Could Googling Take Down A President, a Prime Minister, or an Average Citizen?

Gregory Conti
United States Military Academy
West Point, New York
gregory.conti@usma.edu

Outline

- Information Disclosure
  - Computing Platform
  - Network Eavesdropping
  - Destination Websites
- Vectors
- Cross-site Tracking
  - Advertising and Embedded Content
- User Motivation
  - The survey says
- Solutions



Eliot Spitzer
Former-Governor of New York

"Never talk when you can nod, and never nod when you can wink, and never write an e-mail because it's death. You're giving prosecutors all the evidence we need."

- Eliot Spitzer
Two Years before his resignation

http://abcnews.go.com/Blotter/story?id=4424507&page=1

Maf54 (7:43:27 PM):
well dont ruin my mental picture

Xxxxxxxxx (7:43:32 PM):
oh lol...sorry

Maf54 (7:43:54 PM):
nice

Maf54 (7:43:54 PM):
youll be way hot then

Xxxxxxxxx (7:44:01 PM):
haha...hopefully



Mark Foley
Former-US Congressman

http://abcnews.go.com/WNT/BrianRoss/Story?id=2509586&page=2

Can anyone help me please! This stalking thing is not funny at all. When I type my name in keyword it gives a list of places that show where I have been on aol on the net. This is nobodys business. I have not done anything wrong at all and I have contacted aol about this matter and they keep saying they will do something about it but never do.

-Debbie

How do I get stuff removed from aol stalker? Can anyone tell me? Aol won't respond even though they claim willingness to remove data when requested. Someone, anyone, please help!

-Sally

http://blogs.ittoolbox.com/security/investigator/archives/aol-stalker-website-unleashed-11133

Slashdot: News for nerds, stuff that matters - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://slashdot.org/
Google
USMA | Index of /blackhat&d... | Official Google Blog | Slashdot | Digg | SecurityFocus | Virus Bulletin : Indep... | Dark Reading - The B... | RUMINT Stats
Microsoft Outlook Web Access | Slashdot: News for nerds, stuff th...

Slashdot

NEWS FOR NERDS. STUFF THAT MATTERS.

Search

▼ Sections
Main
Apple
AskSlashdot
Backslash
Books
Developers
Games
Hardware
Interviews
IT
Linux
Mobile
Politics
Science
YRO
▼ Help
FAQ
Bugs

Slashdot is powered by **your submissions**, so send in your scoop

IT: Details of Cyber Storm War Games Released

Posted by Soulskill on Thursday January 31, @07:29PM
from the **defending-against-gravitic-mines** dept.

I Don't Believe in Imaginary Property writes



> "Apparently, the participants in the U.S. 'Cyber Storm' war games are familiar with the Kobayashi Maru, because some of them tried to cheat by hacking the games themselves. They also prepare for some very interesting scenarios. Among other things, the organizers are worried about having too many people on the 'No Fly' list show up at an airport, finding 'mystery liquids' in the subway, and having bloggers reveal the classified location of railcars with hazardous materials. The Department of Homeland Security has already analyzed the results of the games, and plans to hold 'Cyber Storm 2' in March."

▶ government, internet *(tagging beta)*

Read More... | it.slashdot.org | 12 comments



IT: Microsoft Launches IT Superhero Comic

Book Reviews

Recent reviews from Slashdot readers:

The Creature from Jekyll Island
Is a compelling look at the history of the Federal Reserve

AOL Demo

- User #10291
- User #2708

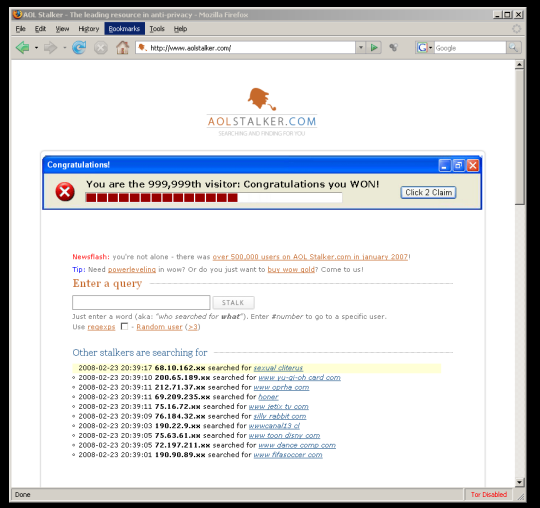
The AOL Dataset Debacle

SIGIR – IR List (August 2006)
Subject: research.aol.com

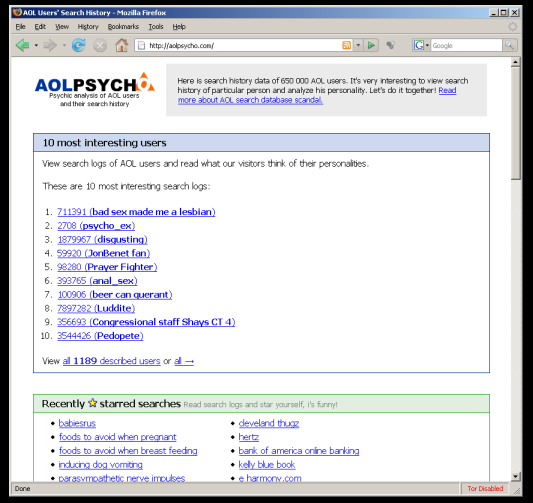
AOL is embarking on a new direction for its business making its content and products freely available to all consumers. To support those goals, AOL is also embracing the vision of an open research community. To get started, we invite you to visit us at http://research.aol.com, where you will find:

- 20,000 hand labeled, classified queries
- 3.5 million web question/answer queries (who, what, where, when, etc.)
- **Query streams for 500,000 users over 3 months (20 million queries)**
- 2 million queries against US Government domains

Also, **please feel free to provide feedback** on the site, datasets you'd like to see in the future, and any other comments about our vision.



AOL Stalker



AOL Psycho

Definitions

- googling: The full spectrum of free online tools and services (such as search, mapping, email, Web-based word processing and calendaring etc.)

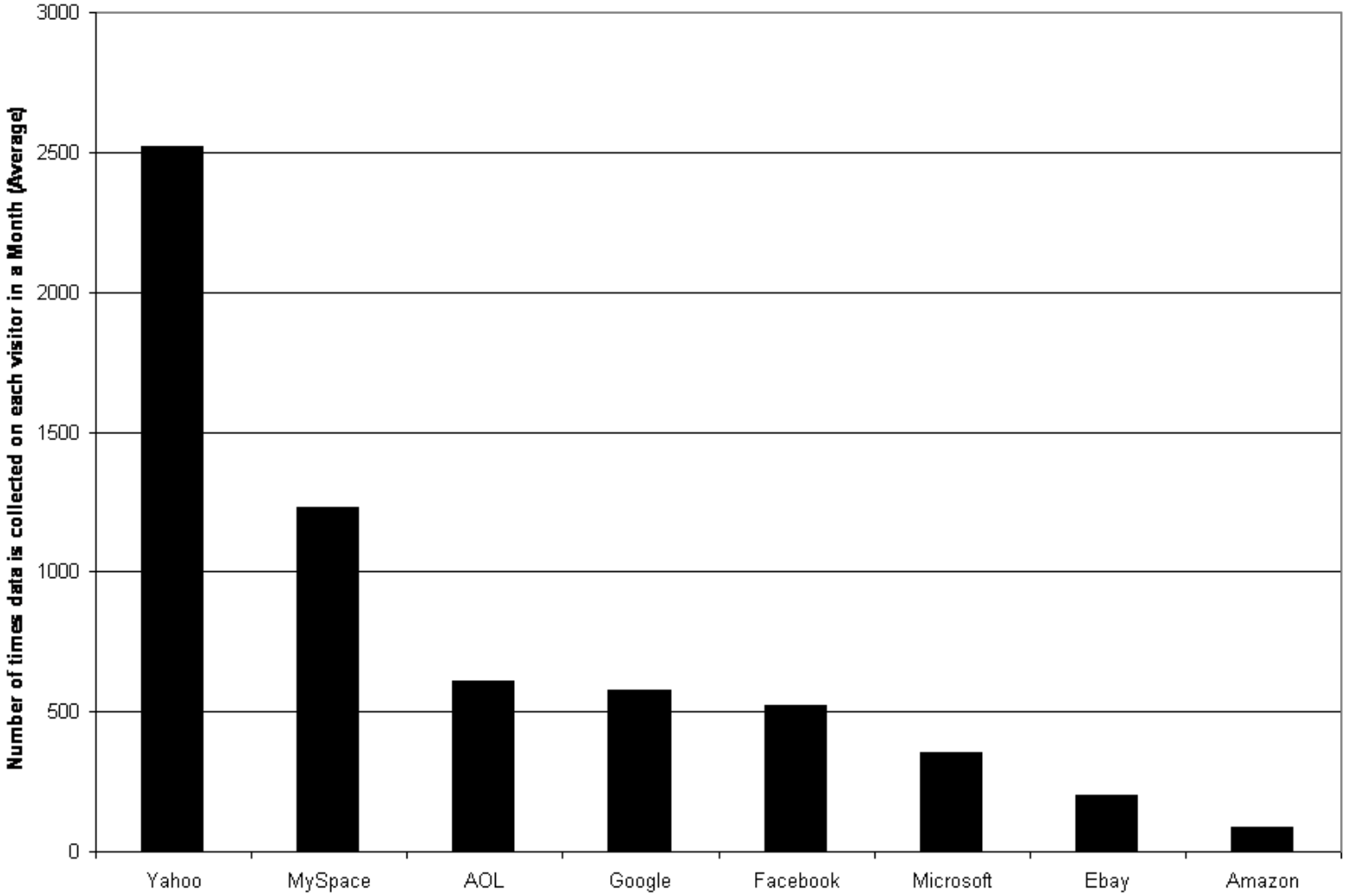
- web-based information disclosure: the information we disclose as we surf the web

Global Computing Statistics

• World Population	~6.6 Billion
• Cell Phones	~3.3 Billion
• Personal Computers	~1.2 Billion
• MP3 Players	~220 Million
• Digital Cameras	~120 Million
• Webcams	~100 Million
• PDAs	~85 Million
• DVRs	~44 Million
• Servers	~27 Million

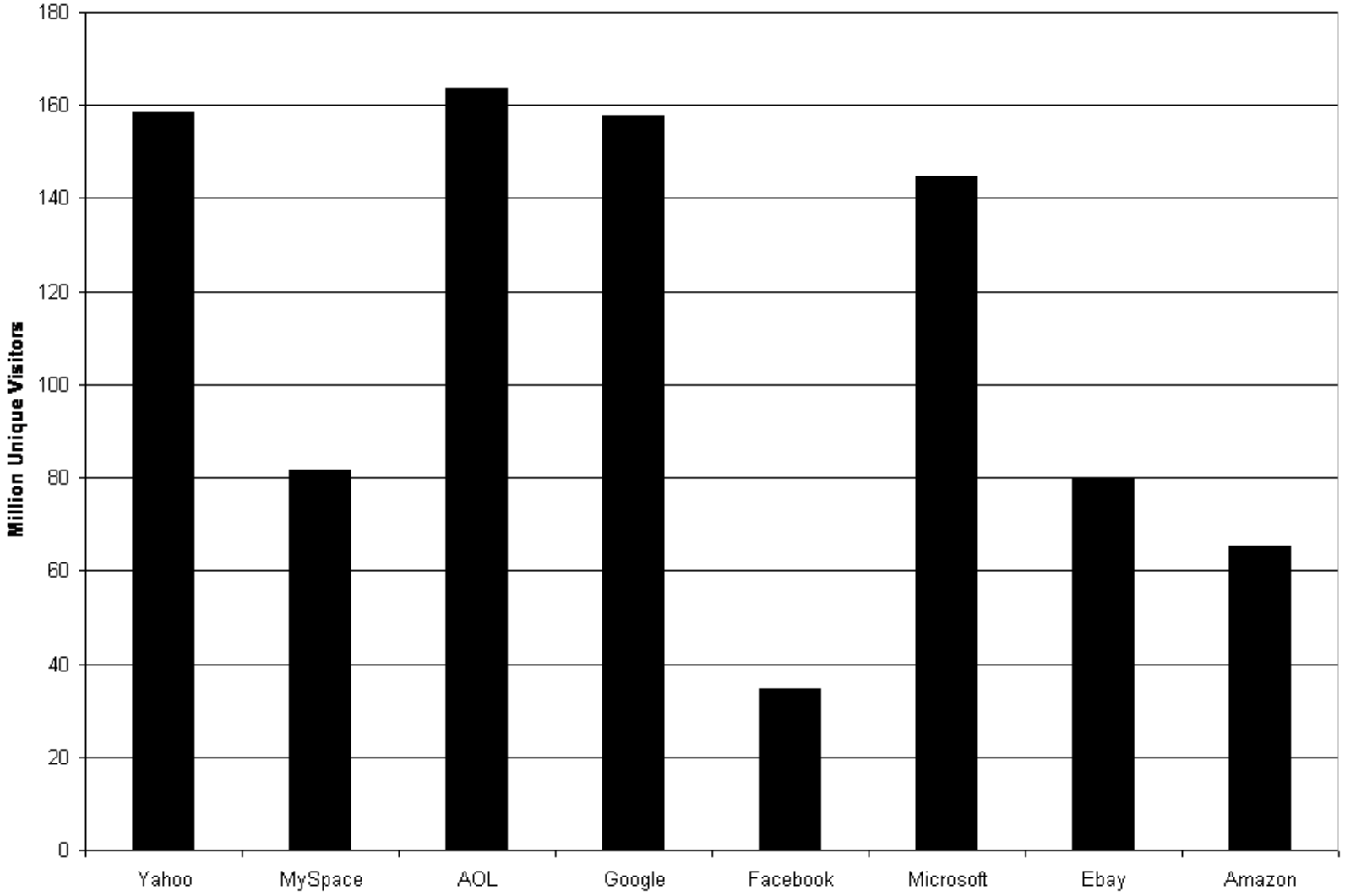
Kevin Kelly, "The Planetary Computer." Wired, 16.07, July 2008, pp52-55

Data Collection

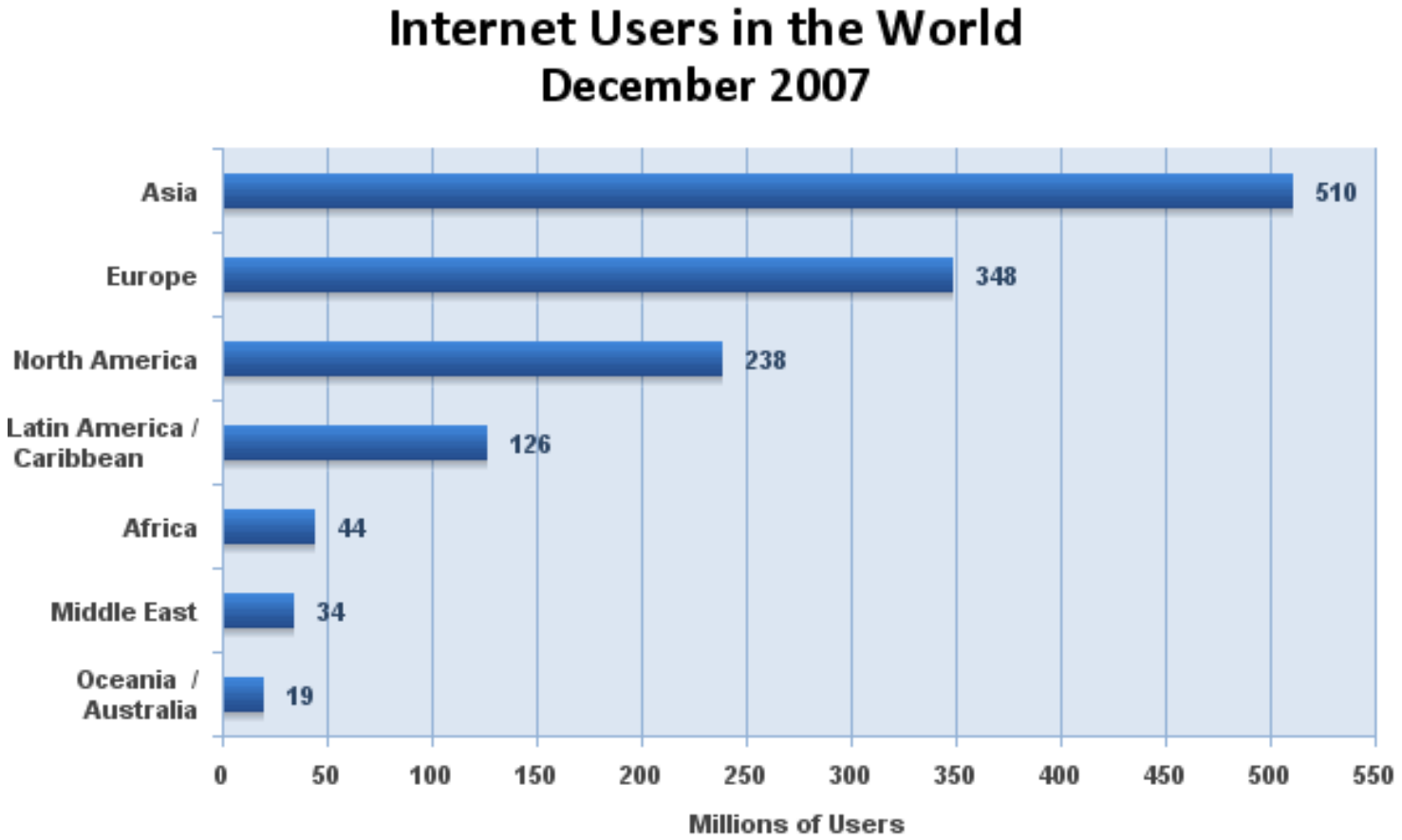


http://www.nytimes.com/2008/03/10/technology/10privacy.html?pagewanted=1&_r=1&hp / Comscore

