

Privacy Implications of Social Networks



Gates Scholars' Symposium
1 March 2009

Joseph Bonneau
Security Research Group
Computer Laboratory



Outline

- ♦ Why Privacy Matters
- ♦ How Social Networks Change The Game
- ♦ The Current Mess
- ♦ Research

Nothing to Hide, Nothing to Fear?

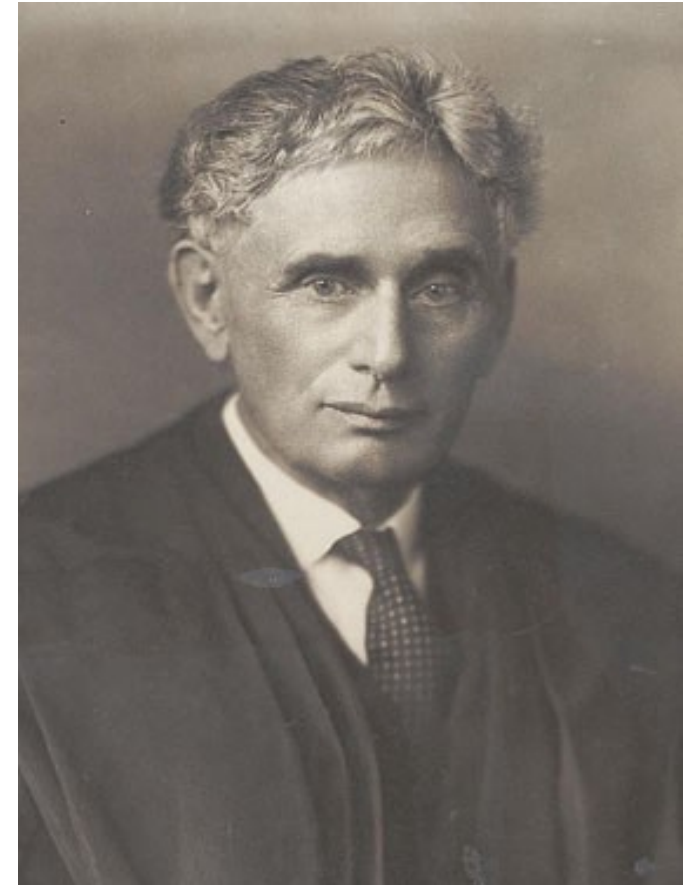
- ♦ Privacy is not just for fundamentalists!
- ♦ Increasing number of real threats:
 - ♦ Online price discrimination
 - ♦ Insurance adjustment
 - ♦ Credit rating
 - ♦ Blackmail & online scams
 - ♦ Employee screening
 - ♦ Government surveillance
 - ♦ Harassment of minority beliefs



Privacy as a Fundamental Right

“It would doubtless be desirable that the privacy of the individual should receive the added protection of the criminal law...”

- Samuel Warren and Louis Brandeis.
“The Right to Privacy.” *Harvard Law Review*. 1890



Privacy as a Fundamental Right

“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation.”

- Universal Declaration of Human Rights, 1948



Privacy as a Fundamental Right



The essential human experiences—
friendship, family, and love—are all based
on shared private emotion

Privacy is Control

- “You should have control over your personal information...” - Facebook Privacy Policy
- Much more than “The right to be left alone”
- Informational Self-Determination

Control requires understanding...

Privacy and Computers

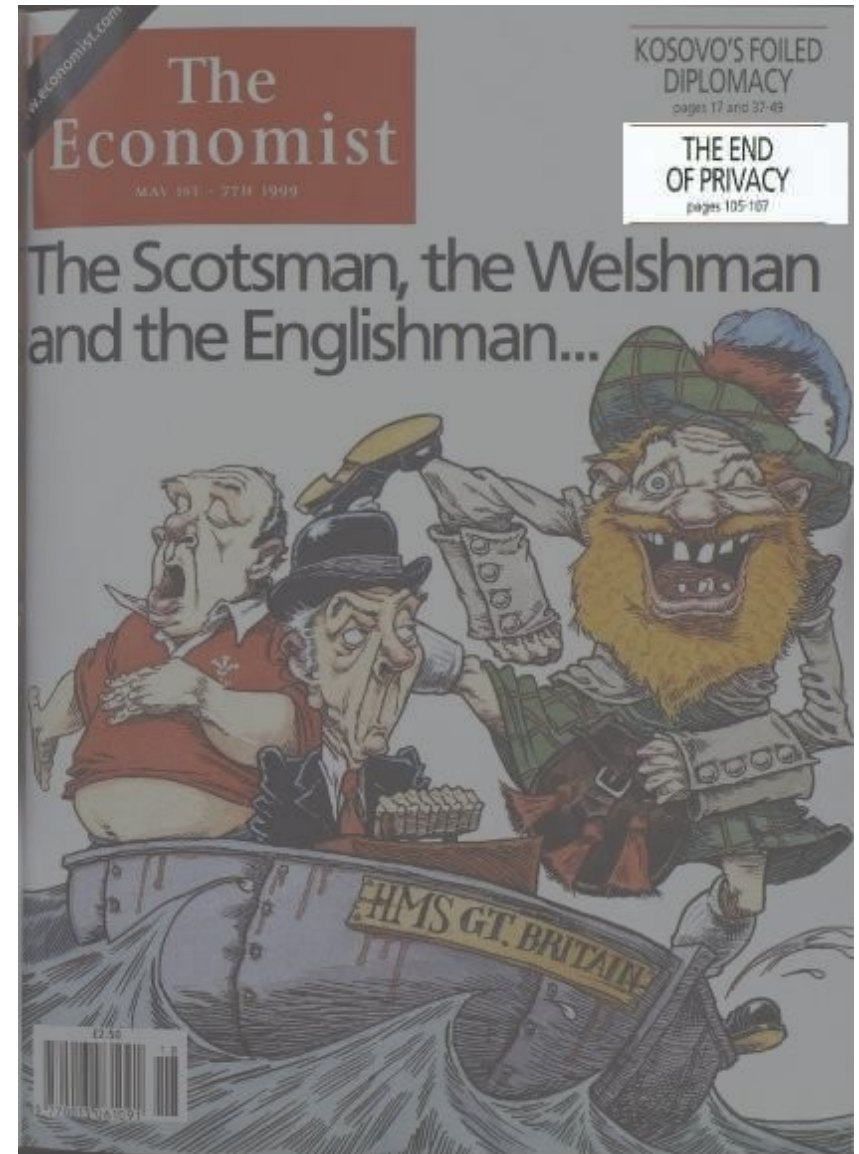
Why computers change the equation:

- ♦ Store data faster than humans can create it
- ♦ Backup and cache data in non-obvious ways
- ♦ Find statistical correlations which humans can't


Privacy and Computers

- ♦ “Many will be disturbed by the idea that most of their behaviour leaves a permanent and easily traceable record”
- ♦ “The market for privacy-protection technology will grow”
- ♦ “All these efforts to hold back the rising tide of electronic intrusion into privacy will fail... **privacy is doomed.**”

-The Economist, 1 May 1999









Privacy and the Web, v 1.0




 [Advanced Search](#)
[Preferences](#)




Search: ☒ the web ☐ pages from the UK




Web




[Joseph Bonneau -- Home Page](#)   - 3 visits - 04:10
5 Jan 2009 ... **Joseph C. Bonneau**. PhD Student 2011 ... As far as I can tell, I have an
Erdos number of 4 (J. **Bonneau**-I. Mironov-S. Jarecki-A. Odlyzko-P. ...
[www.jbonneau.com/](#) - 5k - [Cached](#) - [Similar pages](#) - 




[Joseph Bonneau dit LaBécasse](#)  
This **Joseph Bonneau** is much more frequently mentioned on the web than me. Since I've
managed to overtake him as the #1 Google hit for "**Joseph Bonneau**," I ...
[www.jbonneau.com/laBecasse.html](#) - 3k - [Cached](#) - [Similar pages](#) - 
[More results from www.jbonneau.com »](#)




[Joseph C. Bonneau](#)  
Joseph C. Bonneau. Department email: jcb82 [AT] cam [DOT] ac [DOT] uk ... Page last
updated on 26 Sept 2008 by **Joseph Bonneau**.
[www.cl.cam.ac.uk/~jcb82/](#) - 6k - [Cached](#) - [Similar pages](#) - 

[talks.cam : Joseph Bonneau](#)  
It may not mean that **Joseph Bonneau** actually organised the talk, they may have been
responsible only for entering the talk into the talks.cam system. ...
[talks.cam.ac.uk/user/show12140](#) - 9k - [Cached](#) - [Similar pages](#) - 

[The Gates Cambridge Scholarships - New Scholars - Mr Joseph Bonneau](#)  
My name is **Joseph Bonneau** and I am native to the San Francisco Bay Area in California.
I was raised in the suburb of Ross. I earned bachelor's and master's ...
[www.gates scholar.net/scholars/new_scholars_detail.asp?itemID=147](#) - 8k -
[Cached](#) - [Similar pages](#) - 

[Cryptography Research - Joseph Bonneau](#)  
Joseph Bonneau is a cryptographic scientist specializing in power analysis and other
areas of cryptographic research. He has experience developing timing ...
[www.cryptography.com/company/Joseph-Bonneau.html](#) - 5k -
[Cached](#) - [Similar pages](#) - 

[The Gates Cambridge Scholarships](#)  
Mr **Joseph Bonneau**. Status: Scholar. Citizen: United States. Year of entry: 2008. Course:
PhD Computer Science. College: Churchill College ...
[www.gates scholar.org/Scholars/Biography.aspx?ScholarID=5176&page=4](#) - 10k -
[Cached](#) - [Similar pages](#) - 

[DBLP: Joseph Bonneau](#)   - 04:11
Joseph Bonneau. List of publications from the DBLP Bibliography Server - FAQ ... 1 · EE,
Joseph Bonneau, Ilya Mironov: Cache-Collision Timing Attacks ...
[www.informatik.uni-trier.de/~ley/db/indices/a-tree/b/Bonneau:Joseph.html](#) - 4k -
[Cached](#) - [Similar pages](#) - 

