

Smartphone Privacy & Security

USP Presentation
Sakshi Garg & Bin Liu

Outline:

- Privacy and Security threats in Smartphones
- Android Permissions
- Readings
- Blackphone
- Class Activity
- Urgent Challenges
 - Malware detection
 - Fine-grained access control of resources

Privacy and security threats in Smartphones:

Privacy and security threats in Smartphones:

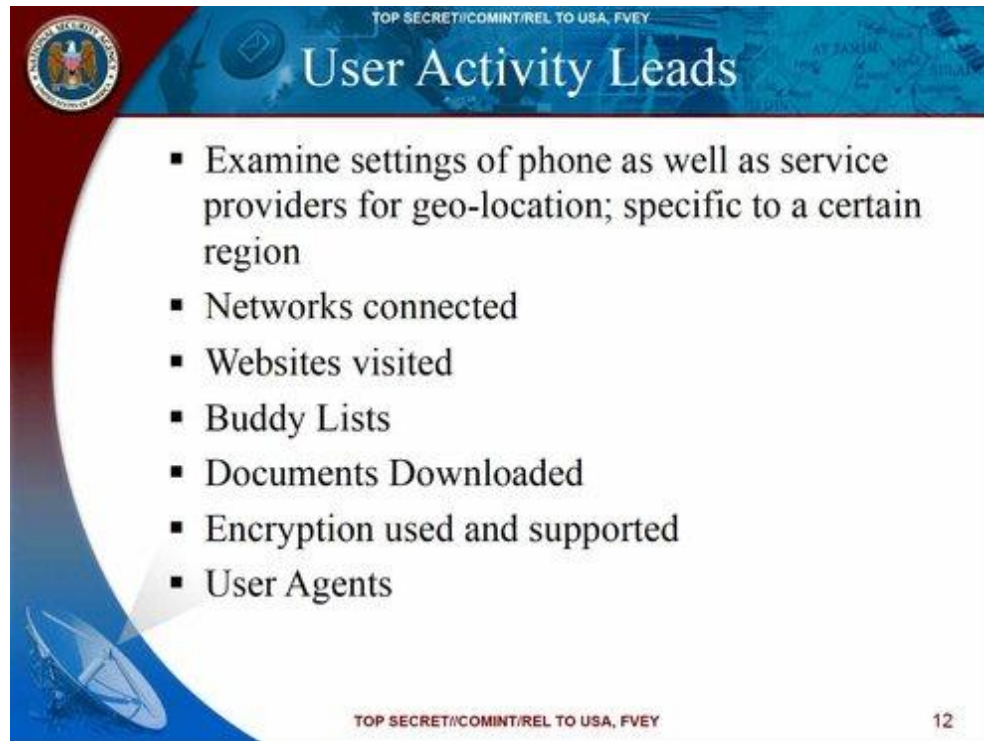
- Malware
- Spyware
- Vulnerable applications
- Phishing attacks
- Browser exploits
- Wi-fi sniffing
- Network exploits
- Lost or stolen device
- Impersonation
- Reselling your phone
- The data available on phone

What data do smartphones have access to?

What data do smartphones have access to?

- Contact lists
- emails
- messages
- pictures
- Videos
- phone calls
- Calendar
- Notes
- Location
- Microphone
- Bluetooth
- Reminders
- facebook
- twitter

Spy Agencies Tap Data Streaming From Phone Apps!! (Jan 27 2014)



TOP SECRET//COMINT//REL TO USA, FVEY

User Activity Leads

- Examine settings of phone as well as service providers for geo-location; specific to a certain region
- Networks connected
- Websites visited
- Buddy Lists
- Documents Downloaded
- Encryption used and supported
- User Agents