Unique Visitors
(millions / month)



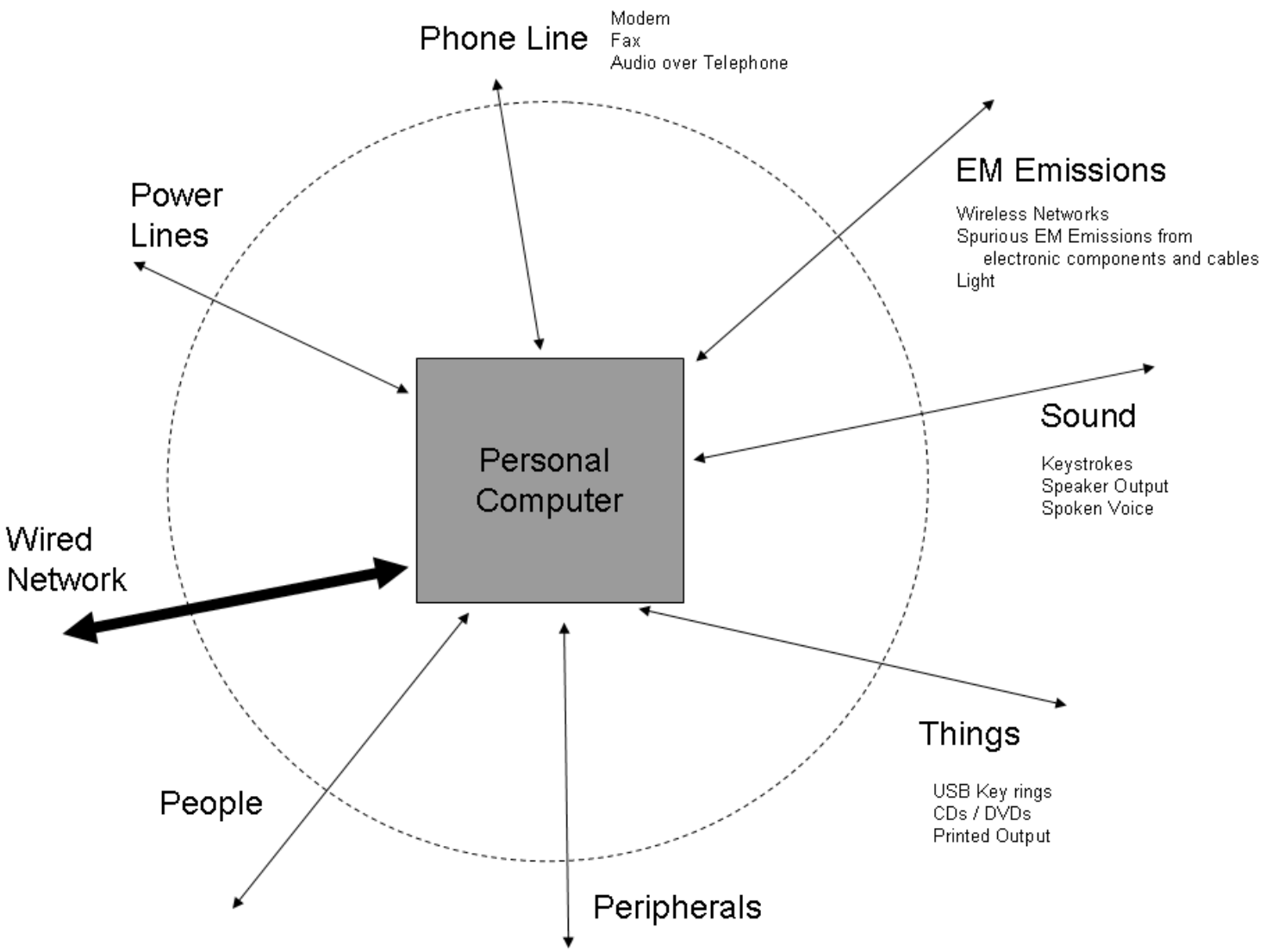
http://www.nytimes.com/2008/03/10/technology/10privacy.html?pagewanted=1&_r=1&hp & Comscore



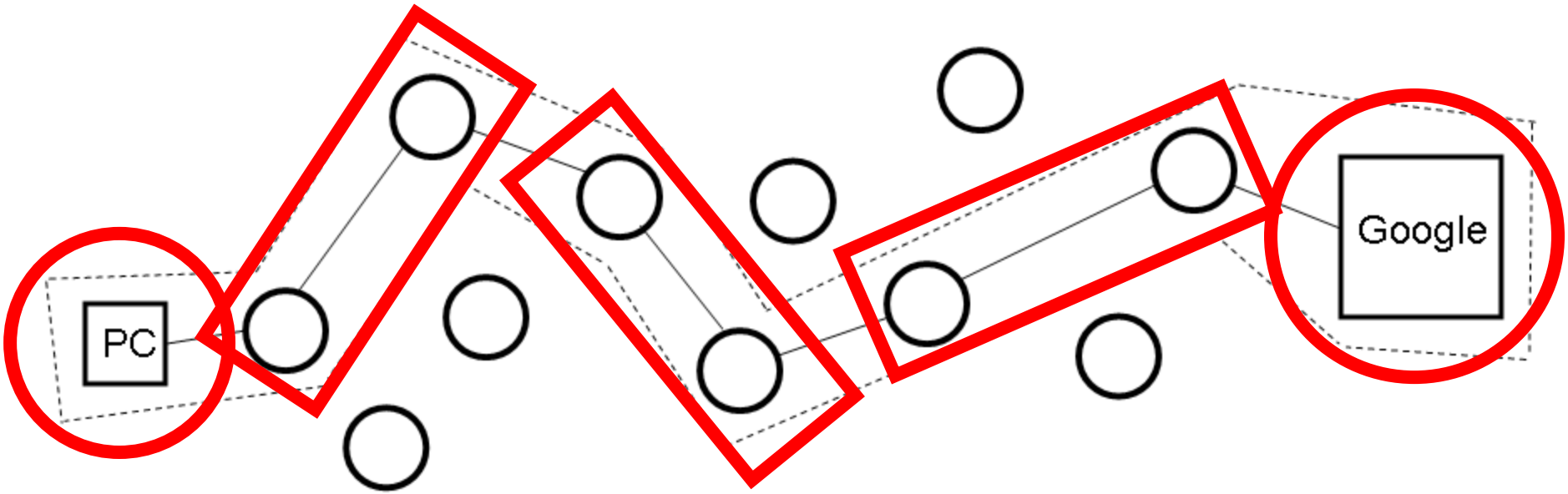
- 1.319 Billion for Year End 2007
- 20% Overall Penetration

source: http://www.internetworldstats.com/stats.htm

Information Leakage on a PC



Information Leakage and Spurious Emanations on a Network



ISPs vs. Large Online Companies

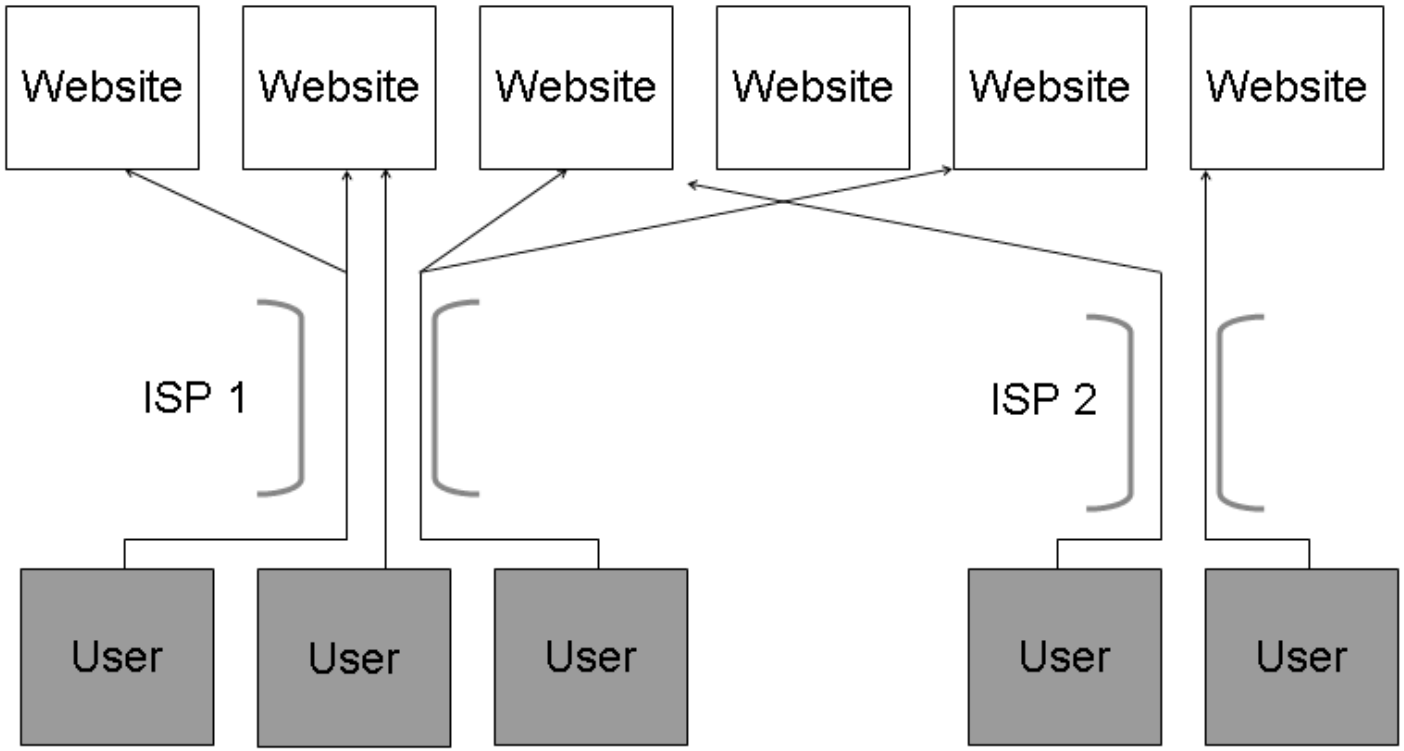
Online Company

- Sees global traffic from many customers
  - domain specific
- Advertising and embedded content brings in additional information
- Limited knowledge of user identity
- Extensive datamining

ISP

- Sees all traffic from its set of customers
  - except encrypted traffic
  - traffic analysis
- Limited to no visibility on non-customers
- Knows identity and location of accounts
- Ability to manipulate network flows
  - DNS
  - blocking P2P

Vantage Points of ISPs vs Online Companies



DNS Based Vulnerabilities



Major Threat Vectors

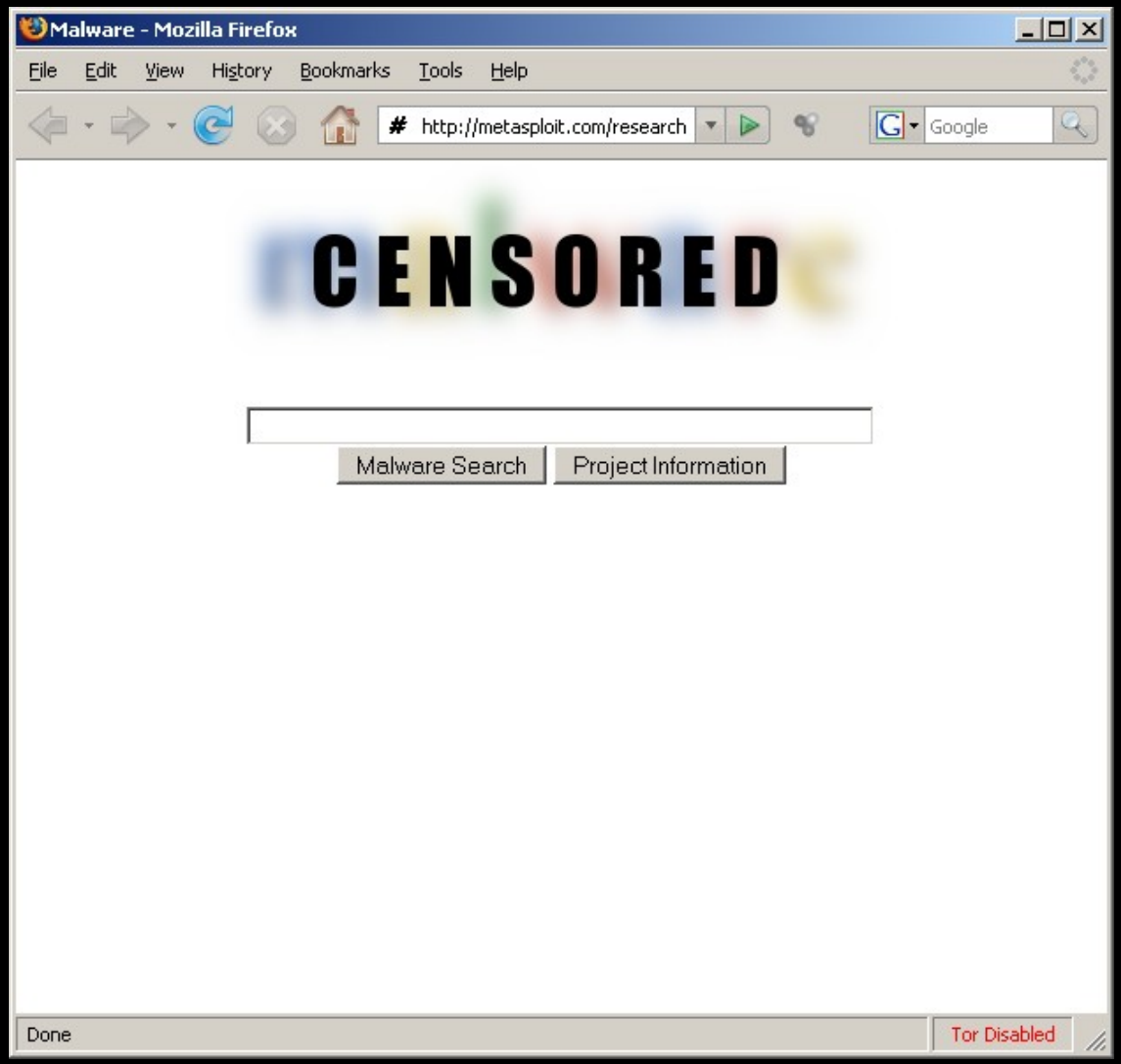
- Email
- Search
- Mobile Phones
- FTP Replacement
- Web office suites
- Mapping
- …

The Many Flavors of Search
(Simply Google)



