

Privacy Protection for Social Networking APIs

Adrienne Felt and David Evans
University of Virginia


W2SP, May 2008

privacy protection for social networking APIs

Facebook Platform

- Third parties get screen real estate
- User information available to developers
 - Installed users and their friends
- Backend code and databases are on third-party servers

Profile edit Friends Networks Inbox (45) home account privacy logout



Adrienne Felt

Updated 16 hours ago edit

Networks: UVA '08
 Birthday: November 8
 Political Views: Solipsism

▶ Mini-Feed
 ▶ Information
 ▼ Education and Work

Education Info
 College: UVA '08
 Computer Science
 High School: High Tech/Orange High School '04

Work Info
 Employer: UVA Computer Science department
 Position: Research Assistant / Dave Evans' minion
 Time Period: May 2006 - Present
 Description: Security & privacy group, interested in web applications and social networking sites

Employer: Google
 Position: Intern
 Time Period: May 2008 - August 2008
 Location: Mountain View, CA
 Description: Web application security group

View Photos of Me (102)
 View My Friends (540)
 Edit My Profile

UVA Friends

Causes X
 2 causes. Give a Gift | See All

Flight 93 National Memorial Fund
 214 members
 \$285 donated
 1 recruited
 \$25 donated

View
 Donate
 Remove

Enemies X

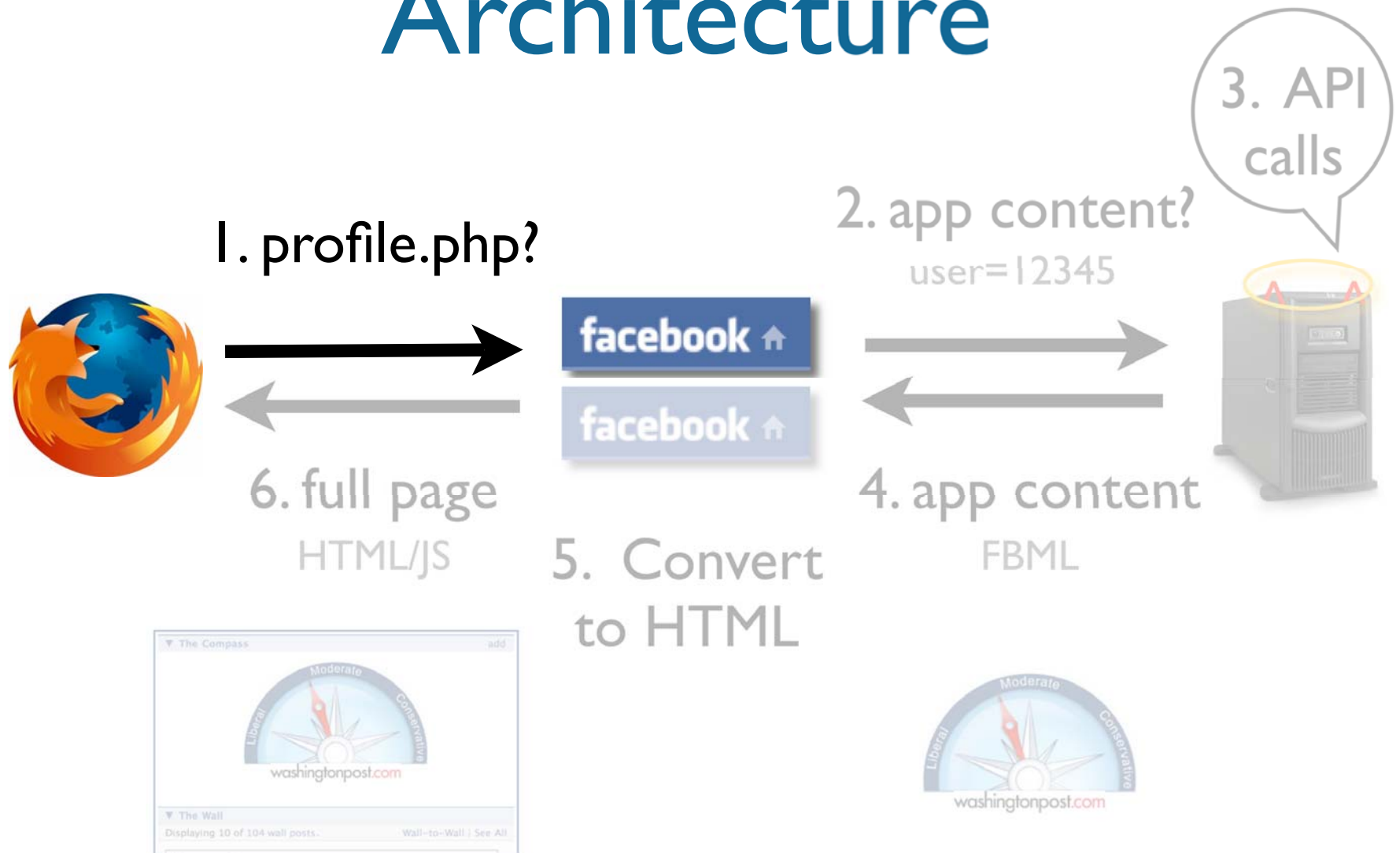
Daniel Gulick

Courses X

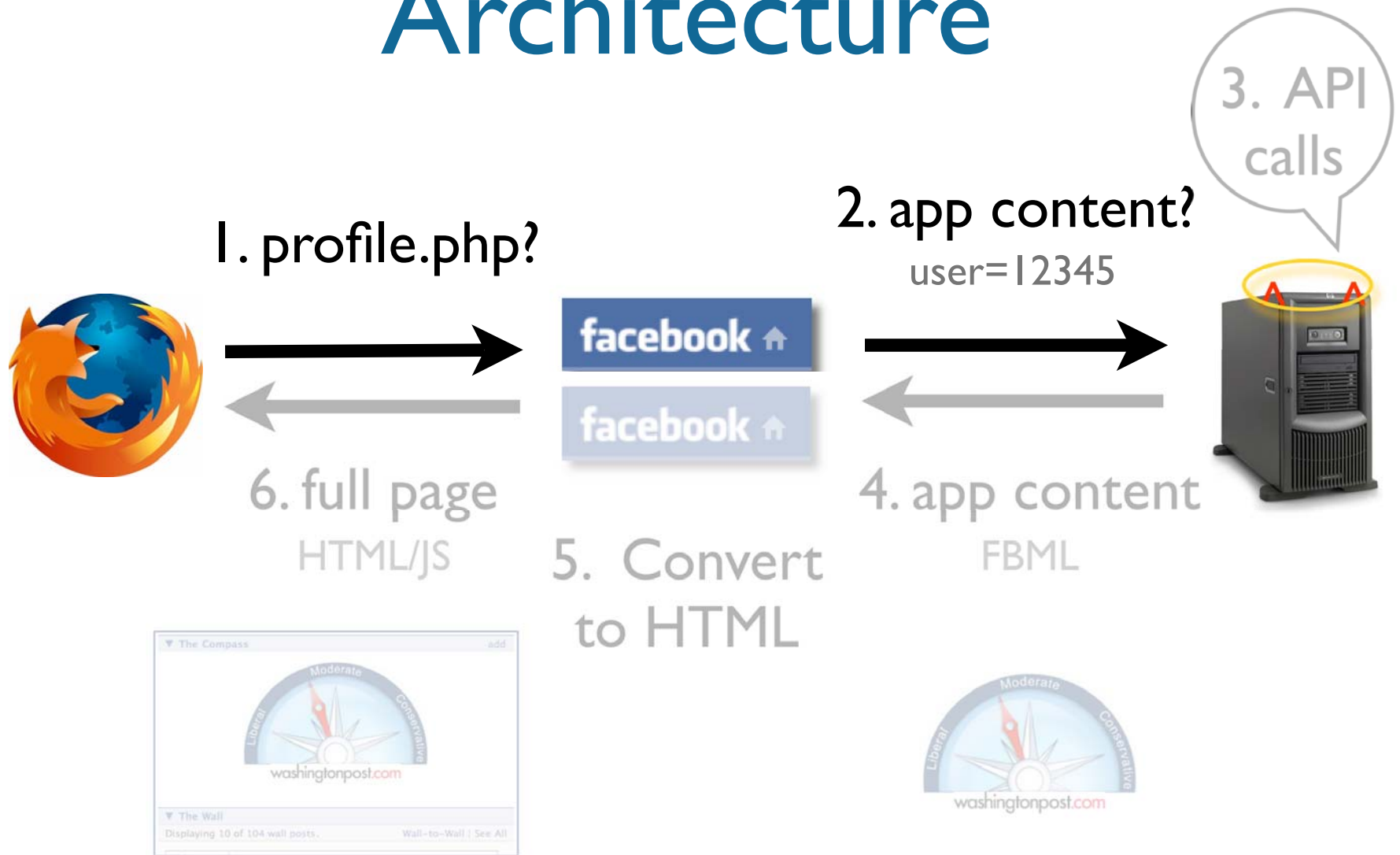
List	Calendar	Classmates					
CS 444	Parallel Computing		M	T	W	Th	F
CS 615	Programming Languages		M	T	W	Th	F
CS 851	Web Application Security		M	T	W	Th	F
PHIL 542	Advanced Logic		M	T	W	Th	F
STS 402	Thesis II		M	T	W	Th	F