TOP SECRET//COMINT//REL TO USA, FVEY

12

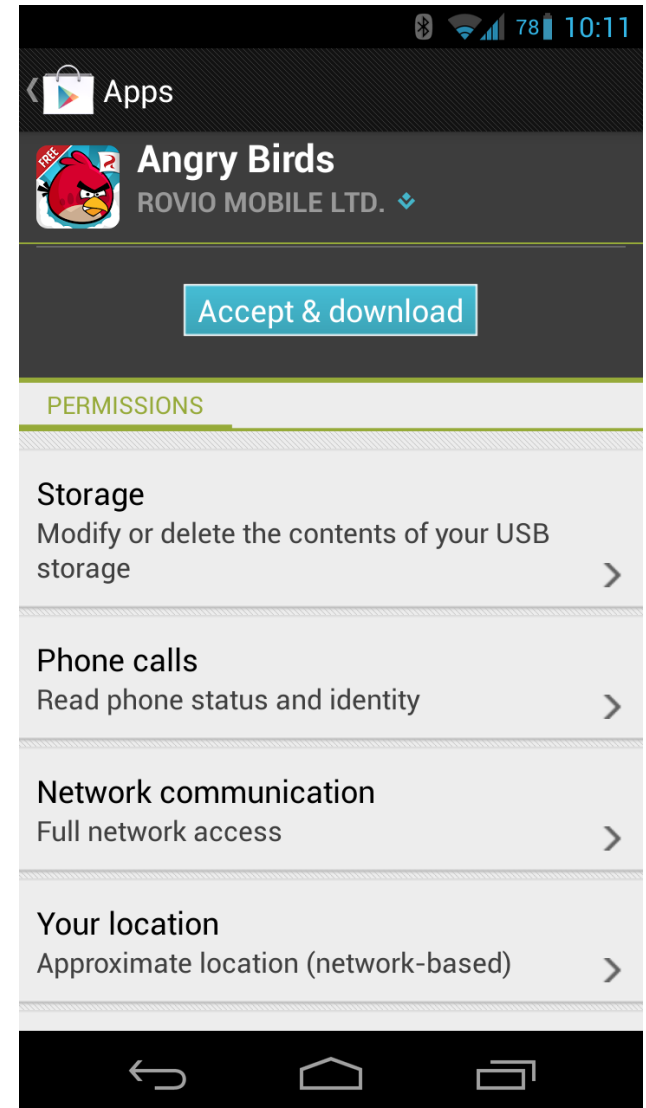
One of several undisclosed classified document provided by Snowden.

Spy Agencies Tap Data Streaming From Phone Apps!!

- The N.S.A. and Britain's Government Communications Headquarters were working together on how to collect and store data from dozens of smartphone apps.
- The project was named "The mobile surge".
- This include applications like **Angry Birds**, **facebook**, **flicker**, **flixster**.
- Just by updating the android software, users send more than 500 lines of data about phone's history and use.

Android Permissions:

- Android permission system is intended to inform users about the risks of installing applications.
- Android users are provided with permission display that appears when users have selected an application to download.
- The display helps to understand that how the information is accessed and users can cancel the installation if permissions are excessive or objectionable



Why permissions are useless in Android?

- Users have no choice but to accept permissions to install the application.
- In most of the cases users do not understand these permissions.
- Vague and confusing terms are used.
- Difficult for users to make informed decisions while installing applications.
- There are around 130 permissions.



Reading 1 !!

Android Permissions: User Attention, Comprehension, and Behaviour

Adrienne Porter Felt, Elizabeth Ha,
Serge Egelman, Ariel Haney,
Erika Chin, and David Wagner.

Reading Summary !!

- 2 usability studies:
 - Internet survey of 308 Android users
 - Interviewed and observed 25 Android users.
- 17% participants paid attention to permissions and 97% failed to answer comprehension questions.
- Low awareness of permission warning and comprehension.

Recommendations for improving usability of Permissions:

- Negative reviews from peer users should be provided.
- Re-organizing and re-naming categories.
- Category headings should be more relevant and convey the right purpose.
- Warnings should convey risks.
- More permissions should be classified as non-dangerous and hidden by default.

One of the biggest security risk!



Phones get lost or stolen.

**How to ensure the security of your
smartphone?**

Mobile passwords:

PIN : Earlier versions of iphone
40% people do not use Pin in
their phones

Unlock Pattern: Most of the
Android Phones

Fingerprint Mechanism: iphone
5s



Blackphone



Blackphone: Privacy and Security focused Android smartphone

- Developed by Silent circle.
- To be released in June 2014.
- 4.7-inch HD IPS screen
- >2GHz quad core CPU
- 2 GB RAM
- 16 Gb storage



What is special about this phone?

