Building Privacy into Your Mobile Apps

Joanne McNabb
Director of Privacy Education and Policy
California Attorney General’s Office
Mobile Privacy Concerns

- All privacy issues of desktops, plus:
  - New types of PII, including sensitive (location, call log, contacts)
  - Devices often not protected
  - Small screens
  - Many players in ecosystem
The Mobile Ecosystem

- User
- Ad NWs, Advertisers
- Carrier
- Device Mfr
- App Developer
- OS Developer
- App Platform
It takes an ecosystem…

…to protect privacy in mobile devices.
PRIVACY PRACTICES FOR MOBILE APP DEVELOPERS
Decision Path for Building Privacy into Apps

1. Use a checklist to consider the types of data your app could access or collect.

2. Decide what personally identifiable data your app needs for its basic functions.

3. Decide whether you will collect any non-essential data or “sensitive information.”

4. Decide on your data use, sharing, retention, and security practices.

5. Prepare a statement of your general privacy policy, covering your data practices including any enhanced measures.

6. Decide on your need for enhanced measures.

   If needed, decide whether to use “special notices” or the combination of a short privacy statement and privacy controls.
Best Practices for App Developers

• Avoid or limit collecting PII not required for app’s functionality
• Avoid or limit collecting sensitive information
• Use app-specific, non-persistent device IDs
Surprise Minimization
Enhanced Privacy Notice

- Alert users with enhanced measures
  - For collection of PII not related to app’s basic functionality
  - For collection of sensitive information
- Two approaches recommended
  - Short privacy statement + privacy settings
  - Just-in-time “special notices”
PROVIDING NOTICE ON SMALL SCREENS
NTIA CODE OF CONDUCT

• National Telecommunications & Information Administration, U.S. Department of Commerce

• Multistakeholder process to develop “code of conduct” for mobile app transparency, July 2012-July 2013
NTIA CODE OF CONDUCT

• App Developers → Focus on “short notice”
  • Collection of data types (biometric, location, browser history, user files, etc.)
NTIA CODE OF CONDUCT

- App Developers → Focus on “short notice”
  - Sharing of user data with third parties (ad networks, carriers, government entities)
Prettier, More Effective Short-Form Privacy Policy

• Apps for iOs and Android
  • Lookout Mobile Security, www.lookout.com
  • Intuit’s Quicken, www.quicken.com/stay-connected-your-money

• User testing > improved design
LOOKOUT: Make It Easy to Notice

In the App Store

In the App

Settings

Done

your data daily.

ABOUT LOOKOUT

Account

Free

Support

Legal

Privacy Policy

Terms of Service

Account: jmcmabb691@aol.com

Lookout Version: 3.10.2
Hit the Key Points

Source: Lookout Mobile Security
Provide Details

Email Address - When you create an account
Phone Number - When you activate the app
Contacts - When you use Contacts Backup
Details on Sharing

To help you with Missing Device features
To remove you from texts or emails promoting Lookout
To analyze product performance
For billing reconciliation purposes

To gain insights that help us improve your experience with our product
To create an engaging marketing experience for you
Create Your Own Visual Privacy Policy

Open source code from Lookout Mobile Security on Github
Mobile Privacy Resources

• California Attorney General, *Privacy on the Go: Recommendations for the Mobile Ecosystem*
  • [www.oag.ca.gov/privacy/business-privacy](http://www.oag.ca.gov/privacy/business-privacy)

• Federal Trade Commission, *Mobile Privacy Disclosures*
  • [http://www.ftc.gov/opa/2013/02/mobileprivacy.shtm](http://www.ftc.gov/opa/2013/02/mobileprivacy.shtm)

• NTIA, Code of Conduct on Mobile App Transparency

• Lookout Mobile Security, Private Parts
  • [https://github.com/lookout/private-parts](https://github.com/lookout/private-parts)
Joanne McNabb, CIPP/US, CIPP/G, CIPT
Director of Privacy Education & Policy
California Attorney General’s Office

www.privacy.ca.gov