

RSA[®] CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

What Is the Future of Data Privacy and Security in Mobile?

SESSION ID: MBS-T08

Charles McColgan

CTO
TeleSign Corporation
cm@telesign.com

Tanya Forsheit

Founding Partner
InfoLawGroup LLP
[@Forsheit](https://twitter.com/Forsheit)



Agenda

- **The Technology – What's Exposed and What's Available?**
 - Unique Identifiers
 - Android and GCM
 - iPhone and APNS
 - SMS and the GSM Network

Agenda (cont.)

- **How Does the Law Address These Issues?**

- California Attorney General Enforcement and Education Regarding Mobile App Privacy Policies
- Federal Trade Commission Guidance and Enforcement
- Cross-Border Data Transfers
- Kids' Privacy and Other Concerns Regarding Kids and Mobile

- **Government Access**

- Technological Issues
- Legal Issues



RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Mobile Architecture – Who Can See Your Data

How does your phone communicate?



WiFi

802.11 interface to phone,
OS and Applications



Bluetooth

Exchange data with other apps
and devices peer to peer over
short distances



GPS

Antenna allows interaction with
Global Positioning Satellite system
to determine precise location



GSM / CDMA

Cellular data protocols to support SMS,
Telephony and data services

What are some ways to identify people?

UDID

Universally Unique Identifier for a device – deprecated on iOS

Registration_id

Unique identifier for a device / app pair on Android



Advertising ID, IDFA, Ad ID, etc

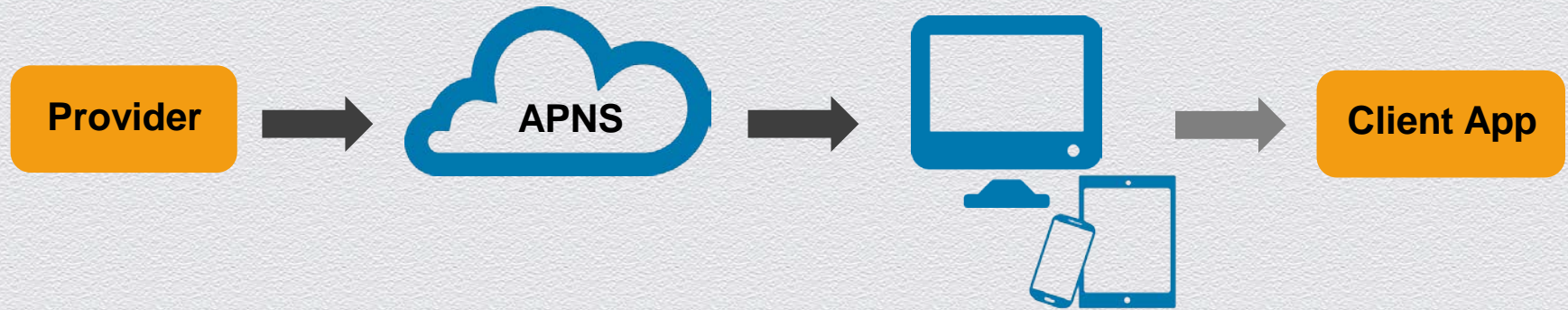
Device Token

Unique identifier for a device / app pair on iOS

IMEI, IMSI, MAC, IP, etc...

How do Mobile Apps Communicate?

Apple's APNS



What does iOS allow an app to see?

Once installed bi-directional communication to the app's servers

Access to information on phone including:



Location



Contacts



Calendar



Microphone



Photos



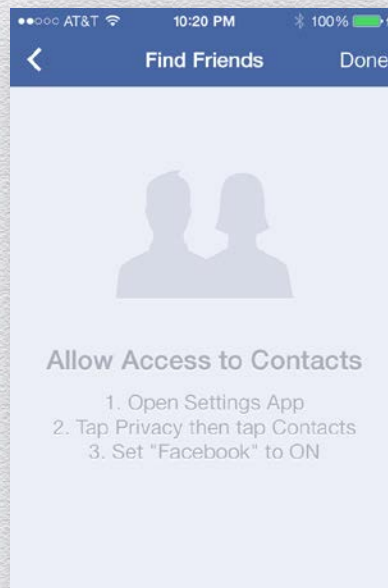
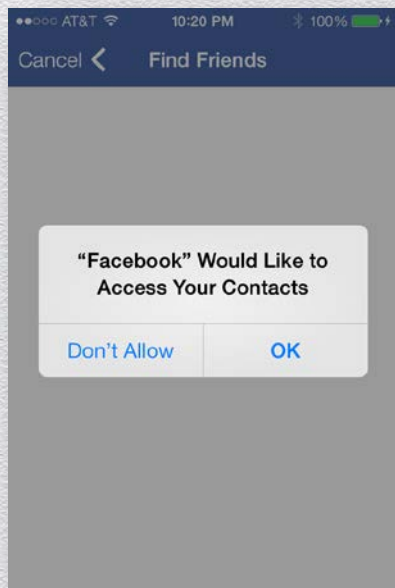
Reminders



Bluetooth

That seems like a lot, what's the catch?

The OS captures access to these items and pushes up an explicit permission window when an app tries to access it.



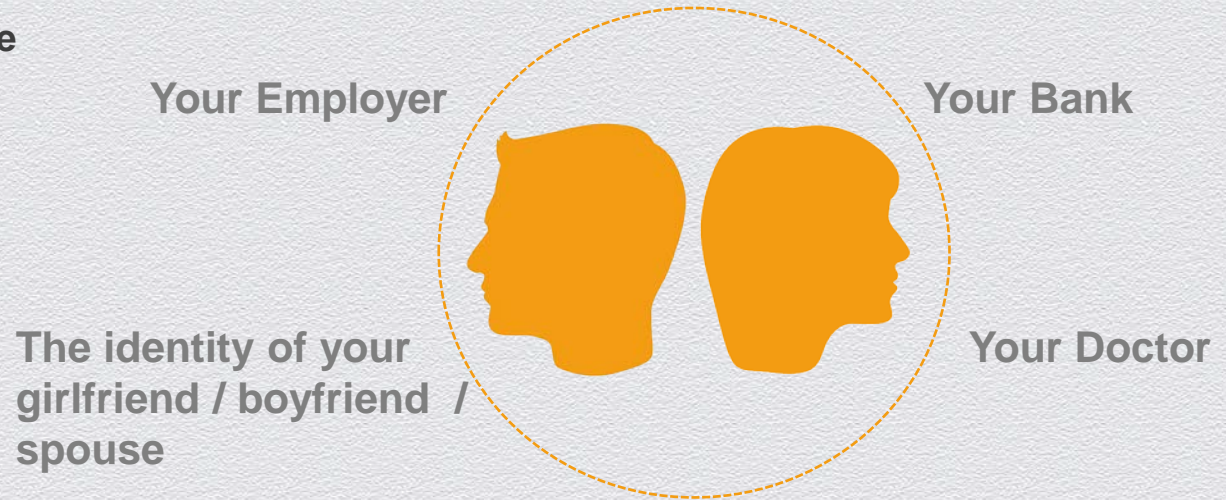
Ok that seems ok...

Well sort of...

