

How Private Is Your Privacy & What Can You Do About It?

Indrajit Ray

Colorado State University

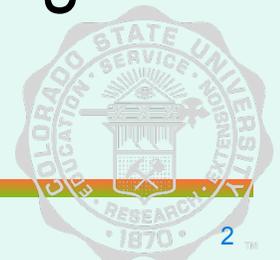
indrajit@cs.colostate.edu

<http://www.cs.colostate.edu/~indrajit>



Privacy of Personal Information

- Personal information is more than just one's name, address or social security number
 - Medical history, Work history, Shopping habits, Driving record, Political views, Sexual orientation, Credit score
- Privacy is an interest that the user has in maintaining such information securely under control without that control being compromised by others for their personal gain
- Privacy violations occur everybody without us being aware of it



Outline of Presentation

- Case study of real life incidents
 - Identify fraud
 - Demographic re-identification
- How privacy violations occur
- Privacy enhancing technologies
- Research at Colorado State University
- Conclusions



Privacy Violation Case Study #1

Identity Fraud from Identify Theft



Identity Fraud – The Michelle Brown Story

- Started with mishandling of rental application of Michelle Brown at property management office and subsequent theft
 - Perpetrator obtains duplicate driver's license with assumed identity
 - Sets up cellular service, residential telephone service, utility services
 - Obtains department store credit card and other loans
 - \$32,000 truck
 - Rents property under assumed identity
 - Gets \$5,000 worth of liposuction on her body



Identify Fraud – The Michelle Brown Story (2)

- Perpetrator runs drug trafficking business under assumed identity
 - Presents forged identification papers when arrested for carrying 1,300 Kg of marijuana
 - Results in erroneous criminal record under Michelle Brown's name
- Perpetrator becomes fugitive
 - Warrant for Michelle Brown's arrest
- Perpetrator arrested
 - Prison record established in Michelle Brown's name

