Context-Specific Access Control

Conforming Permissions With User Expectations

Amir Rahmati, Harsha V. Madhyastha

Sensitive User Data

Messages

Contacts

Camera

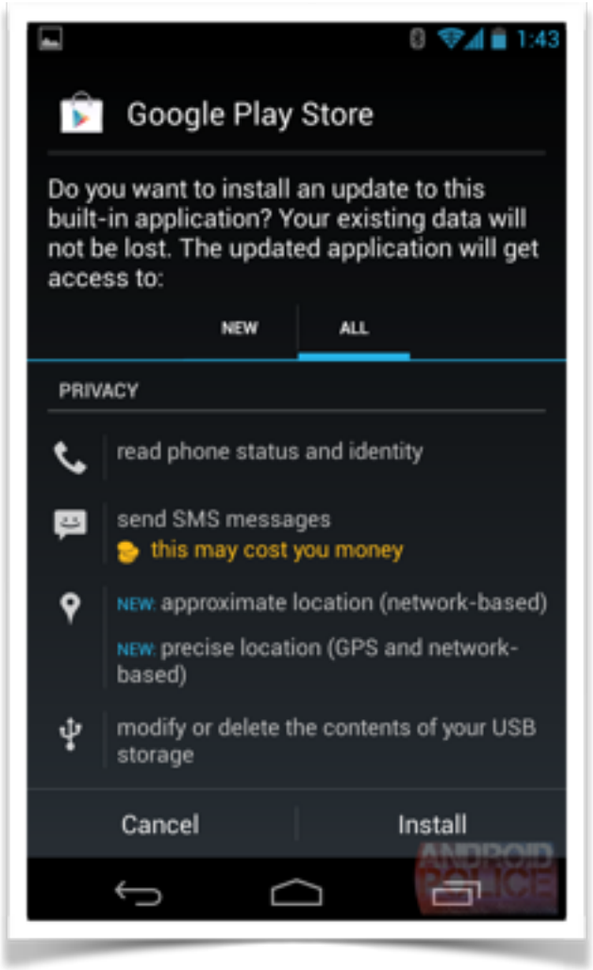
Emails

Files

Location

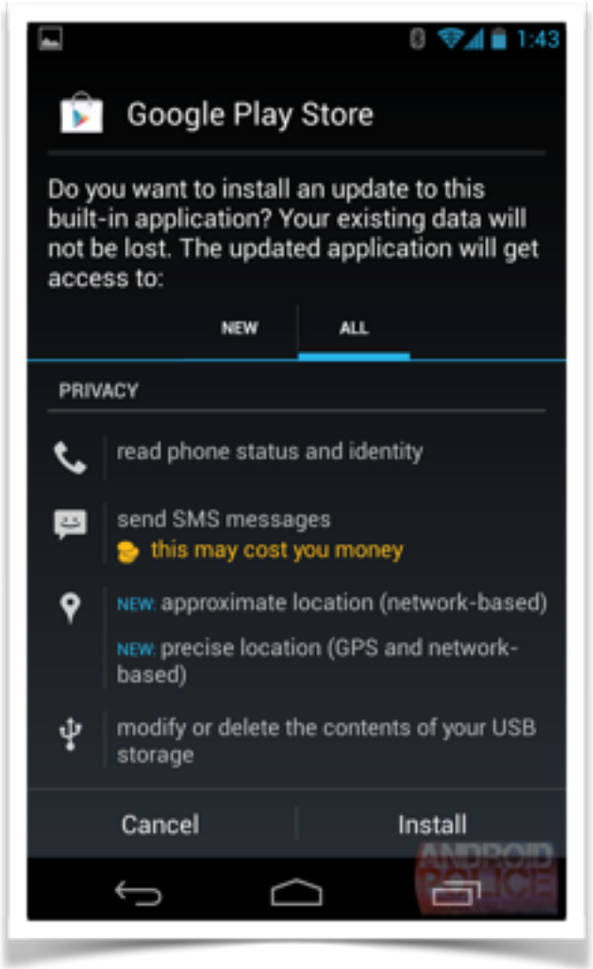
Access Control Systems

Access Control Systems

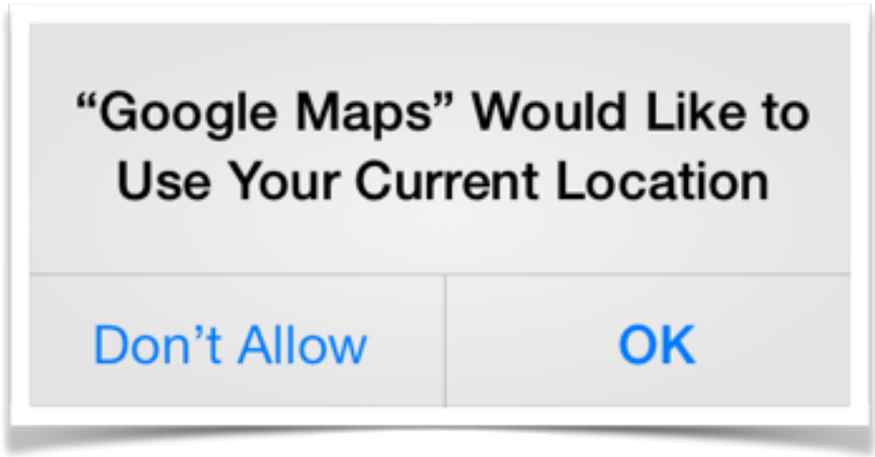


Install Time

Access Control Systems



Install Time



First Use

Access Control Systems

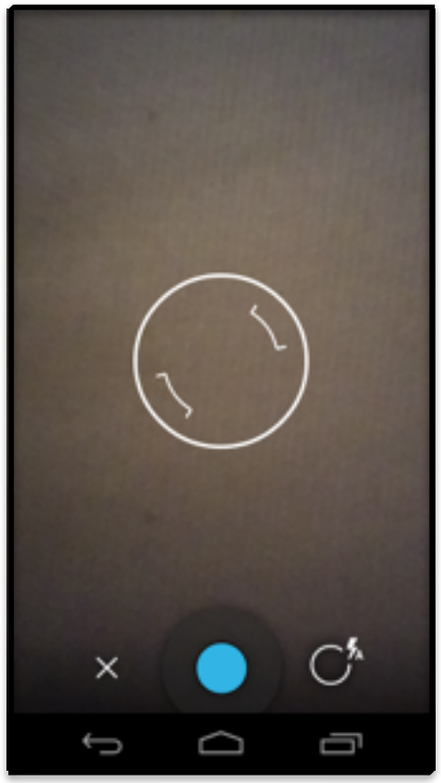
Install Time

First Use

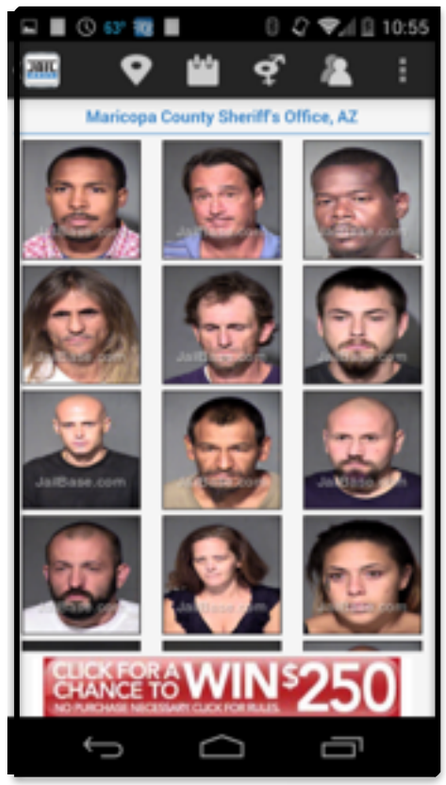
Context Specific Access Control

Context Specific Access Control