- Lets you send peer-to-peer Encrypted texts, Phone Calls, Video Calls and File transfers.
- Silent Circle Apps: provides access to internet services bypassing the government surveillance.
- Provides internet access through VPN.
- Disconnect Secure Wireless.



Android vs. PrivatOS

Feature	Android Default	PrivatOS Enhancement
Search	Trackable	Anonymous
Bundled Apps	Many, with privacy disabled by default	Few, and all privacy-enabled
Wi-Fi usage	Always on for geolocation and user tracking	Smart disabling of all Wi-Fi except trusted hotspots
App permissions	All-or-nothing	Fine-grained control in a single interface
Communications tools	Traceable dialer, SMS, MMS, browser. Vulnerable to spoofed cell networks and Wi-Fi.	Private calls, texting, video chat, file exchange up to 100MB, browsing, and conference calls
Updates	Supplied infrequently after carrier blessing	Frequent secure updates from Blackphone directly
Remote Wipe & Anti Theft	Requires use of centralized cloud account	Anonymous
Business Model	Personal data mining for tracking and marketing	Delivering privacy as a premium, valued feature

Might not be that good of an idea!!

- The cost of the phone is \$630

+

\$120 subscription yearly to use encrypted suite.

- To communicate using blackphone, the other person needs to have blackphone or use silent circle apps on their android or iPhone.
- New OS and hence higher scope of teething troubles and bugs.

Challenge: Malware

(Especially on Android)

Malicious Smartphone Application

Sensitive Information Exposure

Abuse of phone services (Phone, Message)

Root Exploitation

Package Repacking

Update Attack

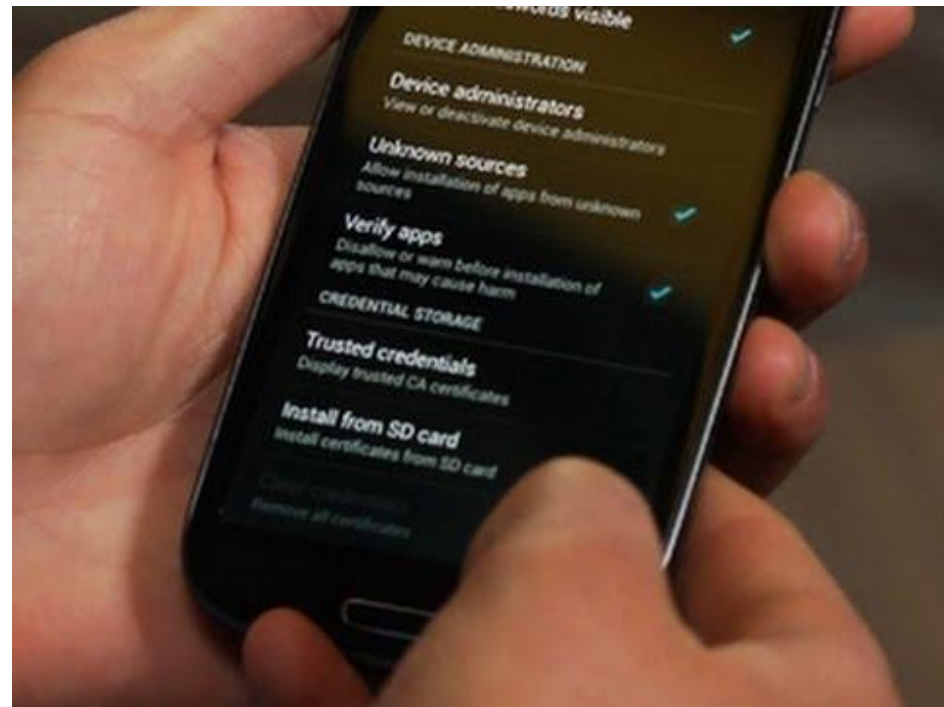


Class Discussion

KNET: “Keep your Android device safe from malware”

Are these security measures enough?

Please find a possible attack in a security perspective.



Why so many malware apps?

Abuse of openness.

- Reduce Openness
 - Review process by human, restrict APIs (iOS)
- Maintaining order
 - Automatic detection (Google Bouncer)
- Tradeoff? Arms Race?



