Context-centric Security

Mohit Tiwari, Prashanth Mohan, Andrew Osheroff,
Hilfi Alkaff, Eric Love, Elaine Shi,
Dawn Song, Krste Asanović
UC Berkeley

Context-centric Security

- Contexts are light-weight real-life events
  - a conference hallway meeting, a birthday party
- User shares contexts with contacts
  - policies not based on permissions or labels
- System infers all low-level details
  - in contrast to current practice…

App-centric Privacy: Problematic

- Permissions are abstruse
  - SD Card, File systems,…
  - 56 of 100+: dangerous
  - Statically assigned
- App owns user's data

Data-centric Privacy: Problematic

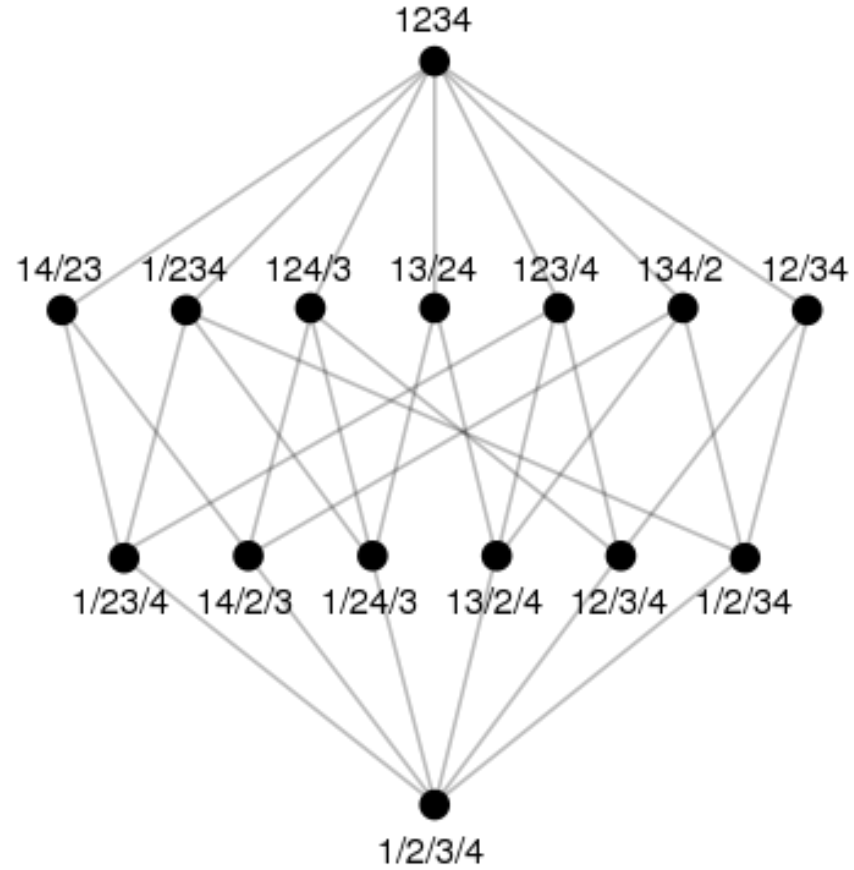
Data

X

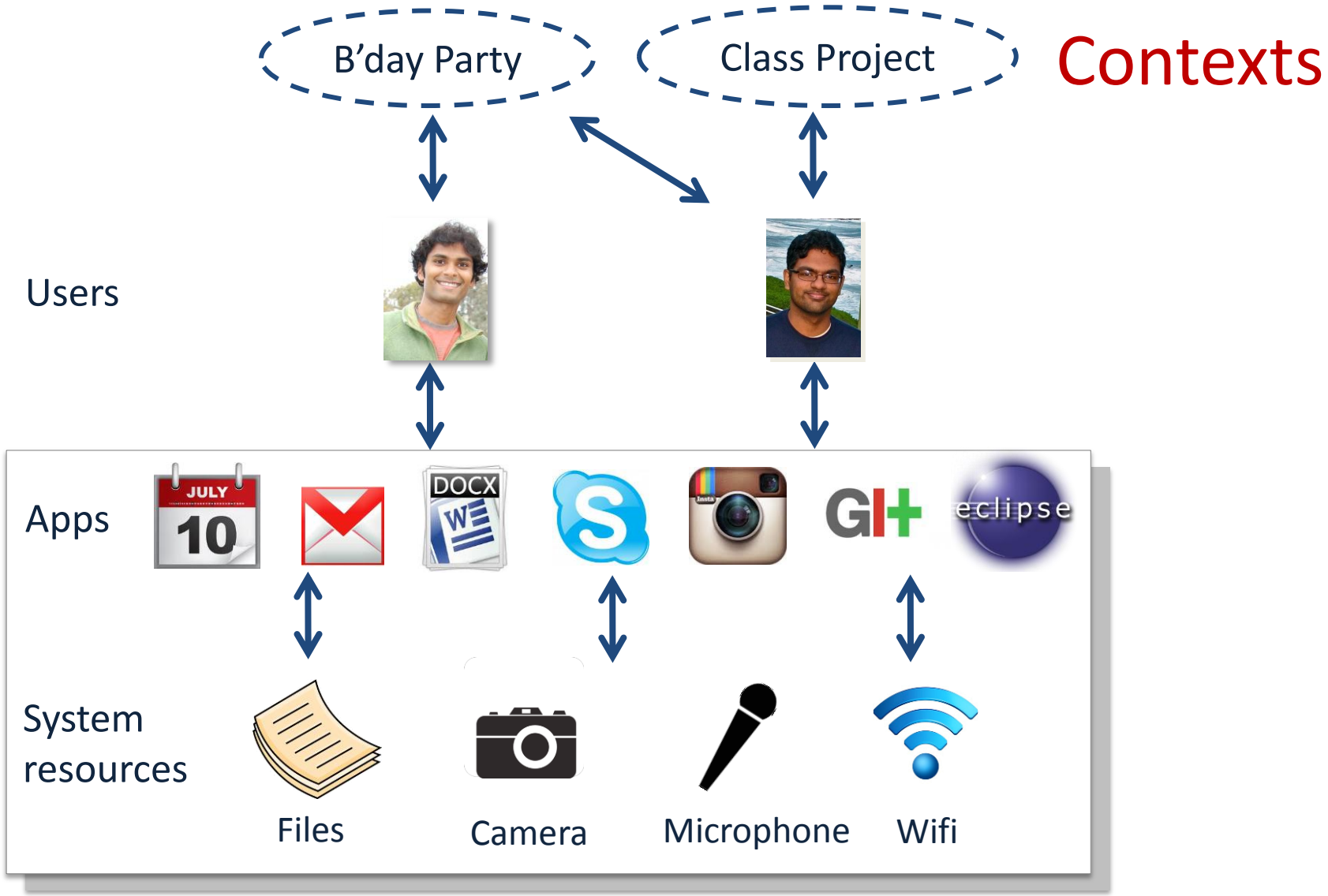
Principals

→