Courses on Facebook Friends Genius

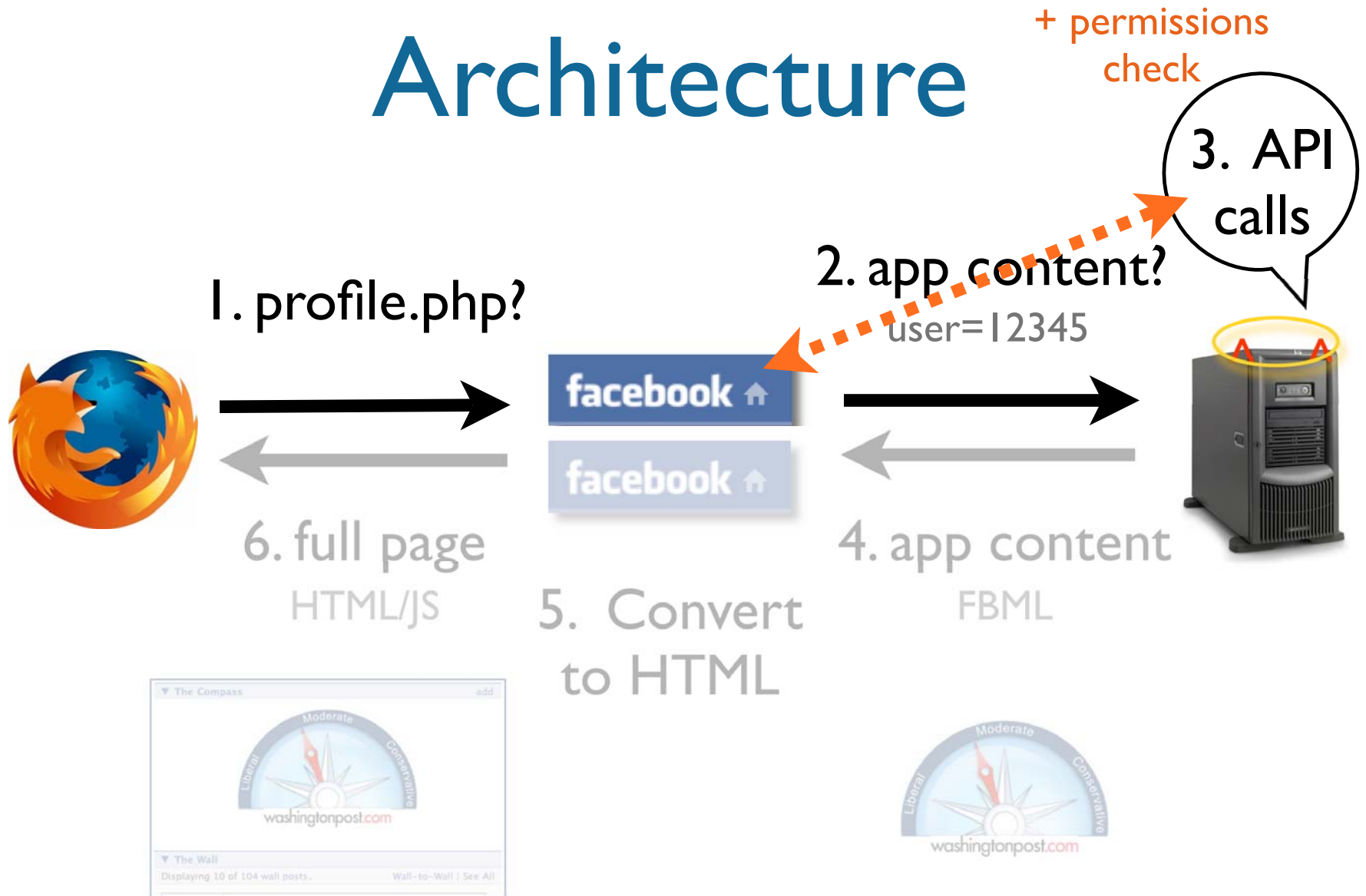
Architecture



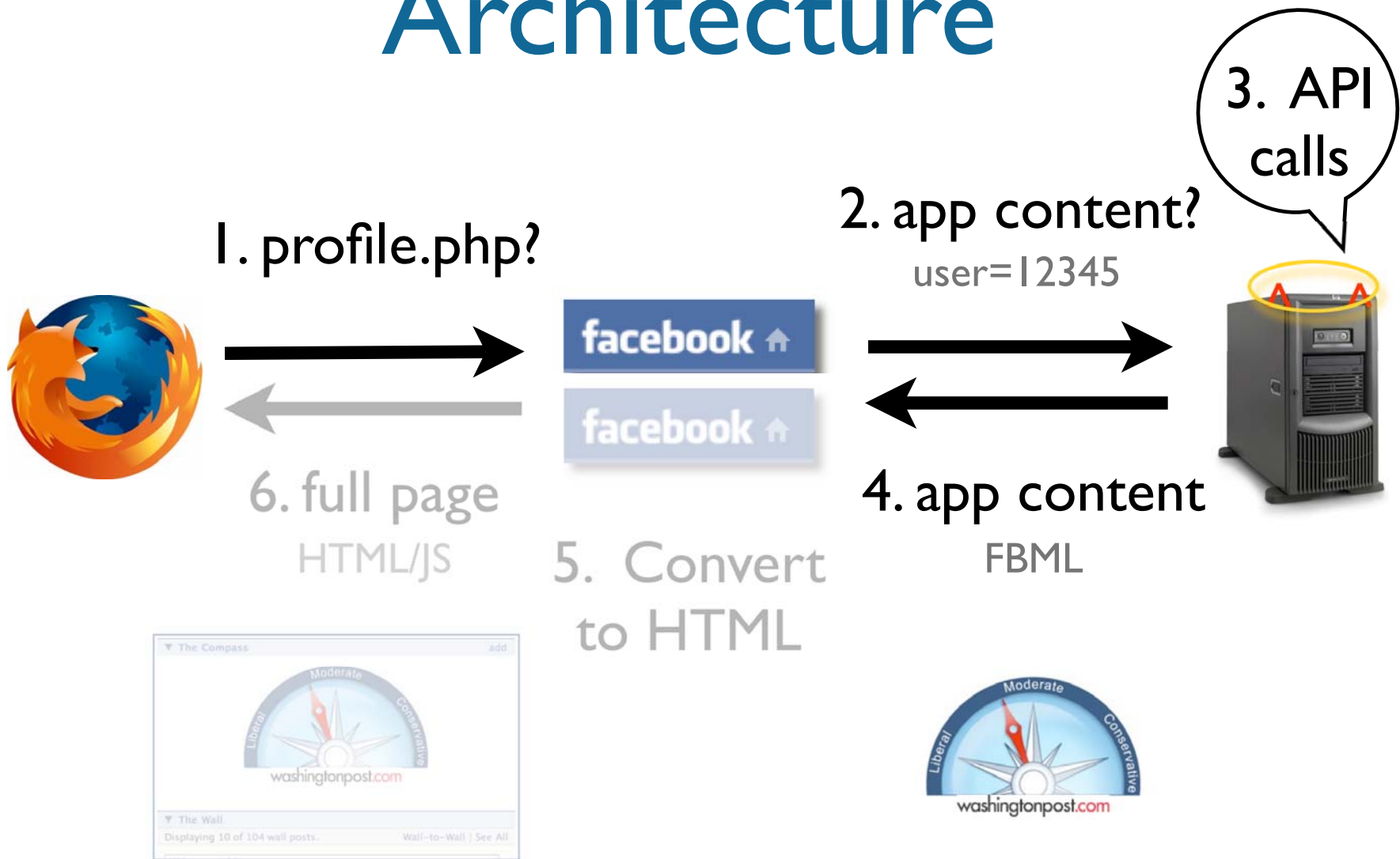
Architecture



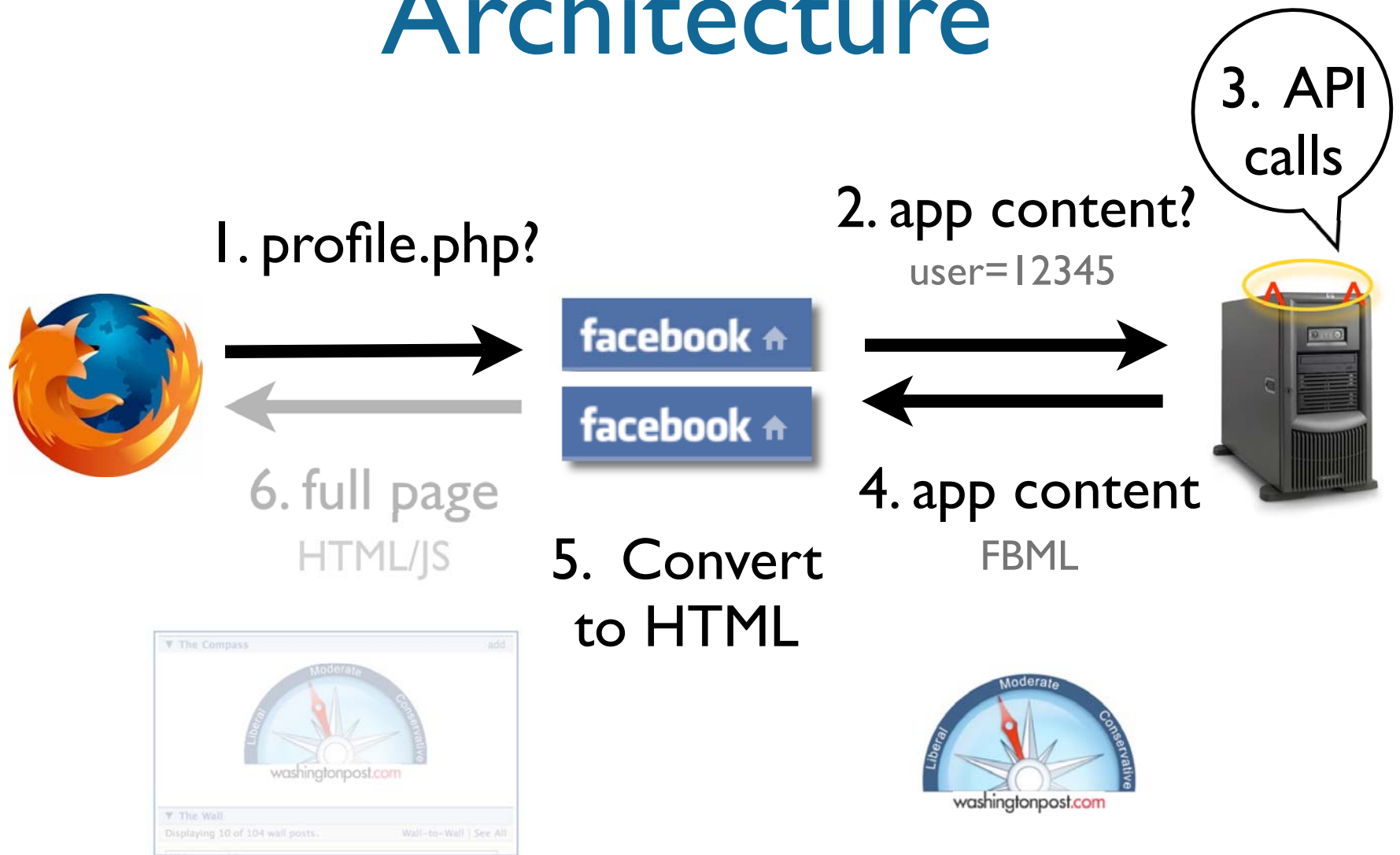
Architecture



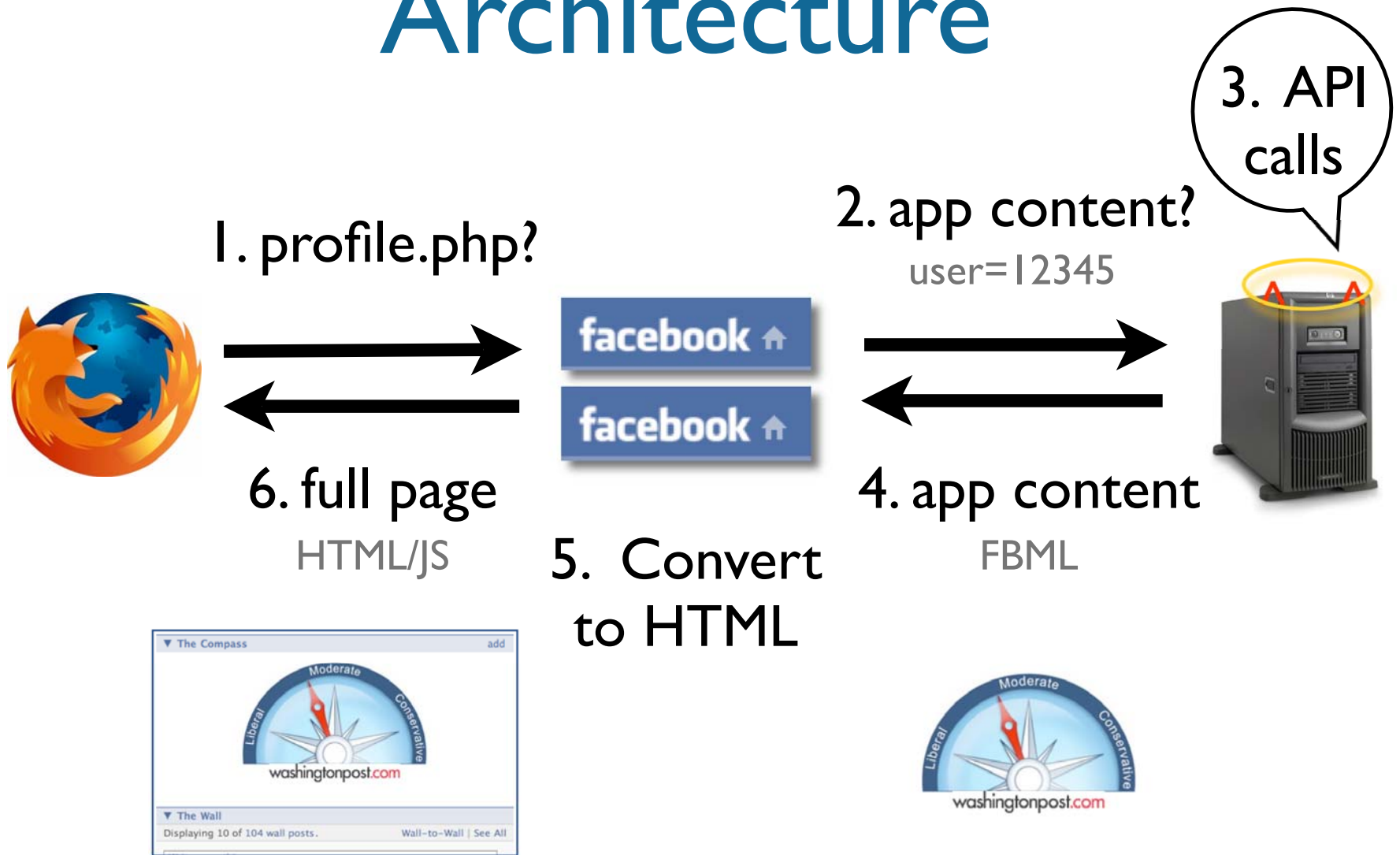
Architecture



Architecture



Architecture

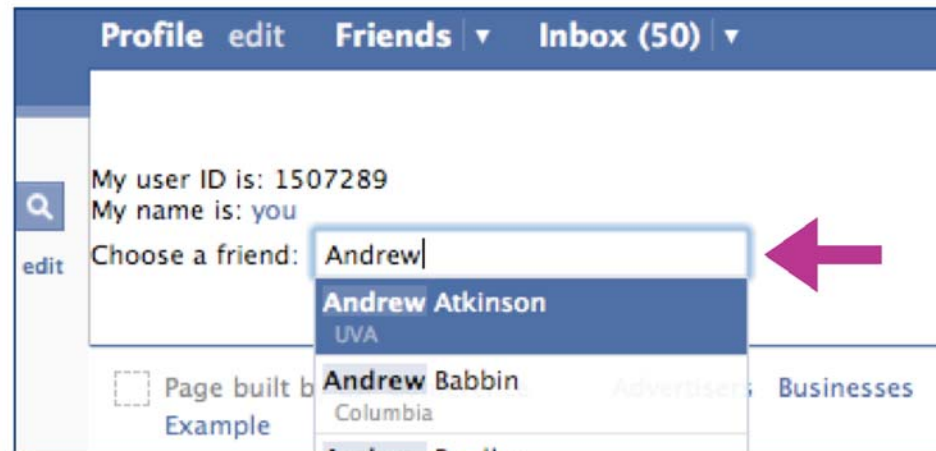


FBML

- No need to make API calls for many cases
- Large subset of HTML
- + extra fancy Facebook tags