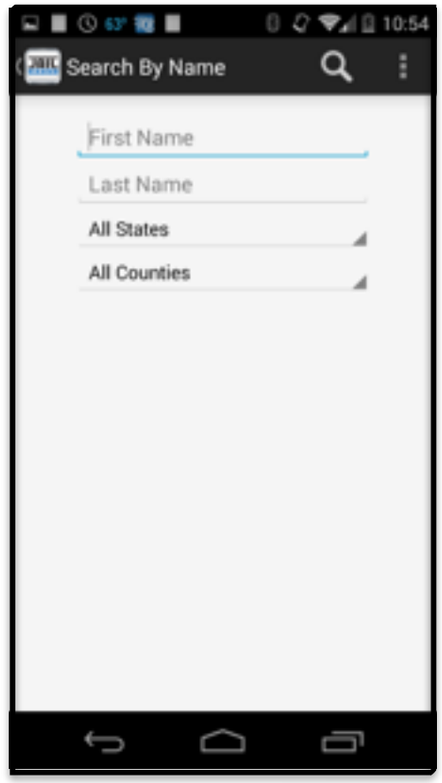
Home



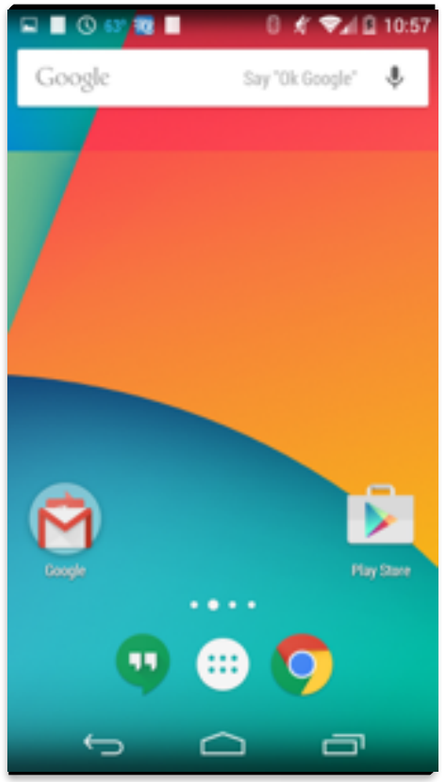
Face Recognition



Arrests



Search

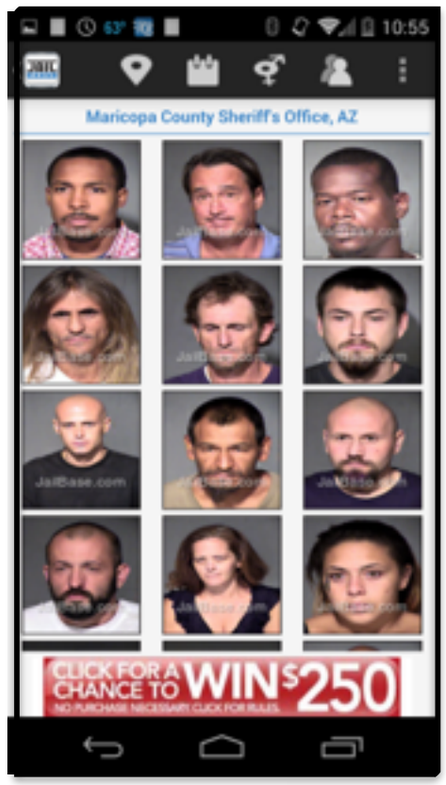


Background

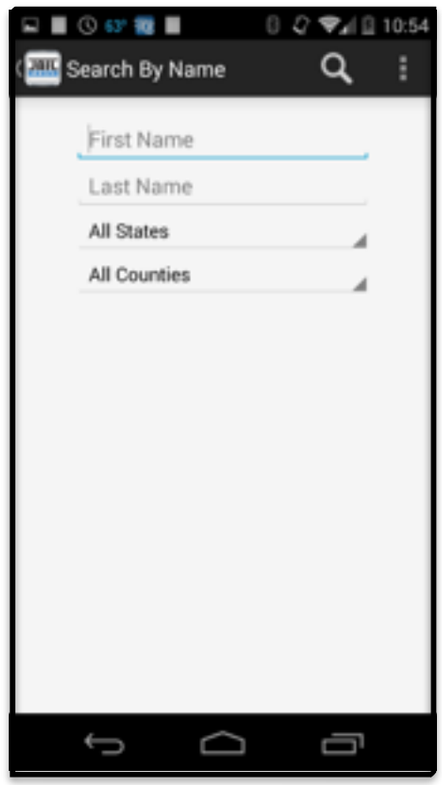
Context Specific Access Control

Home

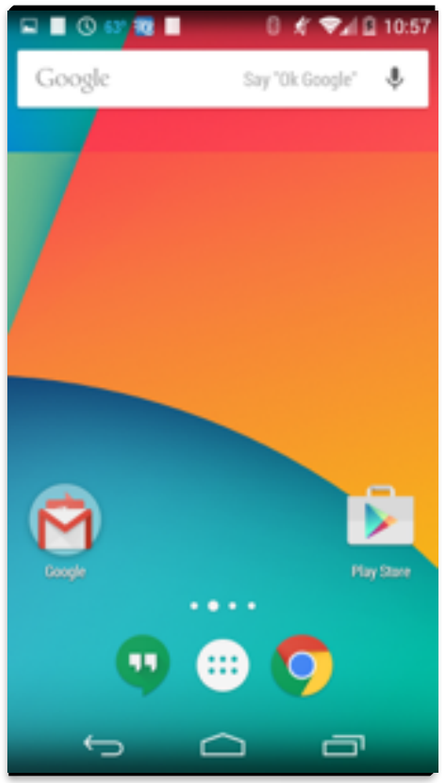
Face Recognition



Arrests



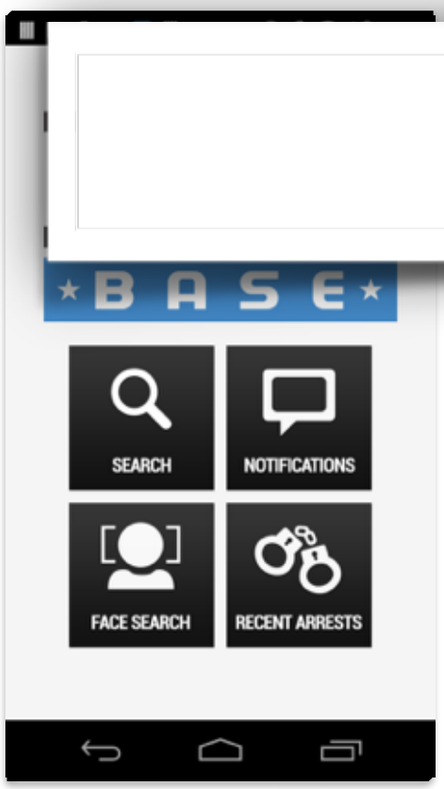
Search



Background

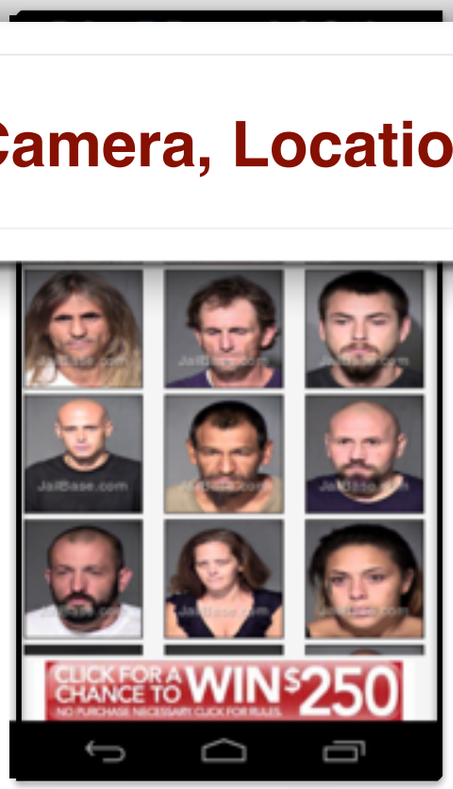
Context Specific Access Control

Camera, Location



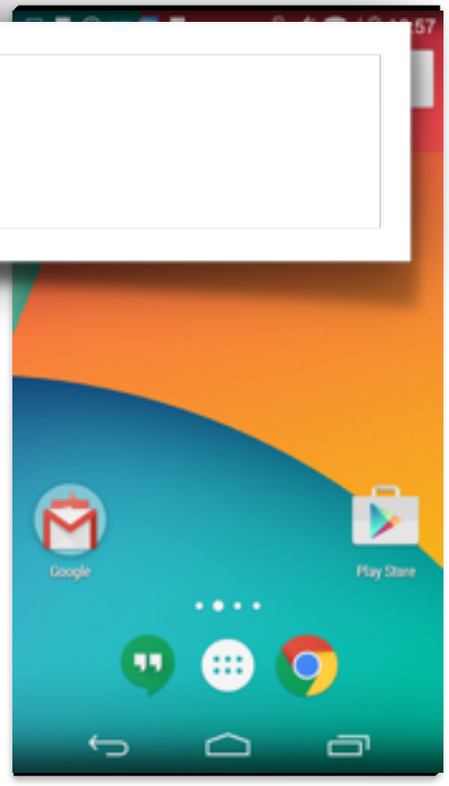
Home

Face Recognition



Arrests

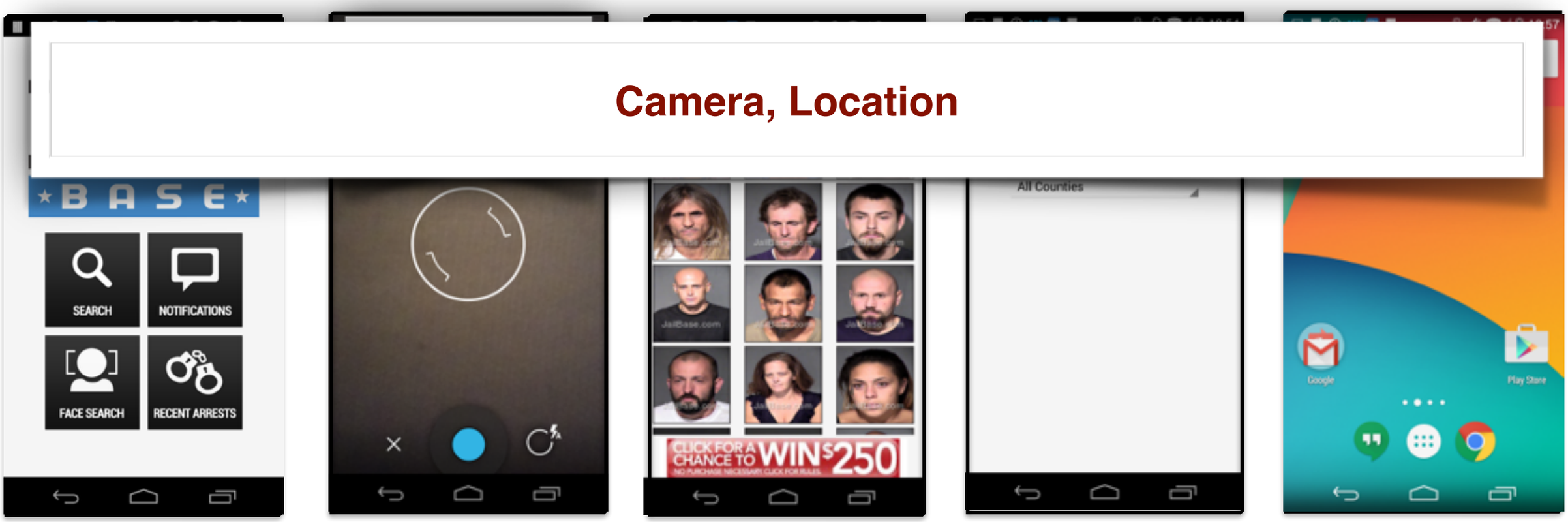
Search



Background

