Digital Data Flows Masterclass #5: Mobile Apps

July 25, 2019
Future of Privacy Forum

The Supporters

150+ Companies

25+ Leading Academics

15+ Advocates and Civil Society

5 Foundations

The Mission

Bridging the policymaker-industry-academic gap in privacy policy
Developing privacy protections, ethical norms, & responsible business practices

The Workstreams

Connected Cars
Student Data

Location & Ad Tech
Internet of Things

Ethics & De-identification
Smart Cities
 DIGITAL DATA FLOWS MASTERCLASS: EMERGING TECHNOLOGIES

<table>
<thead>
<tr>
<th>Curriculum</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session 1: Artificial Intelligence and Machine Learning</td>
<td>25 October 2018 (Brussels)</td>
</tr>
<tr>
<td>Session 2: Location Data: GPS, Wi-Fi, and Spatial Analytics</td>
<td>27 November 2018 (Brussels)</td>
</tr>
<tr>
<td>Session 3: De-identification: Multi-party Computing,</td>
<td>30 January 2019 (Brussels)</td>
</tr>
<tr>
<td>Differential Privacy, and Homomorphic Encryption</td>
<td></td>
</tr>
<tr>
<td>Session 4: Advertising Technologies: Online Data Flows,</td>
<td>1 May 2019 – Virtual</td>
</tr>
<tr>
<td>Behavioral Targeting, and Cross-Device Tracking</td>
<td></td>
</tr>
<tr>
<td>Session 5: Mobile Apps: Operating Systems, Software</td>
<td>25 July 2019 – Virtual</td>
</tr>
<tr>
<td>Development Kits (SDKs), and User Controls</td>
<td></td>
</tr>
<tr>
<td>Session 6: Biometric Data: Facial Recognition, Voice, and</td>
<td>TBD – Virtual</td>
</tr>
<tr>
<td>Digital Fingerprint</td>
<td></td>
</tr>
<tr>
<td>Session 7: Transportation and Mobility: Video Analytics,</td>
<td>TBD – Virtual</td>
</tr>
<tr>
<td>Sensors, and Connected Infrastructure</td>
<td></td>
</tr>
<tr>
<td>Session 8: Tracking in Physical Spaces: Retail</td>
<td>TBD – Virtual</td>
</tr>
<tr>
<td>Technologies, Smart Homes, and the “Internet of Things”</td>
<td></td>
</tr>
</tbody>
</table>

All sessions are free and support remote participation.
Receive updates on the full course at: [www.fpf.org/classes](http://www.fpf.org/classes) (recordings of previous classes are available)

- [www.fpf.org/classes](http://www.fpf.org/classes)
- archived videos and slides available
- year-long program
Guest Experts for Class 5: Mobile Apps

Christy Harris  
*Director of Technology & Privacy Research, Future of Privacy Forum*

Daniel Smullen  
*Software Engineering Ph.D. Candidate, Carnegie Mellon University, Institute for Software Research*

Fares Alraie  
*Chief Information Security Officer, Mattel, Inc.*
Agenda

Part 1: Basic Concepts  
Daniel Smullen (45 min + 15 min Q&A)
- Basic concepts – from “apps” to “APIs”
- Operating systems (OS)
- Permissioned data vs. non-permissioned data
- Design of APIs: software architecture, scalability, reliability, and data portability

Part 2: Identifiers and Third Parties  
Fares Alraie (45 min + 15 min Q&A)
- Mobile identifiers and identifiability
- Designing secure apps
  - Sharing data with “third parties”
  - Ad Libraries
  - Software Development Kits (SDKs)
Part 1: Basic Concepts

- Basic concepts – from “apps” to “APIs”
- Operating systems (OS)
- Permissioned data vs. non-permissioned data
- Design of APIs: software architecture, scalability, reliability, and data portability
basic concepts

- Mobile Apps
- Hardware vs. Software
- Source Code vs. Software
- Front End vs. Back End
- Walled Gardens
mobile apps

What is an “app”? 

