22 - Privacy and security for mobile devices and IoT

Lorrie Cranor

April 10, 2017

05-436 / 05-836 / 08-534 / 08-734 / 19-534 / 19-734
Usable Privacy and Security

Carnegie Mellon University
CyLab

institute for SOFTWARE RESEARCH

Engineering & Public Policy

Today!

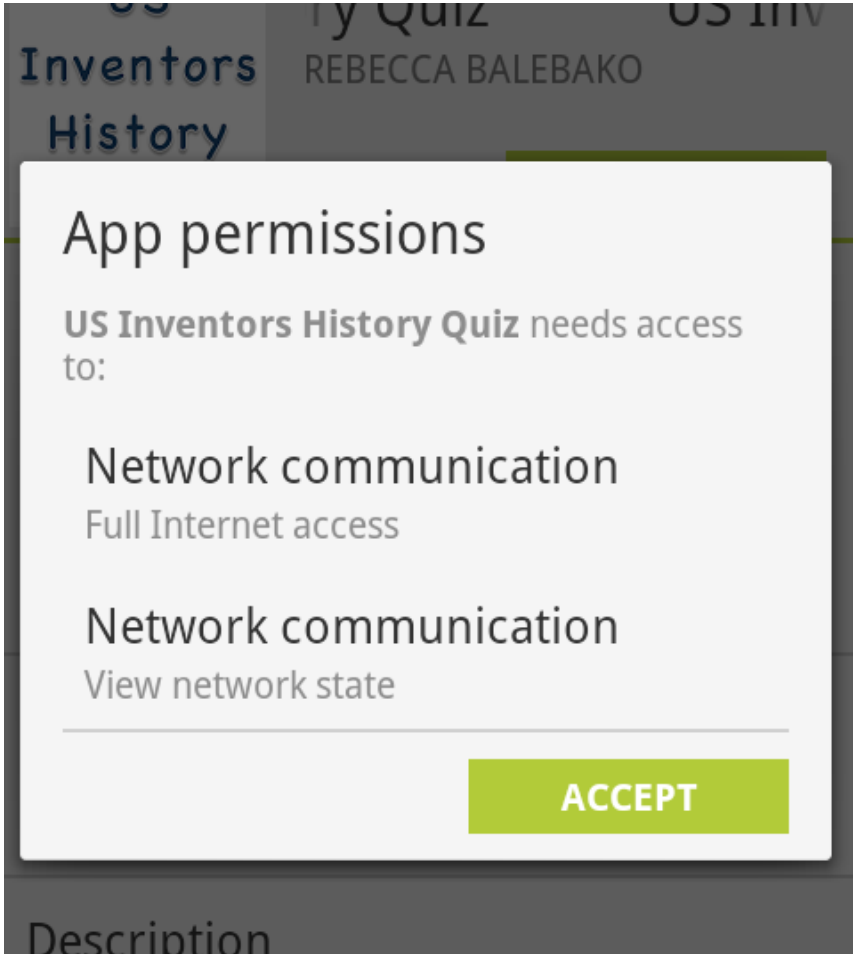
- Announcement: Next homework due May 1
  - Assignment not yet posted
  - Eliminated homework that was supposed to be due April 17
  - Note that the May 1 HW will include 1 optional reading for every class between now and then for 12-unit students
  - Use the extra time to make progress on your projects!
- Homework 8 discussion
- Mobile app permissions
- Usable security and privacy for IoT
- Activity

Homework 8 discussion

- Ghostery browser extension, Ghostery mobile browser, DAA
- How have these tools improved since 2011?
- What problems remain?

Mobile app permissions

Current notices are not sufficient



- Users don't understand what permissions mean
- Users don't understand why permissions are being requested
- Users often click through without reading

Expert interviews

- We interviewed 20 experts from industry, academia, and government
- Asked them to describe smartphone security and privacy risks and mitigations
- Many harms could be addressed by better security practices
- Better privacy notices can address only a subset of these harms

Balebako, R., C. Bravo-Lillo, Cranor, L. Is Notice Enough? Mitigating the Risks of Smartphone Data Sharing. I/S: A Journal of Law and Policy for the Information Society 11, 279, 2015.