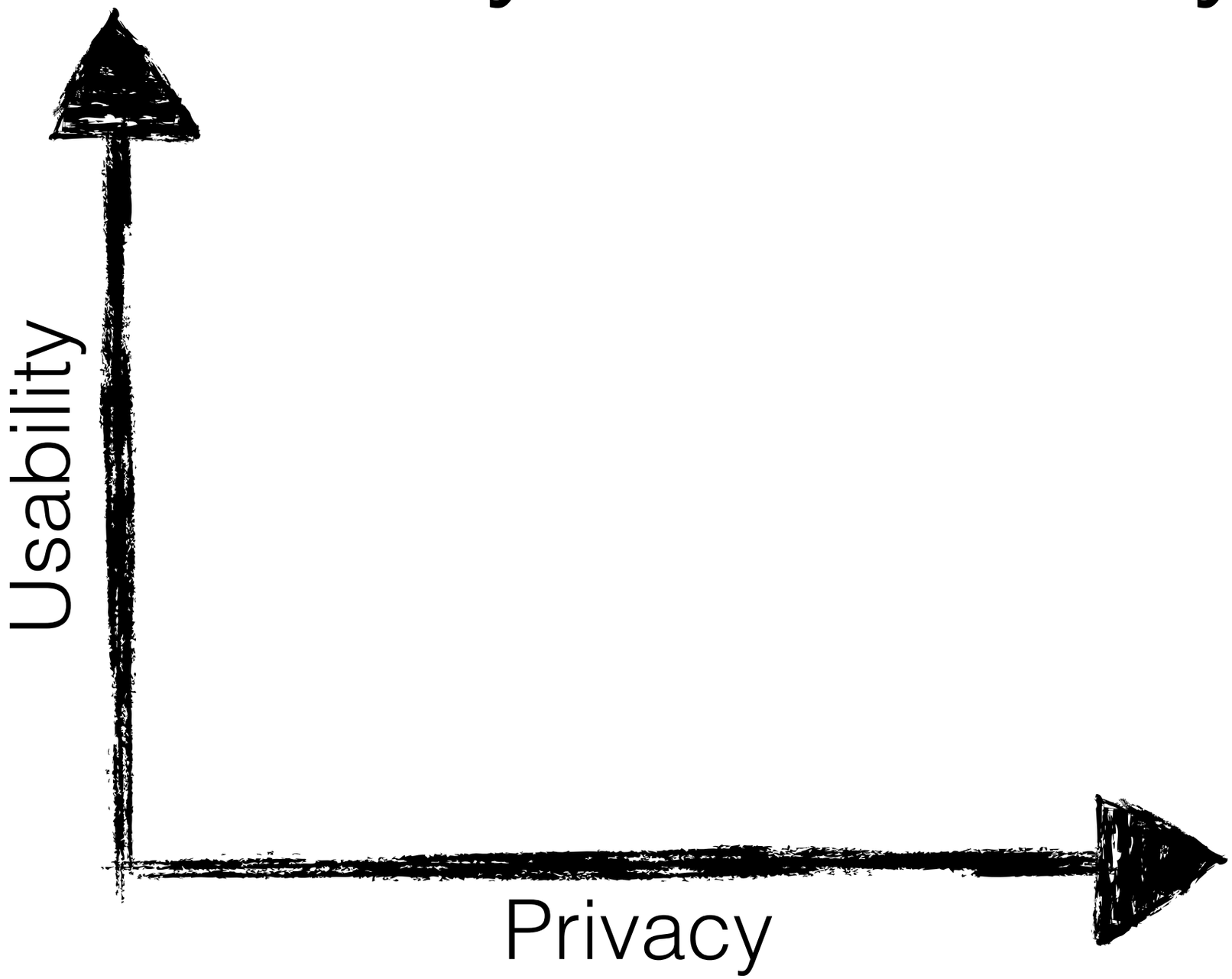
Context Specific Access Control

Camera, Location

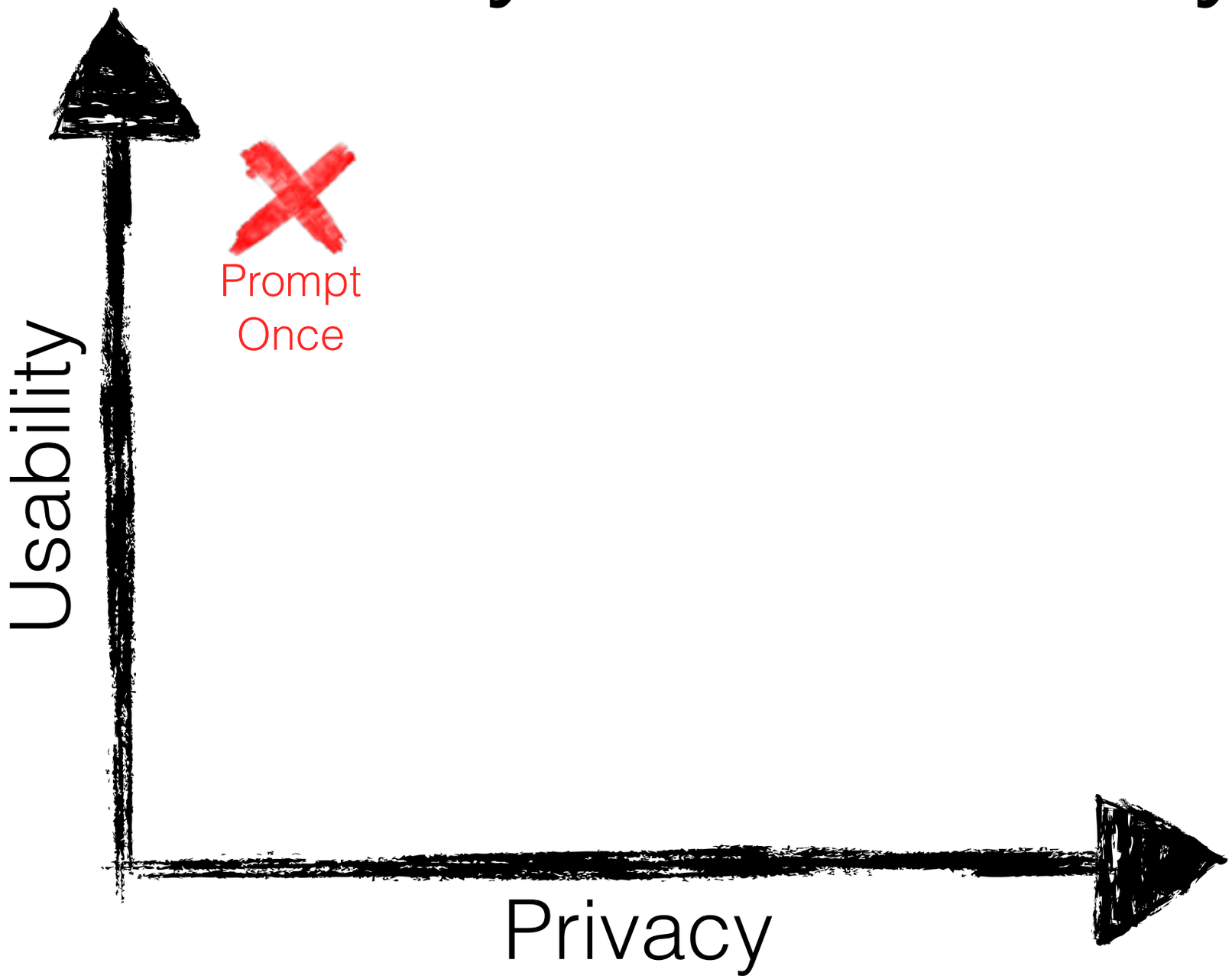


Home | Face Recognition | Arrests | Search | Background

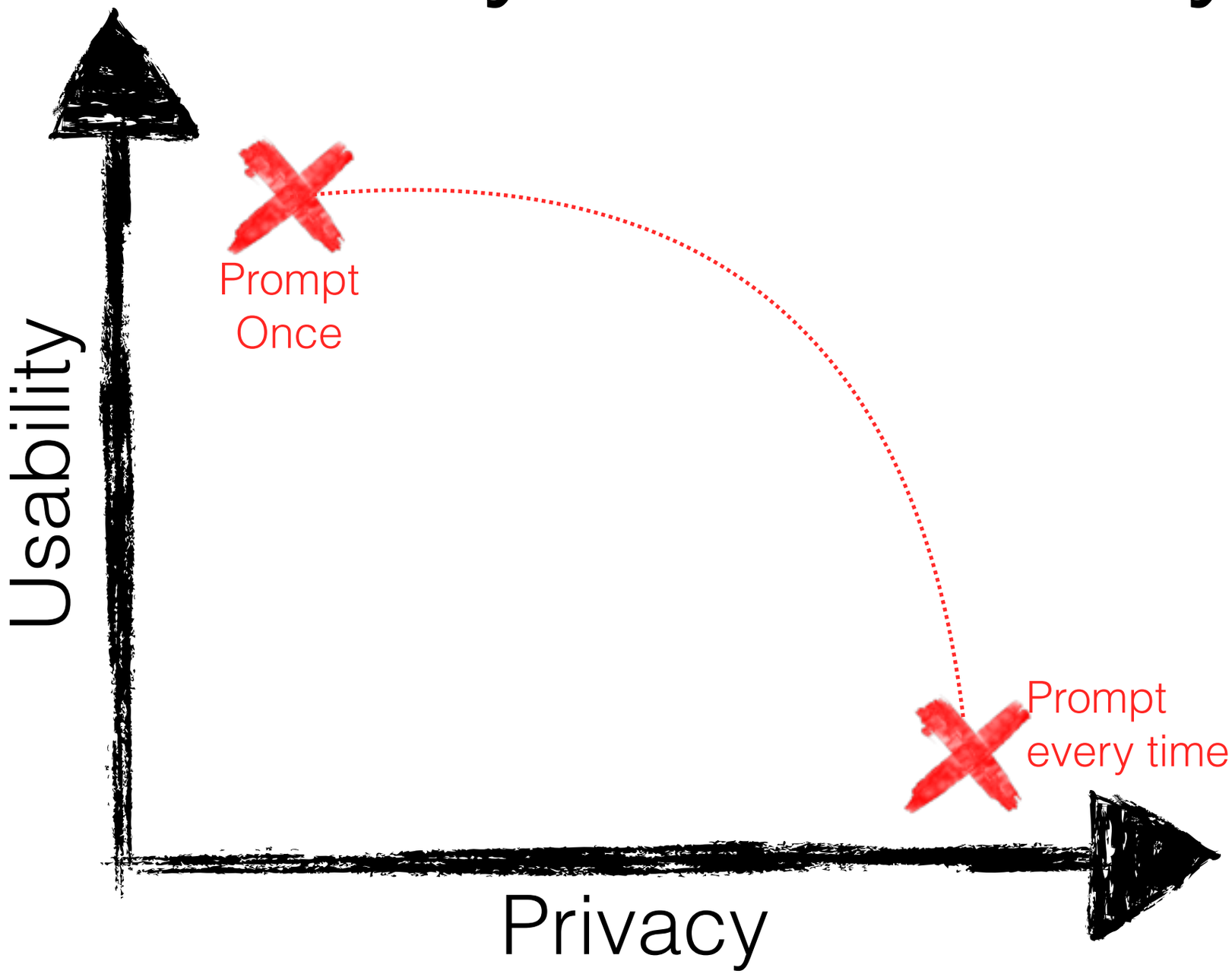
Usability vs. Privacy



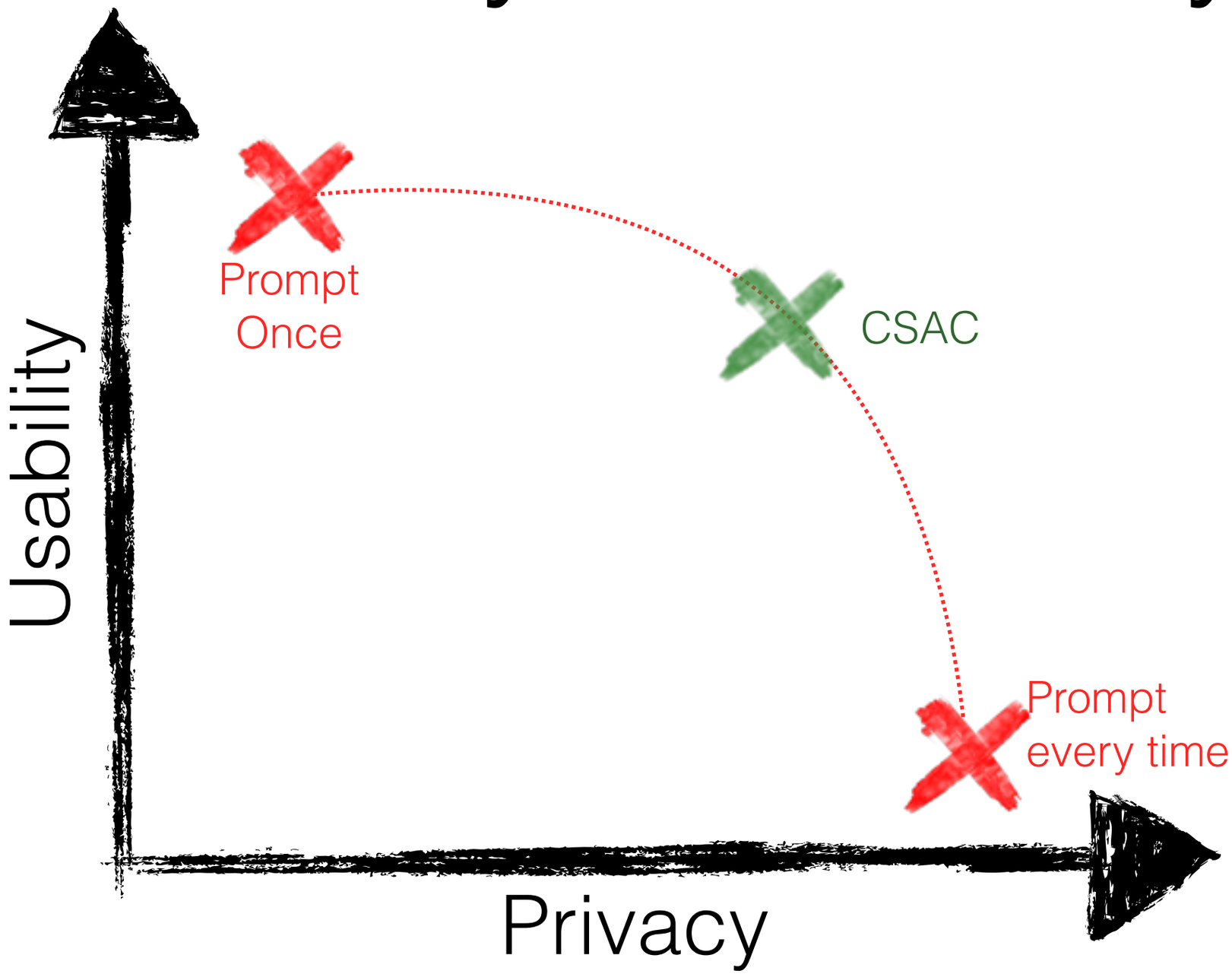
Usability vs. Privacy



Usability vs. Privacy



Usability vs. Privacy



Context-Specific Access Control

Context-Specific Access Control

- Divide user's interaction with application to a limited number of contexts.

- Prompt user for access-control decisions upon first use per-context.

- Reuse access-control decisions when user returns to that context.

