Privacy

Why it's important, and what you can do!

Andrew Zamler-Carhart

December 10, 2013

DevCon 2013: Dec 9th–11th 2013, Monte Carlo

What is privacy?


© Barcroft Media


Something for lawyers to figure out?


Something we gave up to Facebook?


Something the NSA stole from us?

What is privacy?

- Personal data that is collected
- Who has access to it
- What they can do with it
- People expect companies will use their data in limited ways, and protect it from unauthorized access

Who is this presentation for?

- You, whether you're a developer or a manager
- Too important to be left to the lawyers
- Not something to be left until the end of a project (like design, quality, performance, security…)
- Privacy is something you build into a product

Why is privacy important?

- Legal compliance
- Industry certifications
- Internal requirements
- Customer requirements
- Best practices (don’t be evil)

Google Glass Is Banned On These Premises

What data needs protecting?

- Anonymous data
  - logs, statistics, crash logs
- Pseudonymous data
  - unique identifiers, browser cookies, search history
- Personally identifiable information (PII)
  - contact info, demographic data, healthcare info, financial info, online activity
- Sensitive PII
  - credit cards, identification numbers, mother's maiden name, passwords, location

Writing a privacy policy

- What data will be collected
- Why it is necessary to collect the data
- How it will be stored
- How long it will be stored for
- Who has access to it
- How much control the user has over it
- …there is no standard privacy policy

Asking permission

- In the license agreement?
- Ask for what you need, when you need it
- Explain primary and secondary purposes
- Offer a good deal
- Reassure the user
- Limited scope and duration
- Let the user change their mind
- Fail gracefully

Request for Permission

Minor Monitor is requesting permission to do the following:

Access my basic information
Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've shared with everyone.

Access messages in my inbox

Access posts in my News Feed

Access my data any time
Minor Monitor may access my data when I'm not using the application

Check-ins
Minor Monitor may read my check-ins and friends' check-ins.

Access my profile information
Likes, Music, TV, Movies, Books, Quotes, About Me, Groups, Notes, Birthday, Hometown, Current City and Facebook Status

Access my photos and videos
Photos Uploaded by Me, Videos Uploaded by Me and Photos and Videos of Me

Access my friends' information
Birthdays, Hometowns, Current Cities, Likes, Music, TV, Movies, Books, Quotes, Groups, Notes, Photos, Videos, Photos and Videos of Them, 'About Me' Details and Facebook Statuses

Minor Monitor

By proceeding, you agree to the Minor Monitor Terms of Service and Privacy Policy · Report App