Mobile OS Global Market*:
- Android: 76.03%
- iOS: 22.04%
- KaiOS: 0.79%
- Windows: 0.21%
- Samsung: 0.21%

*Source (June 2019): gs.statcounter.com

& emerging app ecosystems…:
“software” – a generic term for the instructions needed for a computer to do specific tasks

- **System software** serves as a base for applications – e.g. operating systems (OSs), compilers, disk formatters, text editors and utilities helping the device to operate more efficiently.
- **Programming software** is a set of tools to aid developers in writing programs.
- **Application software** is intended to perform certain tasks. E.g. games, educational apps, etc.
### Source Code vs. Software

<table>
<thead>
<tr>
<th>Open Source</th>
<th>Closed Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free</td>
<td>Paid</td>
</tr>
<tr>
<td><img src="penguin.png" alt="Penguin" /></td>
<td><img src="ubuntu.png" alt="Ubuntu" /> (paid version for organizations)</td>
</tr>
<tr>
<td><img src="github.png" alt="GitHub" /> <img src="gitlab.png" alt="GitLab" /> <img src="sourceforge.png" alt="SourceForge" /></td>
<td><img src="office.png" alt="Office" /></td>
</tr>
</tbody>
</table>

**Source Code Repositories:**
e.g. Github, GitLab, SourceForge

**Programming languages:**
C++, Java, Swift, Python, Javascript

**Development Environments:**
Xcode, Microsoft Visual Studio
front end vs. back end

Front end ("client side")
- The visible style and design of the app
  - Text, colors, buttons, navigation menus

Back end ("server side")
- Server architecture
- Database administration
- Backup
walled gardens
permissioned data
Example 1: Location Services

“Location Services” derives precise location using many sensors to scan for data – GPS/Satellite, nearby Cell Towers, nearby Wi-Fi access points (routers etc.), Bluetooth signals

Apps request permission from the user to access location using Location Services.

- purpose string
- permission architecture
- policy guidelines prohibit inferring location through other means
Example 2: Bluetooth

Radio-wave signals designed for communicating and connecting devices within short range (~10 meters) using low energy.

Bluetooth “Beacons” are inexpensive radio transmitters that send one-way Bluetooth signals that can be detected by any device equipped to receive them (if within proximity).
Application Programming Interfaces (APIs)
End of Part 1
Questions?
Part 2: Identifiers and Third Parties

- Mobile identifiers
- Designing apps for privacy and security
  - Sharing data with “third parties”
  - Ad Libraries
  - Software Development Kits (SDKs)
# Mobile Device Identifiers

| Universal Device Identifier (UDID) | The manufacturer’s persistent and unique ID for the actual mobile device. *In 2012-2013, Apple and Google disabled access to these persistent IDs in order to protect consumer privacy.*
| Example: 2b6f0cc904d137be2e17302 35f5664094b831186 |
| Media Access Control (MAC) Address | The manufacturer’s persistent and unique ID for each network interface card on the mobile device.
| Example: B8:53:AC:B1:12:87 |
| Advertising Identifier | Device identifier assigned by the Operating System to be used by apps for advertising and marketing purposes.
| Apple: IDFA  
Android: AAID | • Persistent over time and across different apps/developers  
• Can be rotated by the user (or zeroed out in iOS)  
• Sent along with the ”Limit Ad Tracking” flag, if applicable
| Example: 20AEE9FB-D269-45E9-8FC7-184021CF7BEF |
Mobile platform controls

Limit Ad Tracking

iOS allows developers to target ads to app users using a unique ID called “Identifier for Advertising” (IDFA).

Previously, users could select “Limit Ad Tracking” (LAT) and a “flag” would be sent. Most treated this as an opt out of behaviorally targeted advertising (OBA).

In iOS 10, LAT began zeroing out the IDFA. This prevents the previously permitted “frequency capping, attribution, conversion events, estimating the number of unique users, advertising fraud detection, and debugging” uses.
Encryption and Hashing of Identifiers

Common Encryption Methods: SHA1, MD5

Note: one-way hashing provides privacy and security benefits (cannot easily be reversed back to the original ID), yet a hashed identifier can still serve as a persistent ID across time and platforms.

---

Source: IAB Mobile Identity Guide for Marketers
A software development kit (SDK or devkit) is a set of software development tools, libraries, relevant documentation, code samples, processes, and/or guides for app developers to create apps.

Common Uses of Third-party SDKs:
• Social media integration, e.g. Facebook SDK
• Advertising, e.g. AdMob, ChartBoost, ironSource
• Analytics, e.g. Crashlytics, Flurry, Google Analytics
• Cloud storage, e.g. Amazon S3
• Special features, e.g. Maps SDKs (Mapbox, HERE, etc.)
Designing for Privacy and Security in Apps

**Design**
- Privacy Impact Assessment
- Design Review
- Vendor Due Diligence
- Security Requirements

**Develop**
- Threat Model
- Data Inventory / Audit
- Security Scanning
- Code Review
- Penetration Testing

**Release**
- Vulnerability Management
- Security Updates

**Security Consultation**
End of Part 2

Questions?