Text Search

Privacy and the Web, v 1.0

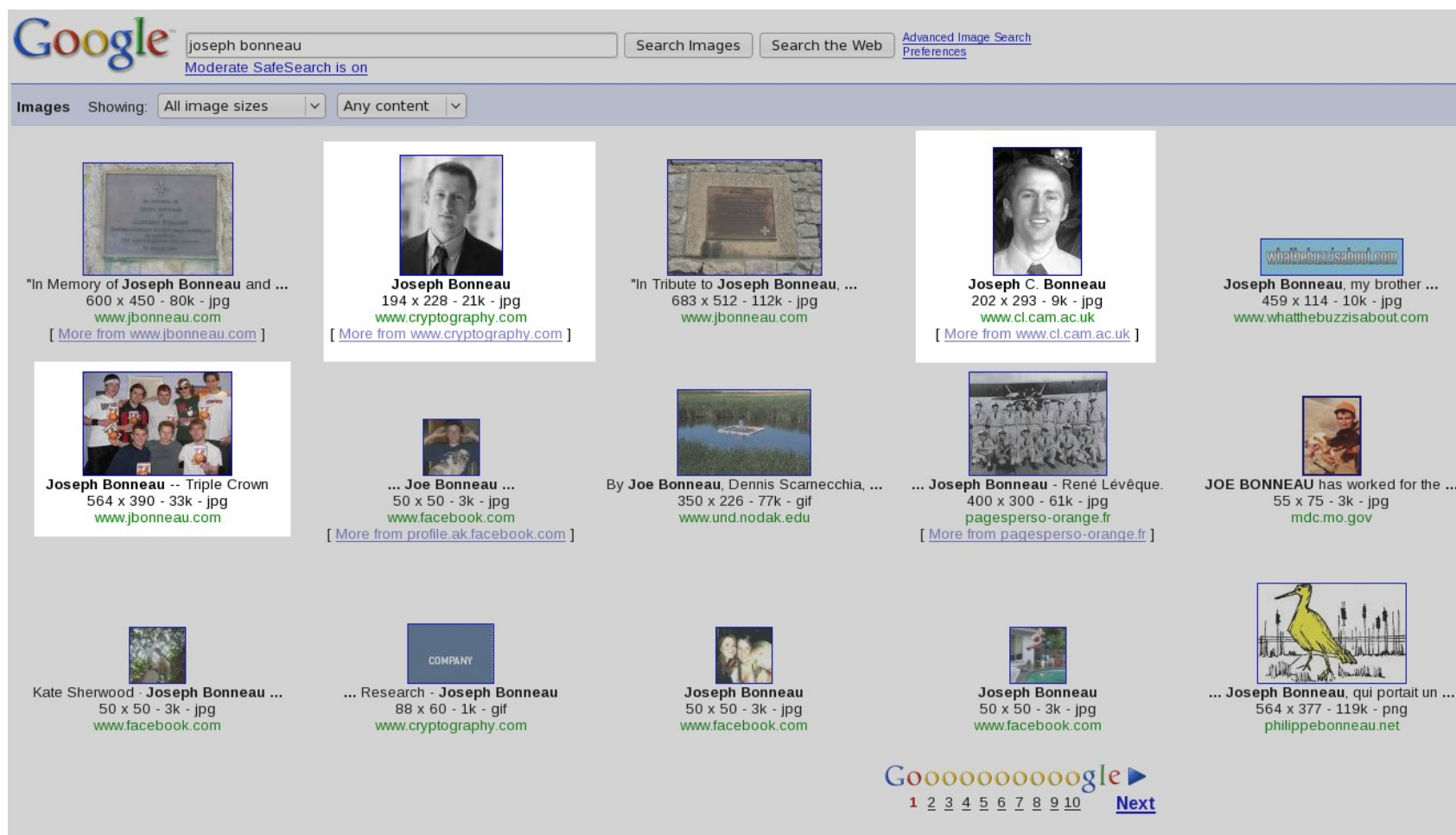


Image Search

Privacy and the Web, v 1.0

Children's social networking site hit over security flaws

Dan Raywood December 15, 2008



PRINT



EMAIL



REPRINT

FONT SIZE: [A](#) | [A](#) | [A](#)



A new social networking site for children has been criticised by a security expert.

Posting on the Light Blue Touchpaper blog, University of Cambridge cryptographic scientist, Joseph Bonneau said that 'School Together Now' is full of security holes including the lack of a username or password login and 'a pattern of poor security choices driven by the desire for rapid commercialisation.'

Bonneau claimed that it 'makes no attempt to ensure that users

RELATED ARTICLES

- [New online wa to protect child](#)
- [Bloxx seeks to by savvy stude](#)
- [New online wa to protect child](#)
- [Underage child visitors to netw](#)
- [Children's inter create security](#)

News Articles

Privacy and the Web, v 1.0

Joseph, Welcome to Your Amazon.com (If you're not Joseph Bonneau, click here.)

Today's Recommendations For You

Page 2 of 16 (Start over)

Here's a daily sample of items recommended for you. Click here to [see all recommendations](#).

| | | | | | | | |
|---|---|---|--|--|---|--|--|
|  |  |  |  |  |  |  |  |
| The Adventurer's Handbook: Life Lessons fr... by Mick Conefrey ★★★★☆ (3) \$4.50 | Microcircuits: The Interface between Neuro... by Sten Grillner \$46.33 | Nike HJ020 Flight Sport headphones ★★★★☆ (52) | The Ultimate French Verb Review and Pract... by David M Stillman ★★★★★ (15) \$10.36 | Africa since 1940: The Past of the Present... by Frederick Cooper ★★★★★ (4) \$17.57 | In Search of Memory: The Emergence of a Ne... by Eric R. Kandel ★★★★★ (53) \$12.21 | Gandhi and Beyond: Nonviolence for an Age... by David Cortright ★★★★☆ (5) \$24.95 | Ion Channels of Excitable Membranes (3rd E... by Bertil Hille ★★★★★ (9) \$79.16 |
| Any Category Biology Card Games Cognitive Psychology Dictionaries Dictionaries & Terminology Dictionaries: Polyglot Fiction French Games Headphones Intelligence & Espionage Neurology Neuropsychology Neuroscience Nonfiction Pathology Public Policy Puzzles Radios Relations Scrabble Spanish Toys United States Word Games | | | | | | | |

New For You®

| | | |
|--|---|--|
|  |  |  |
| Collateral Damage (Paperback) by Chris Hedges (Feb 9, 2009) See more recommended new releases | The Age of American Unreason (Vintage) (Paperback) by Susan Jacoby (Feb 10, 2009) | Streetwise Paris Map - Laminated City Center Street... (Map) by Streetwise Maps (Jan 31, 2009) |

Your Recent Shopping
[Recently Viewed Items](#) (0)
[Your Shopping Cart](#)
[Open & Recently Shipped Orders](#)

Your Lists
[Your Wish List](#)
[Your Gift List](#)
[Your Shopping List](#)

Your Community
[Your Communities](#)
[Your Amazon Friends](#)
[Your Interesting People](#)
[Your Reminders](#)
[Your Profile](#)

Merchant Websites

Privacy and the Web, v 1.0



Joseph C. Bonneau

PhD Student 2011
[Security Group](#), [Computer Laboratory](#), [University of Cambridge](#)
[Gates Cambridge Scholar](#)
[Churchill College](#)

Department email: jcb82 [AT] cam [DOT] ac [DOT] uk
Personal email: jbonneau [AT] gmail [DOT] com

Office telephone (UK): +44 01223.763793
Personal telephone (UK): +44 07590.677117
Personal telephone (US): +1 650.804.6934

Churchill College #62H
Cambridge, UK CB3 0DS

Current Status

I'm currently a first-year PhD Student. More information about my PhD activity can be found at my [Cambridge website](#)

Research Interests

Cryptography, Data Privacy, Social Networks, Obfuscation, Reverse Engineering, Human Authentication, User Interfaces

Professional Information

- [Resume](#)
- [Education](#)
- [Coursework](#)
- [Employment History](#)
- [Research Projects](#)
- [Teaching Experience](#)
- References & Transcripts available upon request.