 - fb:pronoun, fb:if-is-friends-with-viewer
 - fb:board, fb: comments, fb:random

FBML example

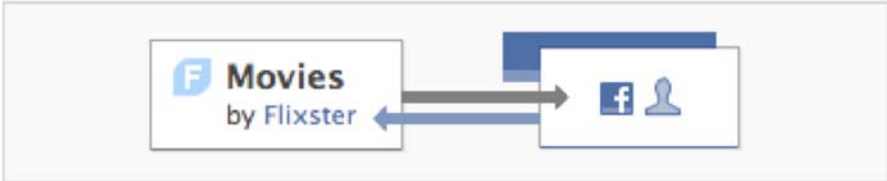
```
"My user ID is: " . $user;  
"My name is: <fb:name uid="" . $user . "'/>" ;  
"Choose a friend: <fb:friend-selector idname='friendset'/'>" ;
```



privacy protection for social networking APIs

Facebook Policy

Add Movies to your Facebook account?



Allow this application to...

- Know who I am and access my information

Granting access to information is **required** to add applications. If you are not willing to grant access to your information, **do not add this application.**

- Put a box in my profile
- Place a link in my left-hand navigation

Applications need data

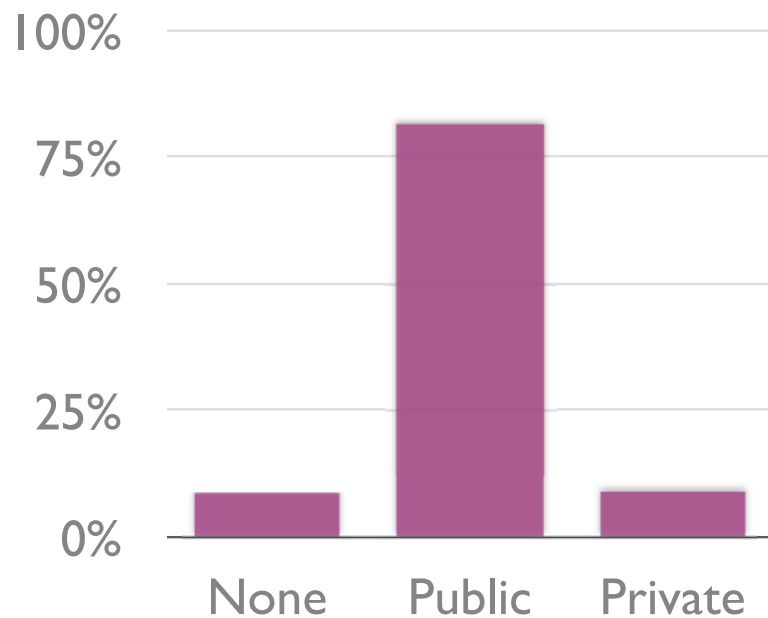
- Can harness social graphs & connections
- Tailor applications to user interests

Should they have data?