Consider what you have in
your contacts

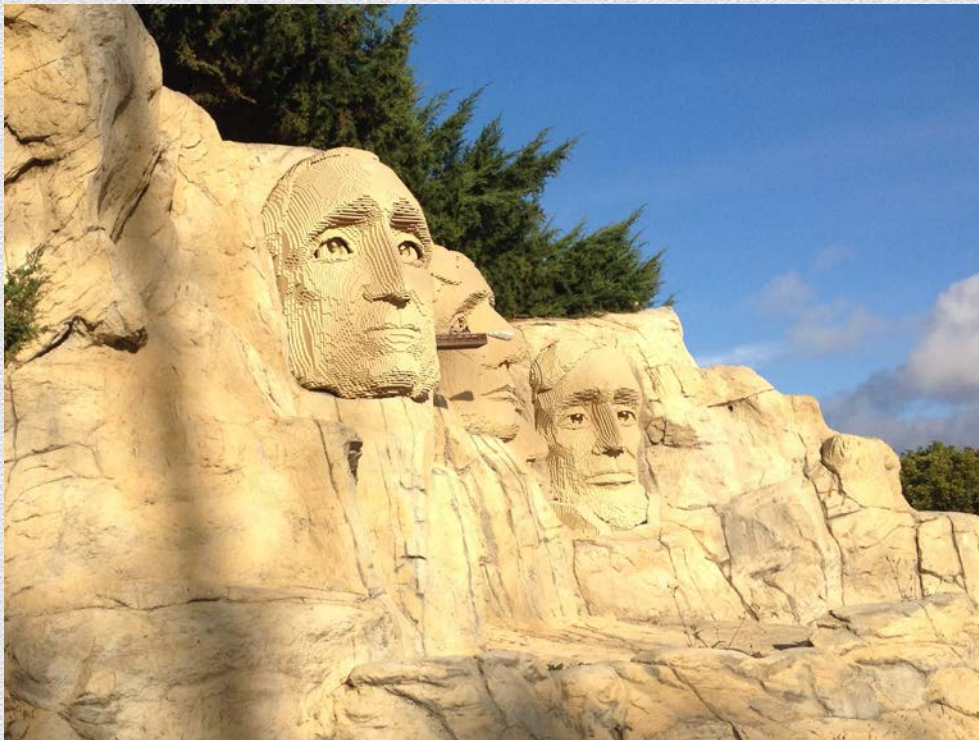
Name, Address, Email, Phone
Number, Notes

What can be determined by this:



Well photos seem harmless (maybe)...

But consider what other data can be determined from this photo that I took at Mt. Rushmore...



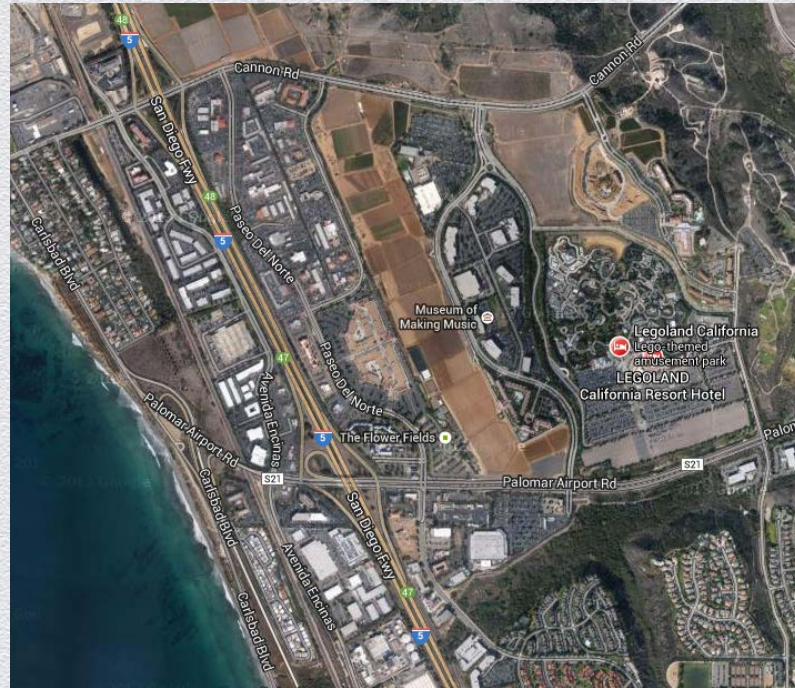
Photos come with EXIF data....

Preset	None
File Name	IMG_3172.JPG
File Path	2014-02-09
Dimensions	3264 x 2448
Cropped	2239 x 1679
Date Time Original	2/9/2014 4:02:50 PM
Date Time Digitized	2/9/2014 4:02:50 PM
Date Time	2/9/2014 4:02:50 PM
Exposure	1/1700 sec at f / 2.4
Focal Length	4.28 mm
Focal Length 35mm	35 mm
Brightness Value	10.14
ISO Speed Rating	ISO 50
Flash	Did not fire
Exposure Program	Normal
Metering Mode	Pattern
Make	Apple
Model	iPhone 4S
Lens	iPhone 4S back camera 4.28mm f/2.4
Software	7.0.4
User Comment	
GPS	33°7'41" N 117°18'43" W
Altitude	147.6 ft
Direction	East

- Name of phone
- Date photo was taken to the second
- Type of camera
- GPS location of photo
- Altitude of photo
- Direction camera was facing

So what do we know?