Malware Search

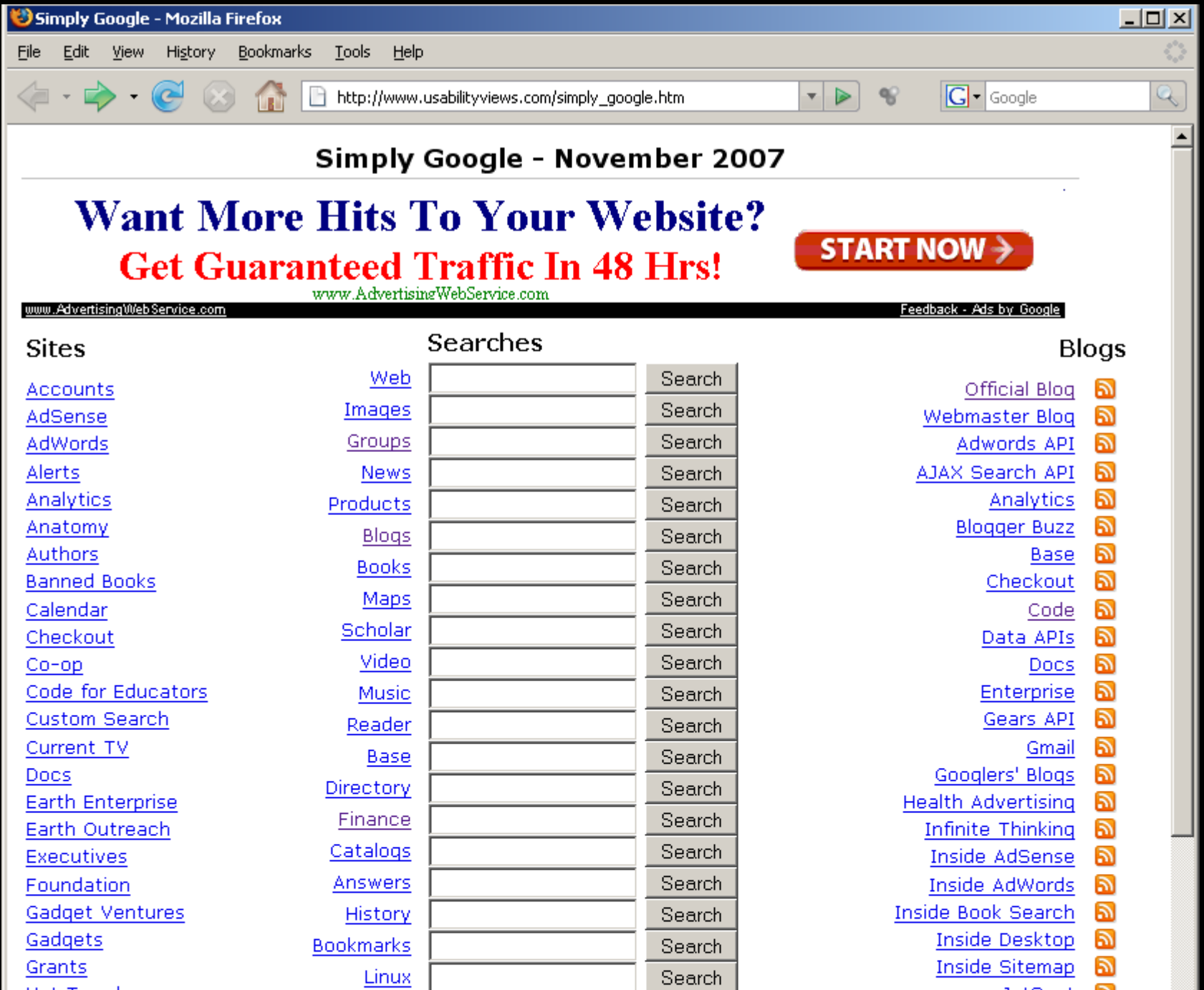
http://metasploit.com/research/misc/mwsearch/index.html



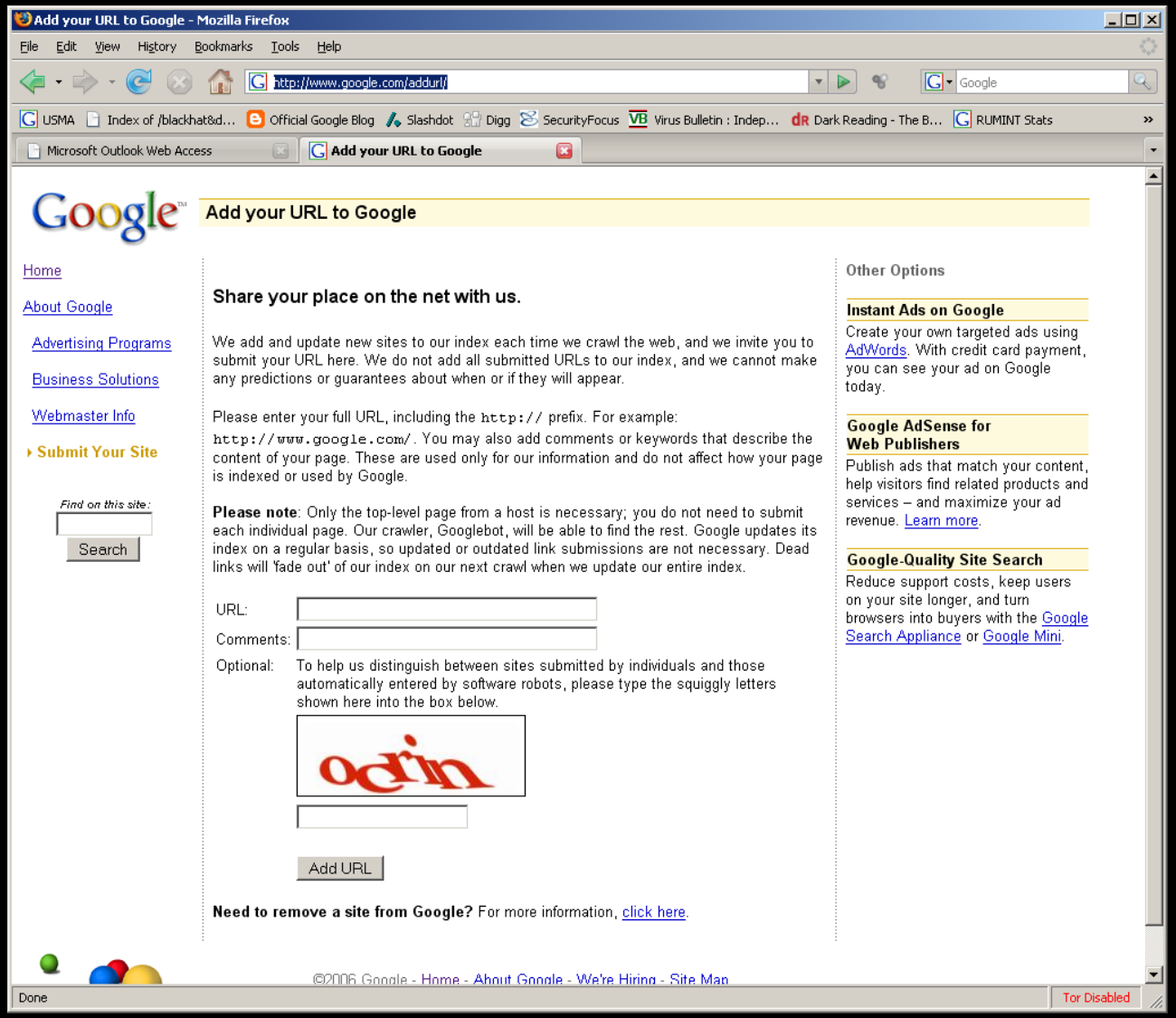
http://www.theregister.co.uk/2006/07/18/malware_search/

Motivation

- Cost benefit analysis
  - users
  - webmasters
  - bloggers
- Short-term gain vs. long term risks
- stats
- boils down to trust and awareness

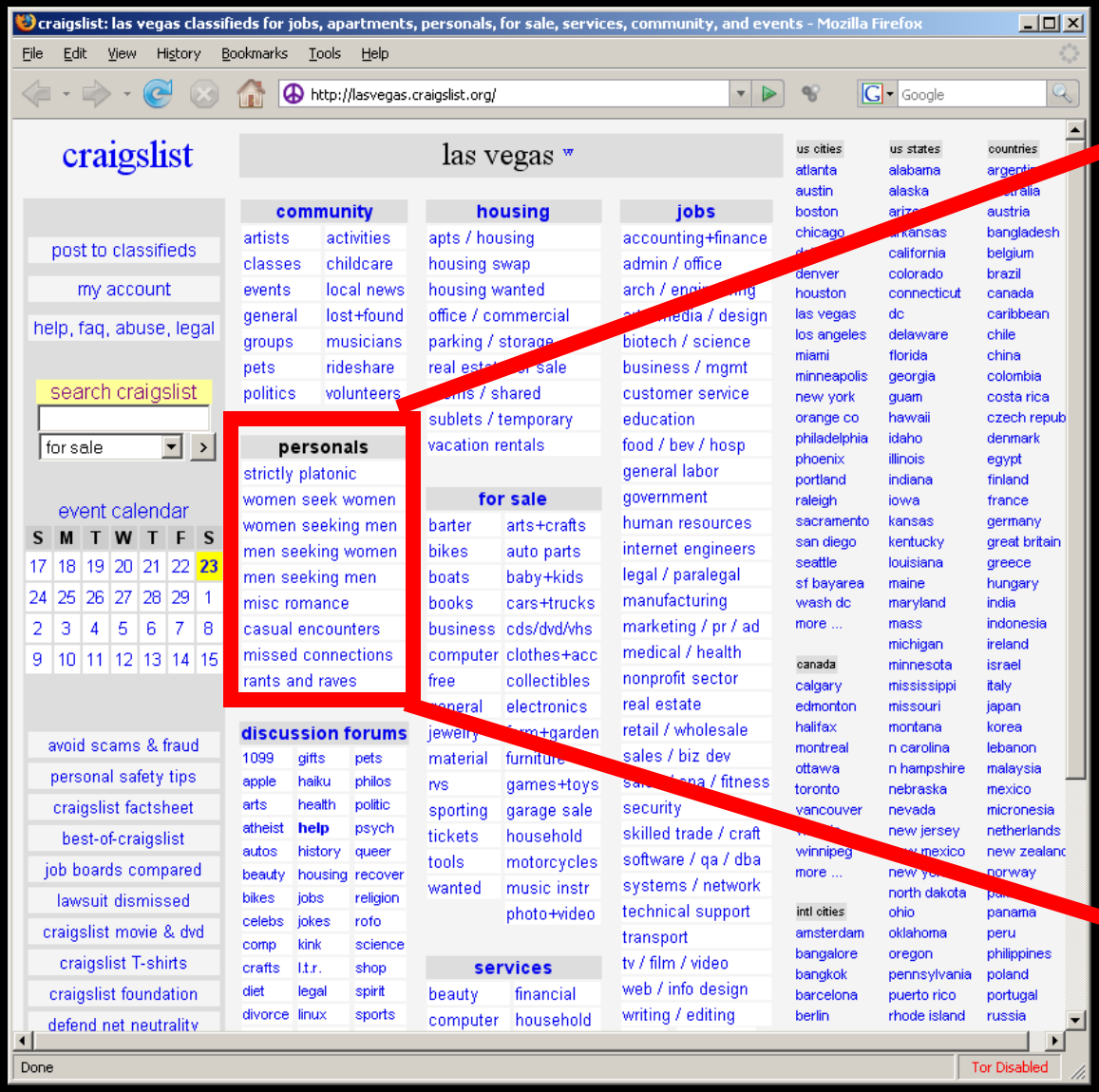

Simply Google - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.usabilityviews.com/simply_google.htm
Google
Simply Google - November 2007
Want More Hits To Your Website?
Get Guaranteed Traffic In 48 Hrs!
START NOW
www.AdvertisingWebService.com
www.AdvertisingWebService.com
Feedback - Ads by Google
Sites
Accounts
AdSense
AdWords
Alerts
Analytics
Anatomy
Authors
Banned Books
Calendar
Checkout
Co-op
Code for Educators
Custom Search
Current TV
Docs
Earth Enterprise
Earth Outreach
Executives
Foundation
Gadget Ventures
Gadgets
Grants
Searches
Web
Images
Groups
News
Products
Blogs
Books
Maps
Scholar
Video
Music
Reader
Base
Directory
Finance
Catalogs
Answers
History
Bookmarks
Linux
Search
Blogs
Official Blog
Webmaster Blog
Adwords API
AJAX Search API
Analytics
Blogger Buzz
Base
Checkout
Code
Data APIs
Docs
Enterprise
Gears API
Gmail
Googlers' Blogs
Health Advertising
Infinite Thinking
Inside AdSense
Inside AdWords
Inside Book Search
Inside Desktop
Inside Sitemap

If the content on the web it is fair game.



Case Studies

Craig's List



personals

strictly platonic

women seek women

women seeking men

men seeking women

men seeking men

misc romance

casual encounters

missed connections

rants and raves

Ebay

eBay Feedback Profile for salesman_jack - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://feedback.ebay.com/ws/eBayISAPI.dll?ViewFeedback2&userid=salesman_jack&&ftab=Feedb

Buy | Sell | My eBay | Community | Help

Welcome! Sign in or register. Site Map

All Categories | Search | Advanced Search

Categories ▾ | Motors | Express | Stores | eBay Security & Resolution Center

Home > Community > Feedback Forum > Feedback Profile — See what's coming up!

Feedback Profile

salesman_jack (66 ★)

Member since Dec-03-07 in Hong Kong

Contact member | View items for sale | More options

Feedback Score: 66
Positive Feedback: 98.5%

Members who left a positive: 67
Members who left a negative: 1

All positive Feedback: 310

Find out what these numbers mean

Recent Feedback Ratings (last 12 months)

	1 month	6 months	12 months
Positive	310	310	310
Neutral	0	0	0
Negative	0	0	0

Detailed Seller Ratings (since May 2007)

Criteria	Average rating	Number of ratings
Item as described		52
Communication		52
Shipping time		52
Shipping and handling charges		52

Feedback as a seller | Feedback as a buyer | All Feedback | Feedback left for others

Ratings mutually withdrawn: 1

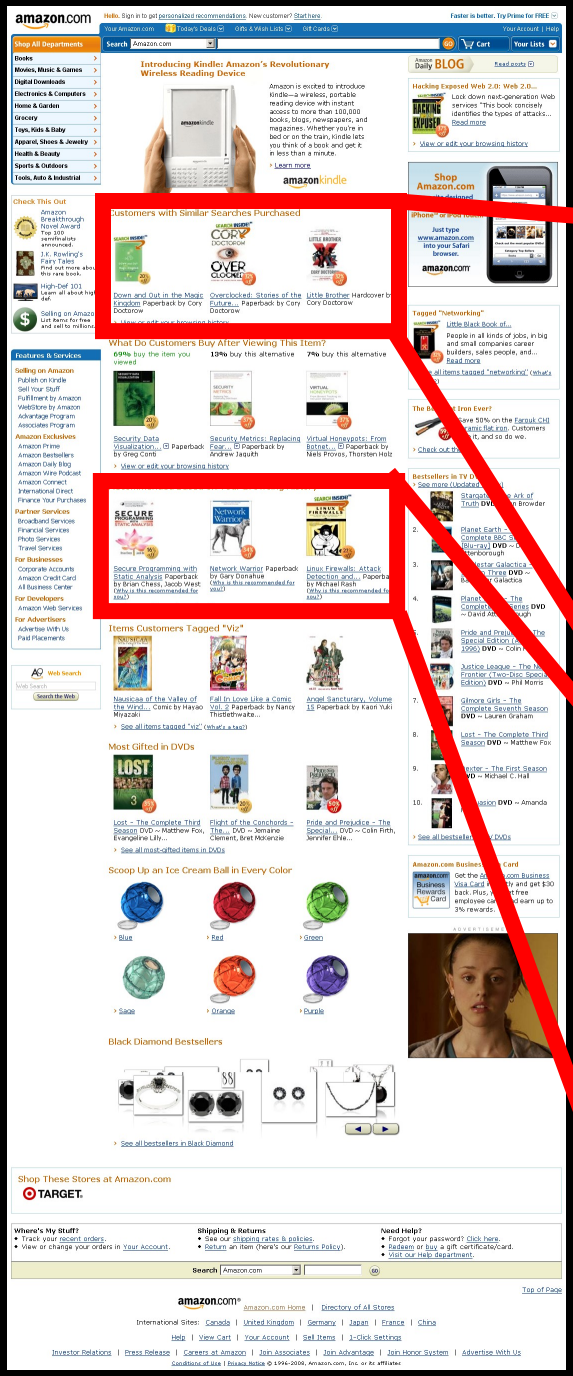
311 Feedback received — Page 1 of 1

Feedback	From Buyer / Price	Date / Time
arrived as described Breast Cancer Awareness Charm Ring Keychain (pink) NIB (#120218565836)	badred98 (545 ★) US $1.04	View Item
Thanks!! great transaction!!! Red Dog Chams Ring Charm Keyfob Keychain NIB (#120219285329)	missy1282 (157 ★) US $1.04	Feb-23-08 12:34 View Item
Great transaction. Thanks Breast Cancer Awareness Charm Ring Keychain (pink) NIB (#120215410482)	mjeent (232 ★) US $5.50	Feb-23-08 09:15 View Item
Excellent price. Product exactly what was described. Fast shipping considering. Pink Heart Heart Crystal Heart Charm Keychain New w/Box (#120218936234)	cheervrsty08 (2) US $2.00	Feb-22-08 18:55 View Item
Beautiful keychain. My daughter loves it. Perfect condition. Thanks!		Feb-22-08 18:41