Google Bouncer

Analyzing Apps on Google Play



<http://hypeline.se/wp-content/uploads/2012/02/Android-Bouncer.png>

- External network available. (:--))
- Run the app in an QEMU emulator for 5 minutes
- Using a Google account with made-up name & email
- Simulate UI clicks (Predictable?)
- Dynamic analysis (Static analysis as well)

<https://www.duosecurity.com/blog/duo-tech-talks-dissecting-the-android-bouncer>

<https://jon.oberheide.org/files/summercon12-bouncer.pdf>

Analysis of Malware

- **Dynamic Analysis**

- Run the app in simulator
- Apply sufficient input (Measuring code coverage)
- Create fake data / responses
- => Slow, incomplete

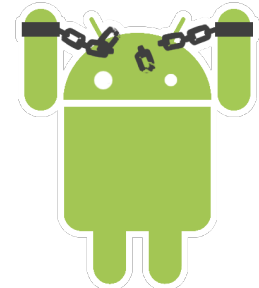
- **Static Analysis**

- Reverse Engineering
- Examining unusual cases
- Tracking data flow
- => Weak against code obfuscation

Fighting against malware apps

Anti-malware apps

Especially for jailbroken / rooted devices



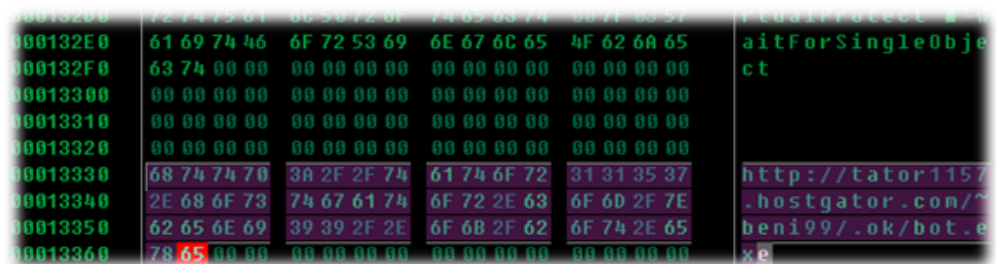
<http://www.xda-developers.com/wp-content/uploads/2013/12/Android-Root.png>

Sophisticated anti-malware analysis

Side channels, etc.

<http://www.csc.ncsu.edu/faculty/jiang/>

<http://www.cs.ucdavis.edu/~hchen/>



<http://blog.malwarebytes.org/intelligence/2013/03/obfuscation-malwares-best-friend/>

Challenge: Resource Control

Phone resource control

Fine-grained controls are **needed**

“Google Map reads my contacts”

“This game consume too much data traffic”