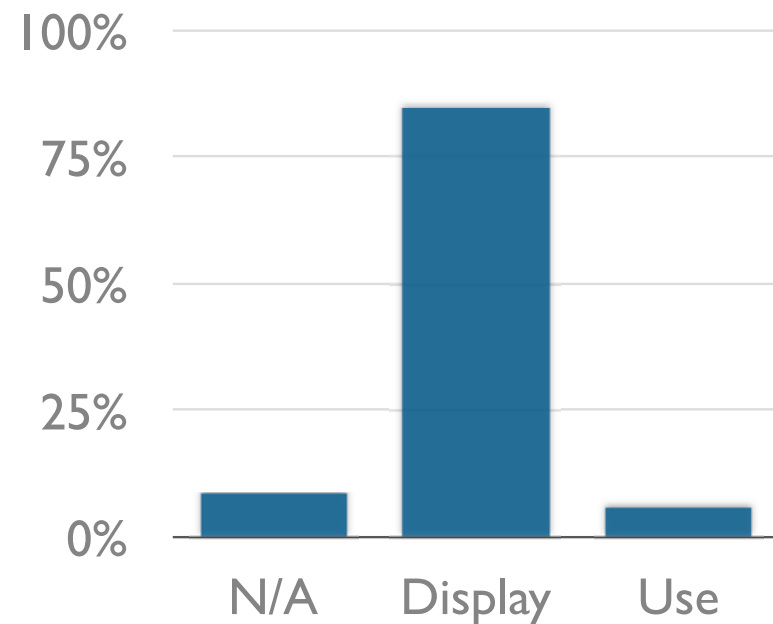
- Developers can't always be screened
- Once data is off the server...can't police it
- Even trusted applications are security weak points

Application Needs

What kind of data?



How is it used?



study of 150 most popular apps, fall 07

Privacy protection

- Only give applications information if they need it
 - Abstract the user with FBML tags
- Minimize how they need it
 - More sophisticated tags

privacy protection for social networking APIs

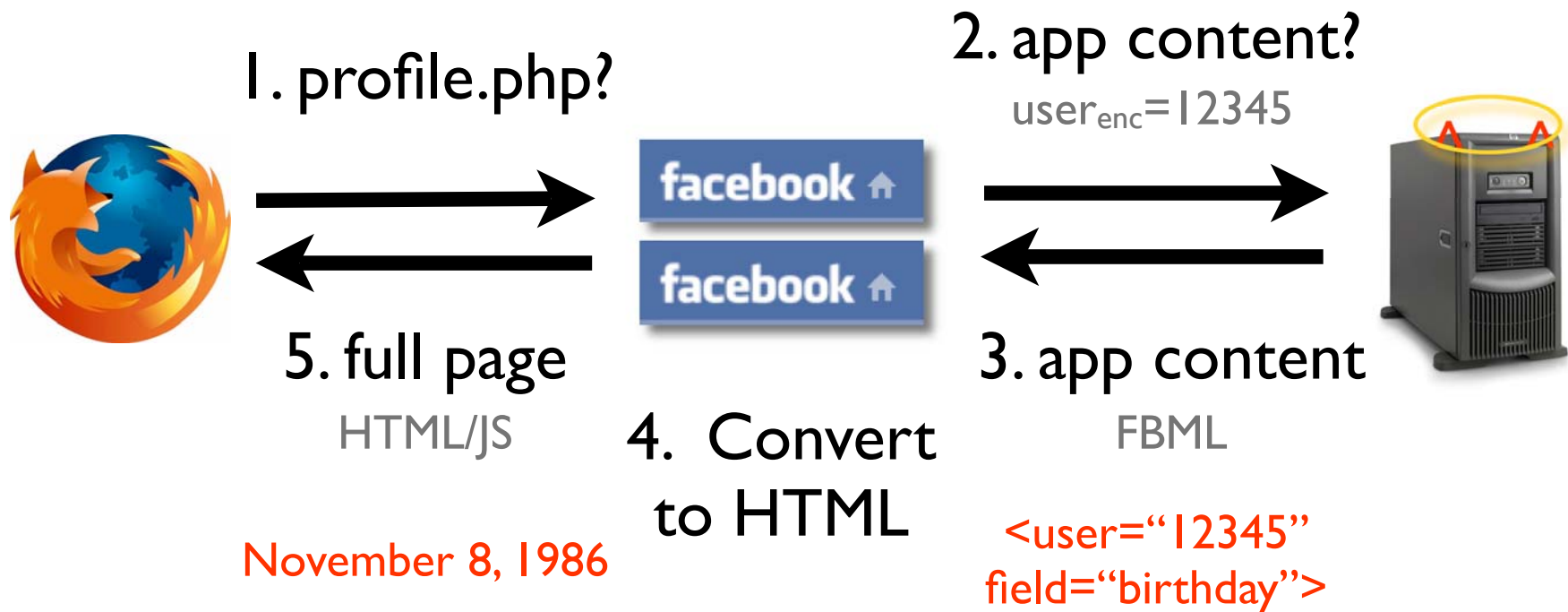
Privacy Goals

- User IDs can't be mapped back to user names
 - Application-specific IDs
- User account information is invisible
 - FBML tags keyed by IDs