Tor Disabled



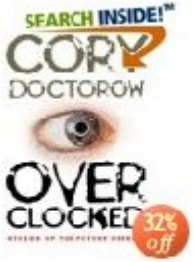
Amazon



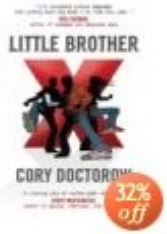
Customers with Similar Searches Purchased



Down and Out in the Magic Kingdom Paperback by Cory Doctorow



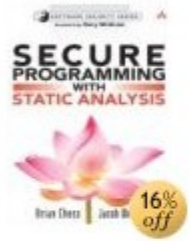
Overclocked: Stories of the Future... Paperback by Cory Doctorow



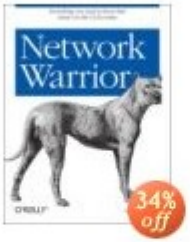
Little Brother Hardcover by Cory Doctorow

› View or edit your browsing history

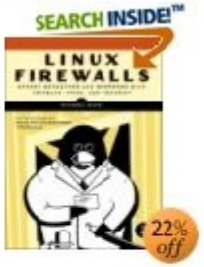
Recommended Based on Your Browsing History



Secure Programming with Static Analysis Paperback by Brian Chess, Jacob West (Why is this recommended for you?)



Network Warrior Paperback by Gary Donahue (Why is this recommended for you?)

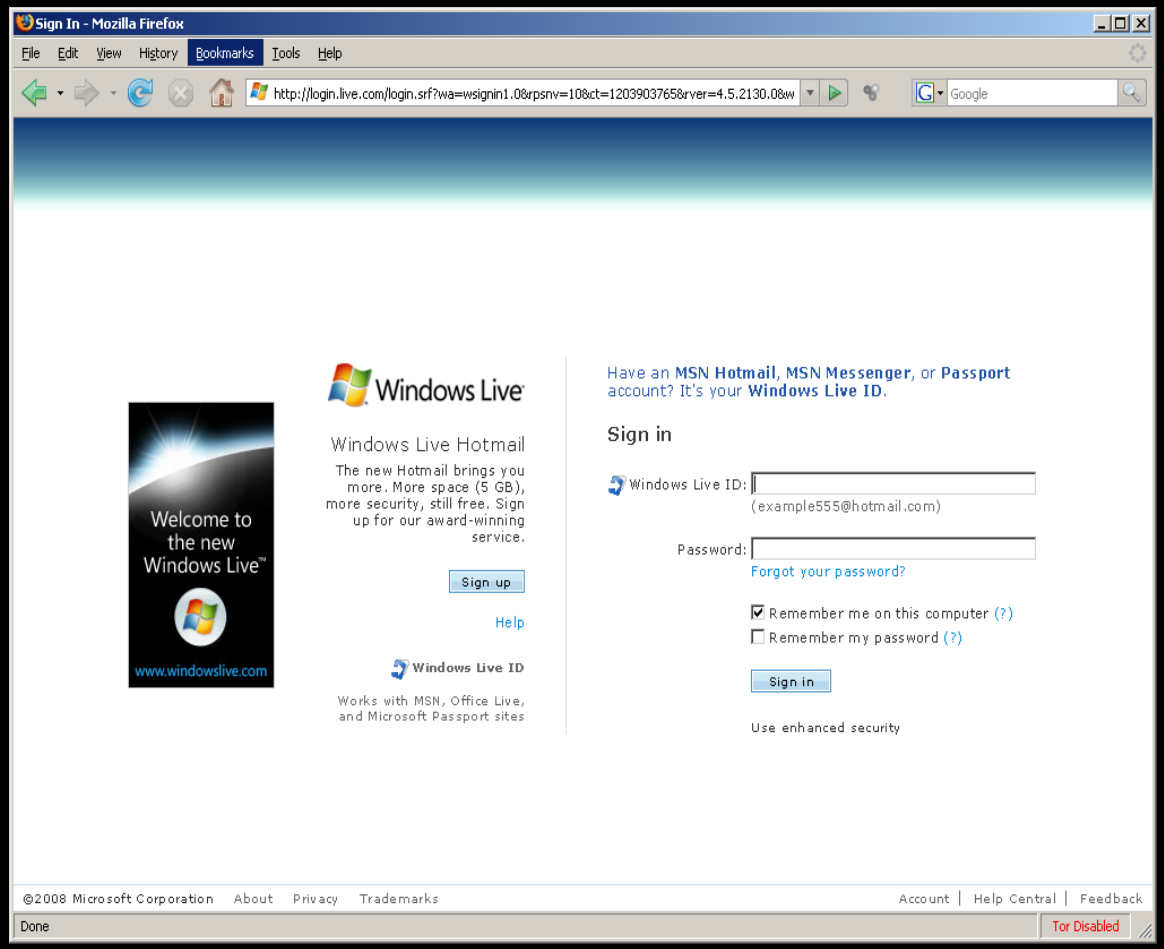


Linux Firewalls: Attack Detection and... Paperback by Michael Rash (Why is this recommended for you?)

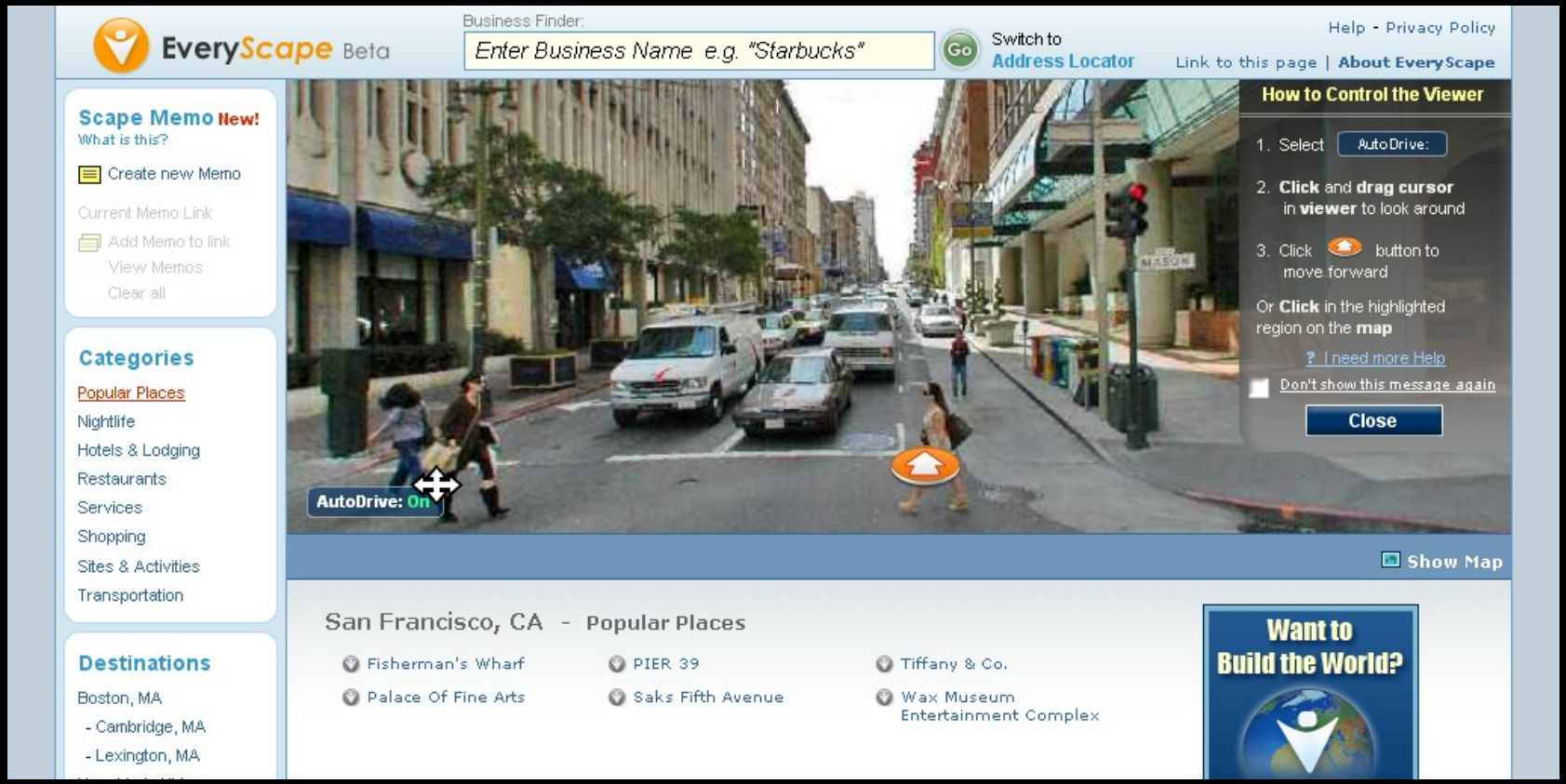
› View or edit your browsing history

Hotmail

Any email that touches any of these servers should be considered compromised.

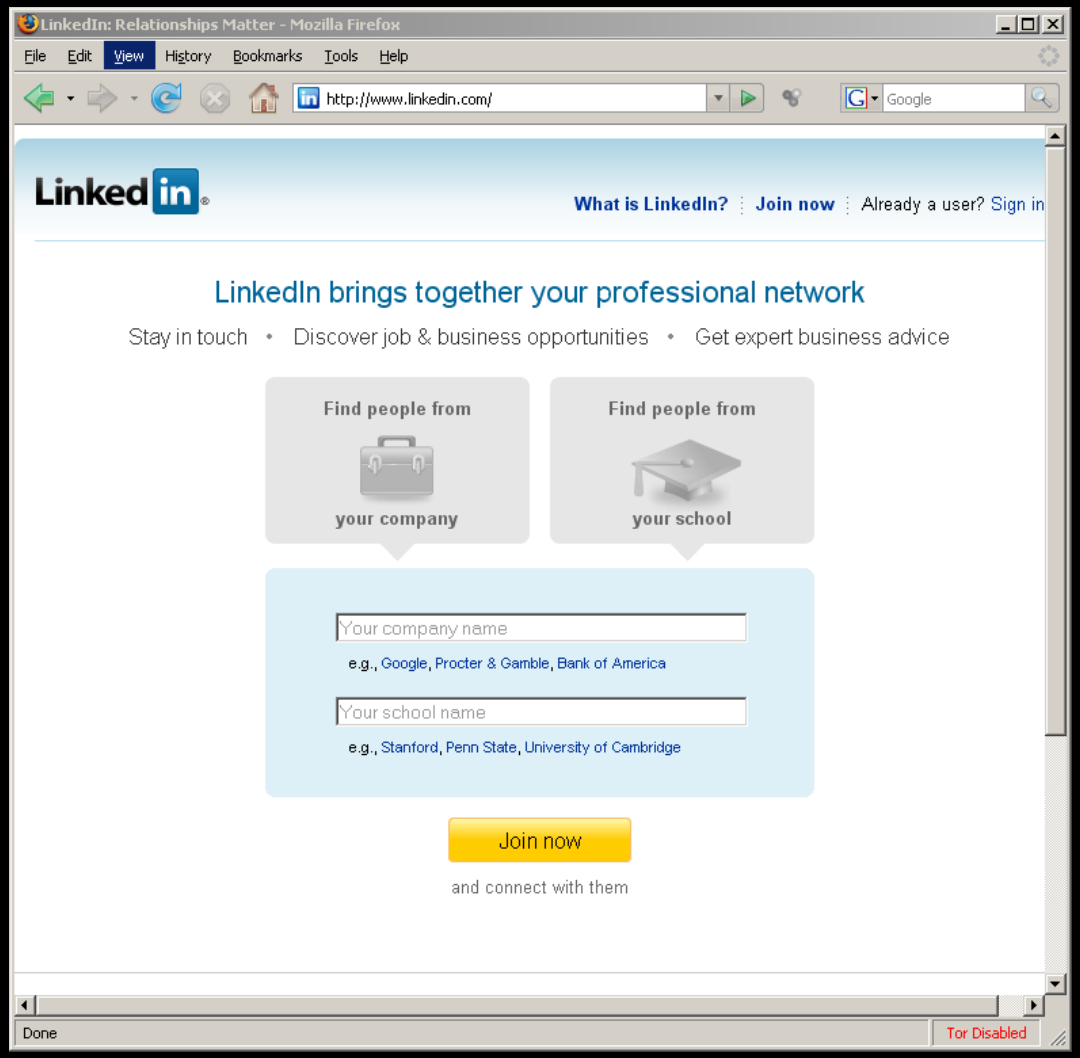


Everyscape



http://www.everyscape.com/sanfrancisco-ca.us.aspx

Linked In



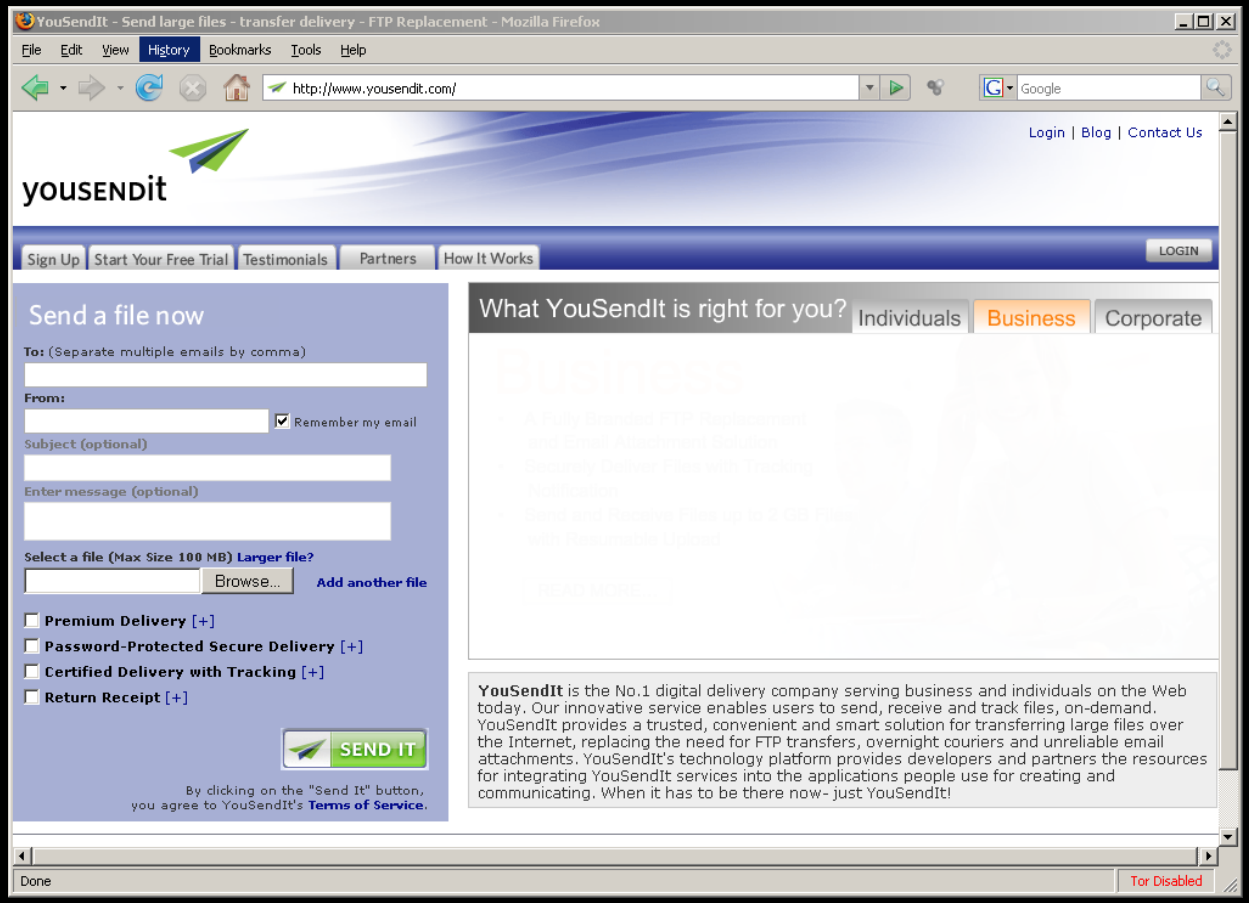
Social networking sites know your contacts and your contacts' contacts. Old friends will find you and let the site know of the relationship.