App developers can protect users

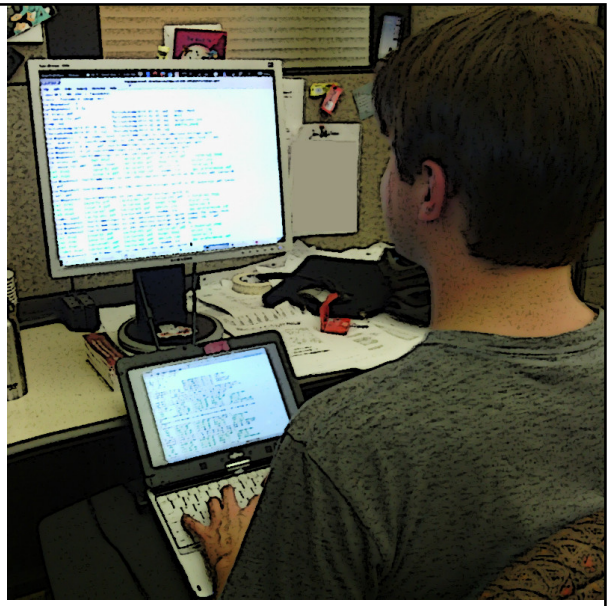
- Best security practices
- Data minimization
- Understand privacy and security of third-party tools they use
- Transparency (privacy policies)

App developer study

- Interviewed 13 and surveyed 228 app developers
- Privacy and security not a high priority
- Small companies tend not to do much to protect security and privacy, rely on web searches and social networks for advice
- Developers use third-party tools without knowing privacy policies
- Many developers unfamiliar with privacy policy or don't have privacy policy

Balebako, R., Marsh, A., Lin, J., Hong, J., Cranor, L. The Privacy and Security Behaviors of Smartphone App Developers. USEC 2014.

App developer views on privacy policies

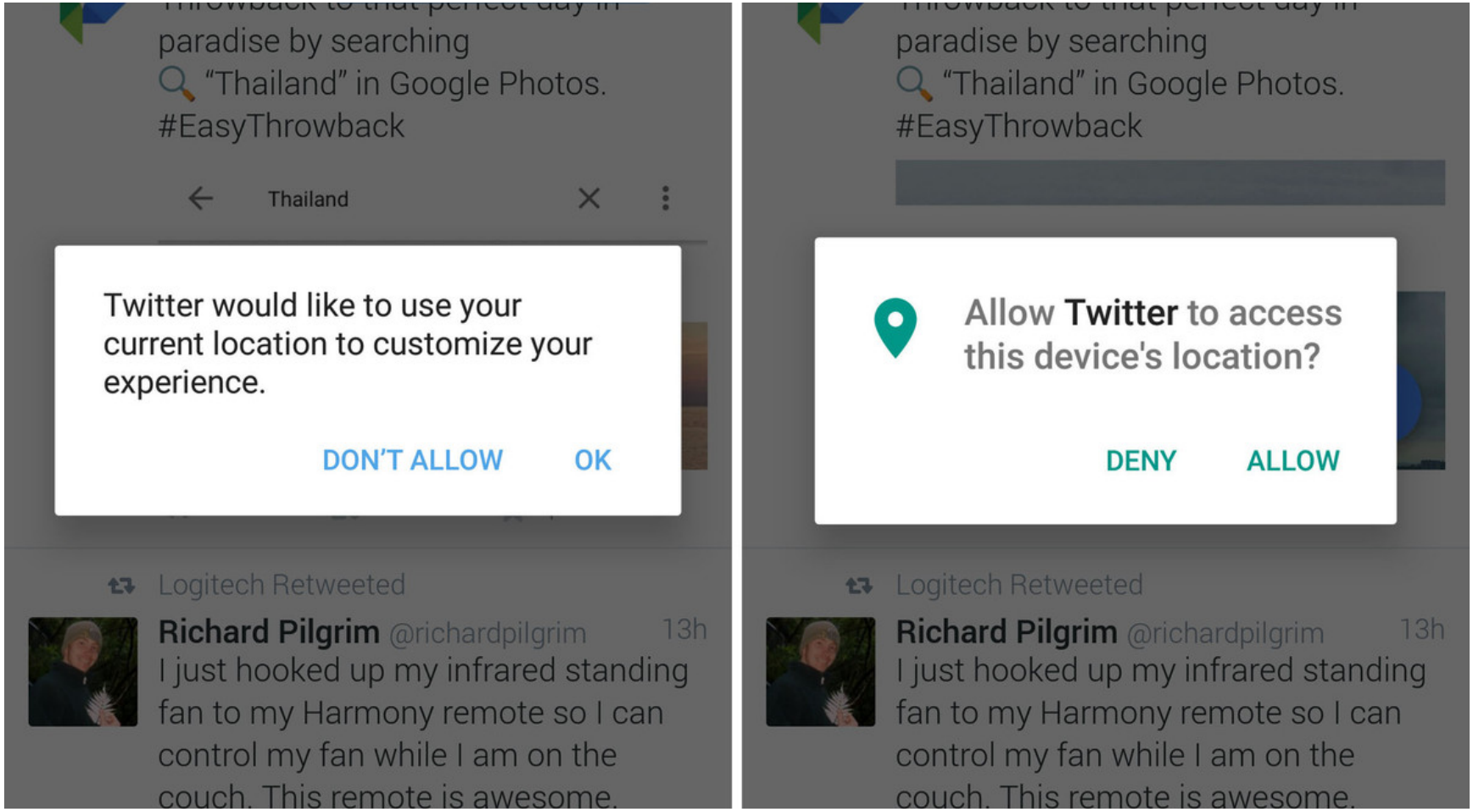


- “I haven’t even read [our privacy policy]. I mean, it’s just legal stuff that’s required, so I just put in there.”
- “I don’t see the time it would take to implement that over cutting and pasting someone else’s privacy policies.... I don’t see the value being such that that’s worth it.”