- Legoland, CA **NOT** Black Hills, South Dakota.
- Every photo on an iPhone or Android device has this data



How do Mobile Apps Communicate?

Android's GCM Service

Google Cloud Messaging



GCM can be used to notify or push content to the device

What does Android allow an app to see?



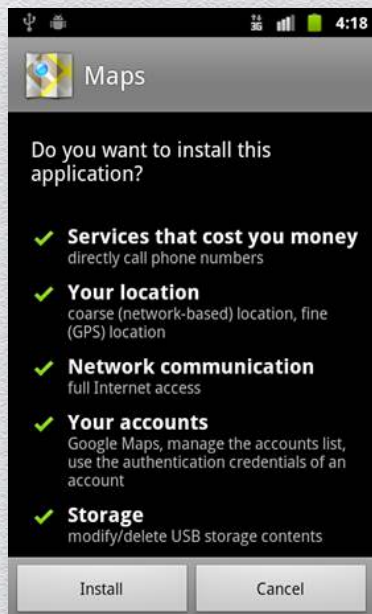
Different model than iOS

Android can basically see everything on a phone but...

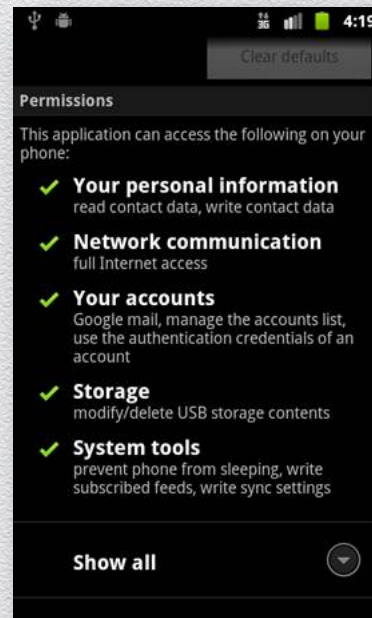
- Very explicit opt in on exactly what the app can do before it launches
- Can be overwhelming or confusing to normal users but to the expert is more specific on what is getting sent to the App's servers