Map Quest

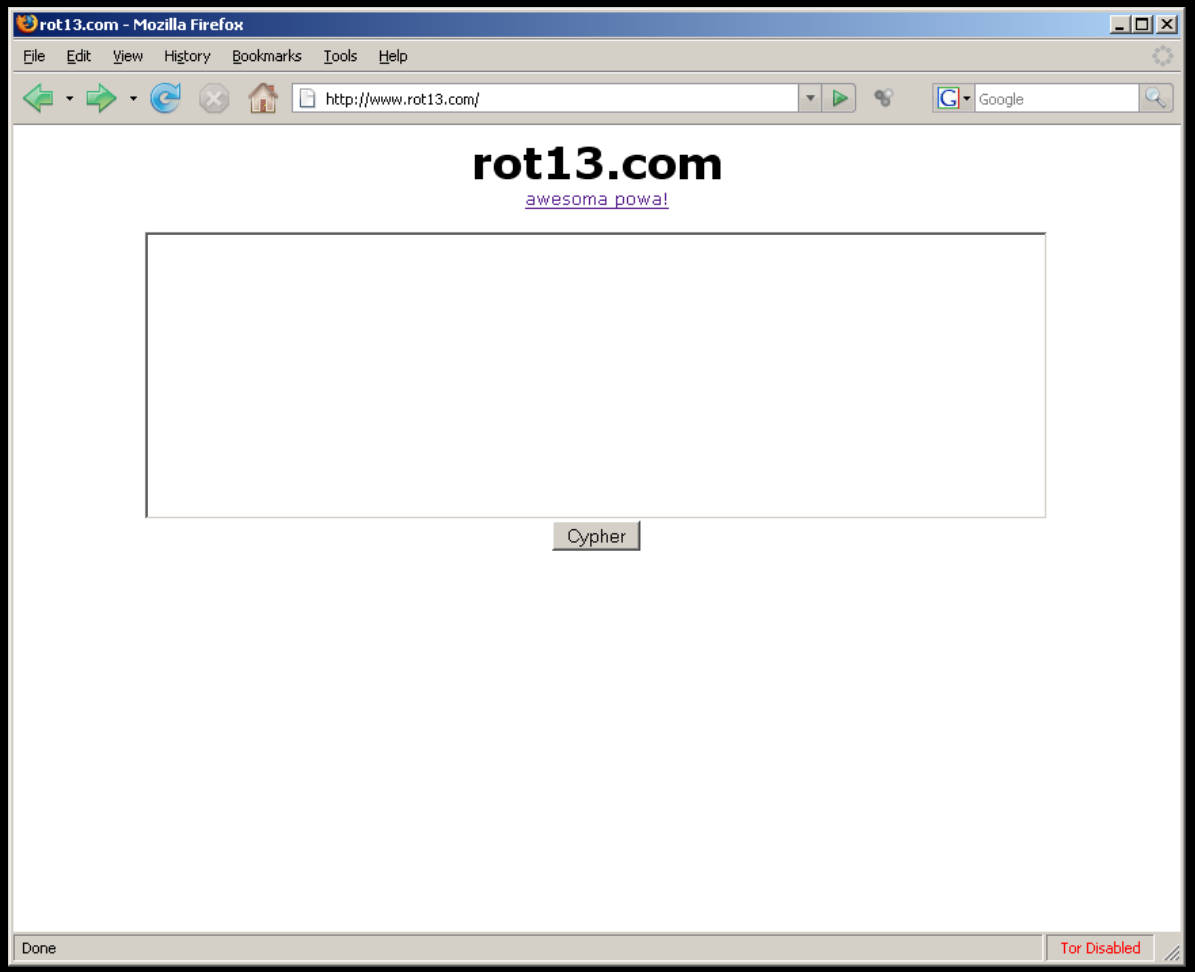
Mapping sites reveal locations of interest, allowing diverse groups of users to be linked.



You Send It


YouSendIt - Send large files - transfer delivery - FTP Replacement - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.yousendit.com/
Google
Login | Blog | Contact Us
yousendit
Sign Up
Start Your Free Trial
Testimonials
Partners
How It Works
LOGIN
Send a file now
To: (Separate multiple emails by comma)
From:
Remember my email
Subject (optional)
Enter message (optional)
Select a file (Max Size 100 MB) Larger file?
Browse...
Add another file
Premium Delivery [+]
Password-Protected Secure Delivery [+]
Certified Delivery with Tracking [+]
Return Receipt [+]
SEND IT
By clicking on the "Send It" button, you agree to YouSendIt's Terms of Service.
What YouSendIt is right for you?
Individuals
Business
Corporate
YouSendIt is the No.1 digital delivery company serving business and individuals on the Web today. Our innovative service enables users to send, receive and track files, on-demand. YouSendIt provides a trusted, convenient and smart solution for transferring large files over the Internet, replacing the need for FTP transfers, overnight couriers and unreliable email attachments. YouSendIt's technology platform provides developers and partners the resources for integrating YouSendIt services into the applications people use for creating and communicating. When it has to be there now- just YouSendIt!
Done
Tor Disabled

rot 13



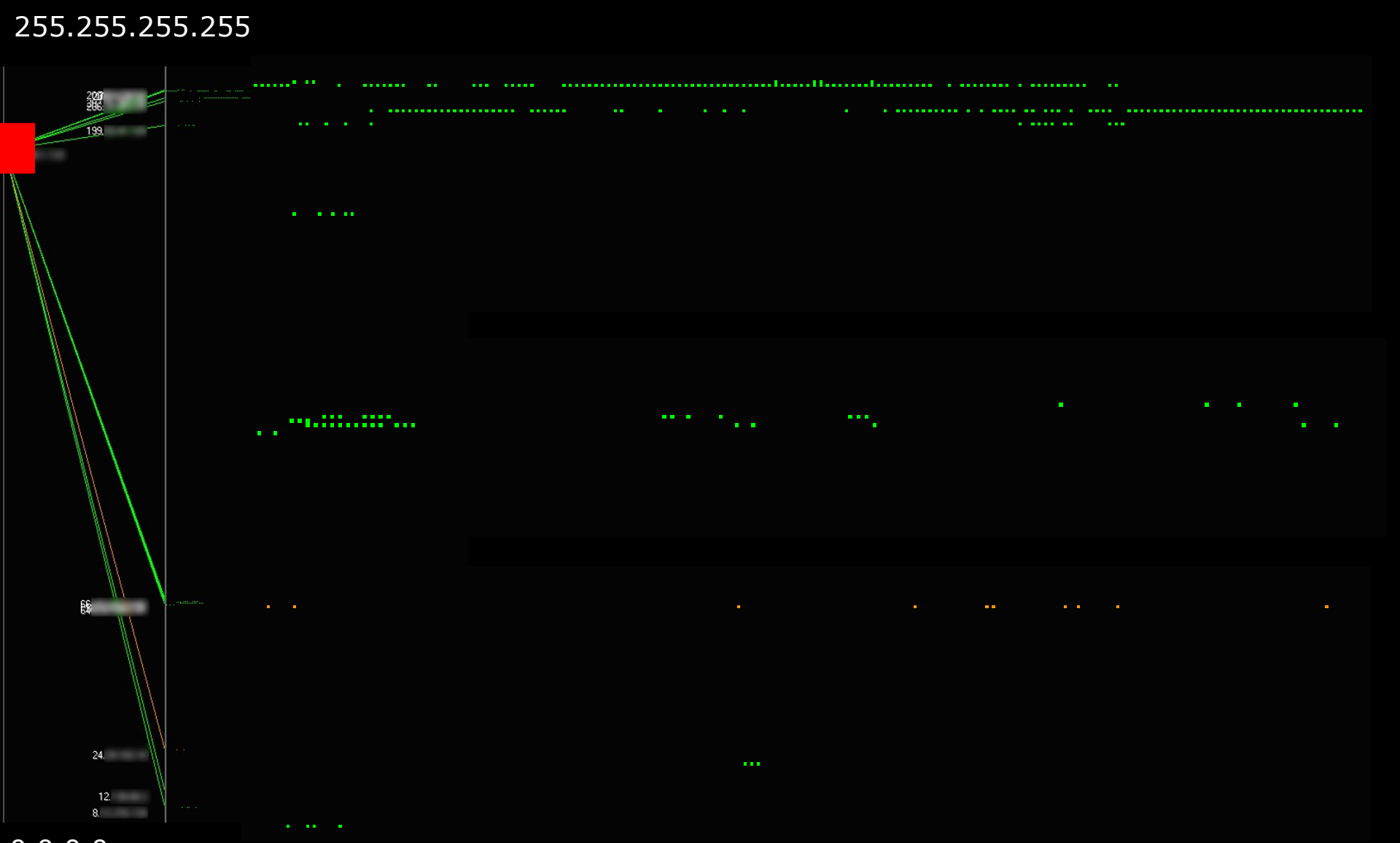
Even the most innocent appearing services should be considered as collecting your data

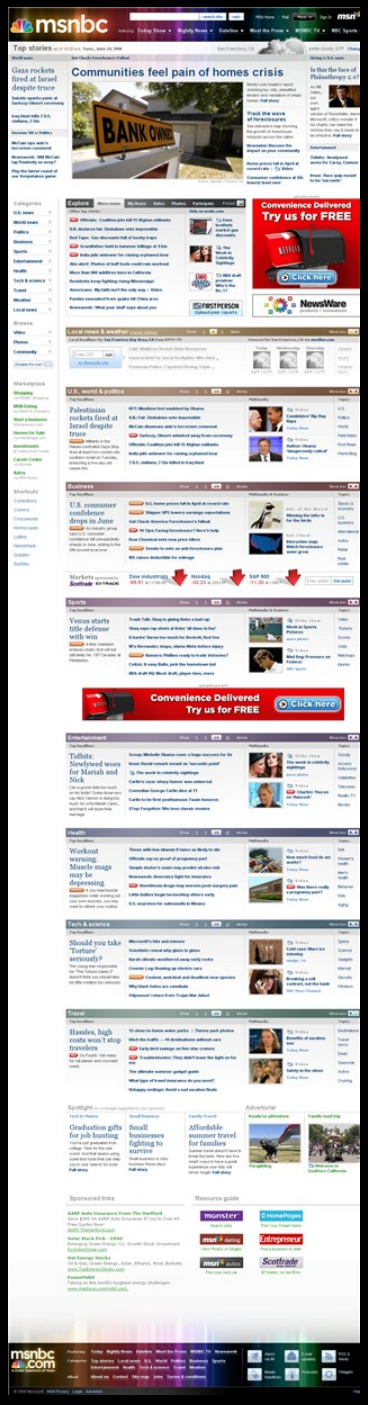
Cross-site Tracking

- Web Analytics
- Embedded content
  - Webbugs
  - YouTube Videos

- Advertising
  - Doubleclick
  - AdSense
- Referer data
- Javascript Libraries
- Clickthrough Tracking

A Visit to MSNBC



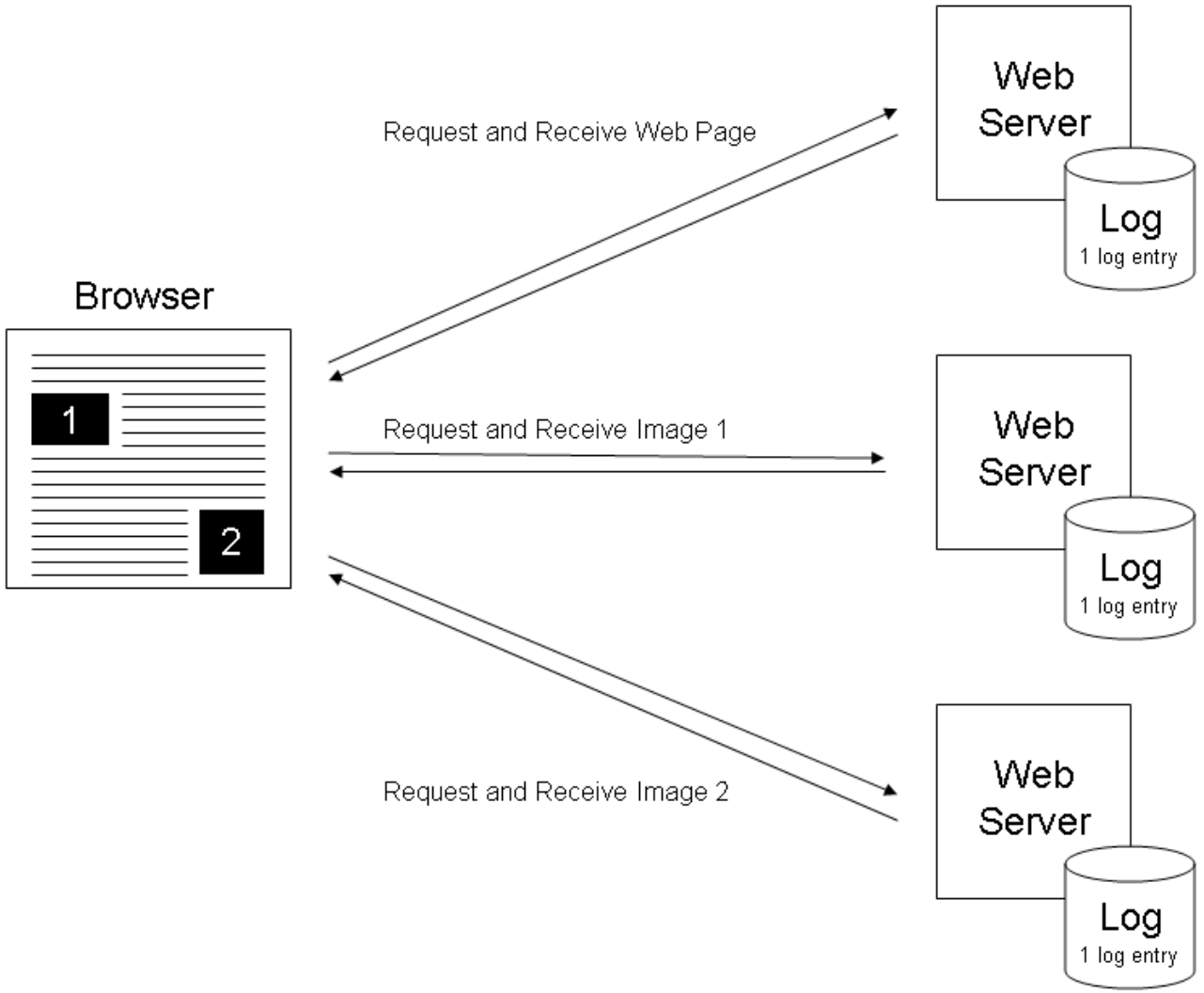


- a365.ms.akamai.net
- a509.cd.akamai.net
- ad.3ad.doubleclick.net
- amch.questionmarket.com
- c.live.com.nsatc.net
- c.msn.com.nsatc.net
- rad.msn.com.nsatc.net
- context3.kanoodle.com
- global.msads.net.c.footprint.net
- hm.sc.msn.com.c.footprint.net
- msnbcom.112.2o7.net
- prpx.service.mirror-image.net
- wrpx.service.mirror-image.net
- switch.atdmt.com
- view.atdmt.com
- www-google-analytics.l.google.com