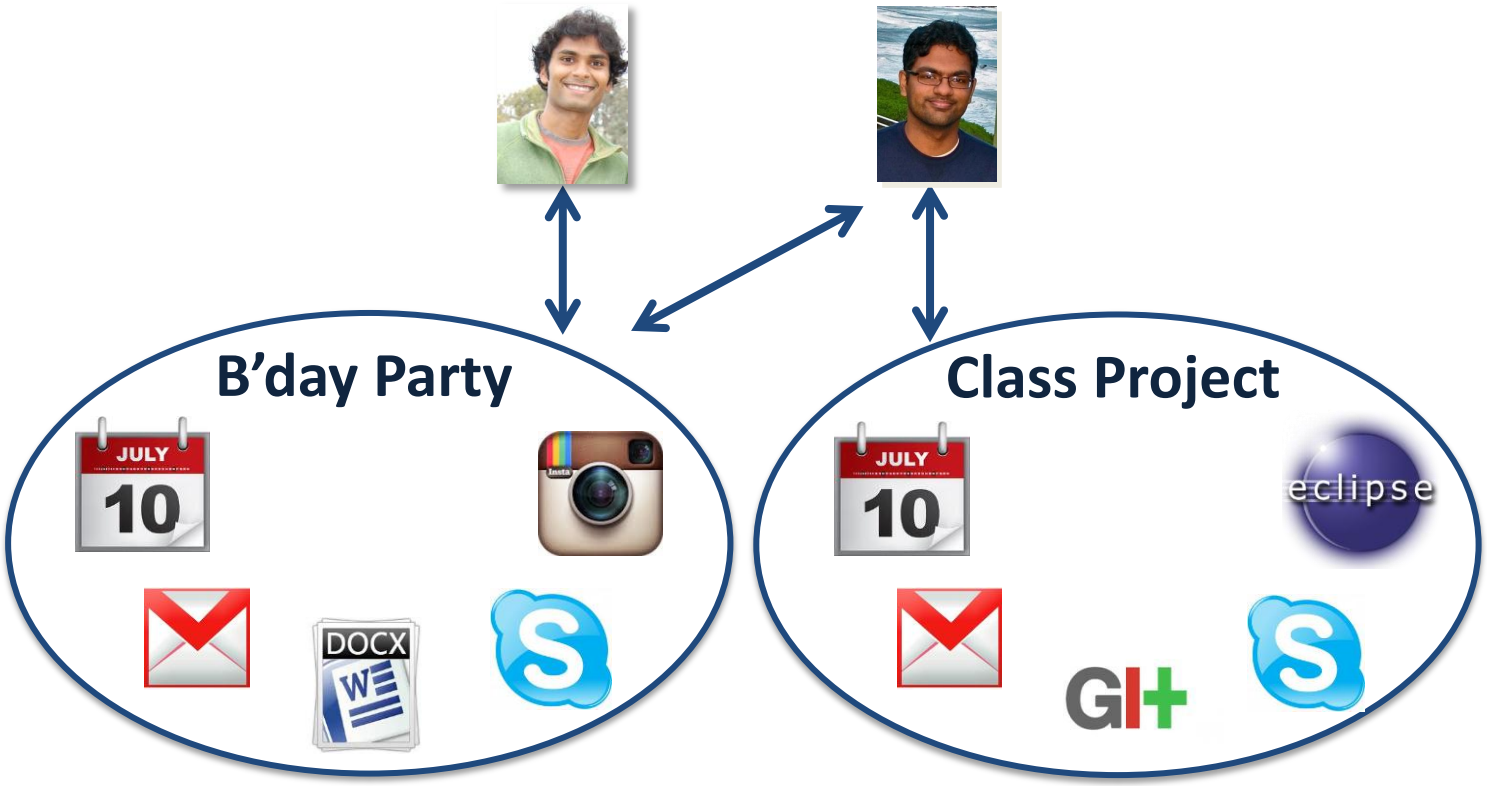
Policies on Labels



Problem: User maps Contexts to Policies

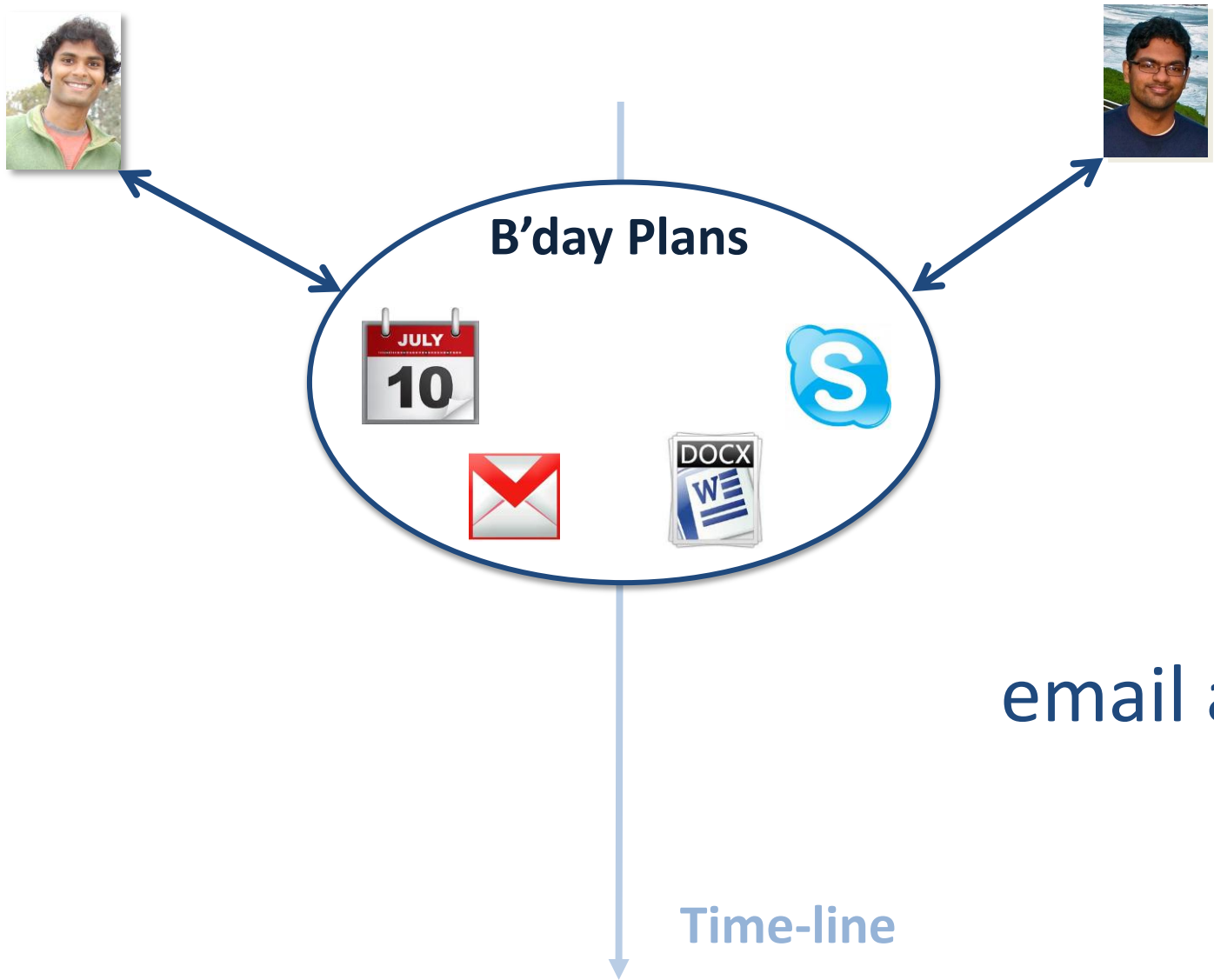


Bubbles: Context-centric Security



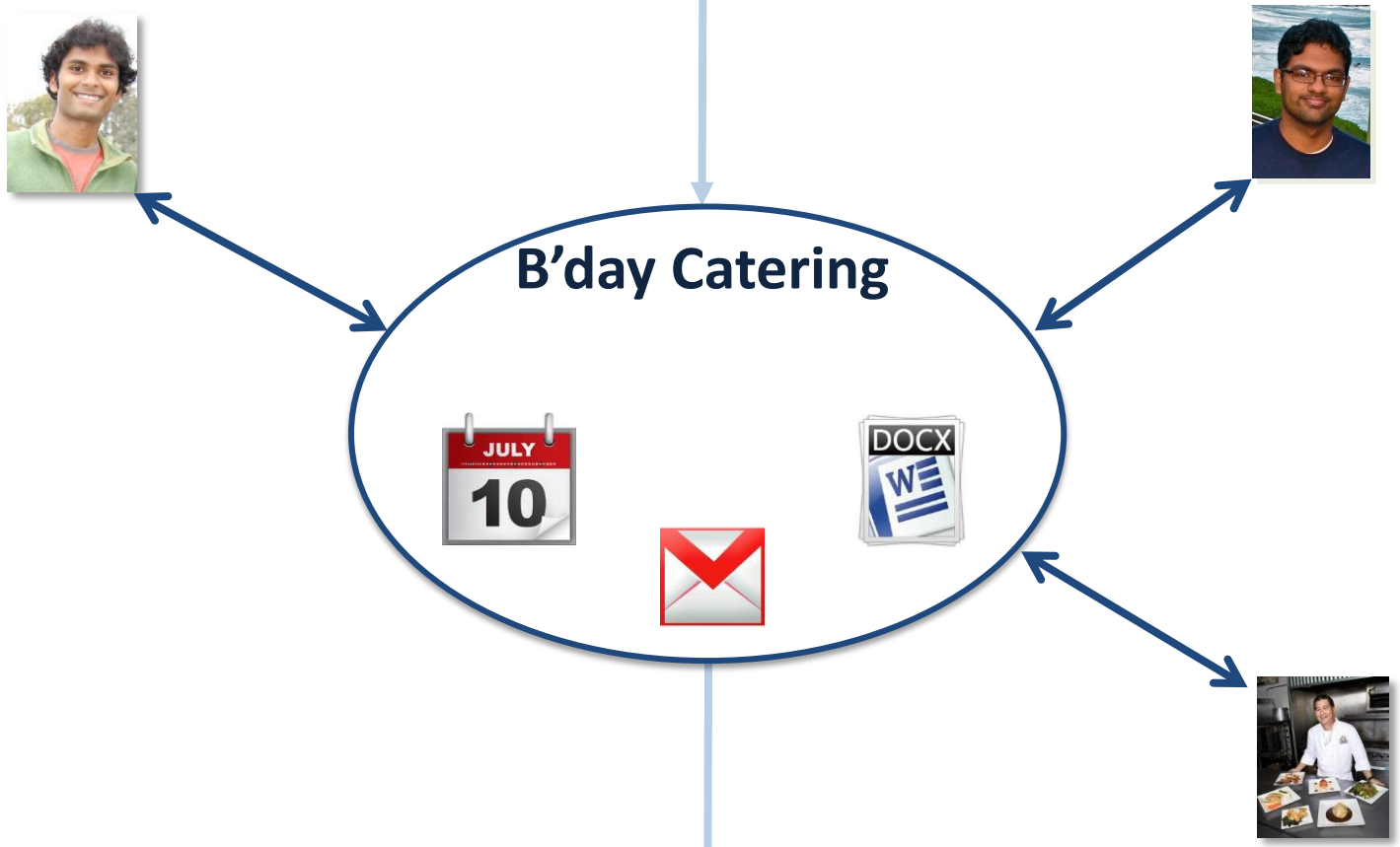
- Data clusters around real-world contexts.
- Privacy policy as access control on contexts.
- Apps run in Bubbles; cannot affect privacy.

Using Bubbles



email a caterer?

Using Bubbles



Using Bubbles

Caterer: not part of party bubble

Two contexts within same event

A Bubble is the Minimum Unit of Sharing

- Untrusted code can arbitrarily mix data inside a bubble.
  - Hence, sharing one item == sharing any item.
- Have to limit cross-bubble declassification
  - So that user has flexibility of re-sharing, e.g. meeting notes
- Bubbles have to be very light-weight contexts
  - I would put every 1:1 meeting at Usenix into a unique bubble

Challenges in implementing Bubbles

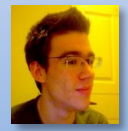
- Lots of bubbles → UI for navigating bubbles
- Apps don’t own data → API for developers
- System implementation → Infer dangerous permissions, and create light-weight containers