Permissions in Android 6.0+

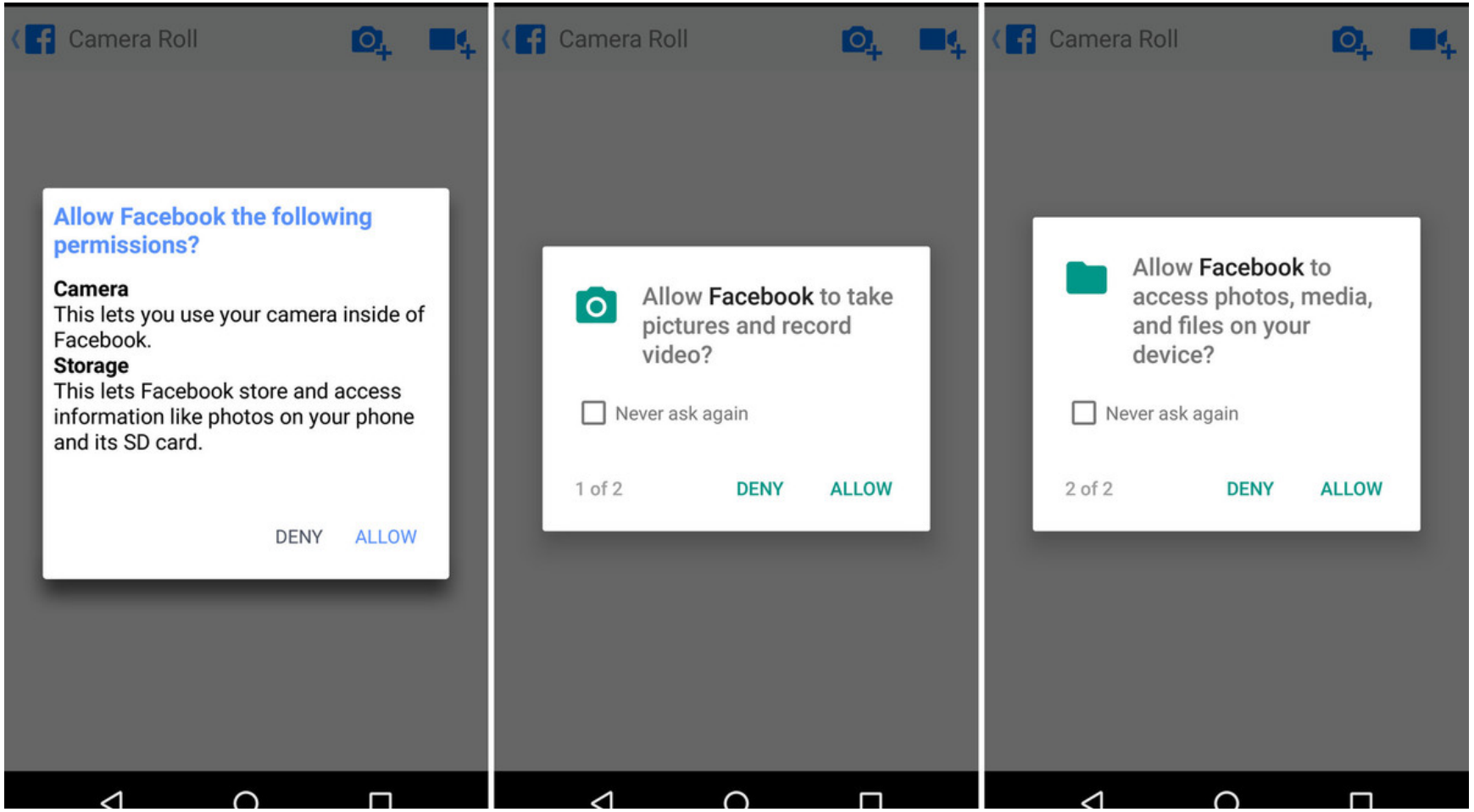
- Runtime permissions model
- Apps encouraged to offer explanation before asking for permission, resulting in double prompt