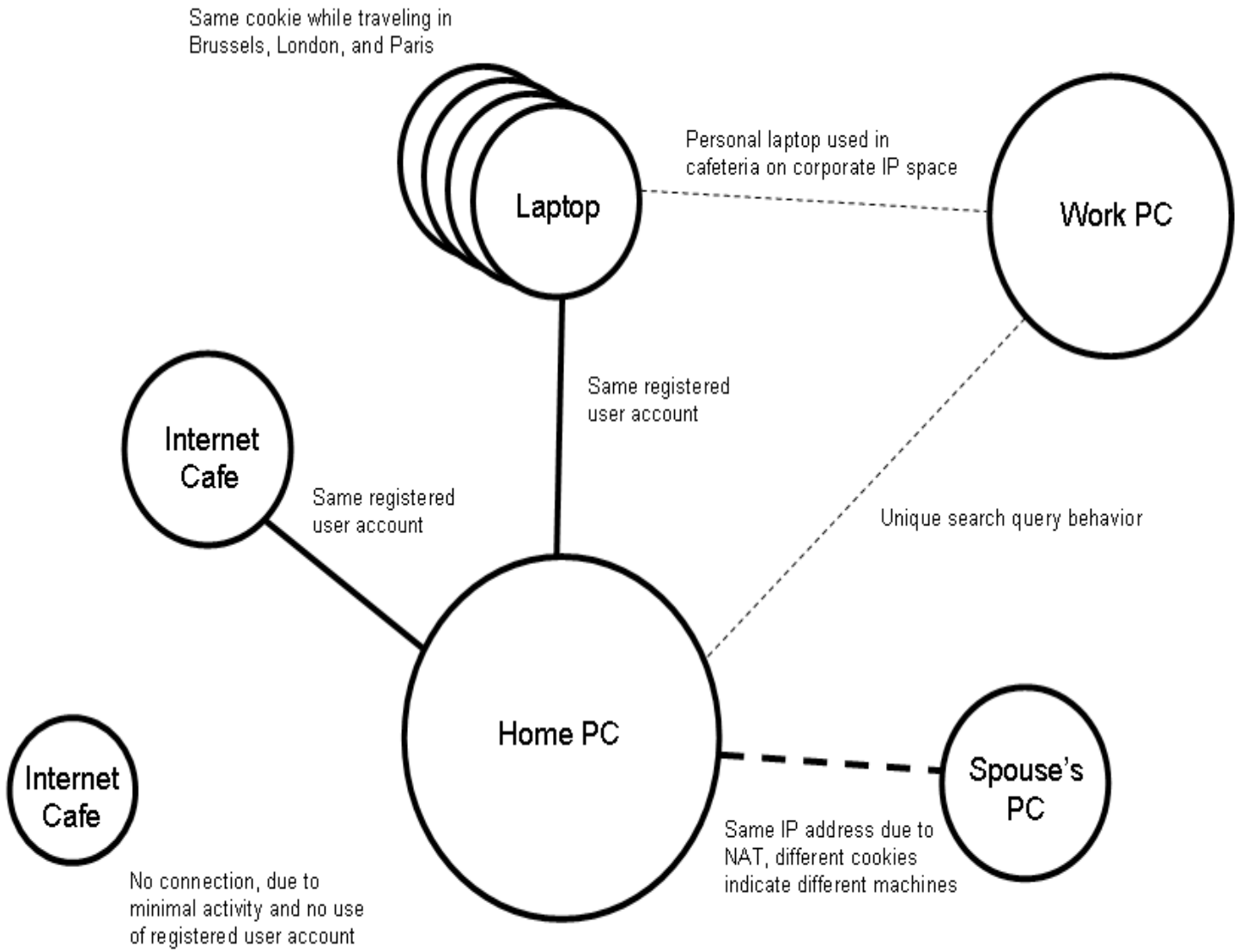
- 16 third-party sites
- 10 separate companies

http://www.msnbc.msn.com/

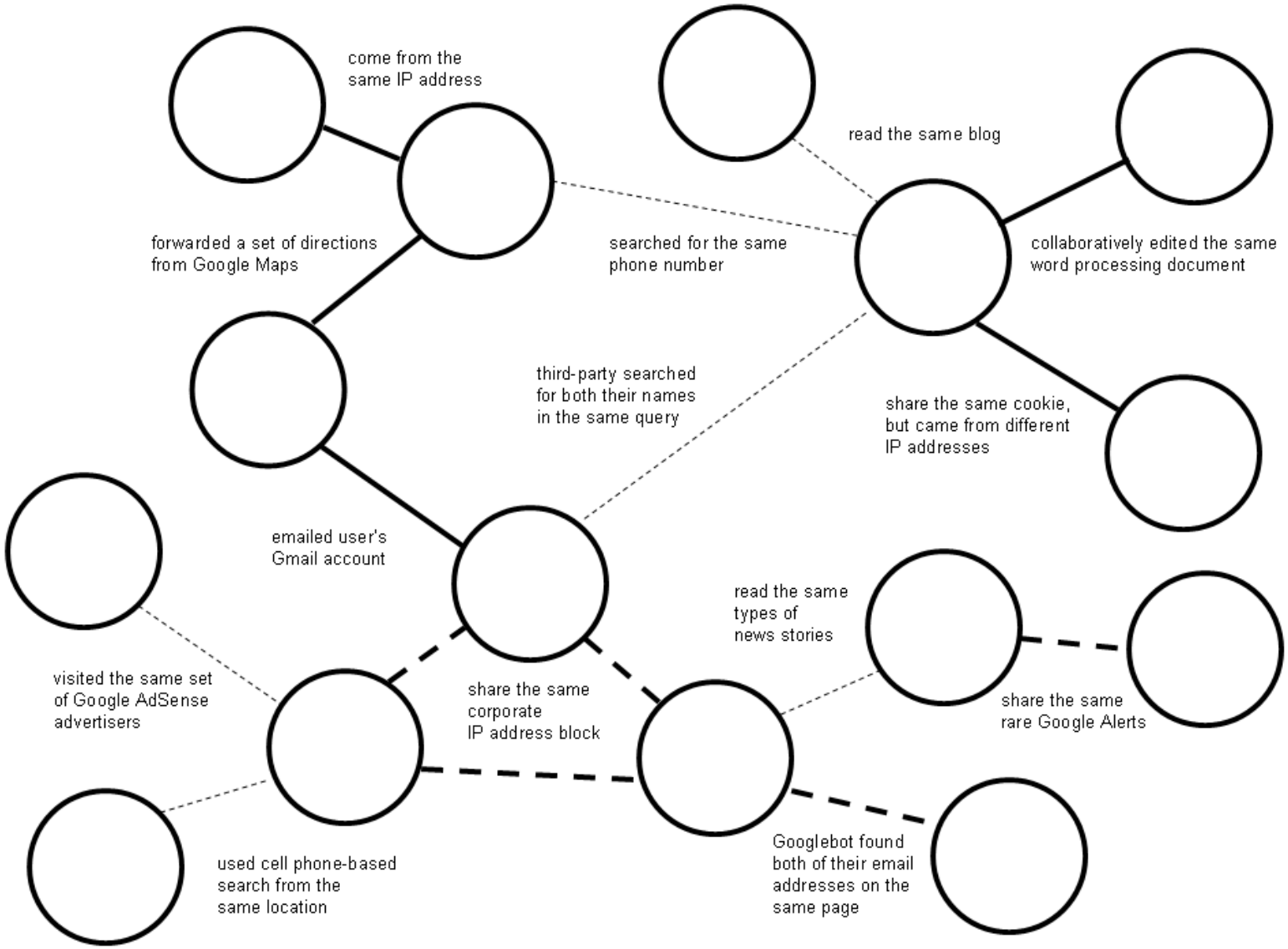
Third Party Content and Web Bugs



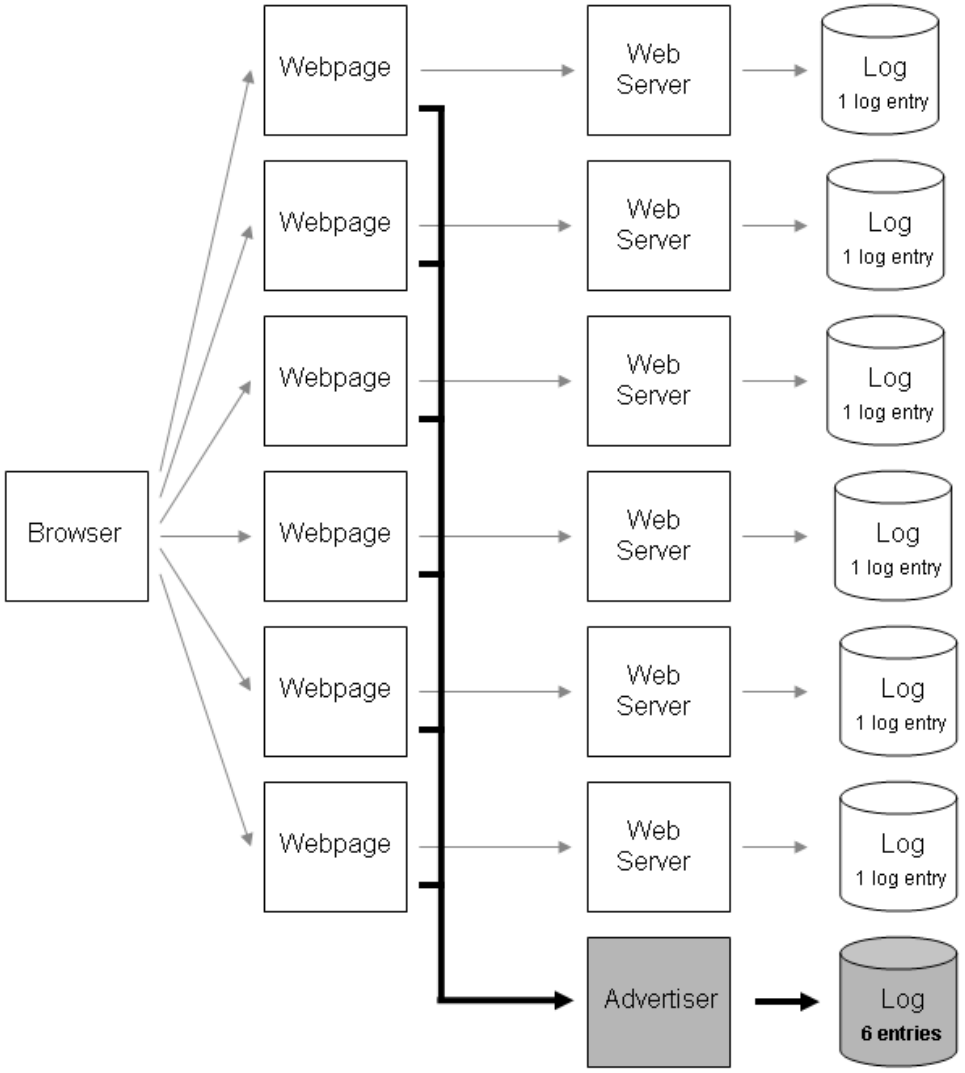
Linking a User Across Many Platforms



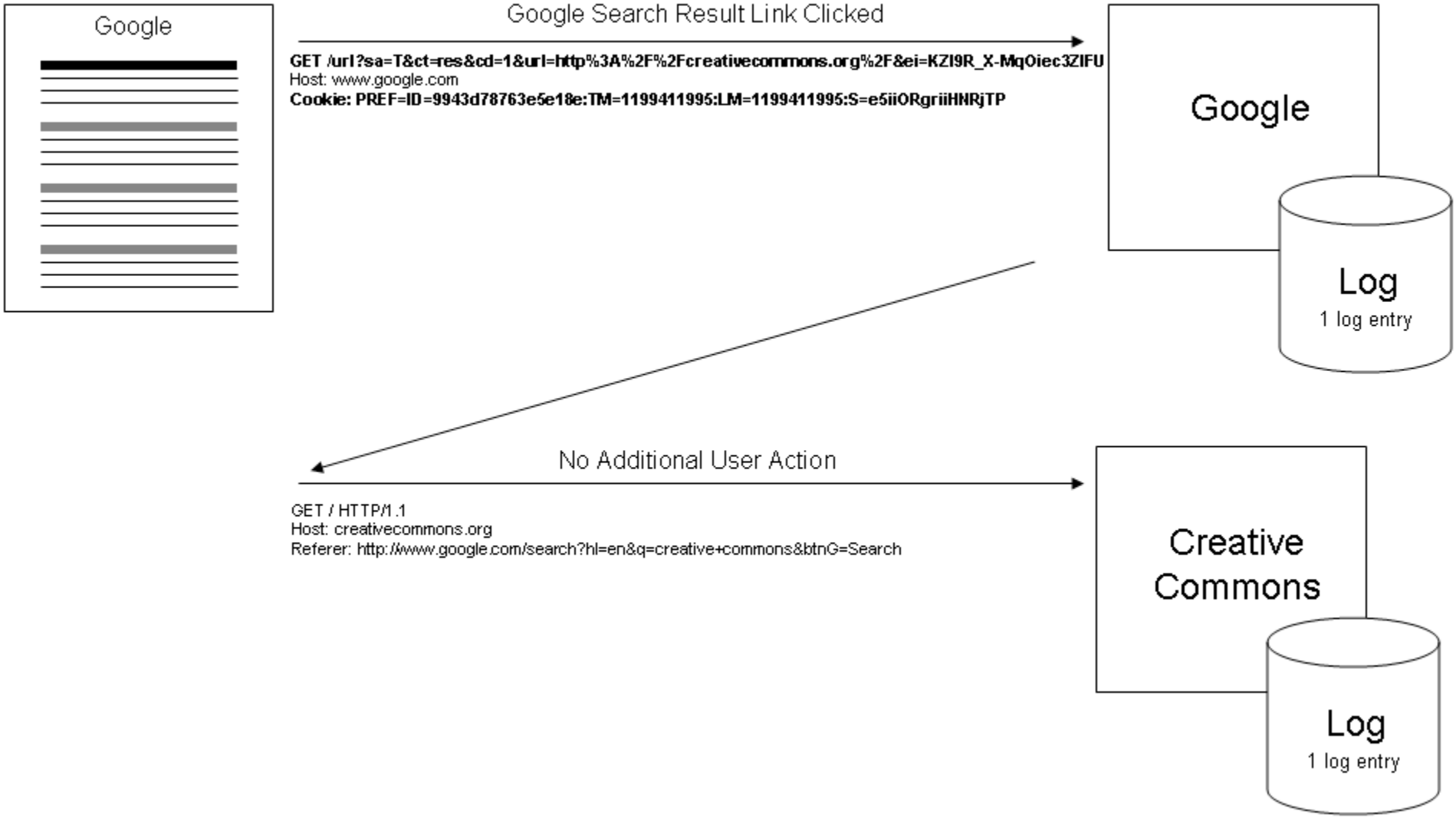
Linking Users, Groups, and Organizations