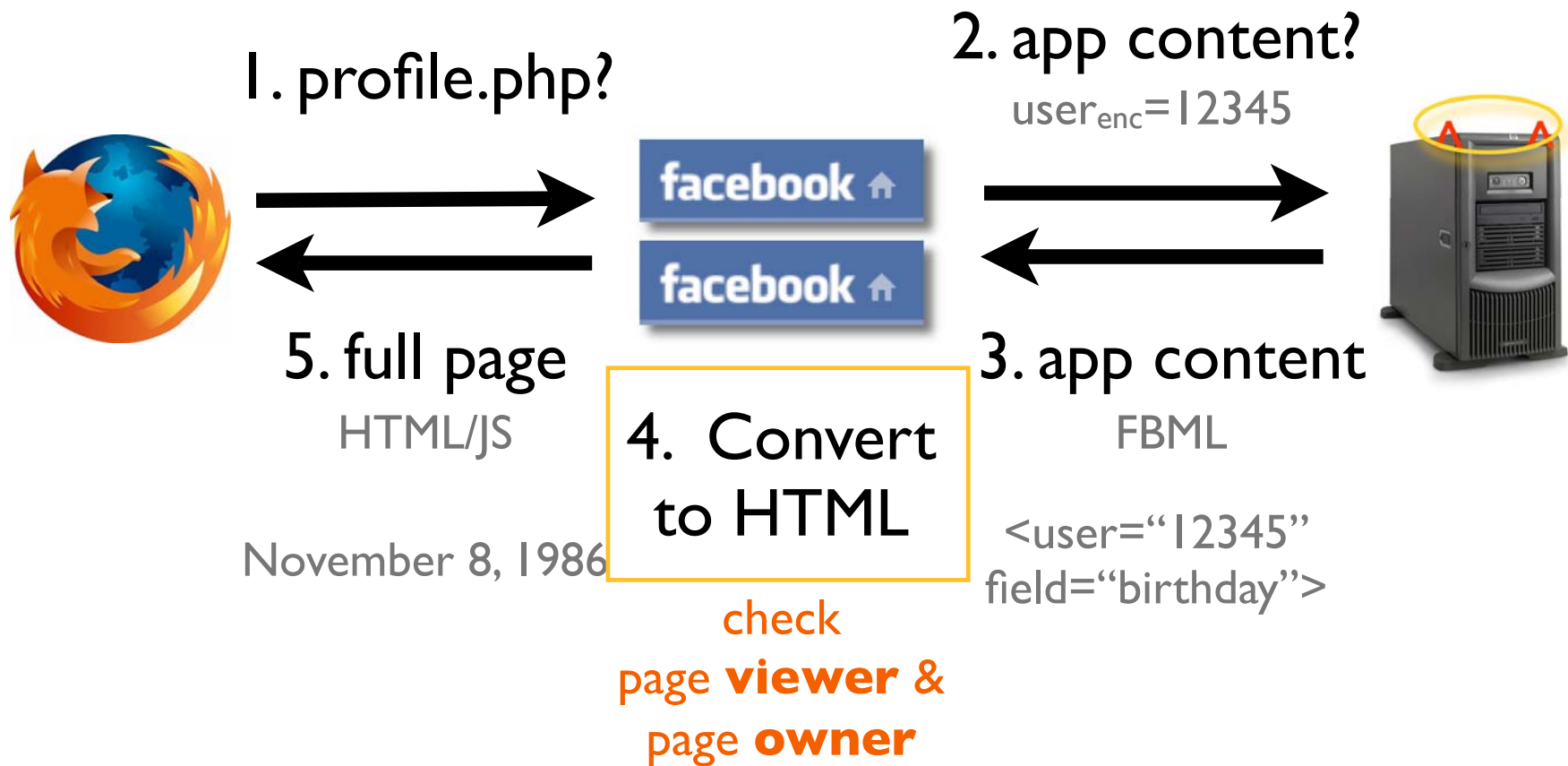
Application IDs

- User IDs are encrypted with an application key
 - Can't be used to reverse lookup users
- Returned by tags like the friend-selector

Privacy by proxy



Permissions Check

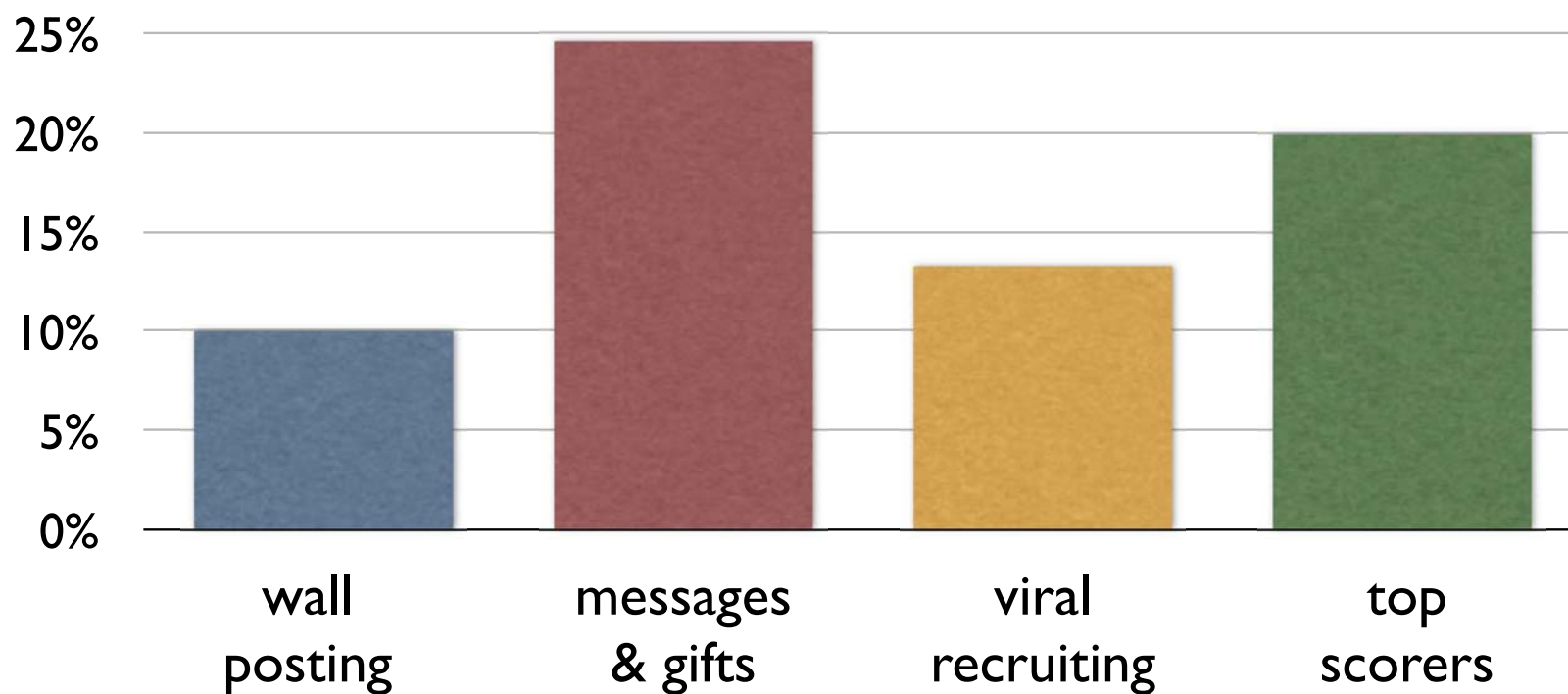


Public Information

- Attacker could iterate through IDs to list public information
- Disallow lookup of strangers
 - Only owner privileges affected