Twitter



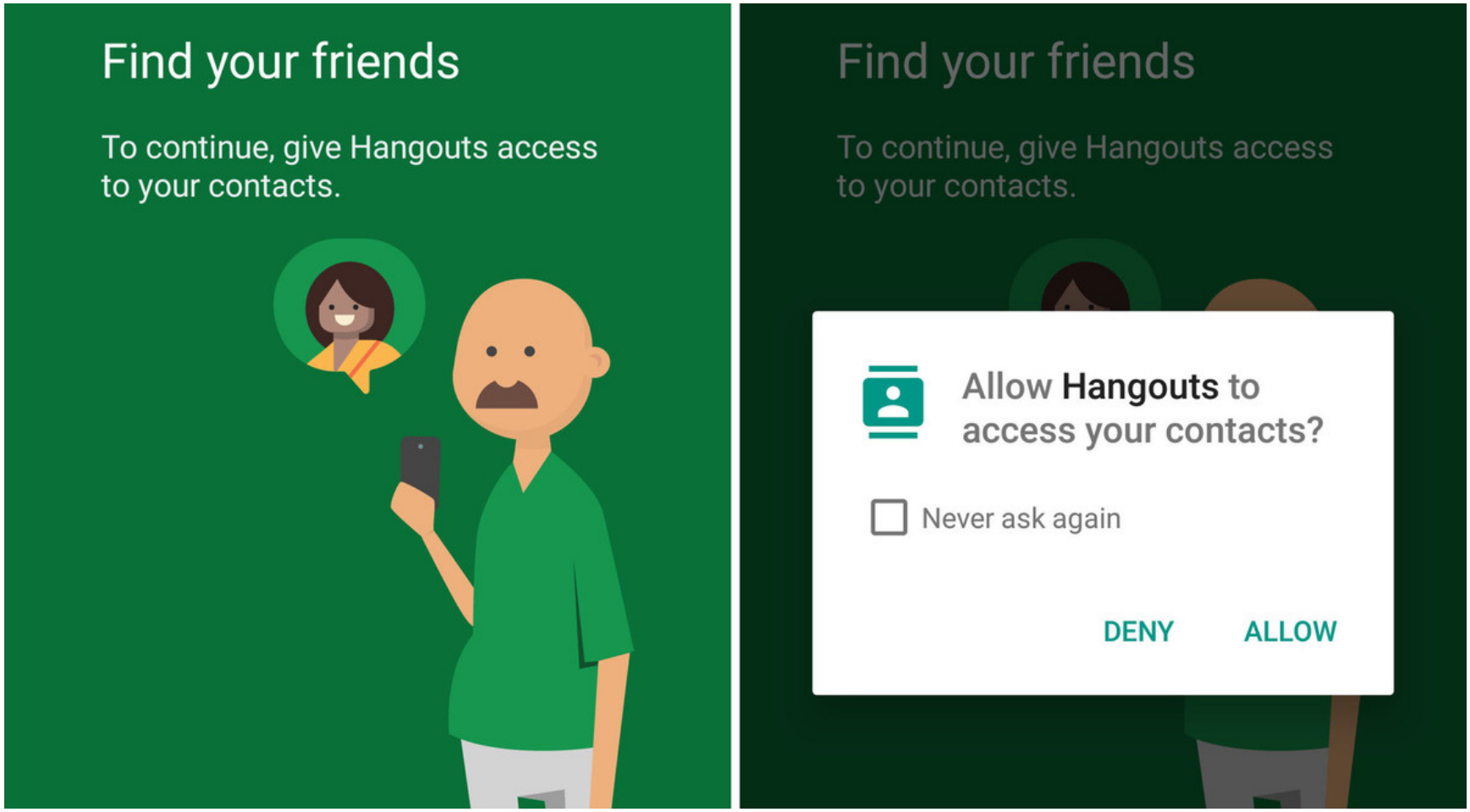
http://www.androidcentral.com/run-permissions-why-change-android-60-may-make-you-repeat-yourself