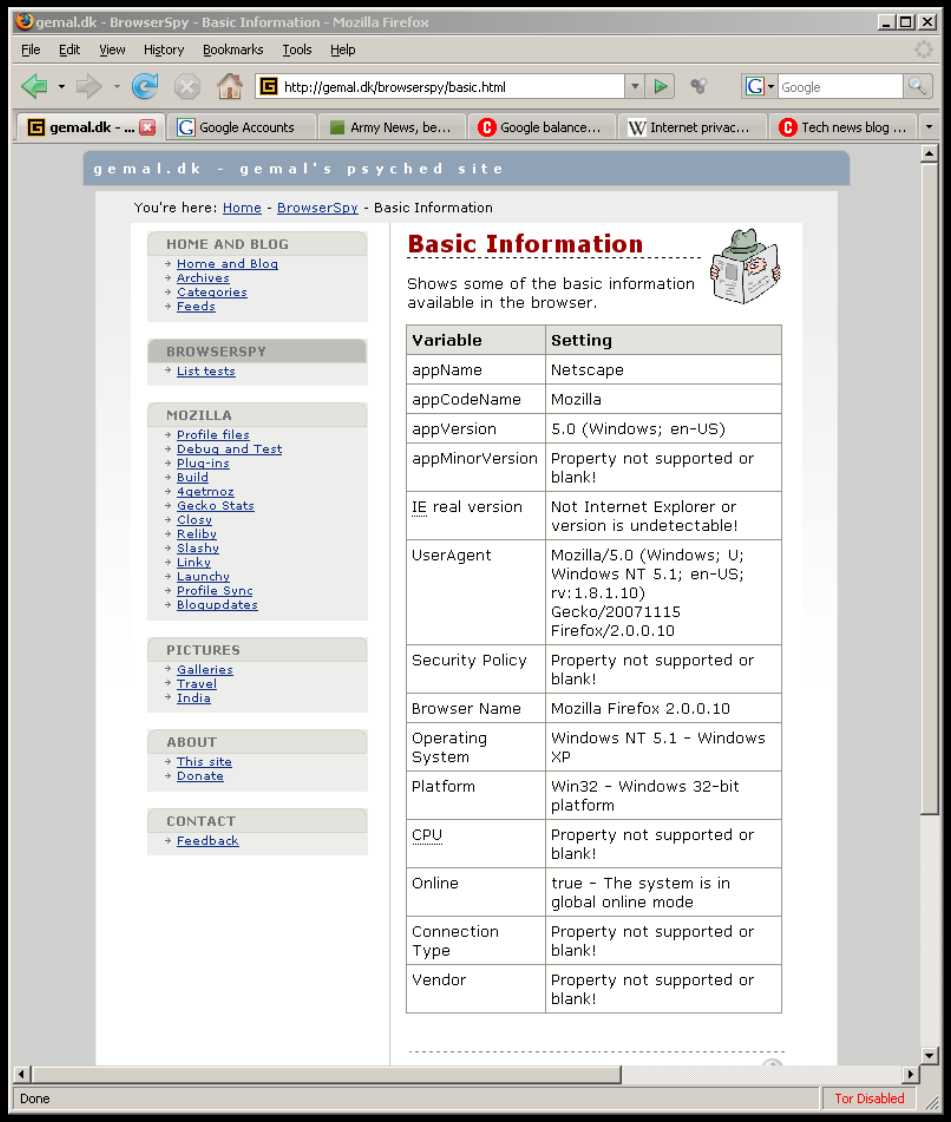
Advertising – The DoubleClick Model



Click Through Tracking



Browser Supplied Information



Google-Analytics


```
var _gat=new Object({c:"length",lb:"4.2",m:"cookie",b:undefined,cb:function(d,a)
{this.zb=d;this.Nb=a},r:"__utma=",W:"__utmb=",ma:"__utmc=",Ta:"__utmk=",na:"__utmv=",oa:"__utmx=",Sa:"GASO=",X:"__ut
mz=",lc:"http://www.google-analytics.com/__utm.gif",mc:"https://ssl.google-analytics.com/__utm.gif",Wa:"utmcid=",Ya:"utmcsr=",
$a:"utmgclid=",Ua:"utmccn=",Xa:"utmcmd=",Za:"utmctr=",Va:"utmcct=",Hb:false,_gasoDomain:undefined,_gasoCPath:undefined,e
:window,a:document,k:navigator,t:function(d){var a=1,c=0,g, o;if(!_gat.q(d)){a=0;for(g=d[_gat.c]-1;g>=0;g--)
{o=d.charCodeAt(g);a=(a<<6&268435455)+o+(o<<14);c=a&266338304;a=c!=0?a^c>>21:a}}return a},C:function(d,a,c){var
g=_gat,o="-",k,m,q=g.q;if(!q(d)&&!q(a)&&!q(c)){k=g.w(d,a);if(k>-1){m=d.indexOf(c,k);if(m<0)m=d[g.c];o=g.F(d,k+g.w(a,"=")
+1,m)}}return o},Ea:function(d){var a=false,c=0,g,o;if(!_gat.q(d)){a=true;for(g=0;g<d[_gat.c];g++){o=d.charAt(g);c+="."==o?
1:0;a=a&&c<=1&&(0==g&&"-"==o||_gat.P(".0123456789",o))}}return a},d:function(d,a){var c=encodeURIComponent; return c
instanceof Function?(a?encodeURI(d):c(d)):escape(d)},J:function(d,a){var c=decodeURIComponent,g;d=d.split("+").join(" ");if(c
instanceof Function)try{g=a?decodeURI(d):c(d)}catch(o){g=unescape(d)}else g=unescape(d);return g},Db:function(d){return
d&&d.hash?_gat.F(d.href,_gat.w(d.href,"#")):""},q:function(d){return _gat.b==d||"-"==d||""==d},Lb:function(d){return
d[_gat.c]>0&&_gat.P(" \n\r\t",d)},P:function(d,a){return _gat.w(d,a)>-1},h:function(d,a){d[d[_gat.c]]=a},T:function(d){return
d.toLowerCase()}, z:function(d,a){return d.split(a)},w:function(d,a){return d.indexOf(a)},F:function(d,a,c){c=_gat.b==c?
d[_gat.c]:c;return d.substring(a,c)},uc:function(){var
d=_gat.b,a=window;if(a&&a.gaGlobal&&a.gaGlobal.hid)d=a.gaGlobal.hid;else{d=Math.round(Math.random()*2147483647);a.gaGlo
bal=a.gaGlobal?a.gaGlobal:{};a.gaGlobal.hid=d}return d},wa:function(){return
Math.round(Math.random()*2147483647)},Gc:function(){return(_gat.wa()^_gat.vc())*2147483647},vc:function(){var
d=_gat.k,a=_gat.a,c=_gat.e,g=a[_gat.m]? a[_gat.m]:"",o=c.history[_gat.c],k,m,q=[d.appName,d.version,d.language?
d.language:d.browserLanguage,d.platform,d.userAgent,d.javaEnabled()?
1:0].join("");if(c.screen)q+=c.screen.width+"x"+c.screen.height+c.screen.colorDepth;else if(c.java)
{m=java.awt.Toolkit.getDefaultToolkit().getScreenSize();q+=m.screen.width+"x"+m.screen.height}q+=g;q+=a.referrer?
a.referrer:"";k=q[_gat.c];while(o>0)q+=o--^k++;return _gat.t(q)}});_gat.hc=function(){var d=this,a=_gat.cb;function c(g,o)
{return new
a(g,o)}d.db="utm_campaign";d.eb="utm_content";d.fb="utm_id";d.gb="utm_medium";d.hb="utm_nooverride";d.ib="utm_source";
d.jb="utm_term";d.kb="gclid";d.pa=0;d.I=0;d.wb="15768000";d.Tb="1800";d.ea=[];d.ga=[];d.Ic="cse";d.Gb="q";d.ab="google";
d.fa=[c(d.ab,d.Gb),c("yahoo","p"),c("msn","q"),c("aol","query"),c("aol","encquery"),c("lycos","query"),c("ask","q"),c("altavista","q"),c
("netscape","query"),c("cnn","query"),c("looksmart","qt"),c("about",
"terms"),c("mamma","query"),c("alltheweb","q"),c("gigablast","q"),c("voila","rdata"),c("virgilio","qs"),c("live","q"),c("baidu","wd"),c("
alice","qs"),c("yandex","text"),c("najdi","q"),c("aol","q"),c("club-
internet","query"),c("mama","query"),c("seznam","q"),c("search","q"),c("wp","szukaj"),c("onet","qt"),c("netsprint","q"),c("google.inte
ria","q"),c("szukacz","q"),c("yam","k"),c("pchome","q"),c("kvasir","searchExpr"),c("sesam","q"),c("ozu","q"),c("terra","query"),c("nost
rum","query"),c("mynet","q"),
c("ekolay","q"),c("search.ilse","search_for")];d.B=undefined;d.Kb=false;d.p="/";d.ha=100;d.Da="/__utm.gif";d.ta=1;d.ua=1;d.G="
|";d.sa=1;d.qa=1;d.pb=1;d.g="auto";d.D=1;d.Ga=1000;d.Yc=10;d.nc=10;d.Zc=0.2};_gat.Y=function(d,a){var
c,g,o,k,m,q,r,f=this,p=_gat,w=p.q,x=p.c,i,z=a;f.a=d;function A(h){var b=h instanceof Array?h.join("."):"";return
w(b)?"-":b}function B(h,b){var e=[],j;if(!w(h)){e=p.z(h,".");if(b)for(j=0;j<e[x];j++)if(!p.Ea(e[j]))e[j]="-"}return e}function n()
{return u(63072000000)}function u(h){var b=new Date,e=new Date(b.getTime()+h);return"expires="+e.toGMTString()+";
"}function l(h,b){f.a[p.m]=h+"; path="+z.p+"; "+b+f.Cc()}function s(h,b,e){var j=f.V,t,v;for(t=0;t<j[x];t++){v=j[t][0]; v+=w(b)?
```


http://www.google-analytics.com/ga.js

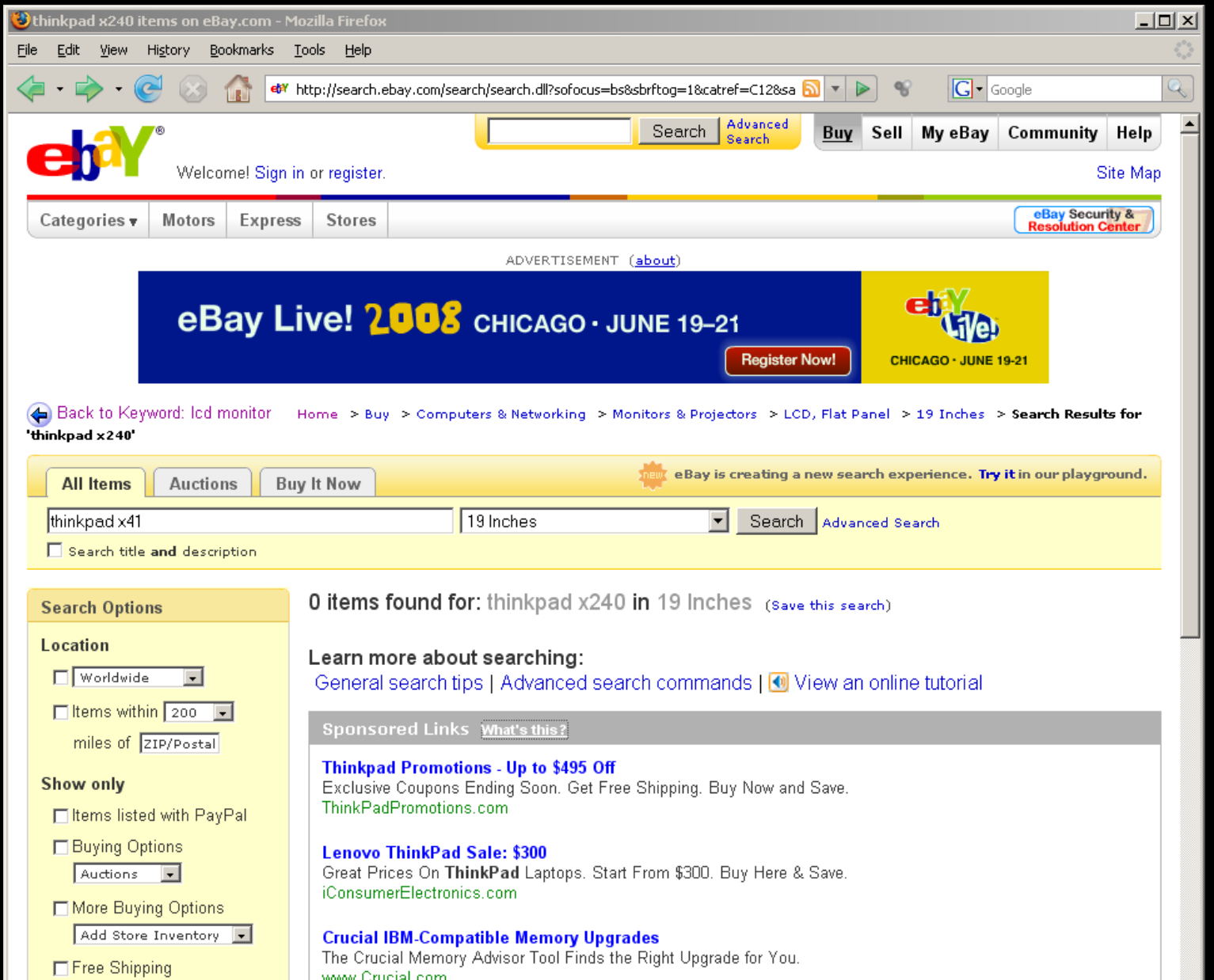
AJAX Libraries API

- jQuery
- prototype
- script.aculo.us
- MooTools
- dojo
- cached

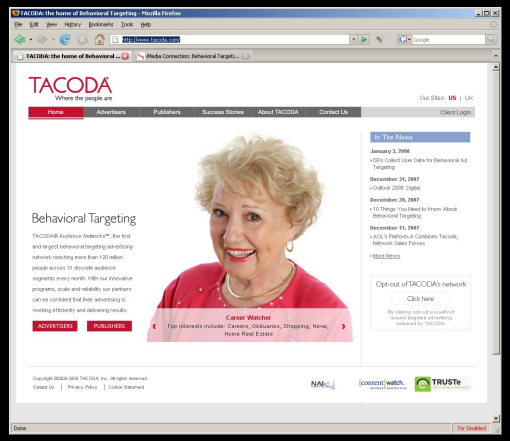
```
<script src="http://www.google.com/jsapi"></
script>
<script>
  google.load("jquery", "1"); // Load jQuery

  google.setOnLoadCallback(function() {

$.getJSON("http://ajax.googleapis.com/ajax/s
ervices/search/web?
q=google&;v=1.0&;callback=?",

  function (data) {
        if (data.responseDate.results &&

data.responseDate.results.length>0) {

renderResults(data.responseDate.results);
        }
      });
    });
```

http://code.google.com/apis/ajaxlibs/

Ebay pulling ads from a Yahoo server



Profiling



"Career Watcher"

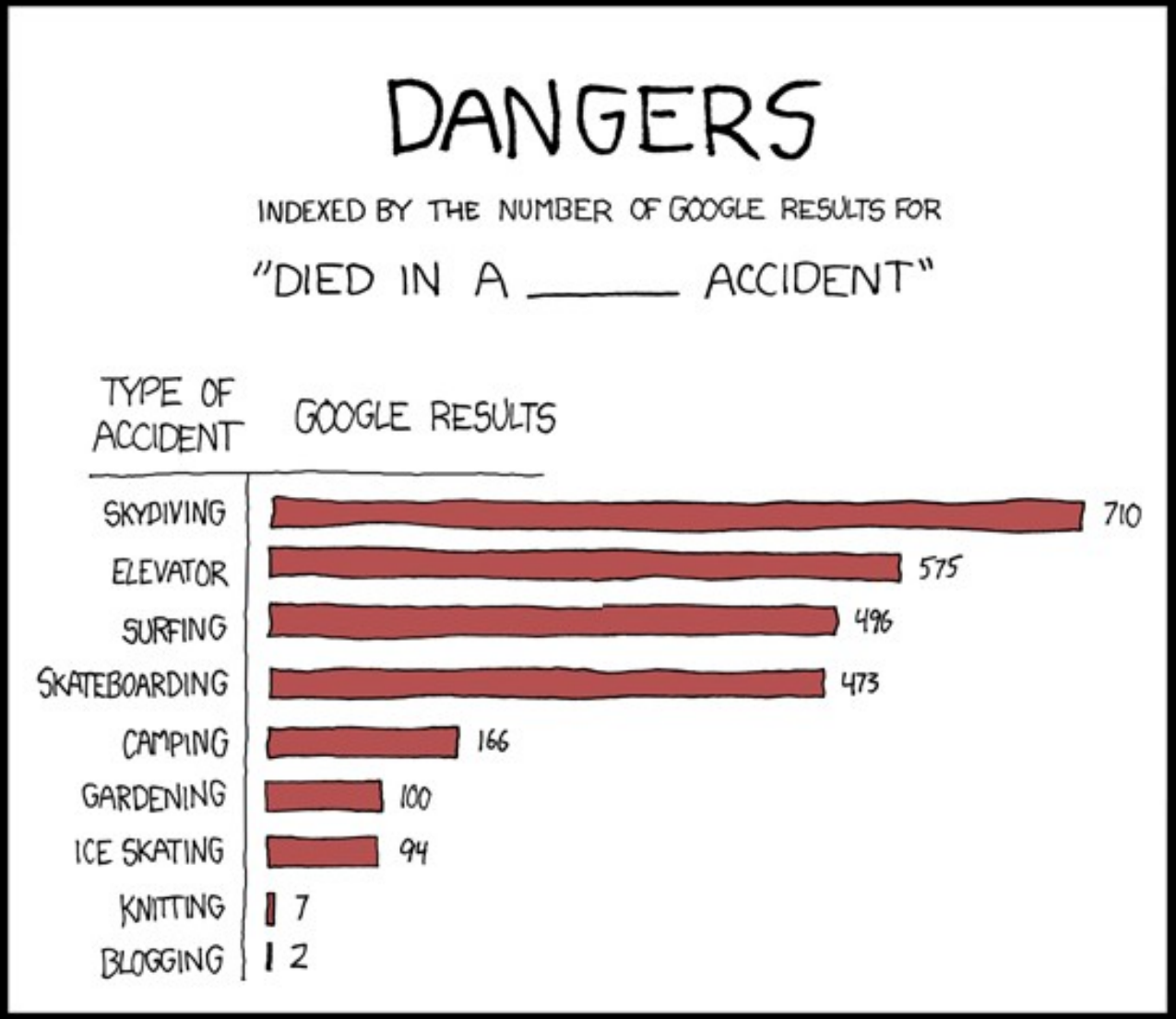


"Active Gamer"

- Google hackers
- Security researchers
- Political activists
- Company XXX employee
- Corporate leaders
- Law enforcement officer
- Government official

Tacoda, The Home of Behavioral Targeting, http://www.tacoda.com/

Data Mining



http://xkcd.com/369/

Countermeasures

- Patching Users
  - Raised Awareness
  - Know What You are Disclosing
  - Usable Security
  - ...
- Technical Countermeasures
  - Cookie Managers
  - Content Filtering
  - Self-monitoring
  - Search Term Chaffing
  - Encryption
  - Anonymizing Proxies
  - Tor
  - NAT Firewalls
  - ...
- Policy Countermeasure
  - Petition Law and Policy Makers
  - Support EFF and other Privacy Organizations
  - ...