Existing Solutions

iOS: Privacy Panel

Android: Permissions, AppOps

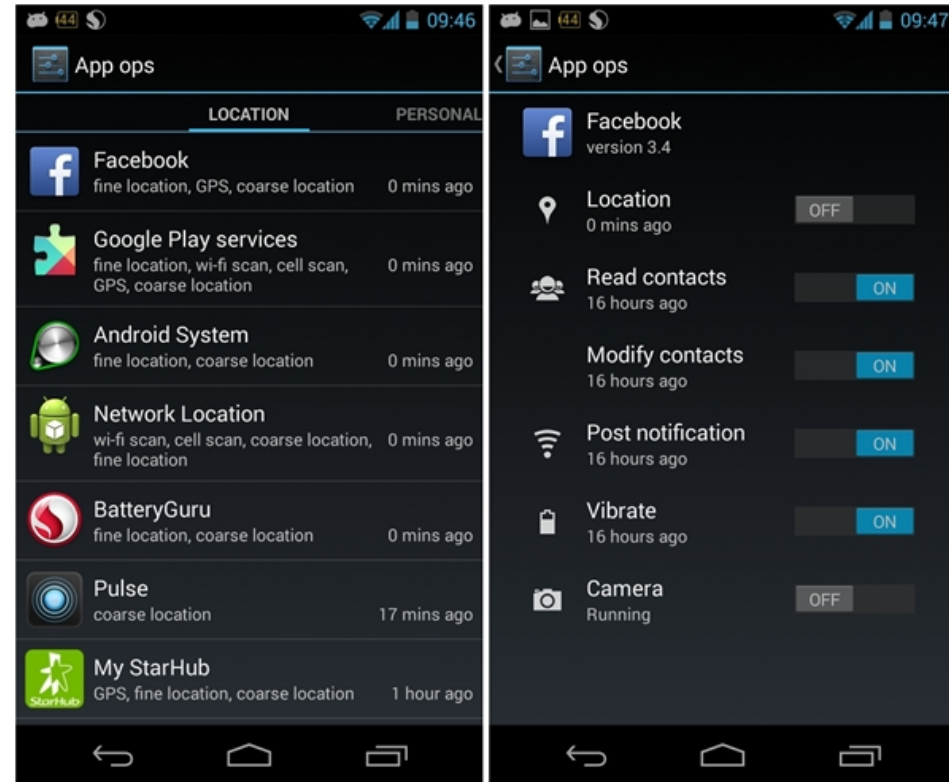
PDroid, LBE, XPrivacy, PMP

iOS Privacy Settings



<http://0.tqn.com/d/ipod/1/0/S/O/-/ios-6-privacy.jpg>

Android AppOps (4.3 only)



http://images.dailytech.com/image/Permission_manager_Screen_shots_News.jpg

Users are overwhelmed with options!



http://images.fanpop.com/images/image_uploads/Lisa-simpson-angry-lisa-simpson-

Reduce Users' Burden

Predictive

- Better default settings

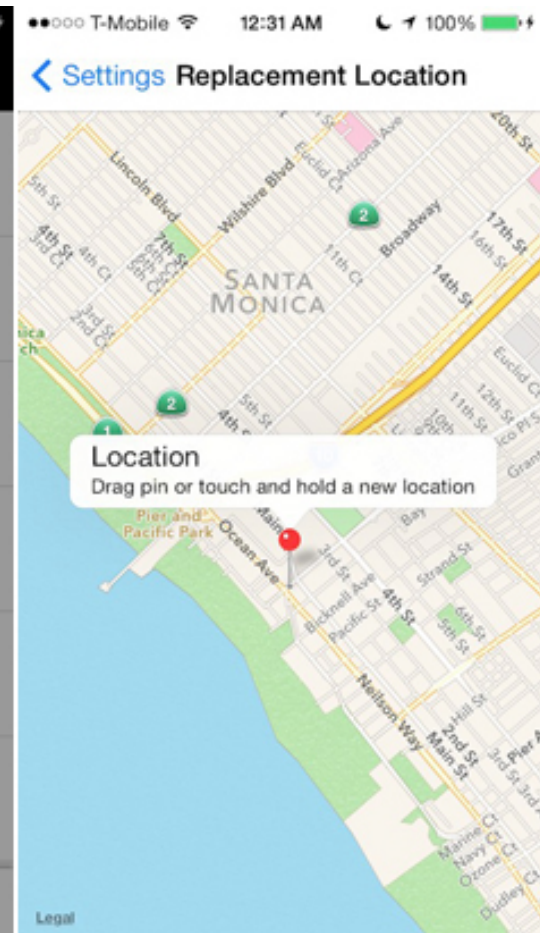
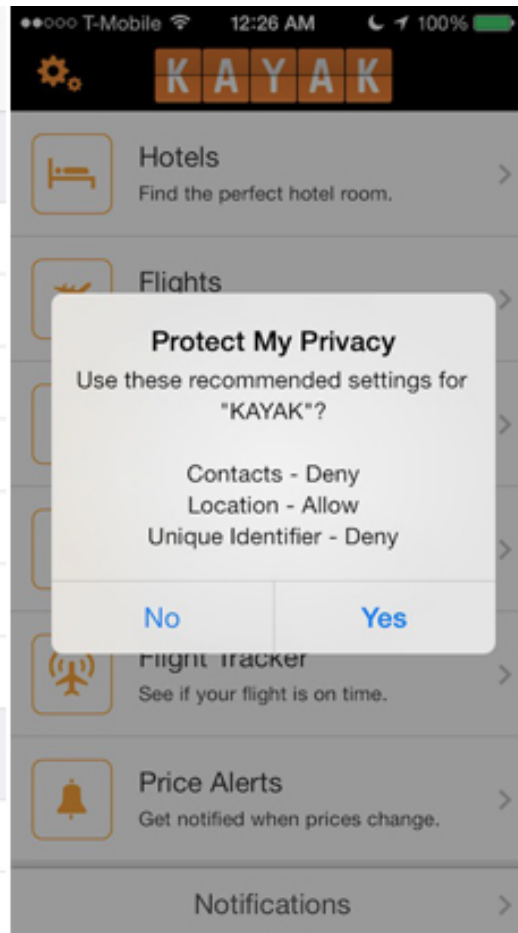
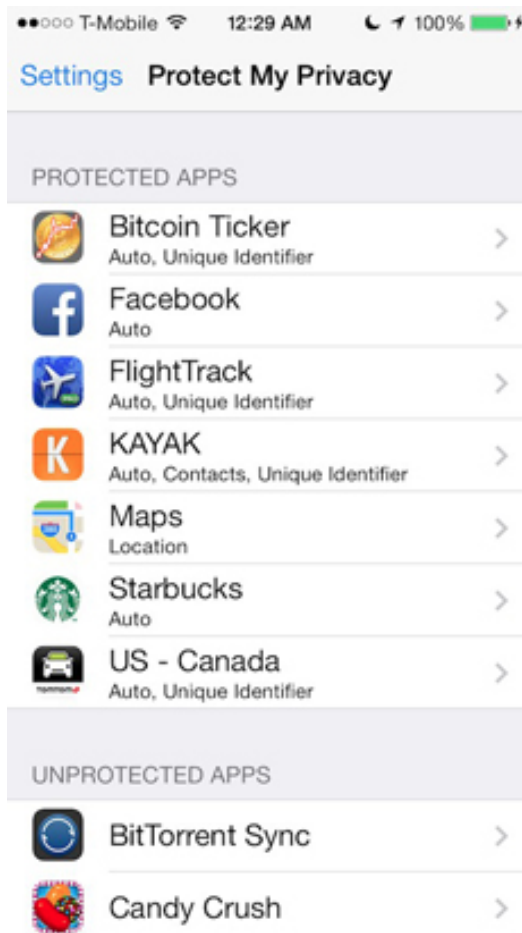
- Labeling only for some of the apps