Recent Bubbles

B'day Party







B'day Catering


B'day Plans

Bubbles

Contacts

Local Bubbles

Hike

Tilden

B'day Party





Farmers Market

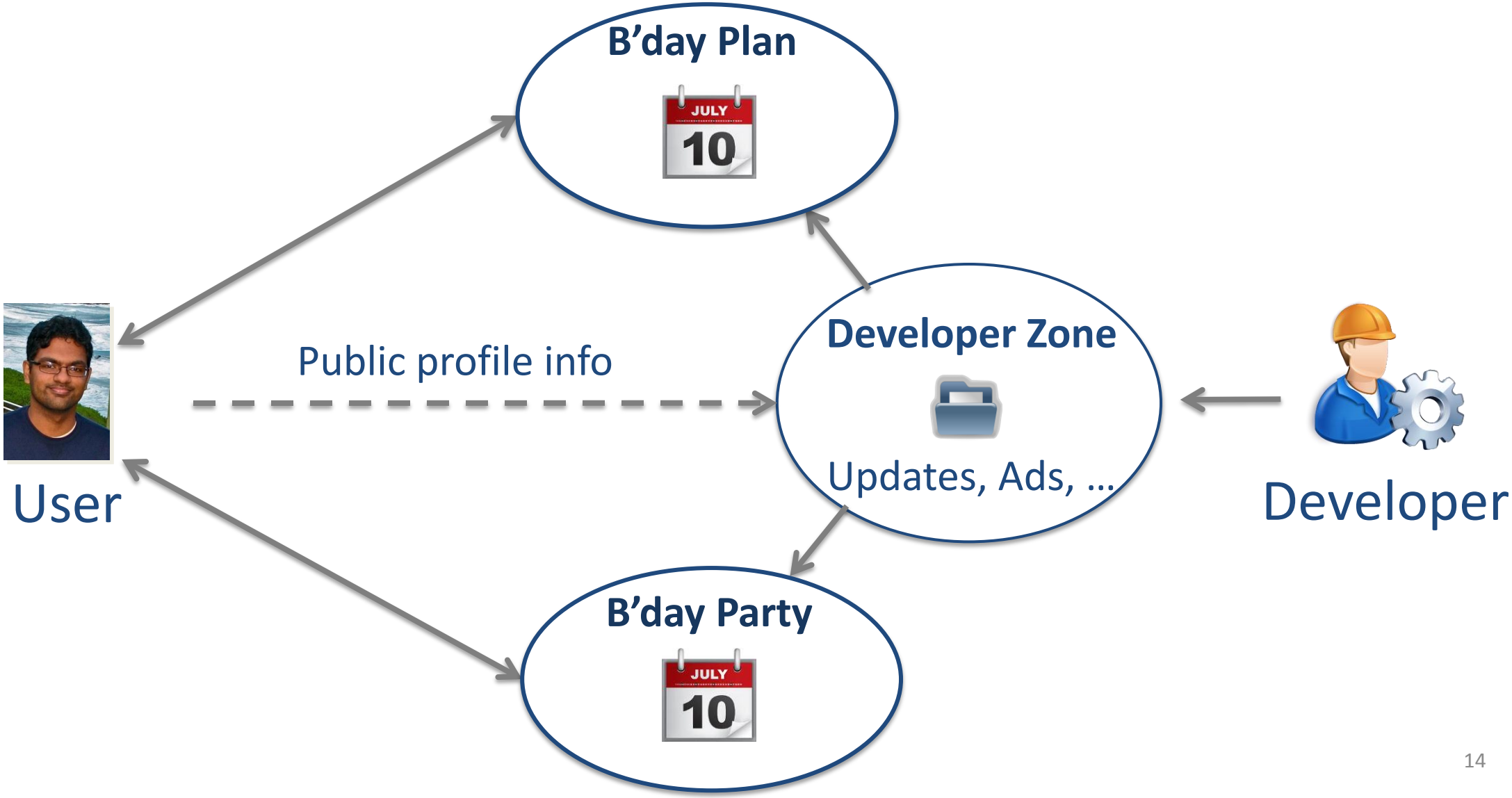
Sailing

Wharf

Henry

San Francisco Bay
Angel Island State Park
Tiburon Uplands Nature Preserve
Keil Cove
Tiburon
Belvedere Cove
Ayala Cove
Brooks Island Regional Shoreline
Albany Bulb
César Chávez Park
Albany
Albany Hill Park
Berkeley Hills
Solano Ave
Marin Ave
Gilman St
San Pablo Ave
Eastshore Fwy
Hopkins St
Henry St
Northwest Berkeley
North Berkeley
Berkeley
Central Berkeley
Dwight Way
MLK Way
Shattuck Ave
College Ave
Cal
South Berkeley
Elmwood
Ashby Ave
California State Route 13
Alcatraz Ave
Telegraph Ave
Paradise Park
Bushrod
Gate
Adeline St
Market St
55th St
51st St
Broadway
40th St
MacArthur Fwy
Clawson
Hoover/ Foster
Nimitz Fwy
Peralta St
Ralph Bunche
14th St
12th St
7th St
Lakeside Park
Lake Merritt
Old Oakland
Chinatown
Acorn
Treasure Island
San Francisco Golden Gate Rugby Clubhouse Bldg 34
Clipper Cove
Yerba Buena Island
Middle Harbor Shoreline Park
Oakland Naval Supply Center
Fisherman's Wharf
Marina Blvd
Marina
Bay St
Lombard St
Russian Hill
Main Post