Amateurish Information

- [Blog about my time in Cambridge](#) (experimental, may die soon)
- [Photos of my some of my travels](#)
- [Countries](#) I have visited
- [Charities](#) I have supported in the past

Personal Homepages

Privacy and the Web, v 1.0



Most predictions wrong!

- Users less aware of privacy
- No market for privacy technology
- The world has not ended...


Privacy and the Web, v 1.0



Saving Graces:

- ♦ Data spread across many silos
- ♦ Natural Language Processing is hard
- ♦ Entity Resolution is hard

Privacy and the Web, v 2.0



[View Photos of Joseph \(390\)](#)

[Send Joseph a Message](#)

[Poke Joseph](#)




Information

Networks:
Cambridge Grad Student '11
Stanford Alum '06
San Francisco, CA

Birthday:
July 17, 1984

Mutual Friends




51 friends in common [See All](#)



Ashley Wessendo
Liz Sefton
Melis Anahtar

Friends

527 friends [See All](#)



Huw Jones
melissa hillard
Jack Grimes

Joseph Bonneau

[Wall](#) [Info](#) [Photos](#) [Boxes](#)

Basic Information

Networks: Cambridge Grad Student '11
Stanford Alum '06
San Francisco, CA

Sex: Male

Birthday: July 17, 1984

Contact Information

Email: jbonneau@gmail.com
jcb82@cam.ac.uk

Mobile: UK 044.07590.677117

Other: US 01.650.804.6934

Skype: joseph.bonneau

Website: <http://www.jbonneau.com>
<http://picasaweb.google.com/jbonneau>
<http://joecambridge.blogspot.com>

Education and Work

Grad Schools: Stanford '07
Master of Science, Cryptography
Cambridge '11
PhD, Computer Science

College: Stanford '06
Computer Science, Mathematics

High School: Redwood High '02

Employer: Cryptography Research Inc.

Position: Cryptographic Scientist

Time Period: April 2007 - May 2008

Location: San Francisco, CA

Groups

[See All \(8\)](#)

Member of: Gates Scholars Ents, Thanksgiving + Roz's welcome back bash, Churchill MCR, Churchill College Rugby Football Club, Gates Cambridge Scholars, Gates Cambridge Scholars Society, Gates Cambridge Scholars 2008, Cambridge 2008: Affiliated, Graduate and Mature

Personal Profiles

Privacy and the Web, v 2.0

You have 154 friends with recent status updates. [1](#) [2](#) [3](#) [4](#) [Next](#)



Ira Renfrew is packing up. Goodbye Abu Dhabi!
about an hour ago



Brett Talbot .
2 hours ago



Charlotte Garing is loving Marie's muffins.
2 hours ago



Mike Barash ball placement is key.
3 hours ago - via Twitter



James Black - just for once...
3 hours ago



Matt Truong is glad PDS is not on the USMLE.
4 hours ago



Kat Smith is super excited for her multiple vacations!!! yes thats right multiple.
4 hours ago

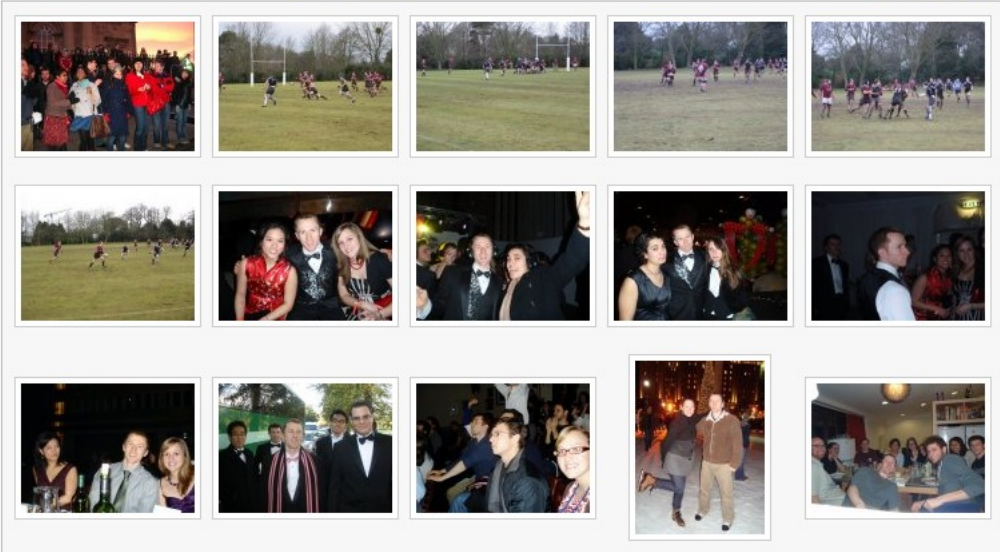


Kate Odell is so glad its the weekend.
4 hours ago






Friendship Information

Privacy and the Web, v 2.0

Photos of Joseph 390 photos | [View Comments](#) 1 2 3 4 5 Next



Joseph's Albums 13 Photo Albums | [View Comments](#) | [Album](#) 1 2 3 4 Next

| | | | | |
|---|---|---|--|---|
|  Cambridge 2008-2009 30 photos |  SF 2007-2008 part 1 45 photos |  Christmas 2008 17 photos |  Rugby Nov 13 19 photos |  Profile Pictures 3 photos |
|---|---|---|--|---|