Facebook



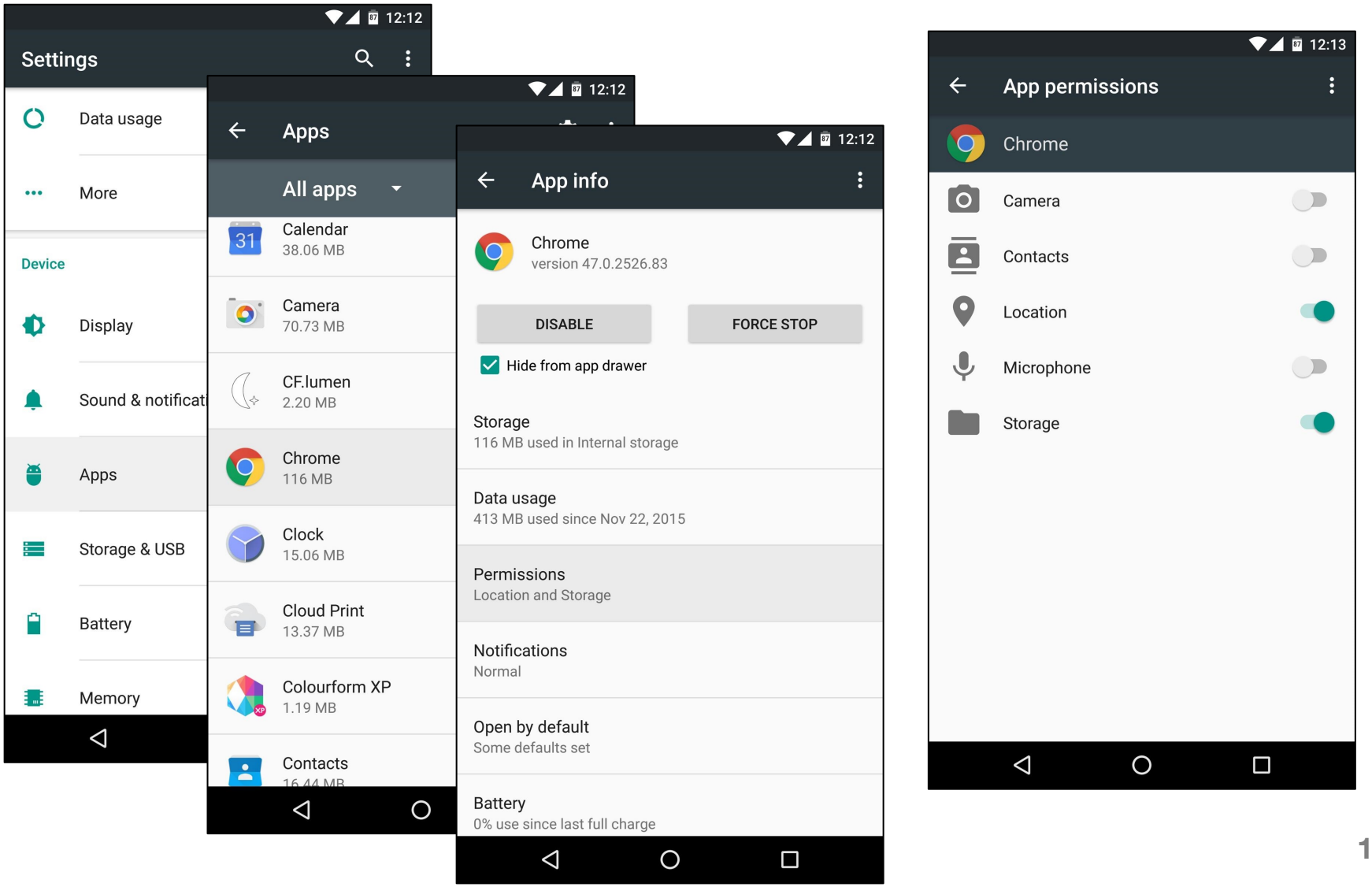
http://www.androidcentral.com/run-permissions-why-change-android-60-may-make-you-repeat-yourself