Bubbles App Design Pattern



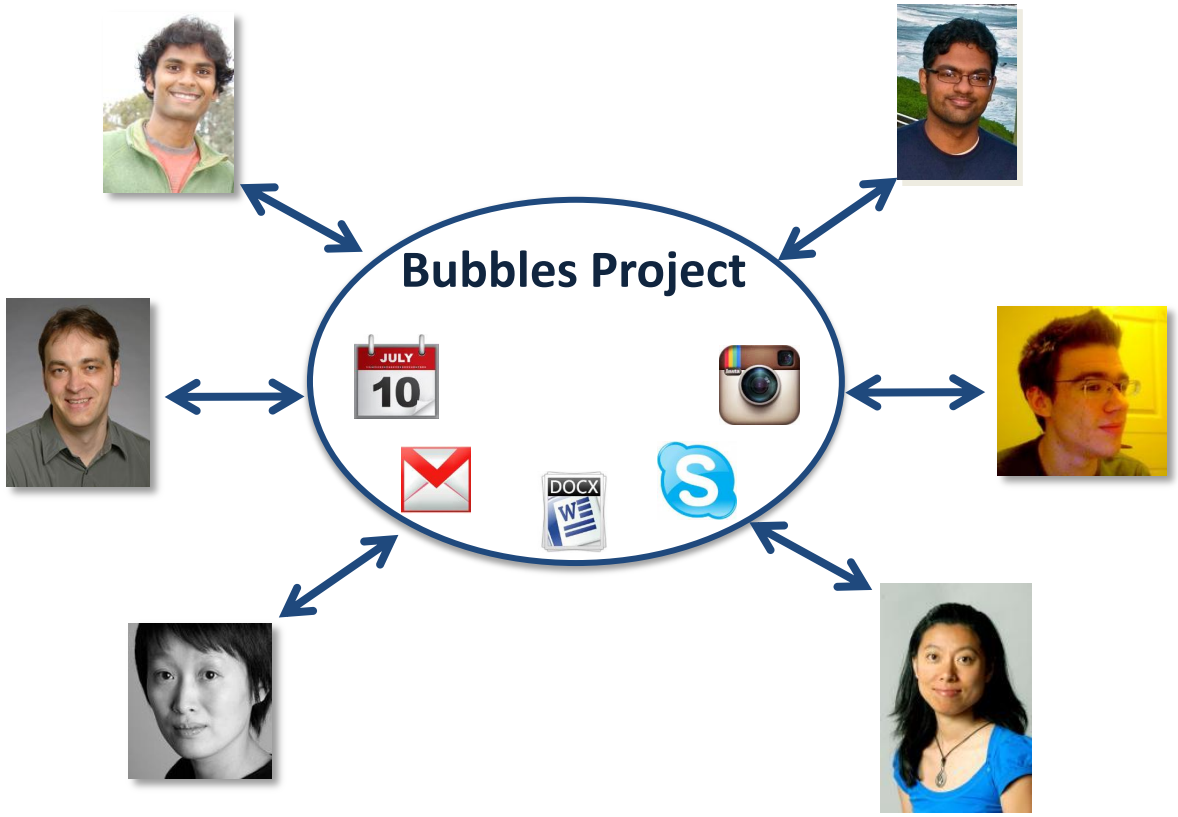
Many Apps fit inside Bubbles

- Application-initiated sharing
  - Recommendation engines, Spam filters
  - Differential privacy, k-anonymity, …
- User-initiated sharing
  - Storing, sharing, and editing docs
  - Real-time communication (voice, video)
- Anonymous: Not tied to real identity
  - Games, flashlights, wallpapers,
  - Browsing news, reviews, recipes, …

System Infers Dangerous Permissions

- User-controlled resources: 7
  - location, camera, microphone, read-contacts
- Virtualized resource: 27
  - internal and external storage, system logs, app cache and history,…
- Communication with firewall rules: 17
  - internet access, wifi, telephony

Context-centric Security



- Context = minimum unit of sharing data.
- Is working in contexts intuitive? Learnable?
- Does API support all useful functionality?