Context Specific Access Control

Context Specific Access Control

Face Recognition

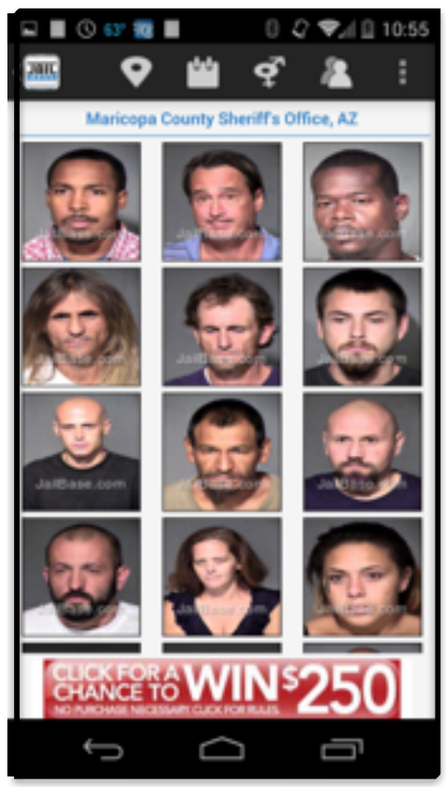
Context Specific Access Control

Face
Recognition

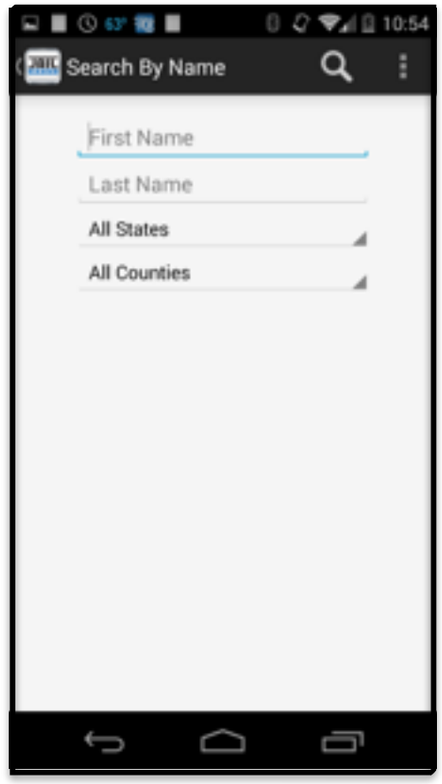
Context Specific Access Control

Home

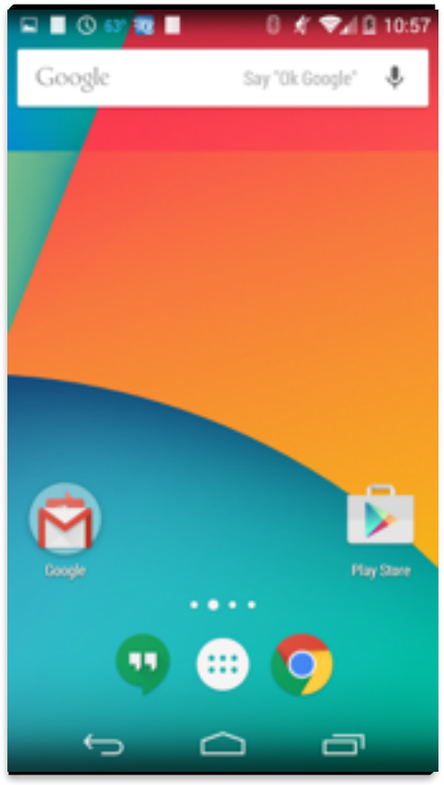
Face Recognition



Arrests



Search



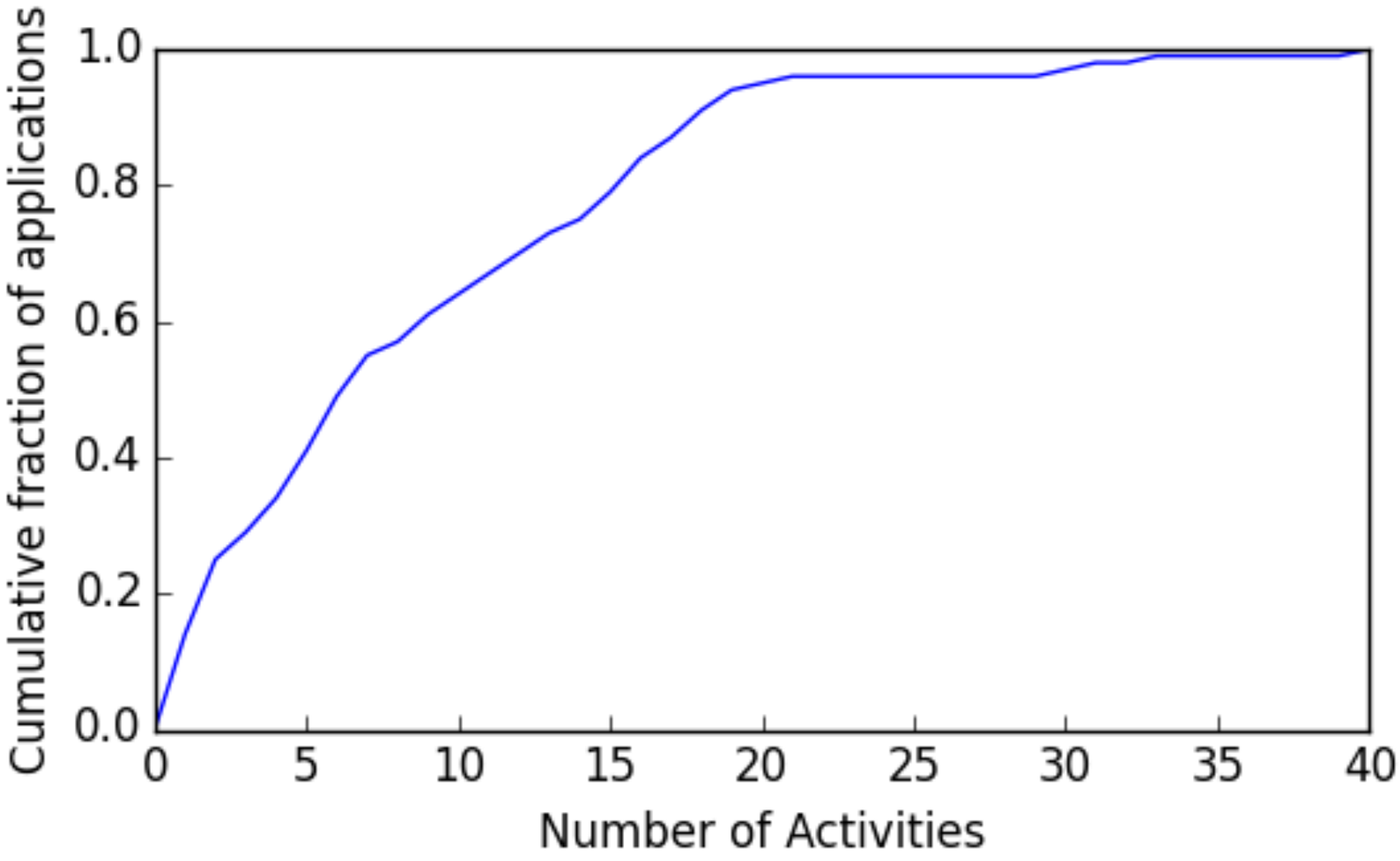
Background

Feasibility

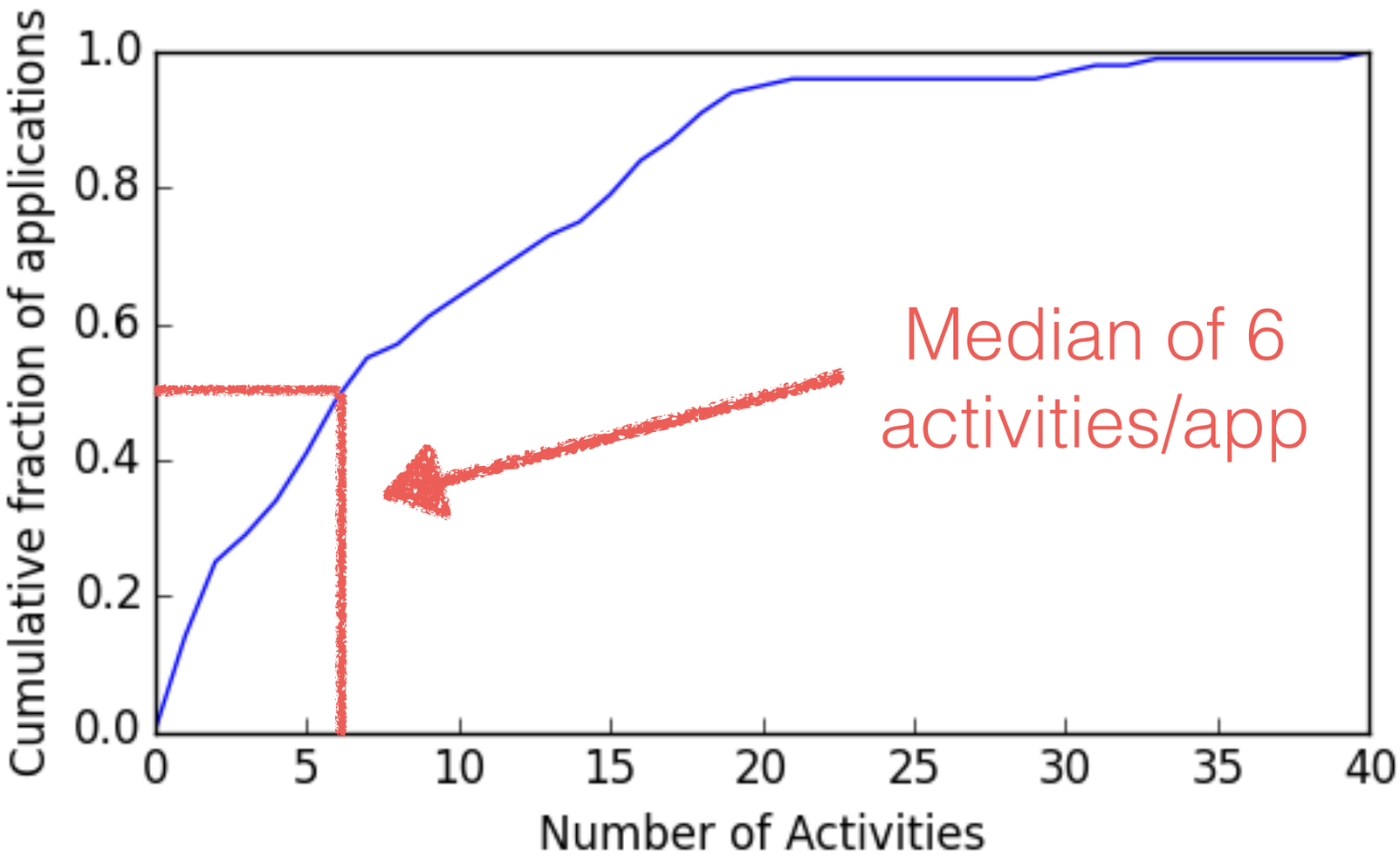
Feasibility

- Applications should be modular.
- CSAC decision overhead should be low

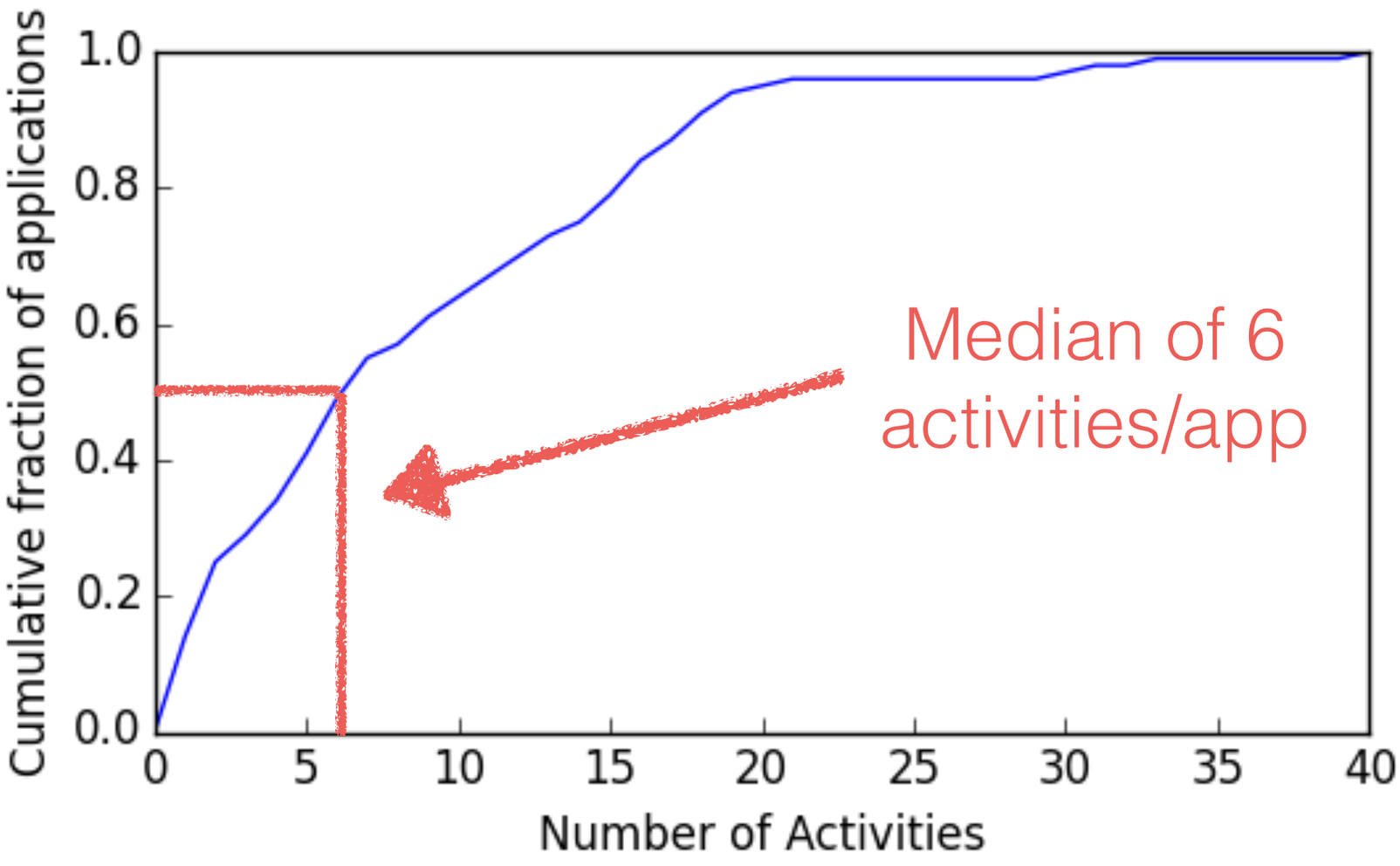
Application Modularity



Application Modularity



Application Modularity



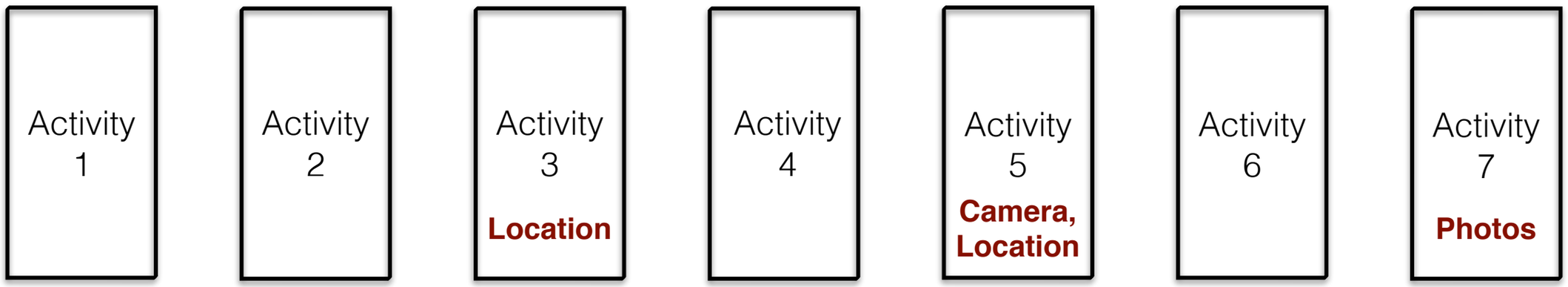
Activities provide meaningful modularity to implement CSAC