Hangouts

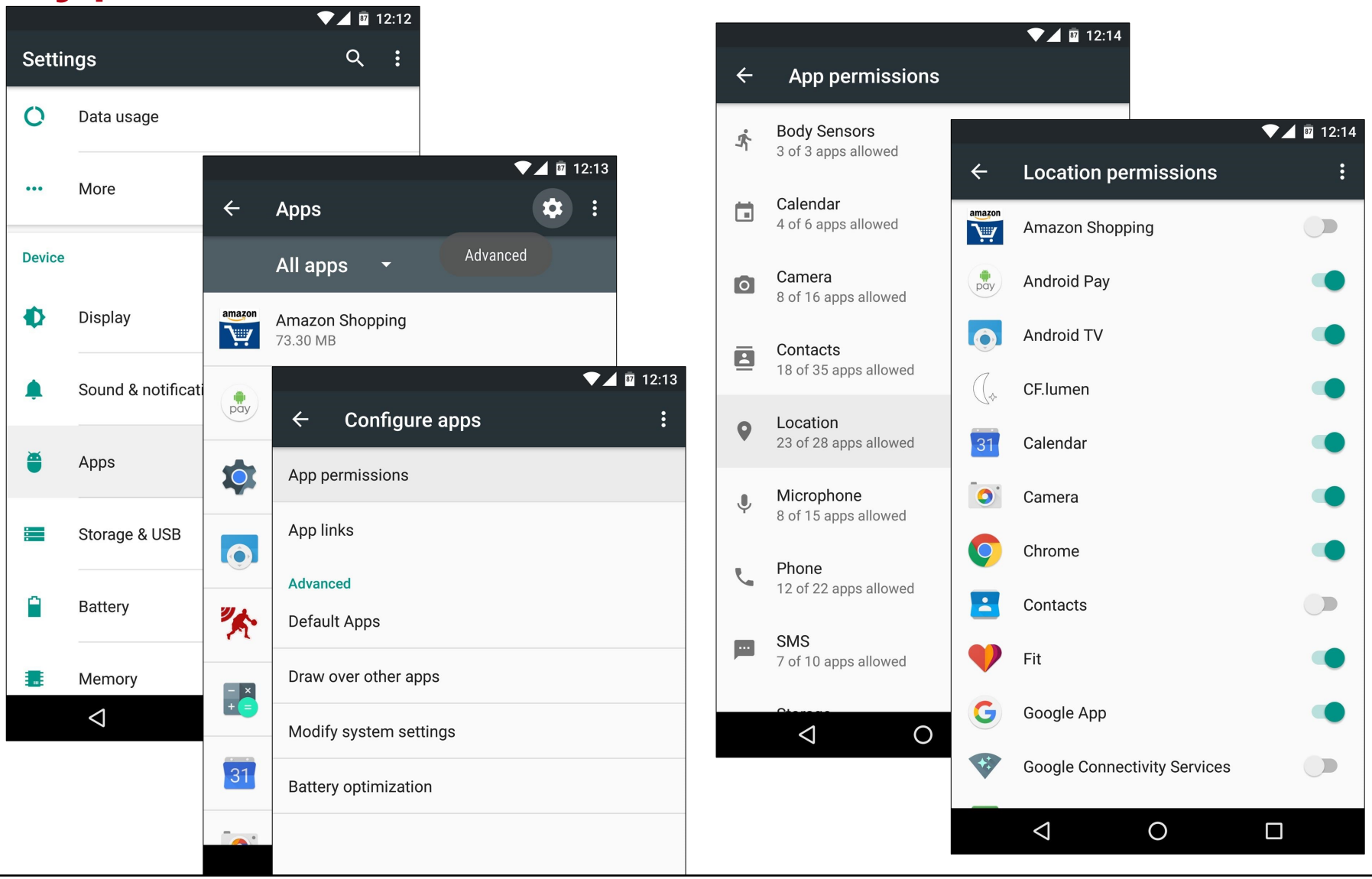


http://www.androidcentral.com/run-permissions-why-change-android-60-may-make-you-repeat-yourself