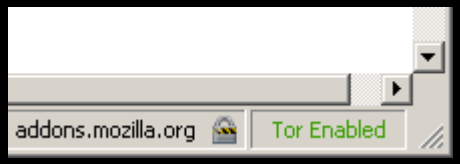
TrackMeNot


TrackMeNot
Options
Help/FAQ
Enabled
Show Status
Show Queries
Current Queries
Search Engines
Ctrl-Click for multiple selections:
AOL Search
MSN Search
Yahoo! Search
Google Search
Select All
Clear All
Query Frequency
Enable Query Bursts
Avg. Query Rate:
1 per min
Logging Options
Disabled
Persistent
ShowLog
ClearLog
Cookie Handling
Clean Cookies (Anonymizes Cookies ONLY on Web Searches)
OK
Cancel

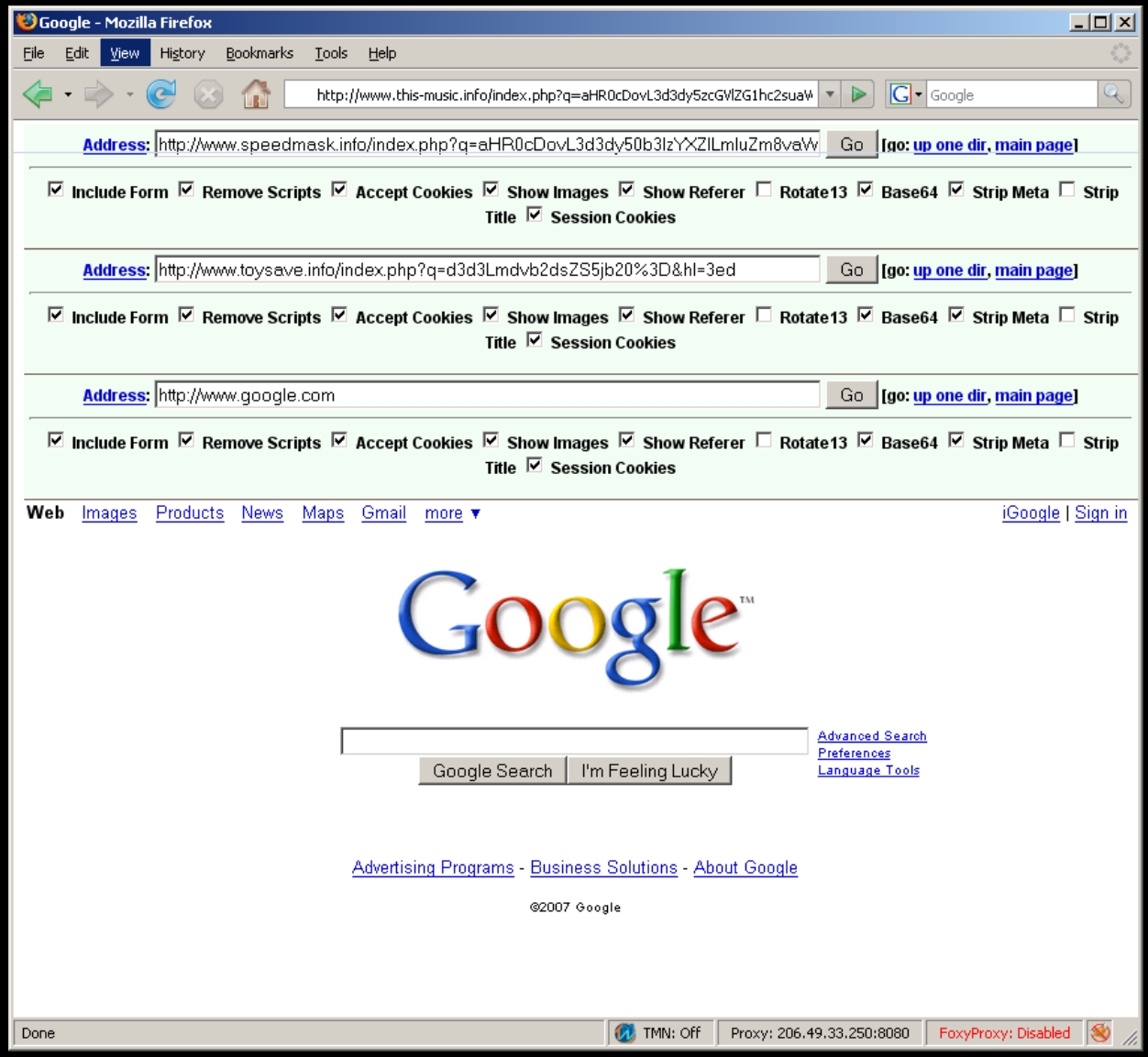
TorCheck


TorCheck at Xenobite.eu - HTTP-Mode - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://torcheck.xenobite.eu/index.php?PHPSESSID=643721fd9aa3af7b5ff3:
Google
TorCheck at Xenobite.eu
HTTP-Mode
Check Again
HTTPS-Mode
CODE VERSION: 2007-11-08 00:18:24 GMT/UTC
CURRENT TIME: 2007-11-23 01:38:02 GMT/
YOUR IDENTITY
Your current IP
Your current FQDN
(none)
Your current Tor-EXIT
"whistlersmother" (US) [LOOKUP]
CONCLUSION
Your IP is identified to be a Tor-EXIT.
So you are using Tor successfully to reach the web!
CHECK RESULT
TorDNSEL
(is a Tor-EXIT IP)
Hidden Services
(color shows reachability of [dige6xxwpt2knqbv.onion])
JavaScript-Support
ENABLED!
ActiveX-Support
(disabled)
Java-Support
(possibly disabled)
Cookies-Support
ENABLED!
Your HTTP-Referer
http://torcheck.xenobite.eu/?
PHPSESSID=643721fd9aa3af7b5ff31bdac208369e
Your HTTP-VIA
(none)
Your HTTP-User-Agent
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.9) Gecko/20071025
Firefox/2.0.0.9
Your HTTP-ACCEPT
LANGUAGE: en-us,en;q=0.5
ENCODING: gzip,deflate
CHARSET: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Your HTTP-CONNECTION
close
SAFETY CHECK
NEXT
READY!
THIS INFORMATION IS PROVIDED WITHOUT ANY WARRANTY
CODE: [INDEX.PHP] [JAVA APPLET] / COUNTER: 441316 [STATS] / EMAIL: BLUESTAR88 AT XENOBITE DOT
WARNING
Your browsers JavaScript [?] support is ENABLED! This could compromise your anonymity, so you should consider to disable JavaScript support!
Check this nice Firefox addon to handle this easily!
WARNING
Your browser is ACCEPTING cookies [?] ! This could compromise your anonymity (re-visit recognition), so you should consider to disable cookies support!
Check this nice Firefox addon to handle this easily!
Find:
Next
Previous
Highlight all
Match case
Done
Tor Enabled

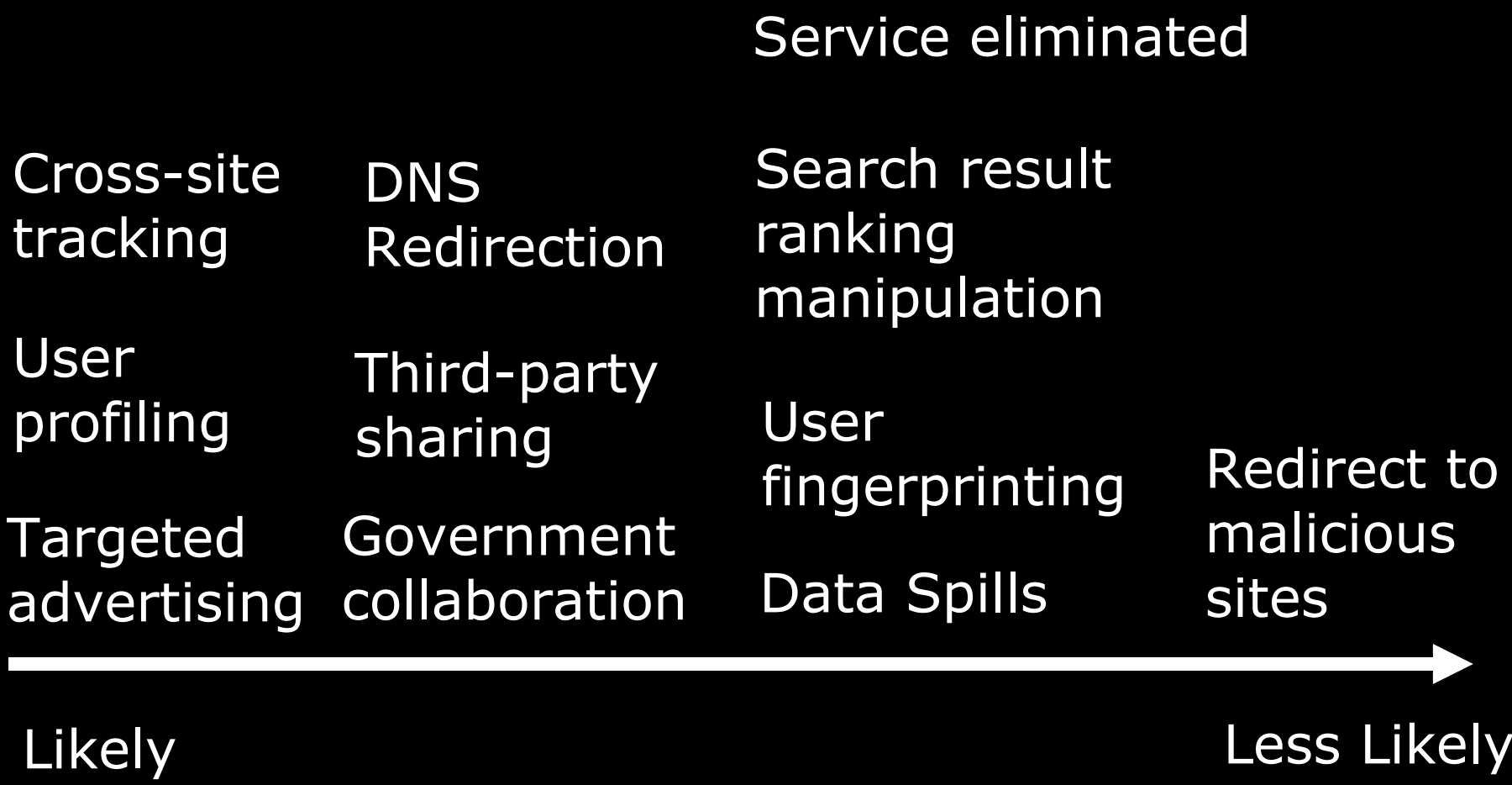
Tor Button



Chained Proxies

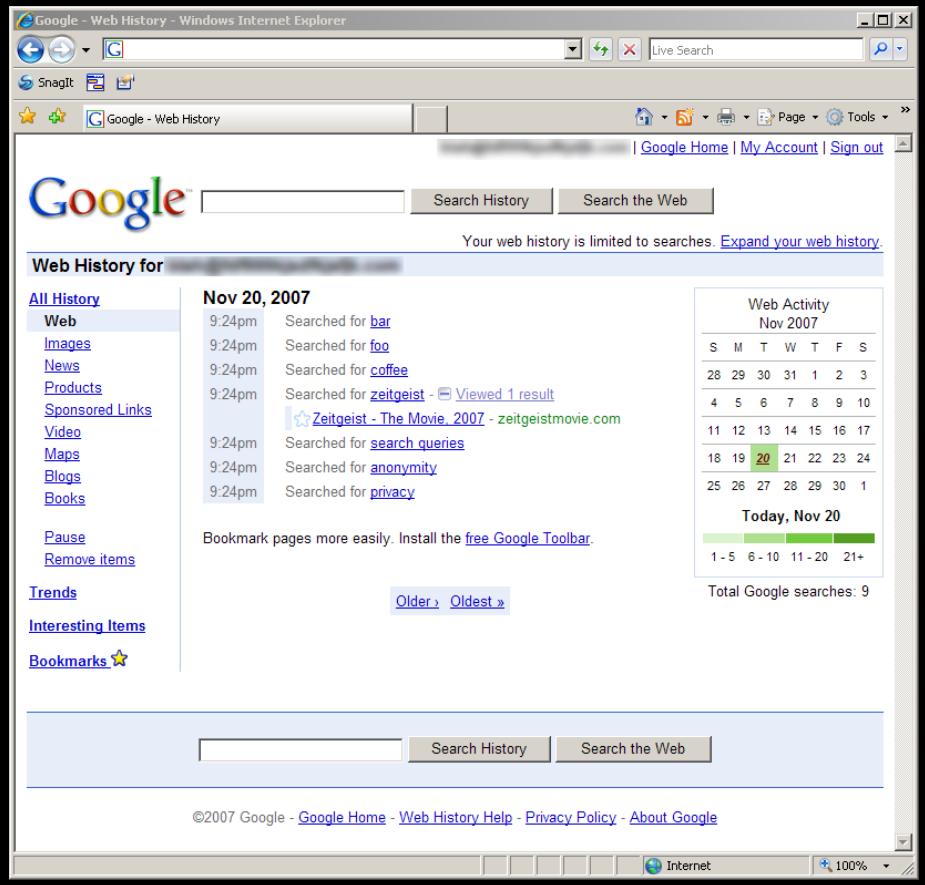


Threat Spectrum



Future Countermeasures

- Plug-in that monitors information disclosures
- Plug-in that displays third-party contacts
  - at least serve as a history function for the status bar



Conclusions

- what online companies posses vs. what they share are two entirely different things
  - blurring streetview
  - blurring google maps
  - internal search logs vs. public interface

Acknowledgements

- 3efd09cddc148ee790d17e35ae323852
- Kulsoom Abdullah
- Ed Sobiesk
- New Security Paradigms Workshop
- Symposium on Usable Privacy and Security


accessed address com countermeasures data disclosed
disclosure fingerprinting google http
information
individual level
network organizations personal privacy protection
providers search service usability
user web www

Questions?