Feasibility

- ✓ ~~Applications should be modular.~~
- CSAC decision overhead should be low

Permission Usage

Permission Usage

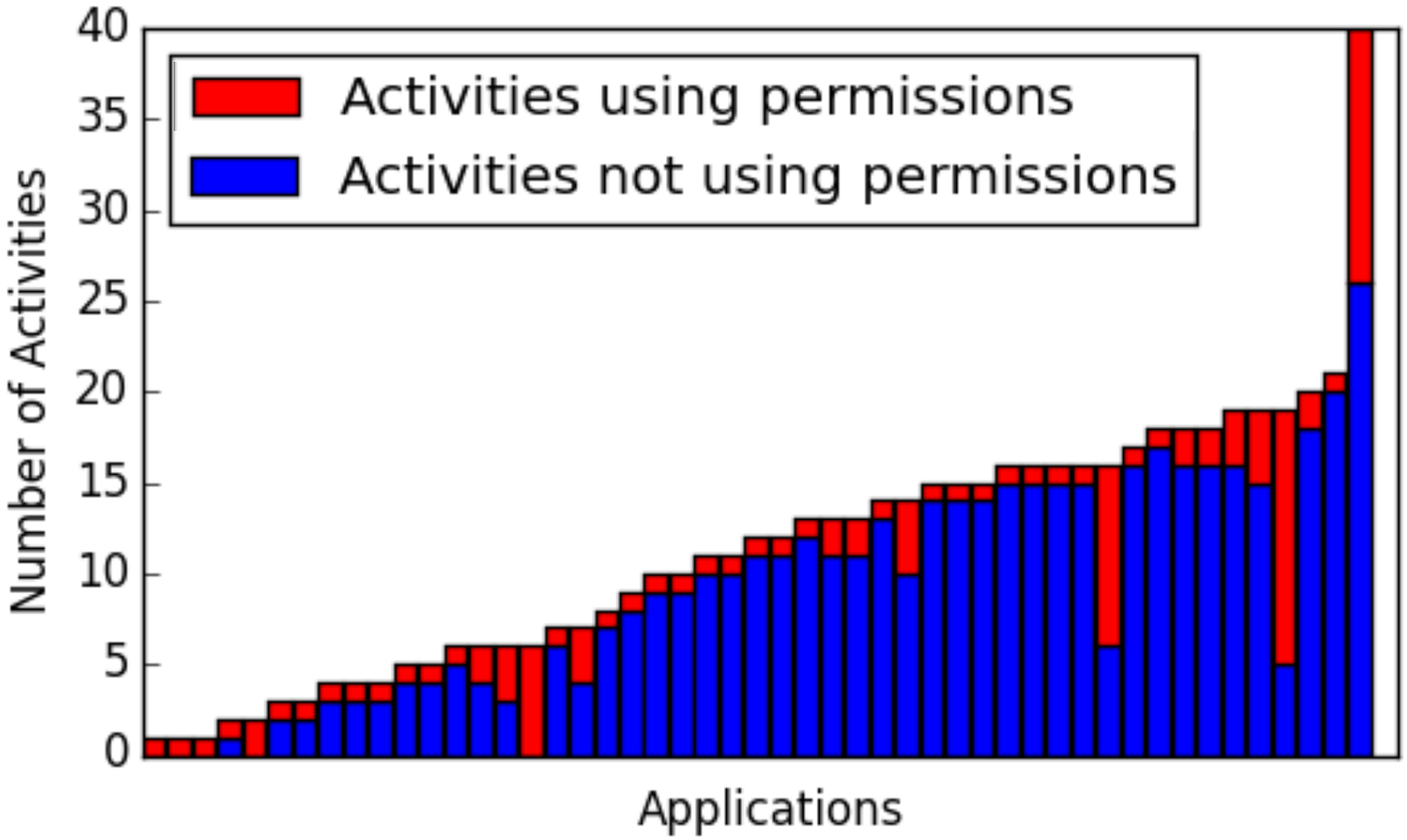


Experimental Setup

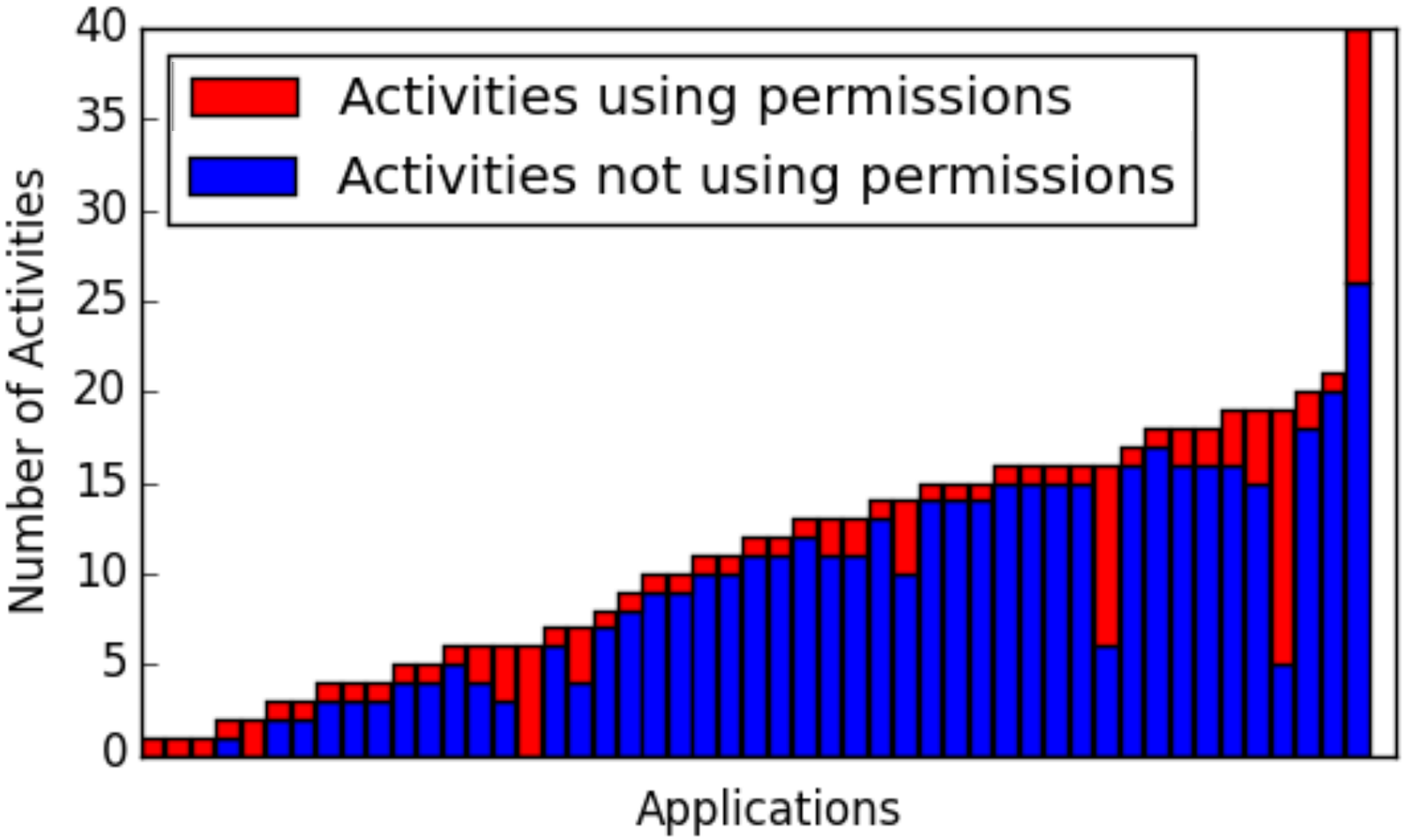
Experimental Setup

- 100 popular free Android applications.
- Dynamic exploration with A3E.
- Tracked use of Camera, Location, Device ID, Bluetooth, and Photos.

Permission usage variation across Activities

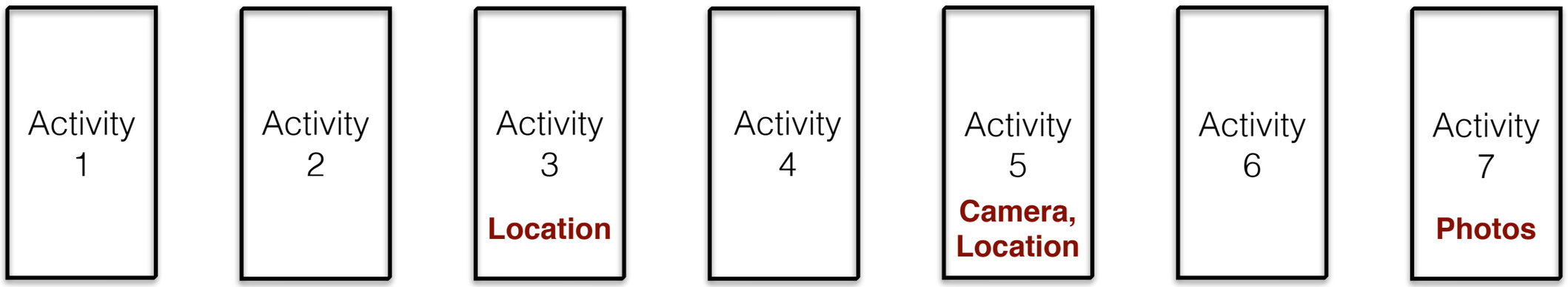


Permission usage variation across Activities



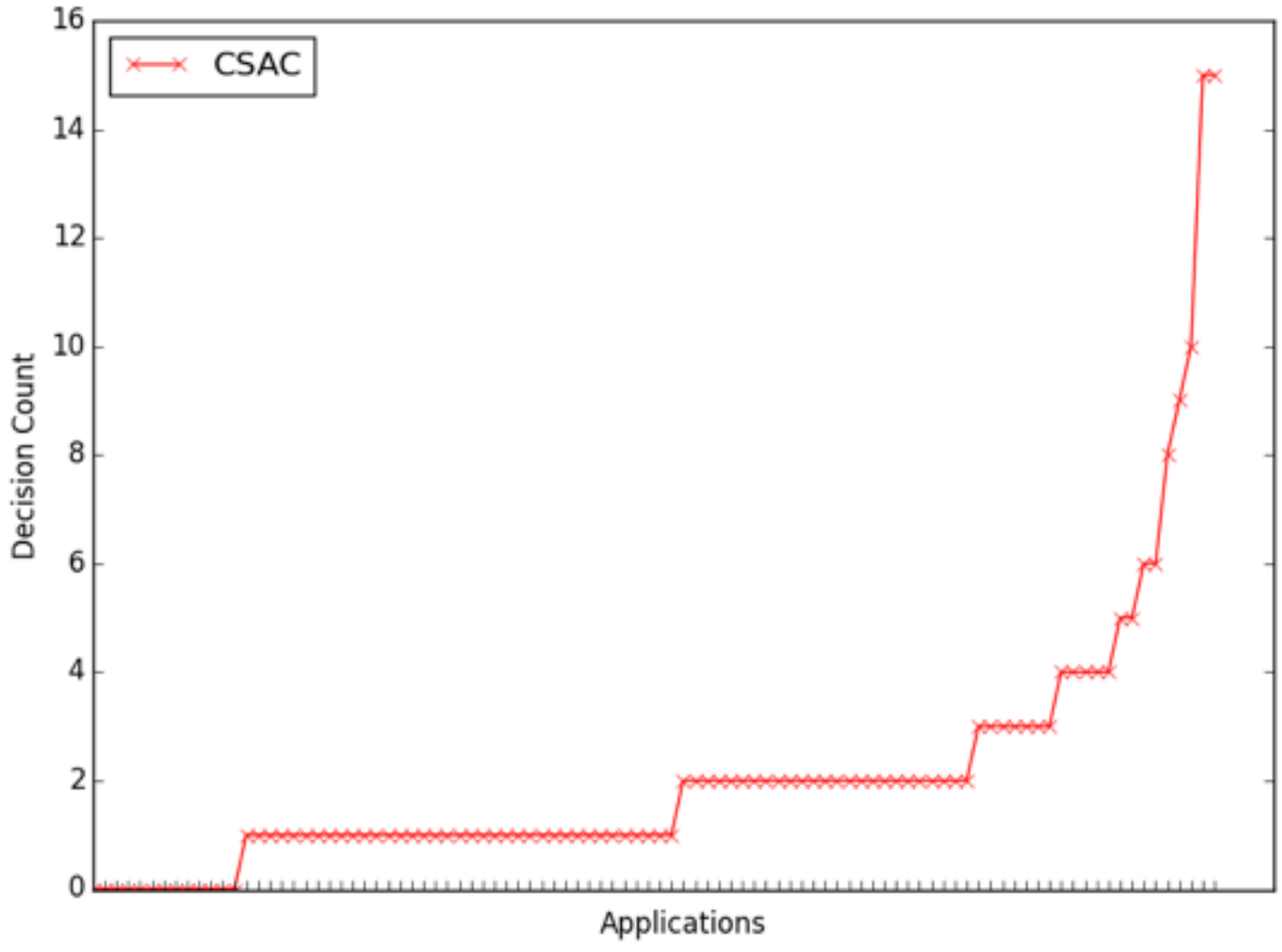
70% of Activities do not use permissions we tracked

