

Digital Data Flows Masterclass #5: **Mobile Apps**

July 25, 2019





BRUSSELS PRIVACY HUB

Future of Privacy Forum

	The Supporters			
150+	25+	15+	5	
Companies	Leading Academics	Advocates and Civil Society	Foundations	
	The M	ission		

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

The Workstreams

Connected CarsLocation & Ad TechEthics & De-identificationStudent DataInternet of ThingsSmart Cities



DIGITAL DATA FLOWS MASTERCLASS: EMERGING TECHNOLOGIES



Curriculum

Date

25 October 2018 (Brussels)

27 November 2018 (Brussels)

30 January 2019 (Brussels)

1 May 2019 - Virtual

25 July 2019 - Virtual

Session 1: Artificial Intelligence and Machine Learning

Session 2: Location Data: GPS, Wi-Fi, and Spatial Analytics

Session 3: De-Identification: Multi-party Computing, Differential Privacy, and Homomorphic Encryption

Session 4: Advertising Technologies: Online Data Flows, Behavioral Targeting, and Cross-Device Tracking

Session 5: Mobile Apps: Operating Systems, Software Development Kits (SDKs), and User Controls

Session 6: Biometric Data: Facial Recognition, Voice, and TBD - Virtual Digital Fingerprints

Session 7: Transportation and Mobility: Video Analytics, Sensors, and Connected Infrastructure

Session 8: Tracking in Physical Spaces: Retail Technologies, Smart Homes, and the "Internet of Things"

TBD - Virtual

TBD - Virtual

- www.fpf.org/classes
- archived videos and slides available
- year-long program





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

₀

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

- 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

- Mobile identifiers and identifiability
- Designing secure apps
 - · Sharing data with "third parties"
 - Ad Libraries
 - Software Development Kits (SDKs)

Fares Alraie (45 min + 15 min Q&A)

Daniel Smullen (45 min + 15 min Q&A)



Part 1

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...:





hardware vs. software



iPhone 7 (source: ifixit)



"**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

Open Source Closed Source



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 • ||||||| IIIII. € ||||||. < ||||||



walled gardens





permissioned data

〈 Set	tings Privacy		
7	Location Services	On	>
	Contacts		>
	Calendars		>
	Reminders		>
	Photos		>
*	Bluetooth Sharing		>
!	Microphone		>
	Speech Recognition		>
6	Camera		>

HUB

÷	App permissions	:
Y	Twitter	
0	Camera	
Ŀ	Contacts	۰
9	Location	٠
Ļ	Microphone	٠
Ľ,	Phone	٠
	SMS	•
	Storage	•
= :	Additional permissions 1 more	

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.



PRIVACY



- 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

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. <i>In 2012-2013, Apple and Google disabled access to these persistent IDs in order to protect consumer privacy.</i> 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	Persistent over time and across different apps/developers
Android: AAID	 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.

Privacy	Advertising	
Limit Ad Trackir	ng	
Reset Advertisi	ng Identifier	
About Advertising &	Privacy	
Important		
In iOS 10.0 and later, the v	value of advertisingIde	ntifier is all zeroes when

the user has limited ad tracking.



Encryption and Hashing of Identifiers

APPLE IDENTIFIER FOR ADVERTISING (IDFA) ENCRYPTION EXAMPLES

RAW Version

SHA1 Version

MD5 Version

AEBE52E7-03EE-455A-B3C4-E57283966239 A7FE134E3C8E805D2FB72151146AB7841F275C36 E69A1078552E13F2734C22322708BD95

GOOGLE ADVERTISING ID ENCRYPTION EXAMPLES

 RAW Version
 97987BCA-AE59-4C7D-94BA-EE4F19AB8C21

 SHA1 Version
 D42B4890298FC4821A52C11F24E2A8AC06FA10B0

 MD5 Version
 BA06C008973B8A1BFF6E087C6149227F

^ source: IAB Mobile Identity Guide for Marketers



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

Software Development Kits



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





End of Part 2 Questions?

