Is Your App Compliant? Designing Your Mobile Privacy Policy

Daniel Rockey
Bryan Cave LLP

Daniel.Rockey@bryancave.com

BRYAN CAVE

A Broader Perspective℠

Overview

- Section 1: Privacy Policies and California law
- Section 2: OPPA applies to Mobile
- Section 3: Requirements
- Section 4: Best Practices

Section 1: Privacy Policies and Cal Law

- California enacts Online Privacy Protection Act (Cal. Bus. & Prof. Code §§ 22575 -22579) in 2004
- Operators of "commercial Web site or online service that collects personally identifiable information through the Internet"
  - Website: "conspicuously post" privacy policy
  - Online service: policy must be "reasonably accessible"
- Became *de facto* national requirement

Section 2: Cal OPPA applies to Mobile

- February 2012: Cal AG announces "Joint Statement" with app platforms to improve privacy protections
  - Amazon, Apple, Google, Hewlett-Packard, Microsoft, Research In Motion, and later Facebook
- "It is the opinion of the Attorney General that the California Online Privacy Protection Act requires mobile applications that collect personal data from California consumers to conspicuously post a privacy policy."
- Joint Statement is "not intended to impose legally binding obligations on the Participants or affect existing obligations under law."

Section 2: A Shot Across The Bow

- October 2012: Cal AG issues "non-compliance letters" to 100 app developers
  - Big names: United and Delta Airlines, OpenTable
- "An operator of a mobile application . . . that uses the Internet to collect PII is an 'online service' within the meaning of Cal OPPA"
  - App is non-compliant
  - 30 days to comply

Section 2: A Shot Across The Bow

- “Violations . . . may result in penalties of up to $2,500 for each violation, i.e., for each copy of the unlawful app downloaded by California consumers.”
- “Having a Web site with the applicable privacy policy conspicuously posted may be adequate, but only if a link to that Web site is ‘reasonably accessible’ to the user within the app.”

Section 2: AG Drops The Hammer

- December 6, 2012: Cal AG files lawsuit against Delta Airlines
- "Fly Delta" app collects user's full name, telephone number, email address, frequent flyer account number and PIN code, photographs, and geo-location information
- No in-app privacy policy

Section 2: AG Drops The Hammer

- Policy at www.delta.com insufficient:
  - doesn't cover app;
  - not "reasonably accessible" from app;
  - doesn't disclose collection of geo-location, photographs
- Seeks $2,500 per non-compliant download -- alleges app downloaded "millions of times"
- Delta moves to dismiss – hearing set for April 10

Section 3: Required Elements

- Must
  - Be “reasonably accessible” to user
  - Identify “categories” of PII collected
  - Identify “categories” of third-parties with whom PII may be shared
  - If allow review and correction, describe process
  - Describe notice of changes
  - Effective Date

Section 4: Best Practices

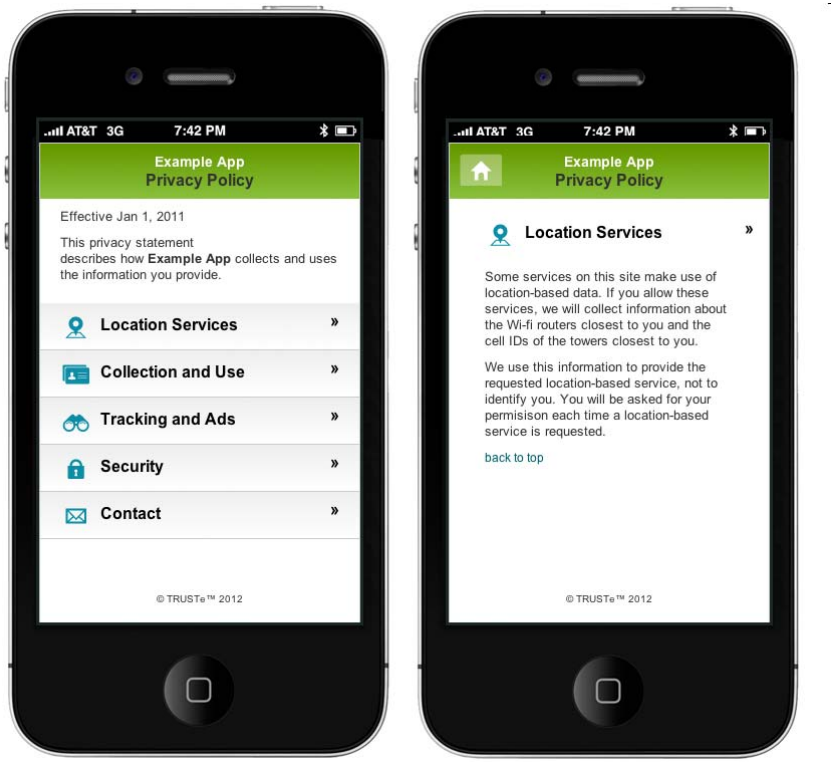
- “Privacy On The Go: Recommendations For The Mobile Ecosystem” (Cal AG)
- “[O]ffer greater protection than afforded by existing law."
- Two Key Principles:
  - Surprise minimization
  - Shared Accountability (i.e., between hardware manufacturers, operating system developers, mobile telecommunications carriers, advertising networks, and mobile app developers)

Section 4: Best Practices

- Apple™ App Store and Android/Google Play:
  - Pre-download disclosure
  - In all events, prior to data collection (i.e. welcome screen)

Section 4: Best Practices

- Compact/Layered policy



BRYAN CAVE

Section 4: Best Practices

- Privacy by Design and Data Minimization
  - Consider privacy in build process
  - Minimize collection of PII for uses not related to app's basic functionality and
  - Avoid or limit collection of sensitive information (PHI, financial account numbers and precise geolocation data)

Section 4: Best Practices

- Limit Data Retention
  - Retain PII only as necessary to support intended function or meet legal requirements
  - Adopt processes for ensuring secure disposal of data

Section 4: Best Practices

- Allow User Access
  - AG recommends companies develop mechanisms to give users access to PII
  - Allow opt-out

Section 4: Best Practices

- Adequate Security Measures
  - Technical (firewalls, AV software and patches, intrusion detection)
  - Physical (limit access to servers; secure authentication protocols)
  - Administrative (employee training; security incident reporting)

Bryan Cave LLP

Daniel Rockey
Bryan Cave LLP

560 Mission St., 25th Fl.
San Francisco, CA 94105
Daniel.Rockey@bryancave.com
415-268-1986

BRYAN CAVE