Permission Usage

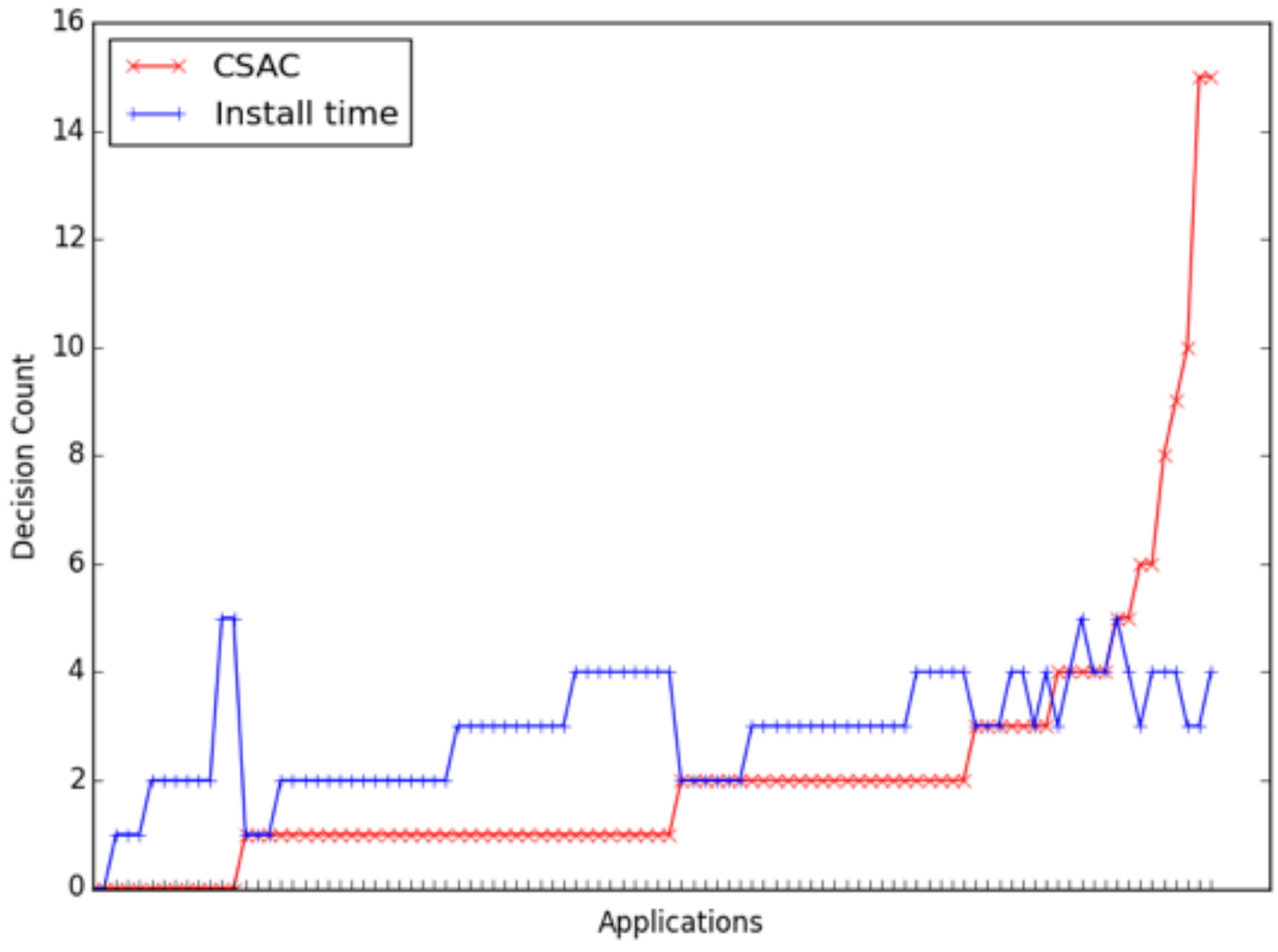


Decision Overhead

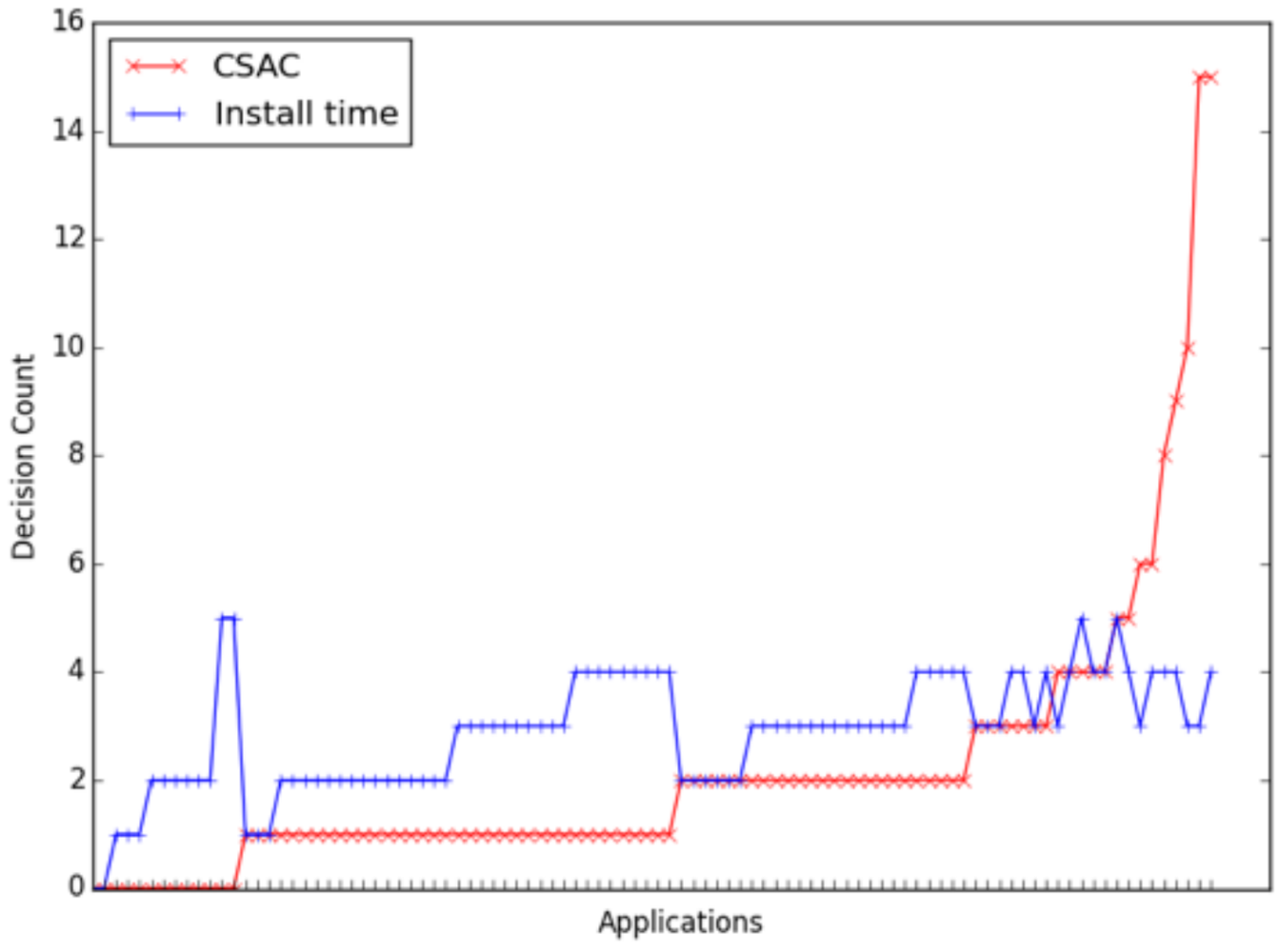
Decision Overhead



Decision Overhead

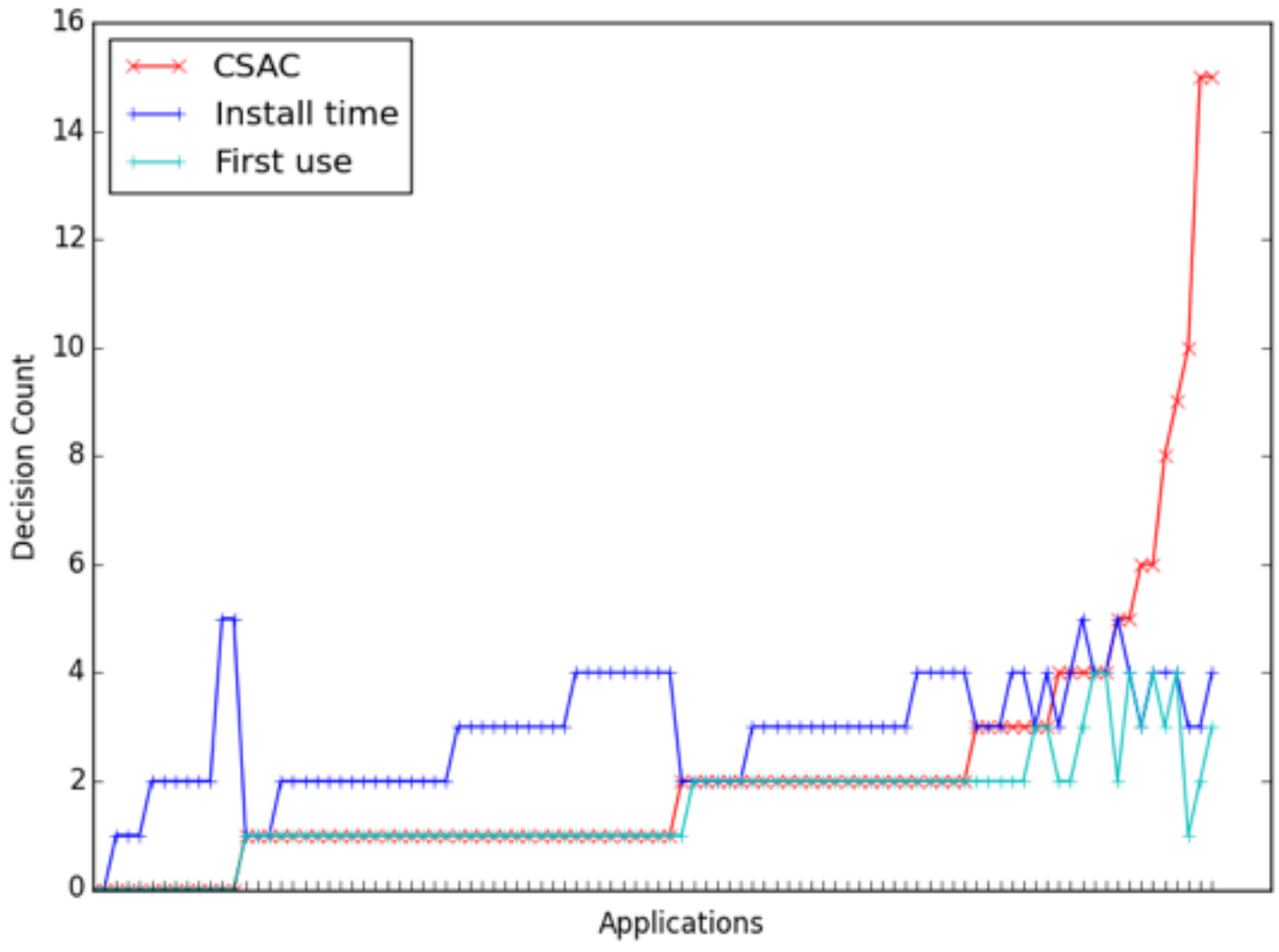


Decision Overhead



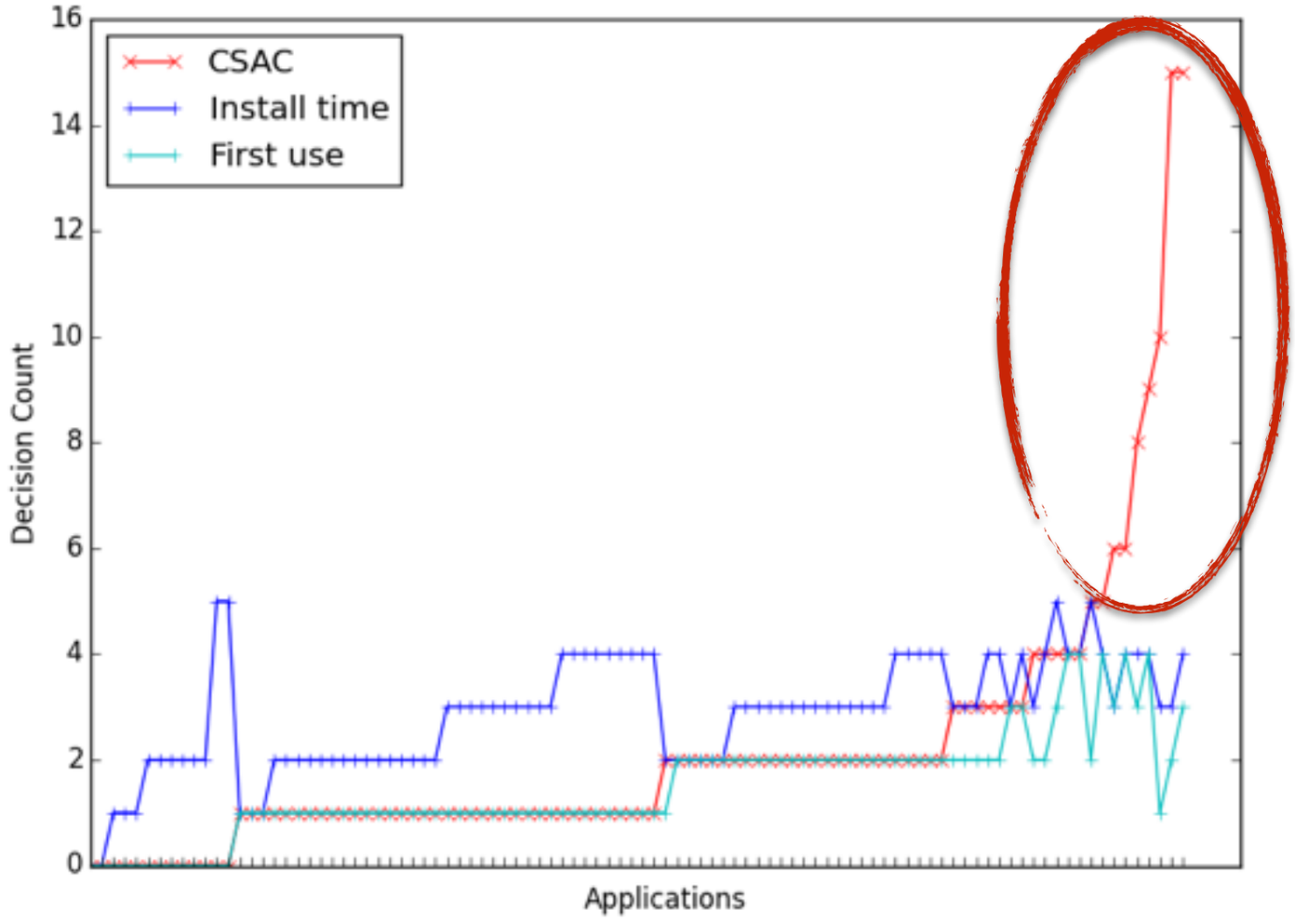
For most of the applications CSAC has no overhead.

Decision Overhead



For most of the applications CSAC has no overhead.

Decision Overhead



For most of the applications CSAC has no overhead.