Abstraction & Aggregation

- Answering several questions only

Crowd-powered Smart Default

ProtectMyPrivacy (PMP)



Crowd-powered Smart Default

XPrivacy: <https://crowd.xprivacy.eu/>

Rows marked with a grey background will be restricted when fetched; **bold text** means data was used

Votes * deny/allow	Exceptions (yes/no)	CI95 ±% **	Restriction
121 / 179 40%	7 / 293	5.5	accounts
171 / 125 58%	0 / 296	5.6	browser
177 / 119 60%	0 / 296	5.6	calendar
218 / 78 74%	0 / 296	5.0	calling
114 / 182 39%	0 / 296	5.5	clipboard
197 / 99 67%	0 / 296	5.3	contacts
156 / 140 53%	0 / 296	5.7	dictionary
174 / 122 59%	0 / 296	5.6	email
195 / 101 66%	0 / 296	5.4	identification
55 / 241 19%	0 / 296	4.4	internet
23 / 15 61%	0 / 38	14.9	ipc
240 / 56 81%	0 / 296	4.5	location
141 / 155 48%	0 / 296	5.7	media
192 / 104 65%	0 / 296	5.4	messages
173 / 123 58%	0 / 296	5.6	network
163 / 133 55%	0 / 296	5.6	nfc
116 / 180 39%	0 / 296	5.5	notifications
54 / 81 40%	0 / 135	8.2	overlay
227 / 69 77%	0 / 296	4.8	phone
96 / 70 58%	0 / 166	7.4	sensors
200 / 96 68%	0 / 296	5.3	shell
78 / 218 26%	0 / 296	5.0	storage
120 / 176 41%	0 / 296	5.6	system
97 / 199 33%	0 / 296	5.3	view