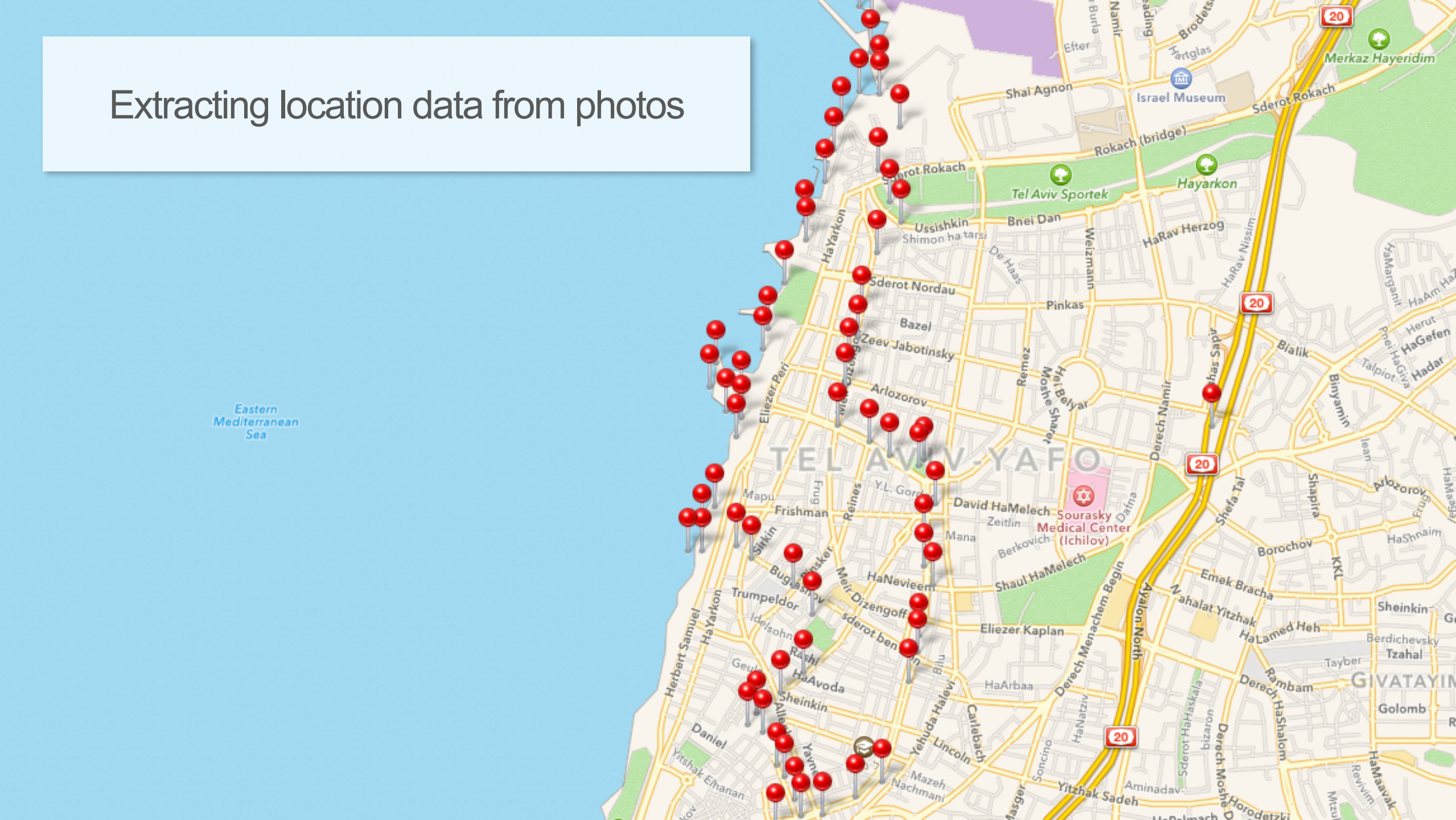
Logged in as Neil J. Rubenking (Not You?)

Allow | Don't Allow

Collecting data

- Provides benefits but reduces privacy
- Balance positive and negative effects
- Don’t collect data you don’t need
- Device identifiers
- Mixing data of different types

Extracting location data from photos



Managing data

- Anonymize
- Aggregate
- Randomly sample
- Reduce precision
- Decay
- Minimize

User control

- Transparency
- Delete some
- Delete all
- Revoke agreement
- Close account and delete data
- Export data
- Coexistence

Data access

- The user
- Household
- Service providers
- Cisco
- Third-party developers
- Advertisers
- Hackers
- Government

Risks

- Creepiness
- Lost devices
- Spying
- Hacking
- Identity theft
- Public violations

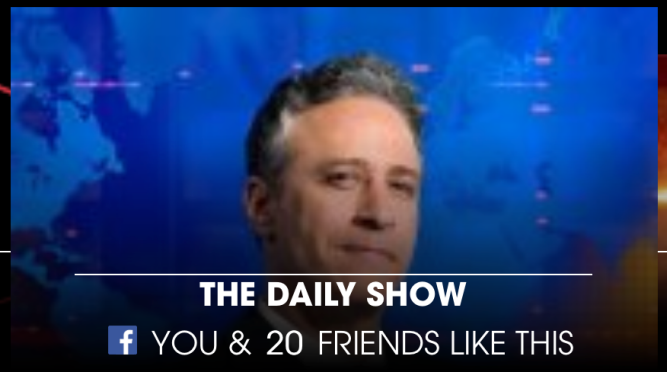
Her Majesty watches telly too.

Cloud considerations

- Encrypt data in motion
- Encrypt data at rest
- Separate sensitive and other data
- Separate data between tenants
- Know where data is being stored
- Use APIs to control access to data

Example: Bento User Identity

SCHEDULED
SHOWS MY FRIENDS LIKE



SHOWS I LIKE
WATCHLIST

Example: Bento User Identity

- Personal and social television services
- Social schedule based on shows your friends like
- Personal metadata for your favorite shows
- Services that increase user engagement
- Users own their personal data
- Aggregated and anonymized data available to service providers through APIs

Links

- External: http://www.cisco.com/go/privacy
- Internal: http://wwwin.cisco.com/legal/privacy
  - Policies & Guidelines
    - Privacy by Design: Product Development Guidelines for Engineers and Product Managers

Thank you.