Tagged Photos

Privacy and the Web, v 2.0

```
<user>
  <name>Joseph Bonneau</name>
  <sex>male</sex>
  <birthday>July 17, 1984</birthday>

  <education_info>
    <name>Stanford</name>
    <year>2007</year>
    <concentration>Cryptography</concentration>
    <degree>Master of Science</degree>
  </education_info>

  <education_info>
    <name>Stanford</name>
    <year>2006</year>
    <concentration>Computer Science</concentration>
    <concentration>Mathematics</concentration>
    <degree>Bachelor of Science</degree>
  </education_info>

  <education_info>
    <name>Cambridge</name>
    <year>2011</year>
    <concentration>Computer Science</concentration>
    <degree>PhD</degree>
  </education_info>

  <work_info>
    <company_name>Cryptography Research Inc.</company_name>
    <position>Cryptographic Scientist</position>
  </work_info>
</user>
```

XML data

Comparison

Traditional Internet

- ♦ Data spread out
- ♦ Entity Resolution difficult
- ♦ NLP difficult
- ♦ Connections hidden

Social Networks

- ♦ Centralised control
- ♦ Unique IDs
- ♦ Tagged Data, XML
- ♦ Explicit Social Graph

Why Privacy Controls Fail

- ♦ **Economics**

- ♦ SNS operators lack a business model

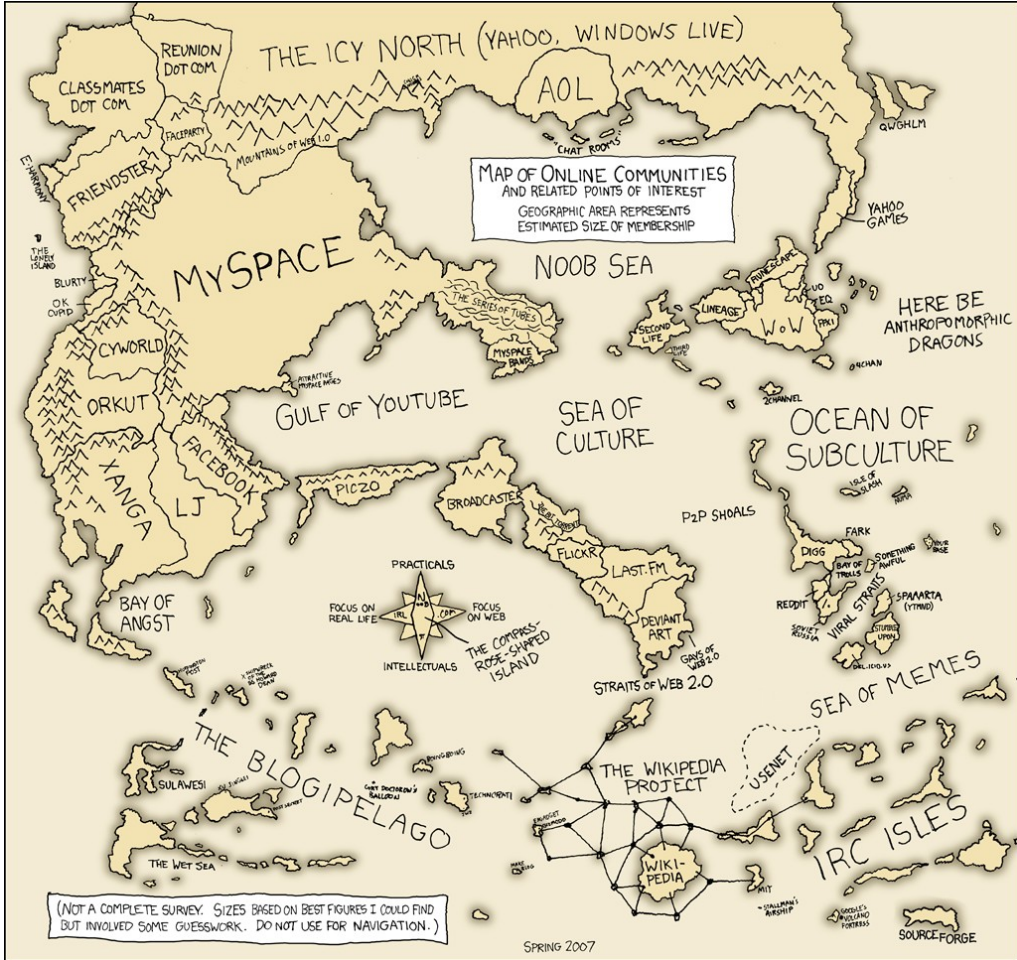
- ♦ **Usability**

- ♦ Very difficult to understand data flow

- ♦ **Sloppiness**

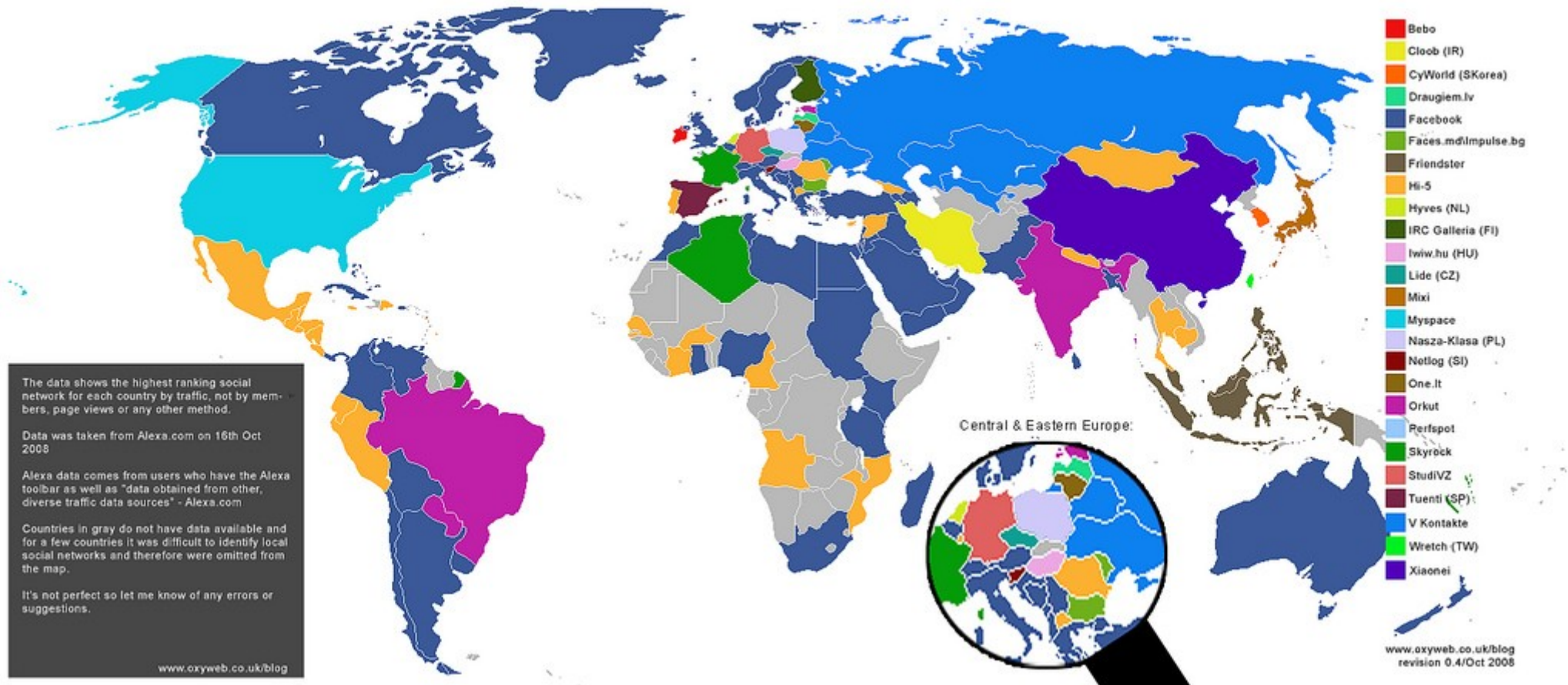
- ♦ Existing controls implemented incorrectly & hacked

Economics



It's a mess out there...

Economics



Contrary to belief, there are dozens of competitors

Economics

- ♦ “Growth is primary, revenue secondary.”
 - Mark Zuckerberg, Facebook CEO
- ♦ Most SNS operators thought to be losing money
- ♦ Viable business models involve privacy violation
 - Targeted advertisements, etc.
- ♦ Common market cap: \$10-\$100 *per account*
 - eg Facebook: \$15 billion valuation, 175 million users

Economics

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.

Privacy Policy, hi5.com (60 M users)

Usability

- ♦ Visibility of Data is complicated
- ♦ People don't want to edit privacy settings
 - Over 90% maintain defaults
- ♦ Defaults chosen in SNS operator's interest
- ♦ Control requires understanding!

Usability

My settings

[Home](#) > My settings

[general](#) [privacy](#) [notifications](#) [chat](#)

enable photo tagging:

- 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

☒ yes

my updates:

show updates for photos, videos, testimonials, and profile changes to my friends. scraps will not be shown [?](#)

☒ show updates
☐ hide updates

profile visitors:

show who visits my profile (and let others see when I visit their profile)

☒ show profile visits
☐ hide profile visits

orkut in google search results:

show my orkut information including my photos as part of my friends' search results on google.com

☒ show information
☐ hide information

allow people to find me through my email address:

let people who know my email address find my profile on orkut

☒ Allow people to find me
☐ Don't allow people to find me

friend requests are allowed to be sent by:

restrict friend requests and only allow people who meet your criteria to become friends with you [?](#)

☒ anyone on orkut.com
☐ anyone who fits one of the following selected options
☐ people who know my email address (required default)
☐ friends of my friends
☐ people from the following countries and regions

[add country or region](#)

allow content to be accessed by:

restrict who is allowed to access my content

view scrapbook:

write in scrapbook:

videos:

testimonials:

Orkut – confusing, open by default

Usability

Public Search Listing

Use this setting to control whether your search result is available outside of Facebook.

☒ Create a [public search listing](#) for me and submit it for search engine indexing ([see preview](#))



Joseph Bonneau

[Add Joseph Bonneau as Friend](#) | [Send Joseph Bonneau a Message](#) | [View Joseph Bonneau's Friends](#)

Here are some of **Joseph Bonneau's** friends:



David
Cottingham



Eirik
George
Tsarpalis



Emma
Alden



Luke
Church



Stella
Nordhagen



Justin
Palfreyman



Jillian
Sullivan



Pedro
Alejandro
Ortega

Not the **Joseph Bonneau** you were looking for? [Search more](#)



Joseph Bonneau is on Facebook.

Sign up for Facebook to connect with Joseph Bonneau.

[Sign Up](#)

It's free and anyone can join. Already a Member? [Login](#) to contact Joseph Bonneau.

- Facebook public search
 - All existing users opted in to new feature
 - Most have no idea it even exists!

Sloppiness

- Building secure applications is notoriously hard
- Very small development teams
 - Sonico – 20 M users, 20 engineers!
- Modern sites are extremely complex
 - Features launched before security is developed

Sloppiness



Facebook connect – No TLS authentication!