What Android tells the user

When you install an App



For an App already Installed



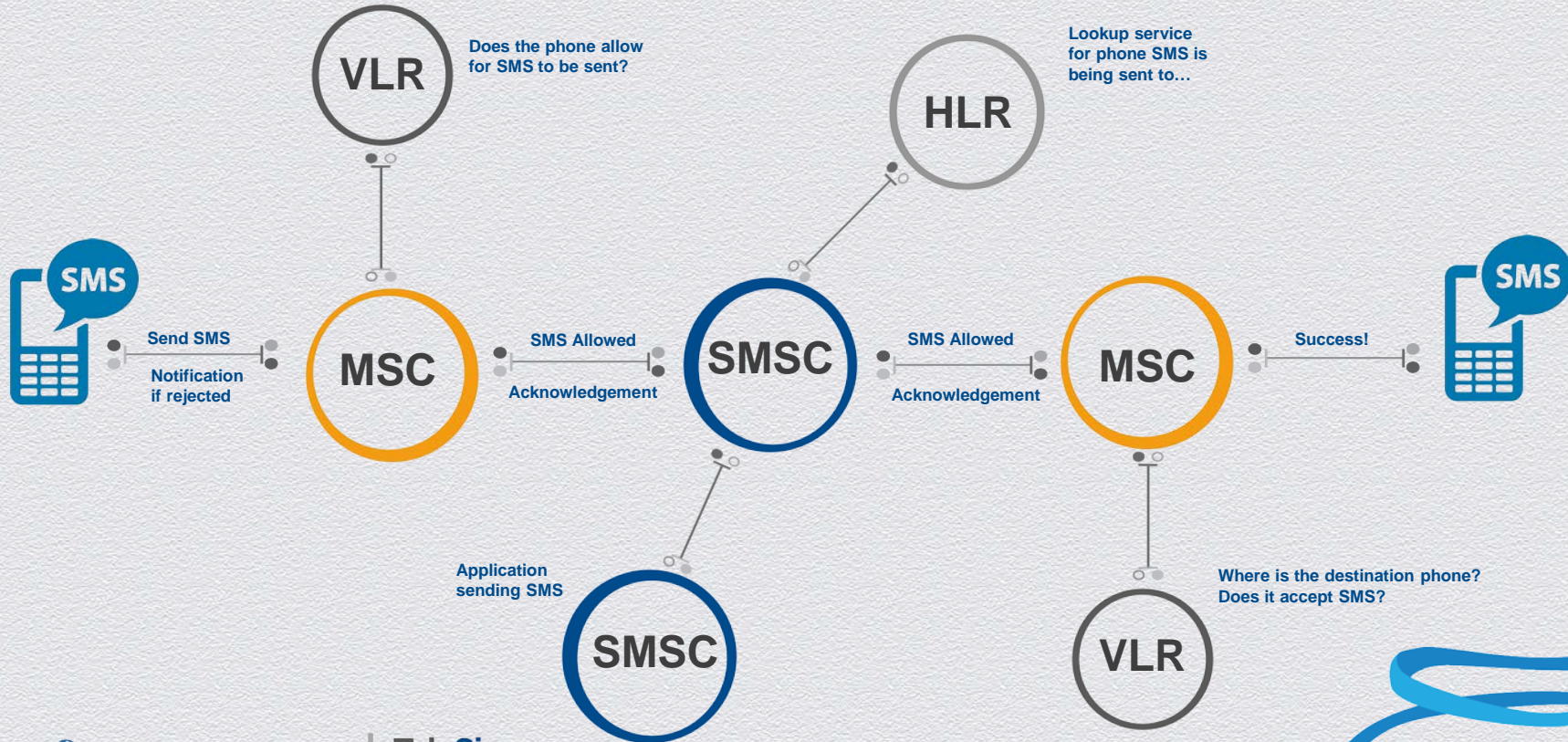


RSA[®]CONFERENCE2014

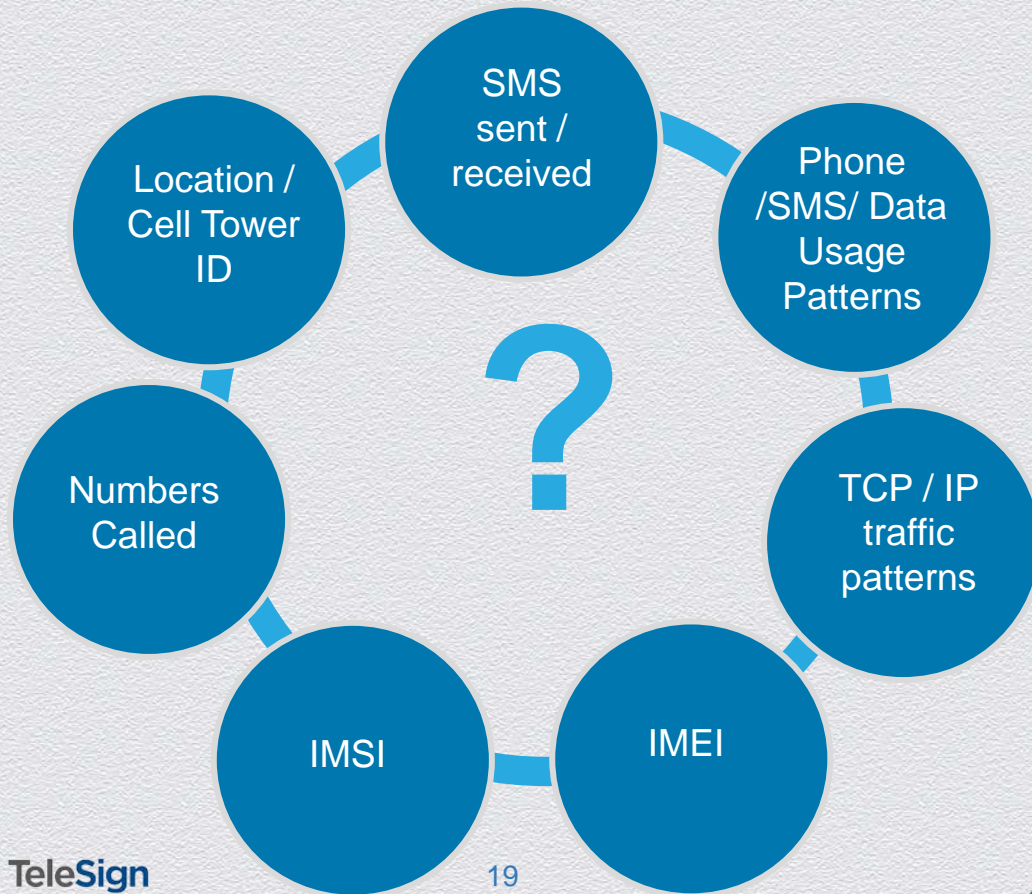
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