User Study

User Study

- 5 Applications, 5 Users

User Study

- 5 Applications, 5 Users

	Dynamic Exploration		
Application	Install time	First use	CSAC
Dictionary	3	2	15
Flipagram	4	3	8
GasBuddy	3	1	10
WeatherBug	3	3	6
Yelp	4	3	15

User Study

- 5 Applications, 5 Users

	Decision Count								
	Dynamic Exploration			User Study					
Application	Install time	First use	CSAC	Union	User #1	User #2	User #3	User #4	User #5
Dictionary	3	2	15	6	4	4	3	3	4
Flipagram	4	3	8	2	2	1	2	1	1
GasBuddy	3	1	10	5	3	3	3	3	3
WeatherBug	3	3	6	6	3	2	3	2	2
Yelp	4	3	15	5	4	3	3	2	3

User Study

- 5 Applications, 5 Users

	Decision Count								
	Dynamic Exploration			User Study					
Application	Install time	First use	CSAC	Union	User #1	User #2	User #3	User #4	User #5
Dictionary	3	2	15	6	4	4	3	3	4
Flipagram	4	3	8	2	2	1	2	1	1
GasBuddy	3	1	10	5	3	3	3	3	3
WeatherBug	3	3	6	6	3	2	3	2	2
Yelp	4	3	15	5	4	3	3	2	3

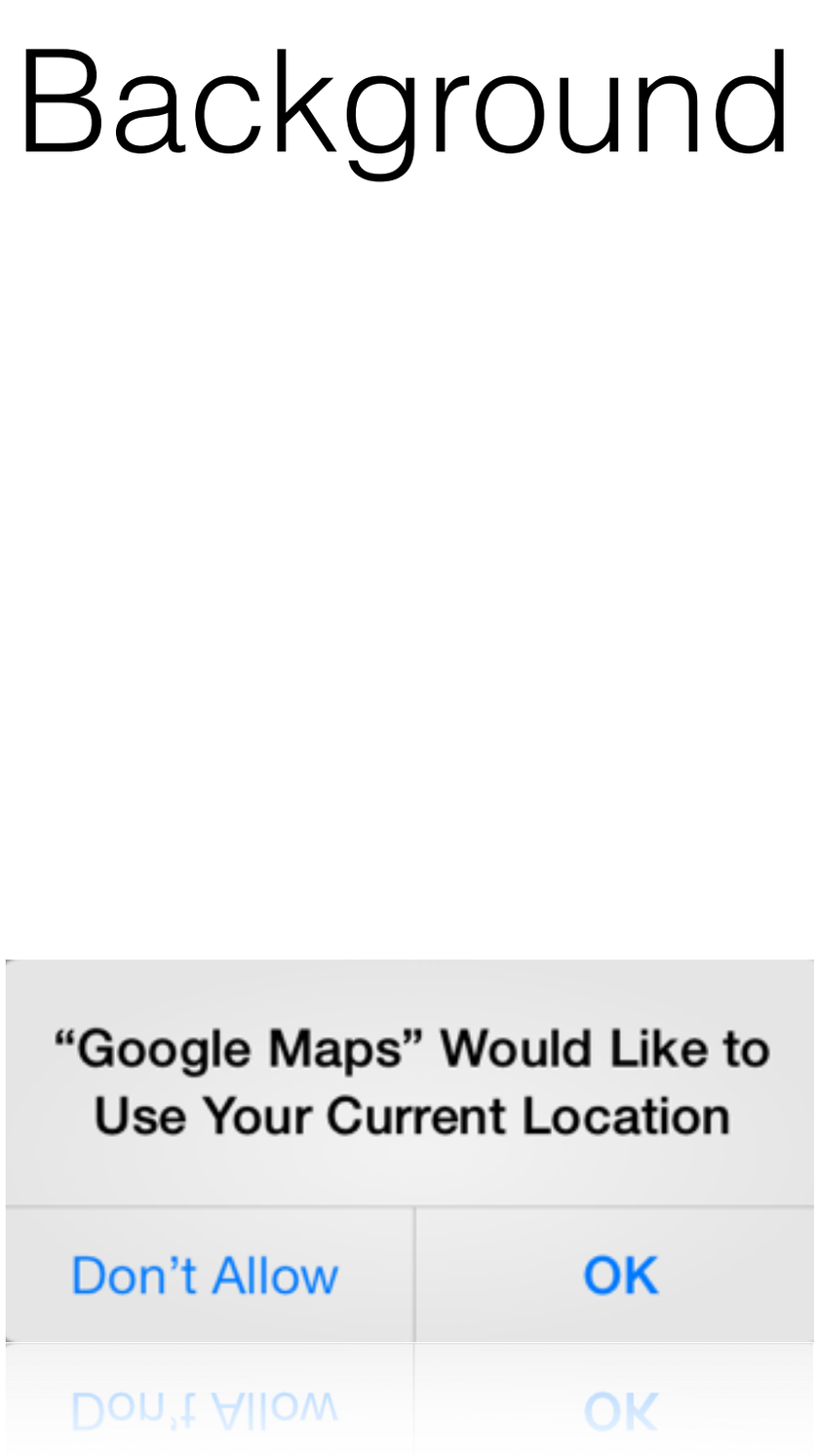
Conclusion

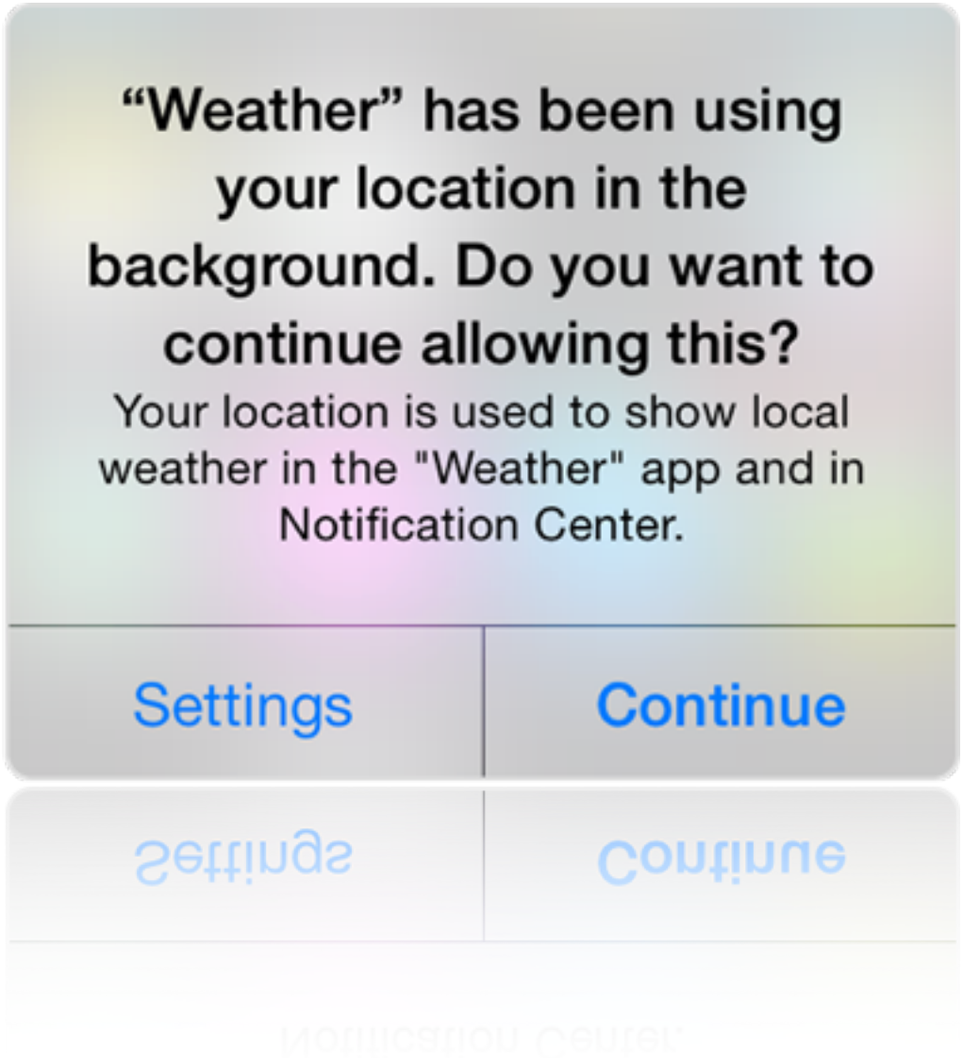
Conclusion

- Applications can be broken down to different contexts.
- Different contexts require a different set of permissions.
- CSAC can get us closer to realizing principle of least privilege.
- Many challenges remain:
  - Data sharing
  - Background services
  - Modifying permissions