Sloppiness

Facebook Markup Language

```
<fb:swf swfsrc="http://myserver/flash.swf"  
imgsrc="http://myserver/image.jpg" imgstyle="-moz-  
binding:url(\'http://myserver/xssmoz.xml#xss\');" />
```

Translated into HTML:

```

```

Result: arbitrary JavaScript execution! (Felt, 2007)

Cambridge Security Group

Researching all aspects of the problem:

- ♦ Sloppiness
 - Poking holes to demonstrate insecurity
 - Facebook receiving most attention
- ♦ Usability
 - Proposing better user interfaces
- ♦ Economics
 - Survey of market, proposal of regulatory steps

Leakage through Public Search



Not the **Joseph Bonneau** you were looking for? [Search more](#) »

Joseph Bonneau

[Add Joseph Bonneau as Friend](#) | [Send Joseph Bonneau a Message](#) | [View Joseph Bonneau's Friends](#)

Here are some of **Joseph Bonneau's** friends:



David Cottingham



Eirik George Tsarpalis



Emma Alden



Luke Church



Stella Nordhagen



Justin Palfreyman



Jillian Sullivan



Pedro Alejandro Ortega

Joseph Bonneau is on Facebook.

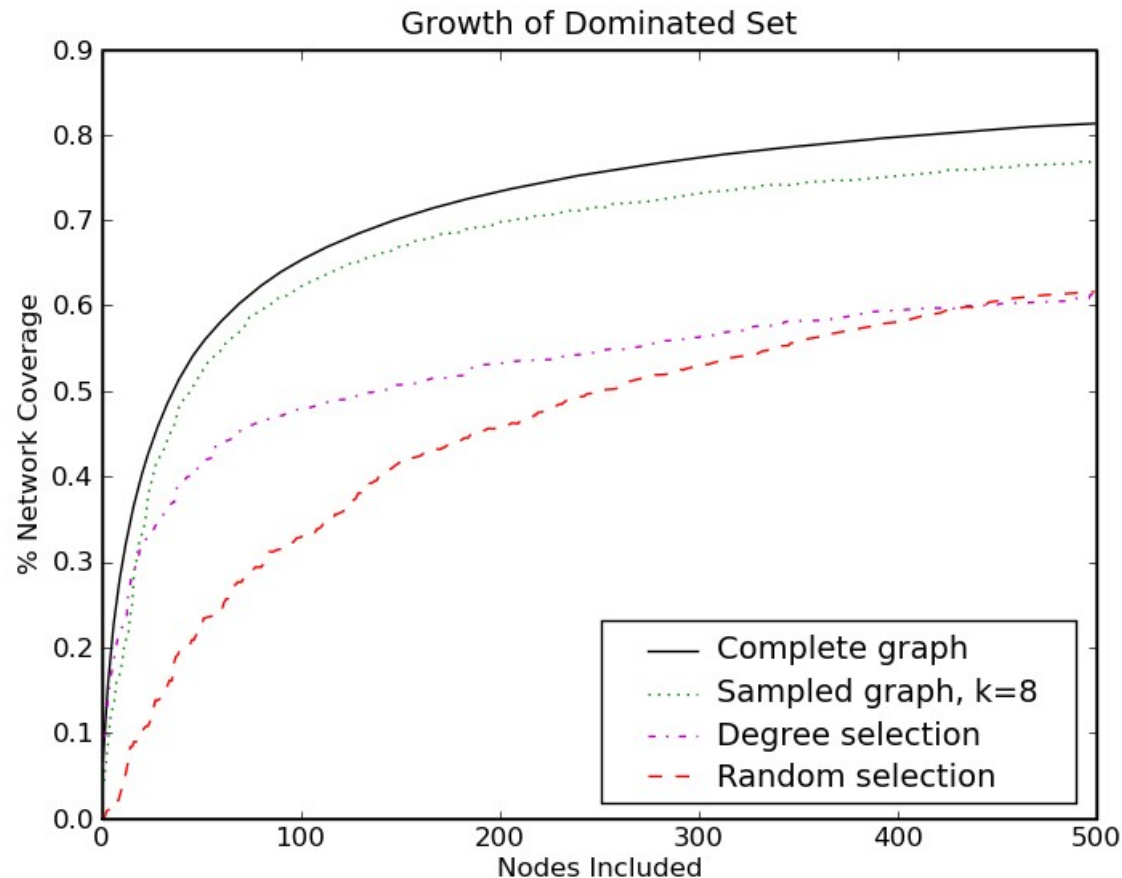
Sign up for Facebook to connect with Joseph Bonneau.

[Sign Up](#)

It's free and anyone can join. Already a Member? [Login to contact Joseph Bonneau.](#)