**What about my cell
phone?**

How SMS is sent...

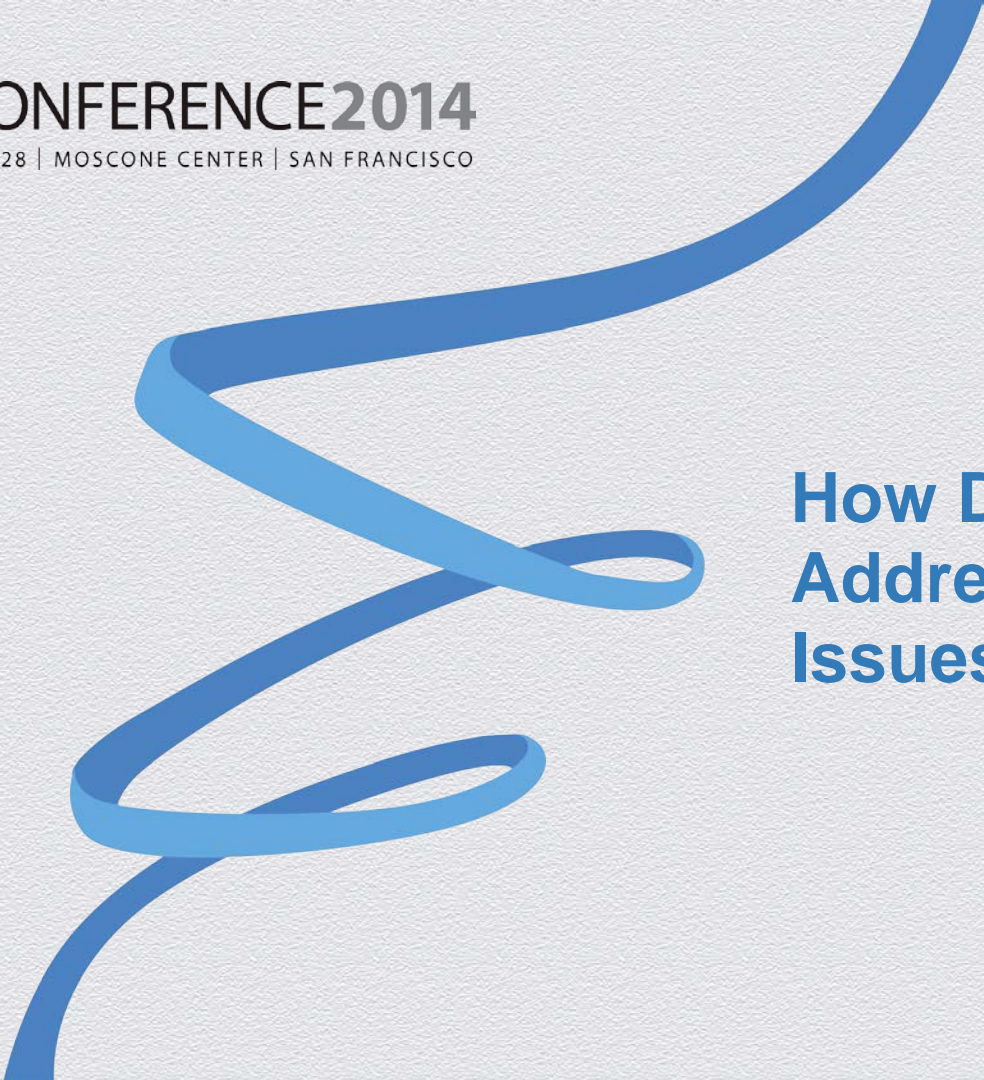


What data is available to an operator?



RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



**How Does the Law
Address These
Issues?**

How Does the Law Address These Issues?

Regulators have taken notice:

- Application and enforcement of existing laws to regulate mobile
- Issuance of new guidance
- Voluntary, self-regulatory efforts
- Updating of old laws to address mobile





RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

**California Attorney
General Enforcement
and Education
Regarding Mobile App
Privacy Policies**

California Attorney General

The California Attorney General's position on mobile app and privacy policies is clear and consistently articulated:

Mobile apps require a conspicuously-posted privacy policy under California Online Privacy Protection Act, Cal. Bus. & Prof. Code §§ 22575-22579 (“CalOPPA”).



California Attorney General (cont.)

February 2012

- Agreement with Amazon, Apple, Google, Hewlett-Packard, Microsoft, and Research In Motion; Facebook later signed on.
- Platforms agreed to include in the application submission:
 - A hyperlink to the app's privacy policy
 - OR a statement describing the app's privacy practices.



California Attorney General (cont.)

October 2012

- California AG Kamala Harris tweets: “Fabulous app, @United Airlines, but where is your app’s #privacy policy?”
- California AG reportedly notifies as many as 100 apps of the need to comply with CalOPPA within 30 days or face penalties of up to \$2,500 *for each download* of a noncompliant app.



California Attorney General (cont.)

- **December 2012:** California AG sues Delta alleging term “online service” covers mobile applications, and requires a privacy policy to be available within the app.
- **January 2013:** California AG issues [“Privacy on the Go”](#) to “educate the industry and promote privacy best practices.”
- **May 2013:** California Superior Court dismisses the lawsuit against Delta on the grounds that the Airline Deregulation Act of 1978 (ADA) preempts CalOPPA. Case is on appeal.





RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Federal Trade Commission Guidance and Enforcement

Federal Trade Commission Guidance and Enforcement



February 2013

- The Federal Trade Commission (“FTC”) issues a staff report, [“Mobile Privacy Disclosures: Building Trust Through Transparency”](#),
- Suggestions for mobile privacy disclosures by (1) mobile platforms, (2) app developers, (3) advertising networks and (4) everyone else, including app developer trade associations, academics, usability experts and privacy researchers.

Federal Trade Commission Guidance and Enforcement (cont.)



March 2013

- FTC issues staff report on mobile payments: ["Paper, Plastic... or Mobile? An FTC Workshop on Mobile Payments"](#), addressing Dispute Resolution, Security and Privacy
- FTC issues updates to [.Com Disclosures](#), with new focus on mobile and social media

Federal Trade Commission Guidance and Enforcement (cont.)



December 2013

- FTC settlement [*In re Goldenshores Technologies, LLC*](#)
- First to impose substantial conditions upon the collection of location data
- Provides guidance for app developers and publishers regarding
 - The sharing of geolocation data
 - When an app may begin collecting and sharing data,
 - Privacy representations made in a license agreement





RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Cross-Border Data Transfers

Cross-Border Data Transfers

- All the same old problems
- Same compliance options:
- **But . . . New EU Regulation on the horizon, could lead to dramatic change.**

RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



Kids' Privacy and Other Concerns Regarding Kids and Mobile

Kids

December 2012: FTC releases report on mobile apps for kids.

- Findings:

- For the most part, privacy and other material disclosures are still not being made available to parents prior to app download or at all.
- Where there are privacy disclosures, the disclosures sometimes contradict the actual practices of the app.