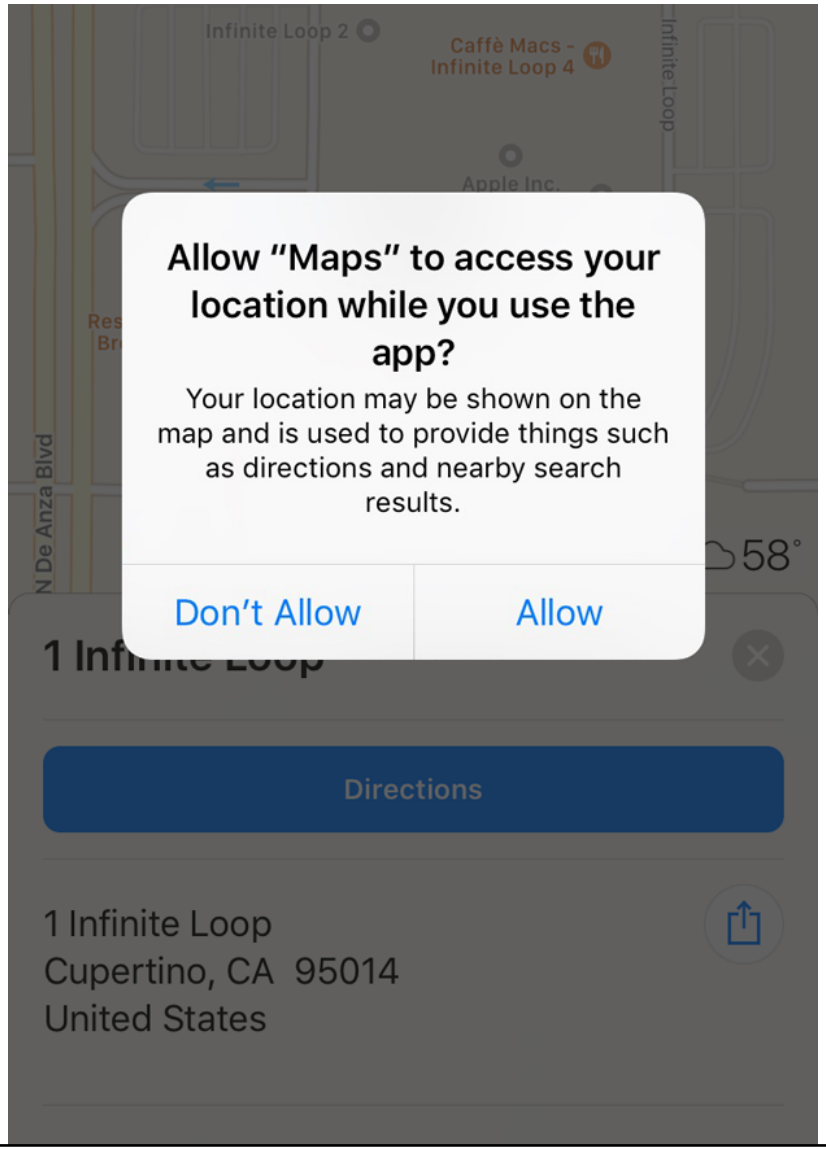
Android 6.0+ settings by app



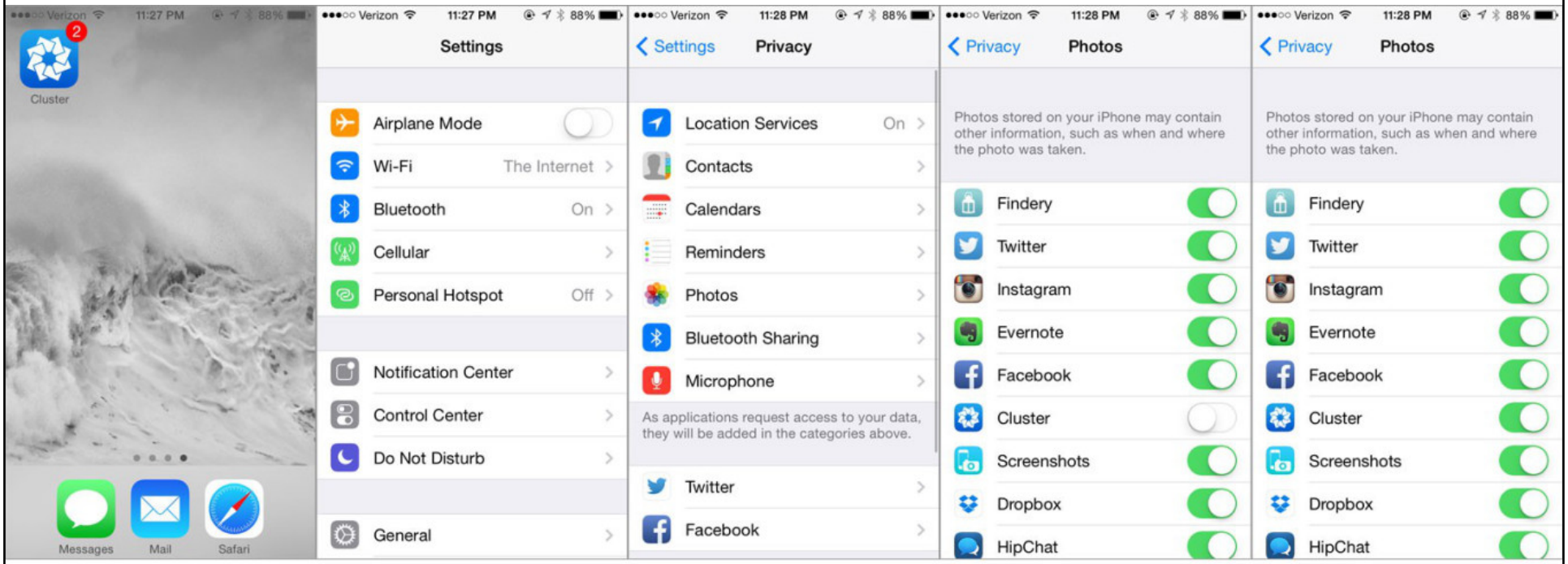
Android 6.0+ settings by permission type



Permissions in iOS



iOS settings by permission type



Close the App

Find and Open the Settings App

Find and Tap "Privacy"

Find and Tap "Photos"
(or permission needed)