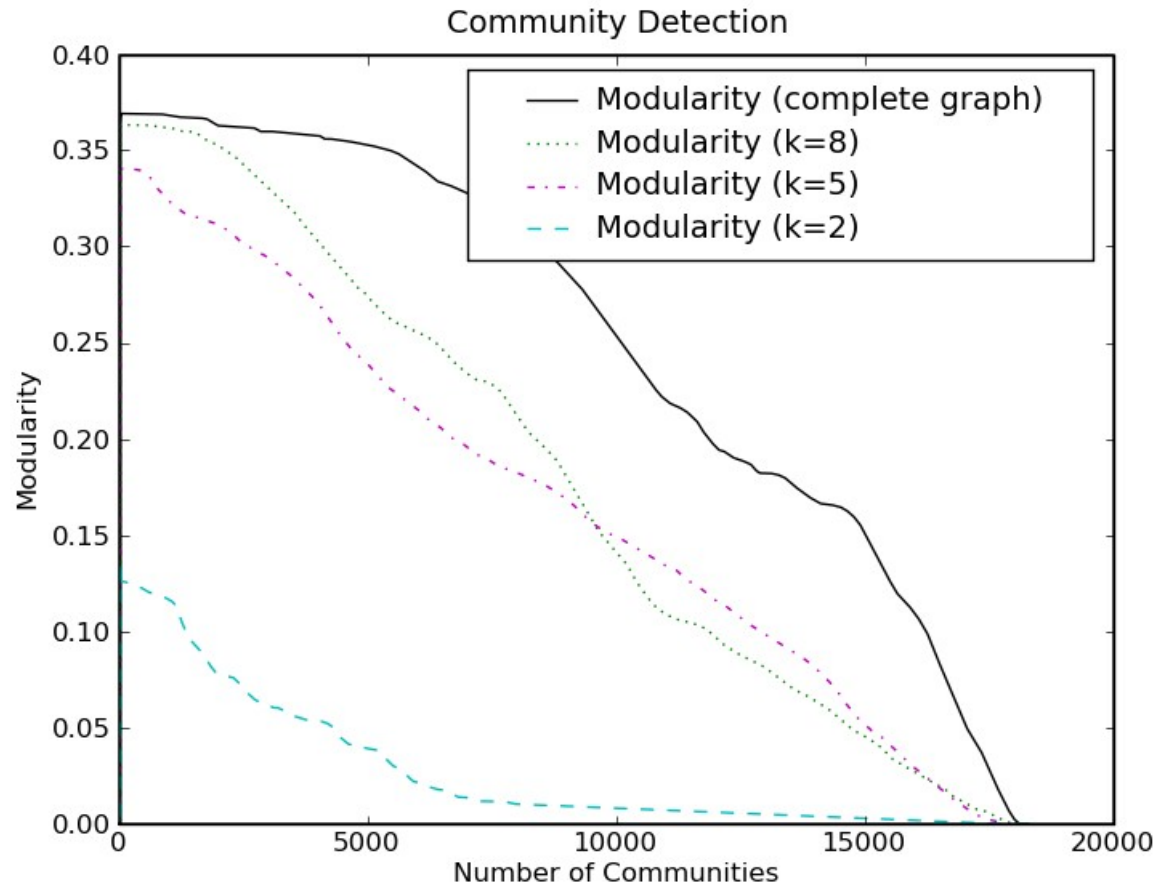
Thought to hide most of social graph...

Leakage through Public Search



Can efficiently find dominating sets

Leakage through Public Search



Can also accurately detect communities

Leakage through FBQL

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)

Call Method

\$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-instance">
 <friend_info>
 <uid1>4</uid1>
 <uid2>5</uid2>
 </friend_info>
 <friend_info>
 <uid1>5</uid1>
 <uid2>4</uid2>
 </friend_info>
</fql_query_response>

Well-crafted queries can access non-public data

Leakage through FBQL



User Querying Example...

210130-210630

Found 357 users

210131 Shirin Rahmanian (Stanford)
210132 Joseph Bonneau (Cambridge Stanford San Francisco, CA)
210137 Jen Cowman (Minneapolis / St. Paul, MN Stanford Northwestern 3M)
210139 Francis Ring (Stanford San Diego, CA)
210140 Robert Negrete (Stanford)
210141 Nicholas Lovell (Stanford Microsoft)
210143 Lisa Feng Yung Chen (Stanford Cornerstone Research)
210145 Weisheng Lee (Stanford)
210147 Pomo Micha (Stanford)
210148 Sheila Dharmarajan (Stanford)
210149 Matt Green (Stanford New York, NY)
210150 Nick Joy (Utah Stanford Washington Seattle, WA)
210151 Modern Micha (Stanford)
210153 AJ Olson (Stanford Meebo Silicon Valley, CA)
210154 Phillip Cameron Morrison (Stanford)

Malicious application can crawl Stanford network in hours

Photo hosting problems



Photo ACL enforced using session cookies

Photo hosting problems



Problem – Photos hosted on separate servers!

Photo hosting problems



- ♦ Can't transfer session cookies between domains
 - Privacy violation!
- ♦ Insufficient entropy in photo URL's
- ♦ Insecure pseudorandom number generator used
- ♦ Result: 'Private' photos accessible!

Usability Improvements

 [Privacy](#) ► **Suites**

Privacy Suites

Use the setting below to control who on Facebook can find you through the search function. Your Friends will always be able to find you.

Search Visibility



Jon's Settings (Paranoid)



Save Changes

Cancel

Privacy Suites – delegate management to trusted friend

Economic Analysis

- ♦ 45 major sites surveyed
- ♦ Result: Evidence of market failure
 - Little competition between sites on privacy
 - Poor usability
 - Obfuscated privacy policies
 - Users unable to assess a site's privacy level
- ♦ Better regulation required

Conclusions

- ♦ Social networks here to stay
- ♦ Privacy needs dramatic improvement
- ♦ Can't currently provide meaningful control
- ♦ Users must exercise caution

Upcoming Publications

- ♦ Joseph Bonneau. “New Facebook Photo Hacks.” *Light Blue Touchpaper*.
<http://www.lightbluetouchpaper.org/2009/02/11/new-facebook-photo-hacks/>
- ♦ Joseph Bonneau, Jonathan Anderson, Ross Anderson, Frank Stajano. “Eight Friends is Enough: Social Graph Leakage Through Public Listings.” to appear in to *SocialNets 2009*
- ♦ Joseph Bonneau, Jonathan Anderson, George Danezis. “Methods of Data Collection from a Social Network.” submitted to *Advances in Social Network Mining and Analysis 2009*.
- ♦ Jonathan Anderson, Joseph Bonneau, Luke Church. “Privacy Suites: Socially Managed Privacy.” submitted *Workshop on Social Networks 2009*
- ♦ Joseph Bonneau, Soren Preibusch. “The Jungle: A Field Study into Privacy in Social Networks.” submitted *Workshop on the Economics of Information Security 2009*.

Questions?

jcb82@cl.cam.ac.uk