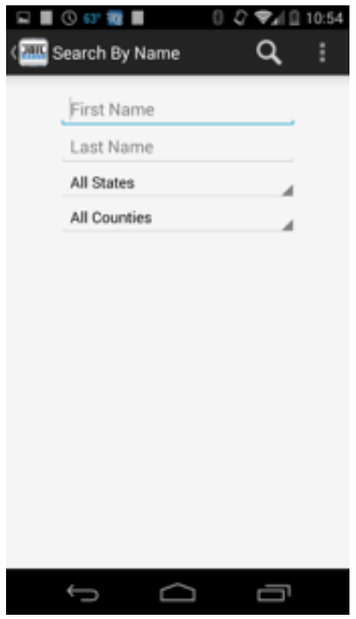
Backup Slides

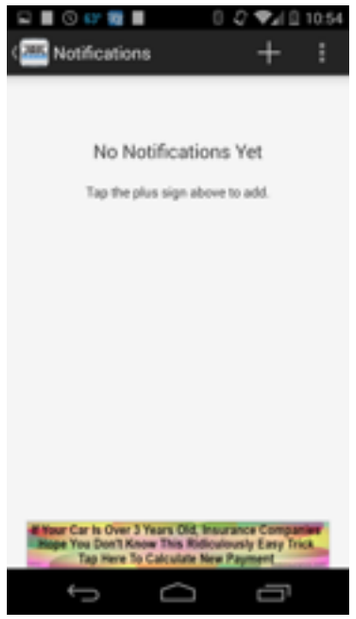
Background vs Foreground

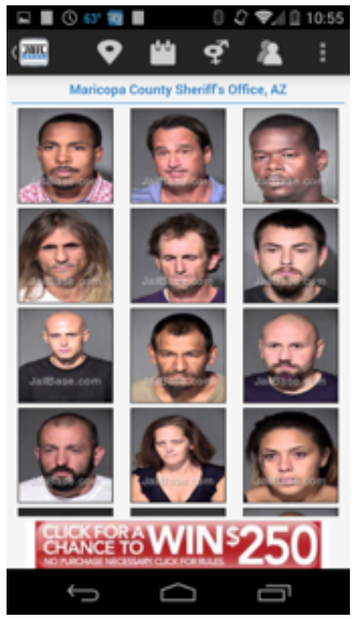


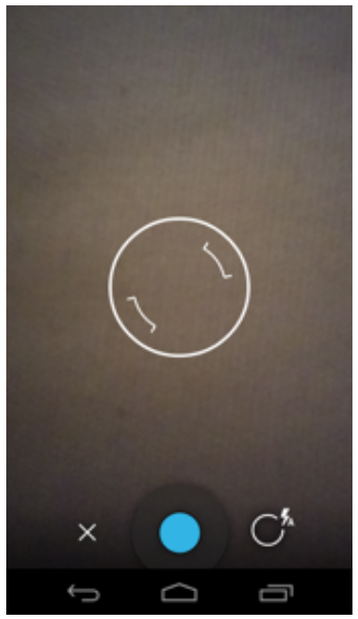


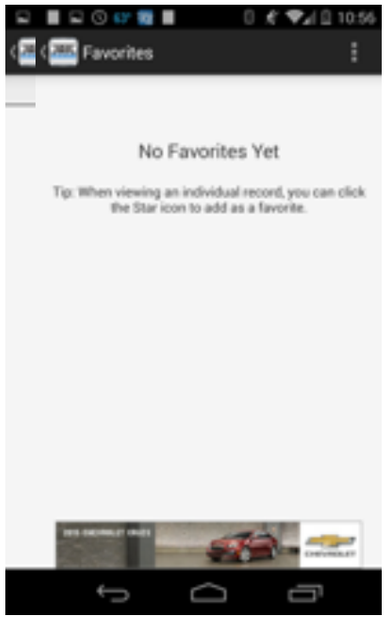
Context Specific Access Control

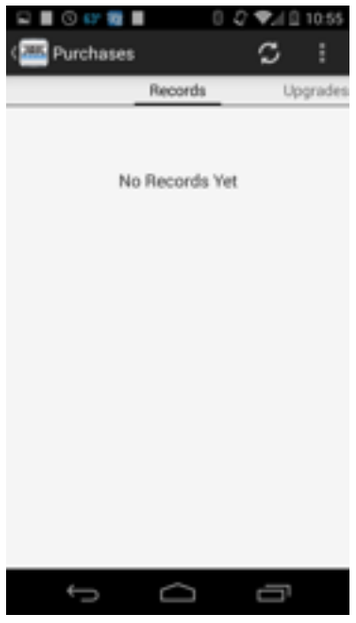


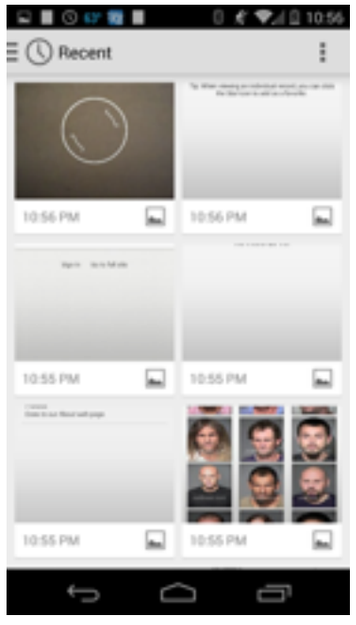


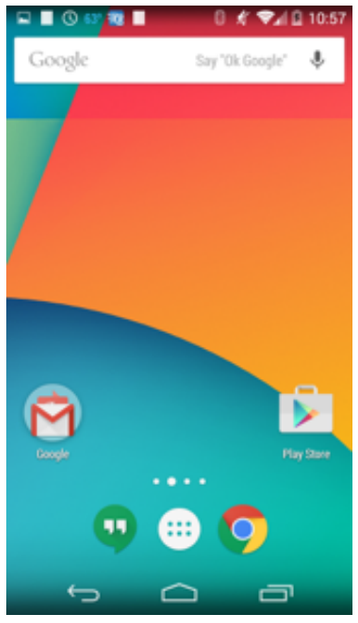




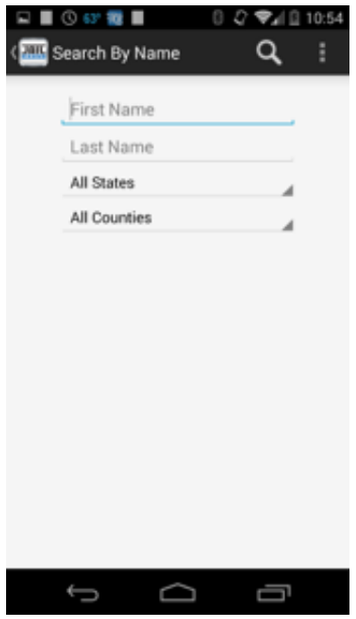


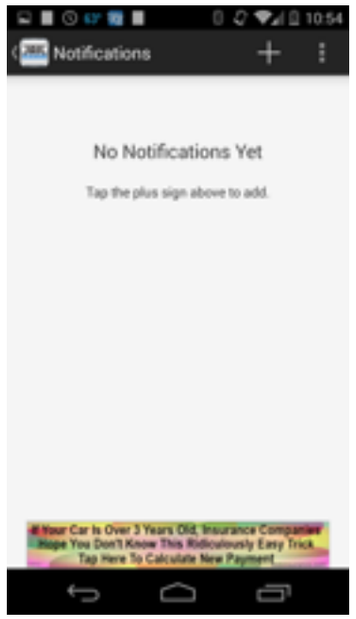


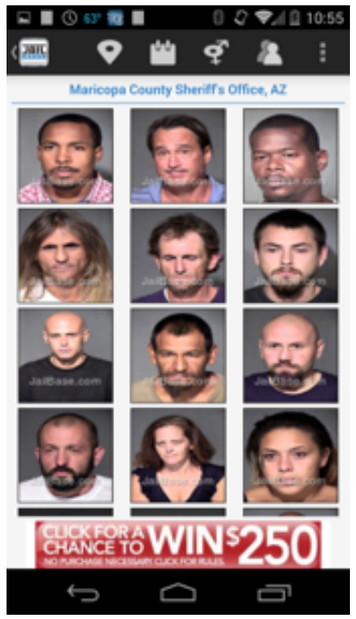


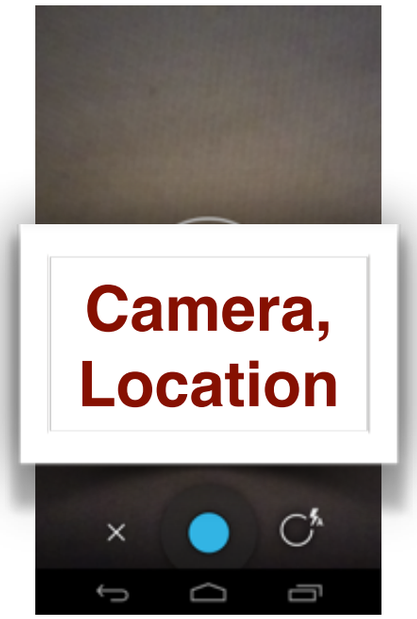


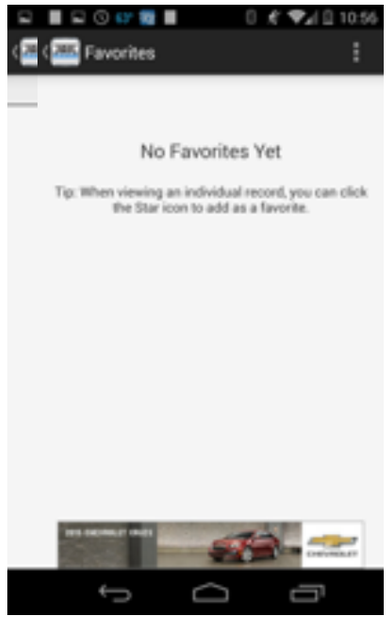
Context Specific Access Control

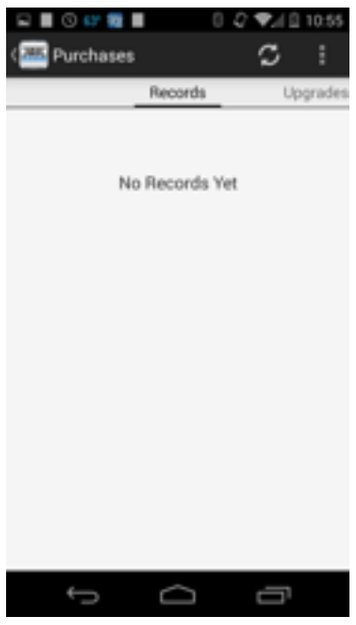


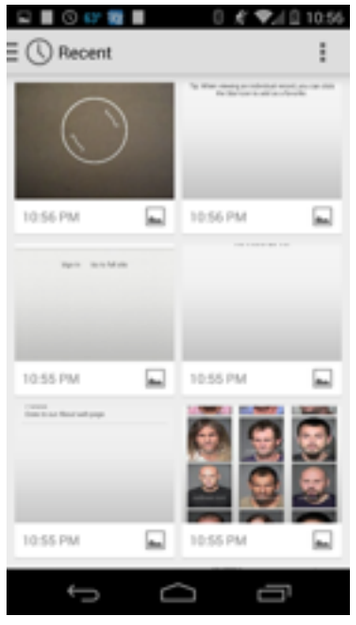


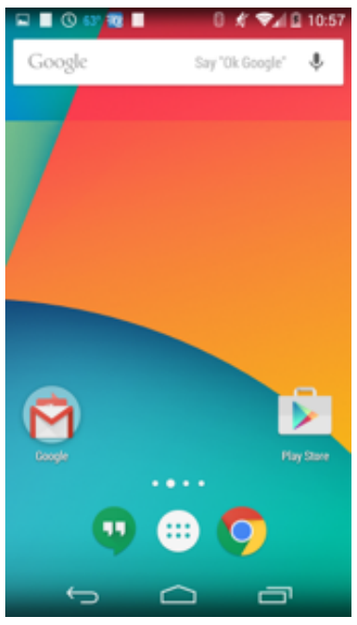




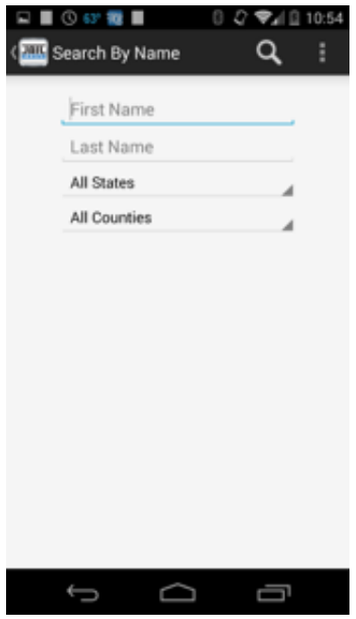


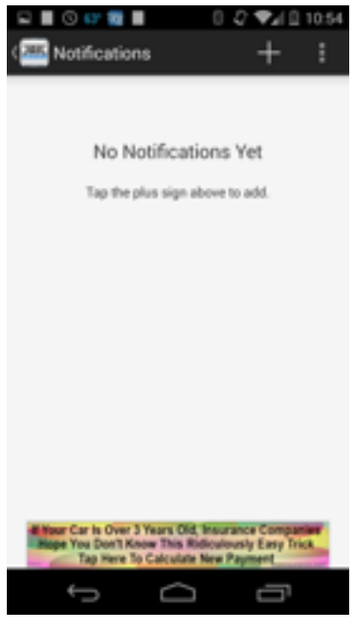


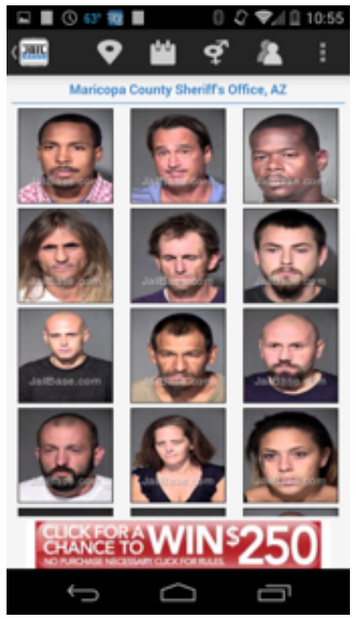


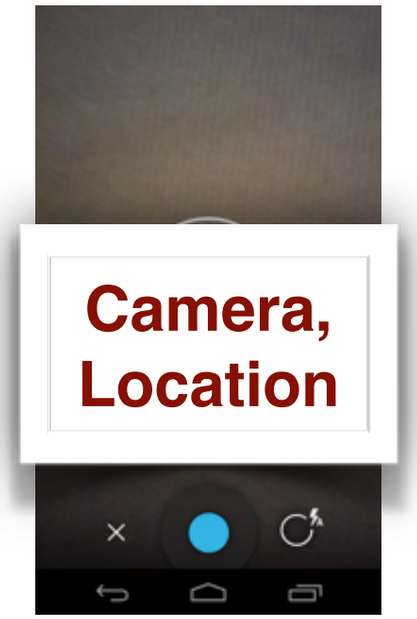


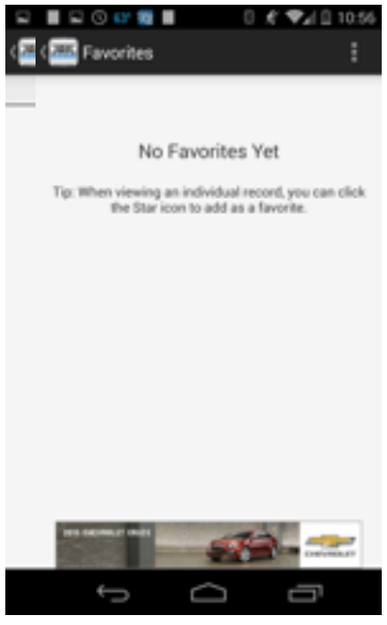
Context Specific Access Control

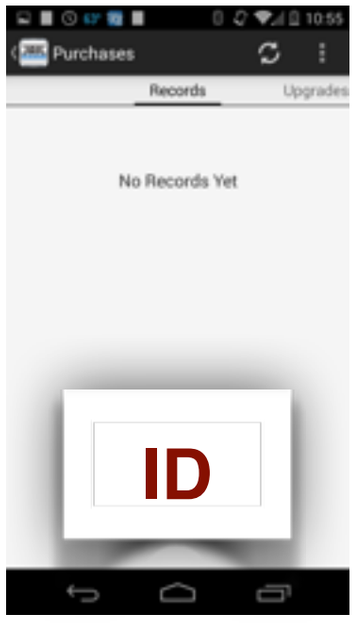


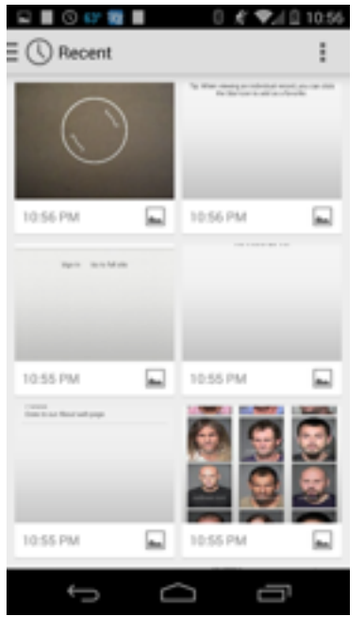


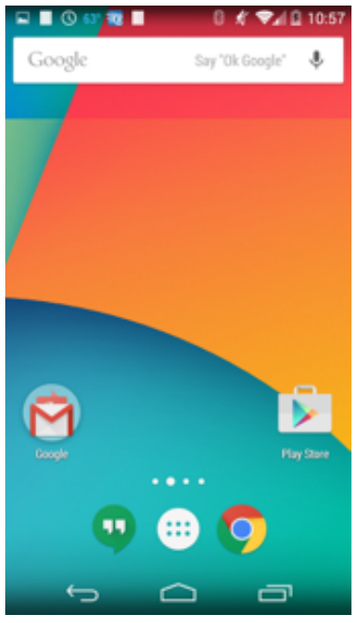












Context Specific Access Control