Kids (cont.)

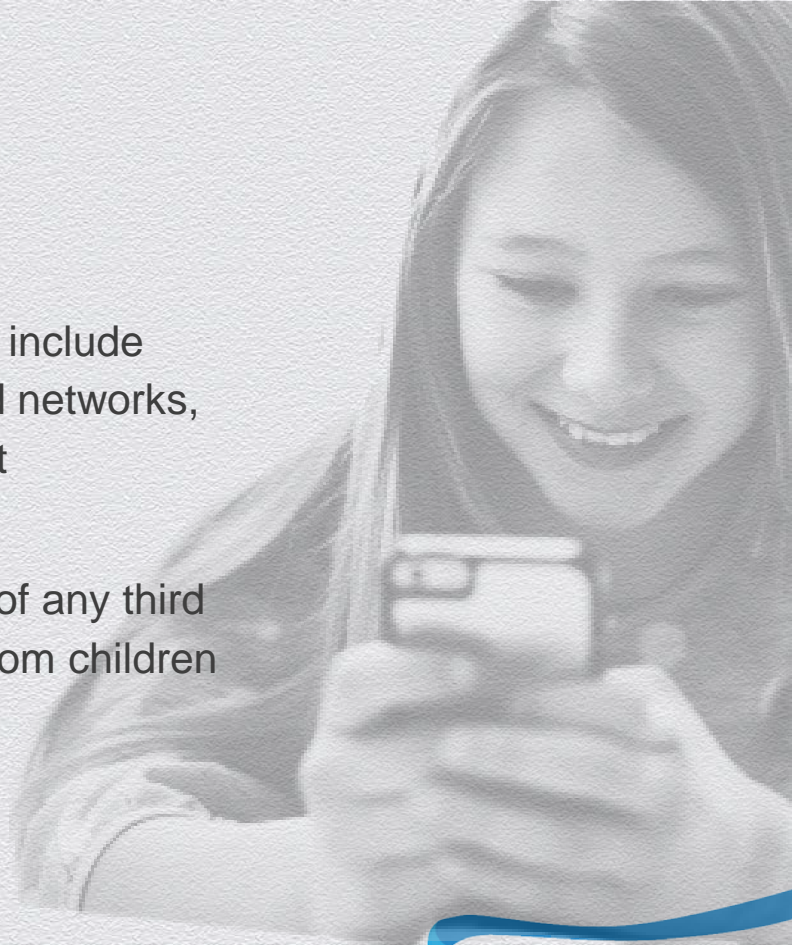
Same month, the FTC finalizes amendments to the Children's Online Privacy Protection Act ("COPPA") Rule, originally enacted in 2000.

- In response to the pace of change of technology on websites and other services, particularly mobile apps.
- Revised definition of "personal information"

Kids (cont.)

COPPA (cont.)

- New Rule expands the definition of “operator” to include certain service providers, including third party ad networks, which operate on websites and knowingly collect information from users of those websites.
- Operators are now directly liable for the actions of any third party service providers that collect information from children on their sites.



Kids (cont.)

January 15, 2014

- FTC settles case with Apple Inc.
- FTC alleges Apple charged for kids' in-app purchases without parental consent
- Apple will provide consumer refunds of at least \$32.5 Million



RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Government Access

Technological Issues

- PRISM surveillance program for Server infrastructure with major providers
 - Email, voice, text, video chats
- UPSTREAM surveillance program for fiber surveillance
 - Raw data on fiber between countries / data centers
- Court orders to many / most telecom providers
- Efforts to weaken or crack encryption standards



Legal Issues

- Fourth Amendment
- Stored Communications Act
- NSA Litigation



The Future

- Know what information you are collecting
- Work with your privacy lawyer to create an updated privacy policy
- Be fluid with changing technology and platforms
- Keep your eye on EU, California, and the FTC

Resources:

- **For Apple:**
["Privacy Support in iOS and OS X from the 2012 Apple WWDC"](#)
(This link may require registration)
- **For Android:**
["Android Security Overview – How users understand third party applications"](#)



RSACONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



Thank you.