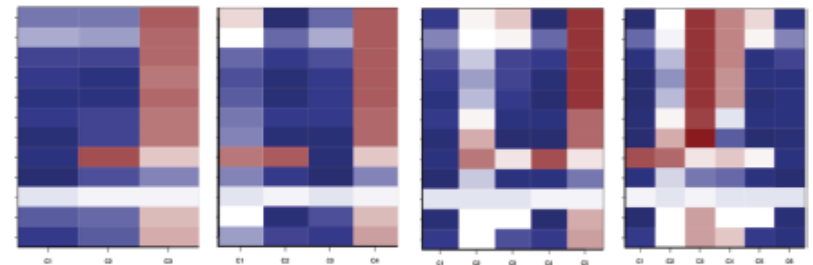
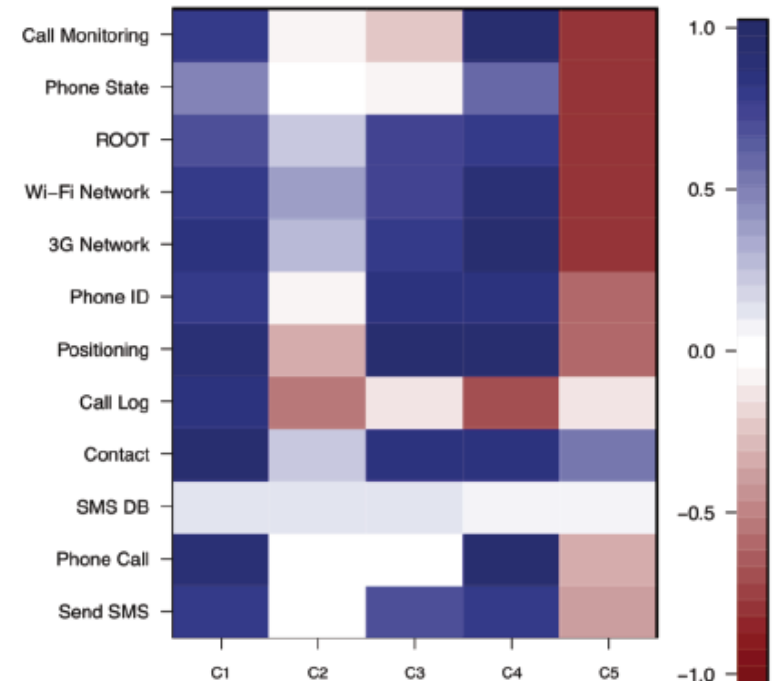
Facebook

We need personalization

Profile 1 (25.4%)			Profile 2 (15.8%)		
✗ Call Log +	✓ Call Monitoring	66%	✗ Positioning +	✓ Wi-Fi / 3G	32%
✗ Call Log +	✓ Wi-Fi / 3G	63%	✗ Positioning +	✓ ROOT	31%
✗ Call Log +	✓ Phone State	62%	✗ Call Log +	✓ Wi-Fi / 3G	29%
✗ Call Log +	✓ ROOT	61%	✗ Positioning +	✓ Phone State	28%
✗ Call Log +	✓ Positioning	61%	✗ Call Log +	✓ ROOT	28%

Profile 3 (17.8%)			Profile 4 (8.8%)		
✗ Positioning + ✗ Wi-Fi / 3G		86%	✓ Positioning + ✗ Wi-Fi / 3G		60%
✗ Positioning		85%	✓ Positioning + ✗ ROOT		58%
✗ Positioning + ✓ SMS DB		83%	✓ Positioning+ ✗ Call Monitoring		54%
✗ Positioning + ✗ ROOT		82%	✓ Positioning + ✗ Phone State		49%
✗ Positioning + ✗ Phone ID		80%	✗ Wi-Fi Network		42%

Profile 5 (14.8%)			Profile 6 (17.2%)		
✓ Positioning + ✓ ROOT		40%	✓ Call Log + ✓ Call Monitoring		81%
✓ Positioning + ✓ 3G / Wi-Fi		40%	✓ Call Log + ✓ Wi-Fi / 3G		79%
✓ Phone ID + ✓ ROOT		39%	✓ Call Log + ✓ Phone State		78%
✓ Phone ID + ✓ 3G / Wi-Fi		39%	✓ Call Log + ✓ ROOT		77%
✓ 3G / Wi-Fi + ✓ ROOT		37%	✓ Call Log + ✓ Phone ID		75%



Smart Default

Intelligently predict users' preferences

Minimum users' burden

Transparent decision making process

First step of this (shamelessly): our paper! :)

Bin Liu, Jialiu Lin, and Norman Sadeh, ***Reconciling Mobile App Privacy and Usability on Smartphones: Could User Privacy Profiles Help?***, To appear in WWW'14, Seoul.

http://www.cs.cmu.edu/~bliu1/publications/Bin_WWW2014.pdf

Thanks!