How Apps on Android Share Data with Facebook - Report

Saturday, December 29, 2018
Example: Health Insurance Endorsed Health App

- Mobile app Ada helps users to log health conditions and provides automated diagnoses.
- App incorporated Facebook login and in-app analysis with Amplitude.
- In Q1 2018, TÜV Nord certified ADA: ISO/IEC 27001.
- In 09/2019, app was found to transfer identifiers and health data to third parties, amongst others: session id, android ad id, user id, device id, age, sex, and user input like finding=UrinaryIncontinence.

The EDPS Mobile App Inspection comes certainly

Step 1: Guidance (link)

Step 2: Awareness Training in Florence

Step 3: Inspection
Hands-On Exercise in Groups (inverse class)
# Work in Groups: Data Collection Practices of Mobile Apps

Use your smartphone to investigate data processing practices of any app!

<table>
<thead>
<tr>
<th>Transparency</th>
<th>App Permissions</th>
<th>Consent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who is the controller?</td>
<td>Which permissions do apps have?</td>
<td>In the life cycle of an app, when are users asked to give consent?</td>
</tr>
<tr>
<td>How to contact the DPO?</td>
<td>Can you link these permissions to app purposes?</td>
<td>How can valid consent be obtained on smartphones?</td>
</tr>
<tr>
<td>Which personal data is processed by the app?</td>
<td>Are some permissions too broad or not always necessary?</td>
<td>How is consent withdrawn?</td>
</tr>
</tbody>
</table>

Find the shortest and longest policy for apps on your phone!  
Find the app with most and least permissions on your phone!
Plenum Debate: App Stores

- Are App Stores Data Controllers, Processors or Joint-Controllers?

Apple App Store Statistics

Google Play Store Developer Dashboard

(more: Apple Developer)  
(more: Google Blog)
Progressive Web Apps: Concept

- PWA are websites optimised for modern mobile browser and their web APIs.
- They provide several features that give them the same user experience advantages as native apps (offline, notifications, etc). Read more.
Progressive Web Apps: Advantages

Data Protection Advantages
● no app stores means less 3rd parties
● one version for all terminal devices for less complexity/documentation
● no interference with other installed apps (shared contacts, calendar, etc.)
● open standards, linkable, searchable

Examples
● https://www.instagram.com
● https://mobile.twitter.com
● https://m.uber.com
● https://m.alibaba.com
● https://tinder.com
● https://app.ft.com
Wrap-Up
Personal Data Processing with Mobile Apps: Cheat Sheet

Is a mobile app required or is a mobile-friendly website (PWA) enough?

### Transparency
- Employ layered data protection notices and in-context notices
- Consider target audience (children, etc.)

### Privacy by Default/Design
- Limit processing to the strictly necessary
- Use as few permissions as possible
- Employ optional permissions if possible
- Monitor security throughout lifecycle
- Test the app and assess all its data flows

### Third-Party Services
- Avoid 3rd-party services whenever possible
- Conclude data processing agreements
- Monitor for changes of their terms of service

Check [EDPS Guidelines on Mobile Apps and Devices!](https://edps.europa.eu)
Homework
Mobile App Inventory

Some EU institutions and bodies required several months to compile the inventory of their web services for the EDPS inspection.

1. Please update your mobile app inventory.
2. Please update your related records of processing activities (EU-DPR Art. 31)
3. Please ensure that data processing agreements with third-parties are in place.

The Mobile App Inspection team may inquire technical documentation and software from controllers to carry out their analysis.
Your Questions
Further Reading

- EDPS Guidelines: [Mobile Applications (2016), Mobile Devices (2015)]
- WP29 Opinion: [Opinion 02/2013 on apps on smart devices]
- Progressive Web Apps: [https://developer.mozilla.org/en-US/docs/Web/Progressive_web_apps]
Credits

● Images:
  ○ Crowd with Mobile Phones: unsplash/@bpro1360 (unsplash license)
  ○ Smart Phone Teardown: ifixit/Sam Goldheart (Creative Commons BY-NC-SA license)
  ○ Florence Photo: Pexels/@Tookapic (Creative Commons Public Domain)
  ○ Magnifying Glass: unsplash/@olloweb (unsplash license)

● Screenshots:
  ○ https://www.zdnet.com/article/mobile-security-these-health-apps-arent-good-for-your-phone-or-your-privacy/
  ○ https://www.privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruation-apps-are-sharing-your-data
  ○ https://privacyinternational.org/appdata