Find "[App Name]" and Set Toggle to On

Usable security and privacy for IoT

IoT devices

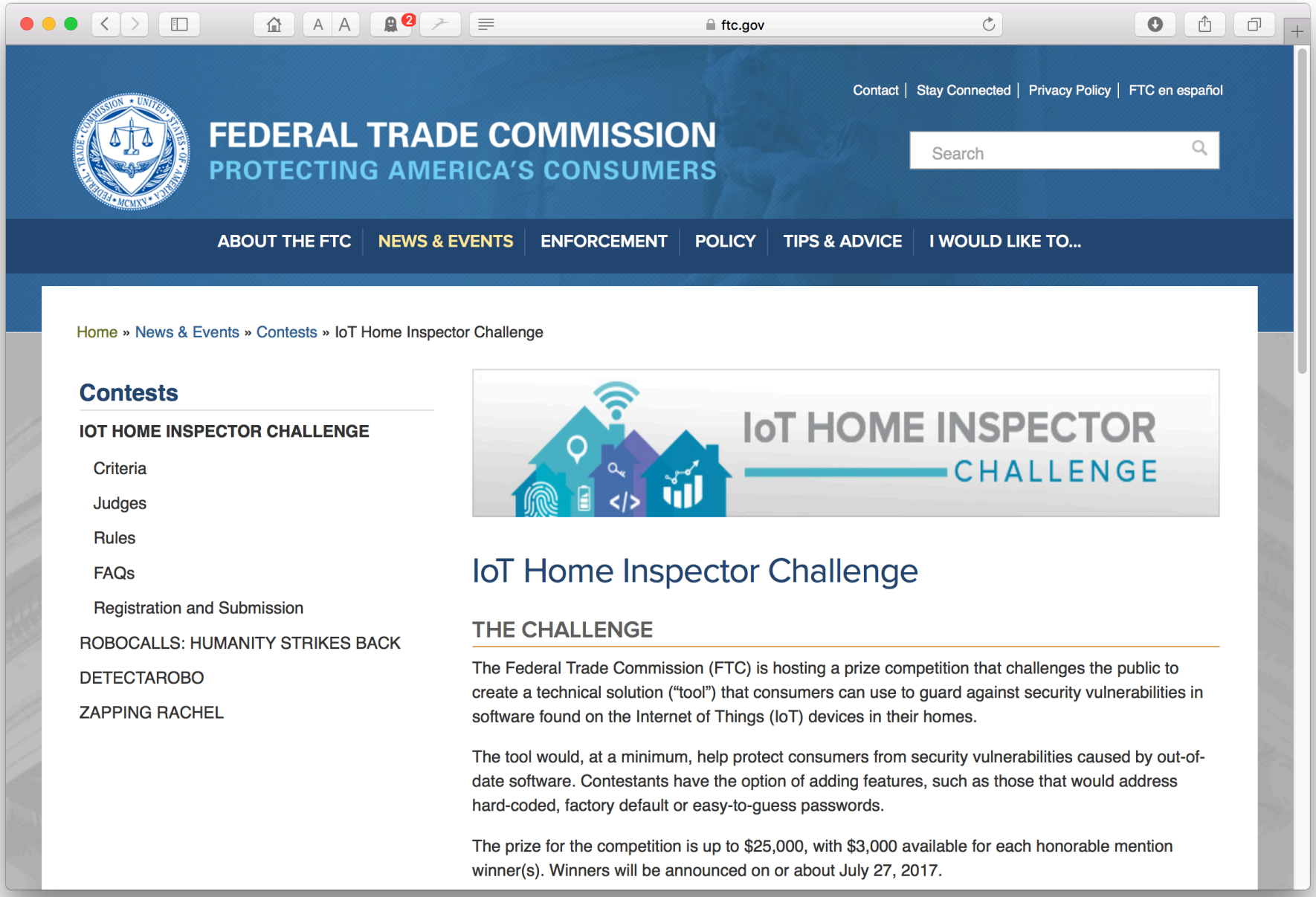
- Light bulbs
- Thermostats
- Smoke detectors
- Air monitors
- Moisture sensors
- Light sensors
- Motion sensors
- Smart plugs

http://iotlist.co

- Surveillance cameras
- Speakers
- Toys
- Fitness devices
- Smart watches
- Kitchen appliances
- Dash buttons
- Voice controllers
- Smart toilets

IoT security and privacy challenges

- Minimal or non-existent display for notice and consent
- Manufacturers want to make it fast and easy for users to install and use
- Devices need to communicate with other local devices and/or remote devices or servers
- Difficult for end users to find out about security problems and availability of updates, and actually update devices
- Devices likely to remain in use after manufacturer stops issuing security updates


ftc.gov
Contact | Stay Connected | Privacy Policy | FTC en español
FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS
Search
ABOUT THE FTC | NEWS & EVENTS | ENFORCEMENT | POLICY | TIPS & ADVICE | I WOULD LIKE TO...
Home » News & Events » Contests » IoT Home Inspector Challenge
Contests
IOT HOME INSPECTOR CHALLENGE
Criteria
Judges
Rules
FAQs
Registration and Submission
ROBOCALLS: HUMANITY STRIKES BACK
DETECTAROBO
ZAPPING RACHEL
IoT HOME INSPECTOR CHALLENGE
IoT Home Inspector Challenge
THE CHALLENGE
The Federal Trade Commission (FTC) is hosting a prize competition that challenges the public to create a technical solution ("tool") that consumers can use to guard against security vulnerabilities in software found on the Internet of Things (IoT) devices in their homes.
The tool would, at a minimum, help protect consumers from security vulnerabilities caused by out-of-date software. Contestants have the option of adding features, such as those that would address hard-coded, factory default or easy-to-guess passwords.
The prize for the competition is up to $25,000, with $3,000 available for each honorable mention winner(s). Winners will be announced on or about July 27, 2017.

FTC IoT Home Inspector Challenge

- FTC has released the following challenge
  - Create a technical solution (“tool”) that consumers can use to guard against security vulnerabilities in software found on the Internet of Things (IoT) devices in their homes
  - The tool would, at a minimum, help protect consumers from security vulnerabilities caused by out-of-date software. Contestants have the option of adding features, such as those that would address hard-coded, factory default or easy-to-guess passwords
- In small groups come up with an approach to addressing this challenge