Functionality

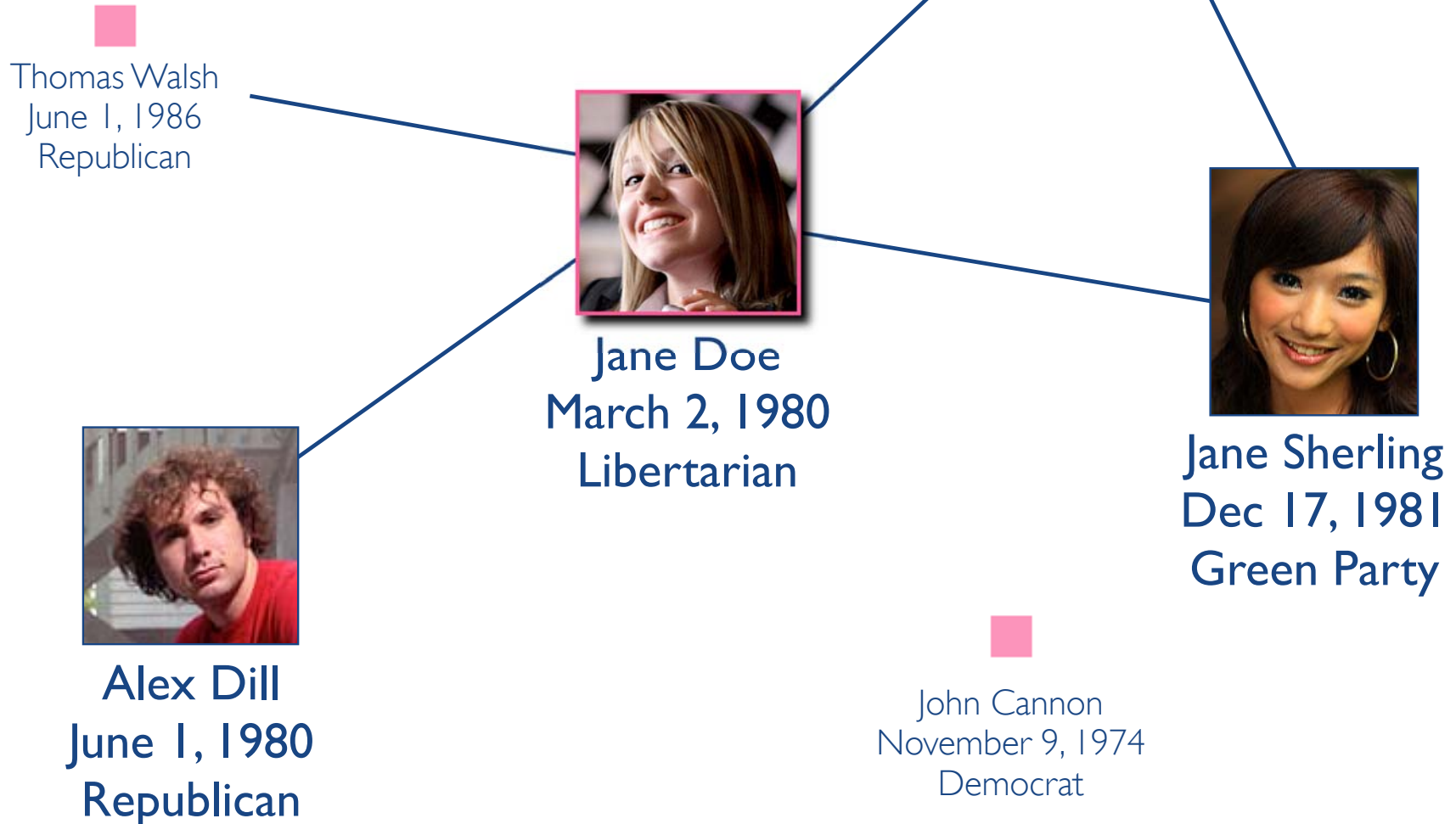
breakdown of 150 most popular apps, fall 07



Contact List

- Superset of friend list
- New addition: one-way relationships
- Alice messages Bob;
Now Bob can “see” Alice.

Original network view



Privacy by proxy

234
birthdate, 234
politics, 234



111
birthdate, 111
politics, 111

583
birthdate, 583
politics, 583



586
birthdate, 586
politics, 586



8472
birthdate, 8472
politics, 8472



Initiating contact

234
birthdate, 234
politics, 234



111
birthdate, 111
politics, 111



8472
birthdate, 8472
politics, 8472

583
birthdate, 583
politics, 583



586
birthdate, 586
politics, 586



View with contact list

234
birthdate, 234
politics, 234



|||
birthdate, |||
politics, |||



8472
birthdate, 8472
politics, 8472

583
birthdate, 583
politics, 583



586
birthdate, 586
politics, 586



835
birthdate, 835
politics, 835

Impact of contact lists

- Message-passing works fine now
- Top scorers still affected
 - Not crucial to application
 - In-game profiles, nicknames

OpenSocial

- Google provides a “standardized” API
- Still in beta, differs slightly between sites
- Applications written in XML and then transformed

Conclusion

- Most applications don't need access to full user information
- Many can be satisfied with anonymous users and server-side transformations
- Applicable to both Facebook and OpenSocial

Questions?

Adrienne Felt
felt@cs.virginia.edu