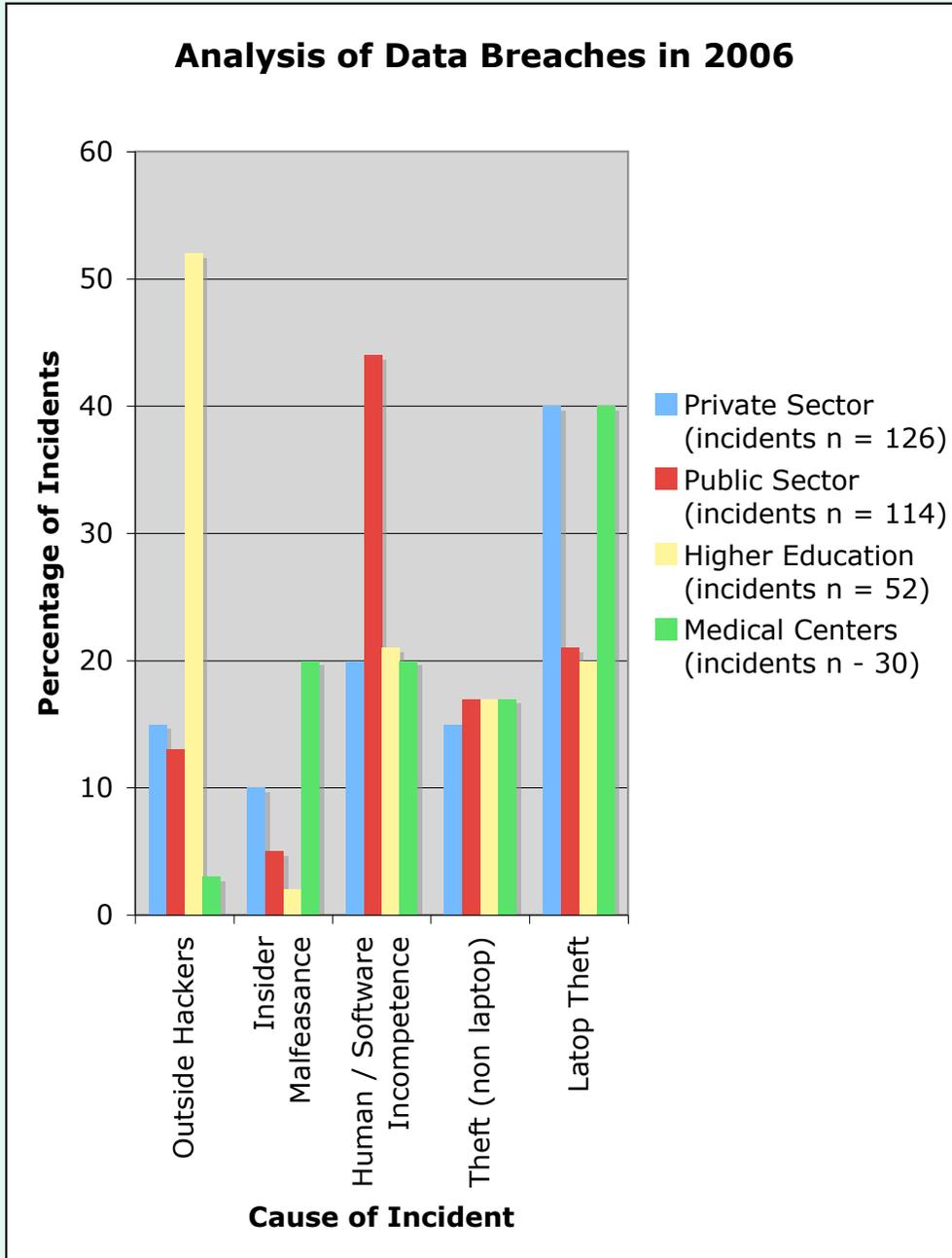


Identify Fraud – The Michelle Brown Story (3)

- Real Michelle Brown eventually cleared after months of anguish and enormous financial drain
- However, months later was wrongly stopped by an international airport's customs agents and held for several hours



Analysis of Data Breaches in 2006



Source - Beth Rosenberg (Sandstorm.net). Available from Privacy Rights Clearinghouse www.privacyrights.org



Analysis of Privacy Breaches in 2006

Total Number of Major Data Breach Incidents reported	327
Approximate Minimum Total # of Personal Records Potentially Compromised in 2006	100,453,730
# Data-Breach Identity Thieves Sentenced in 2006	5
# Individual Victims of Sentenced Identity Thieves	238

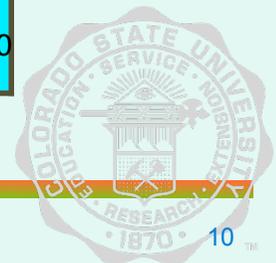


Average Cost of Data Breach

Total # of affected records = 250,000

Internal Investigation	
Cybercrime Consulting	533,508.0
Attorney Fees	540,930.5
	1074,439.0
Notification / Crisis Management	
Customer notification (Certified mail)	983,510.5
Call center support	695,880.0
Crisis management consulting	389,693.0
Media management	77,010.5
	2,146,095.0
Regulatory / Compliance	
Credit monitoring for affected customers	4,472,189.0
Regulatory investigation defense	1,654,338.5
State / Federal fines or fees	3,509,091.0
	9,635,619.0
	12,856,153.0

Source: Tech//404 Data Loss Calculator <http://www.tech-404.com/calculator.html>



Privacy Violation Case Study #2

Demographic Re-identification & Its Consequences



Latanya Sweeney's Work (1)

- In Massachusetts, the Group Insurance Commission (GIC) is responsible for purchasing health insurance for state employees
- GIC has to publish the data for research purposes

GIC (zip, dob, gender, diagnosis, procedure, ...)

Latanya Sweeney's Work (2)

- Sweeney paid \$20 and bought the voter registration list for Cambridge, MA

GIC (zip, dob, gender, diagnosis, procedure, ...)

VOTER (name, party, ..., zip, dob, gender)



Latanya Sweeney's Work (3)

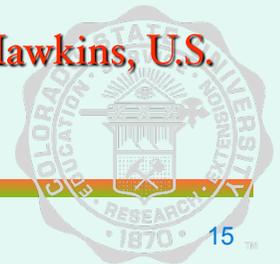
- William Weld (former governor) lives in Cambridge, hence is in VOTER
- 6 people in VOTER share his date of birth
- Only 3 of them were men (same gender)
- Weld was the only one in that zip
- Sweeney learned Weld's medical records



Medical Records Misuse

- Burlington Northern allegedly obtained genetic tests results on employees who had filed worker's compensation claims for carpal tunnel syndrome, without their knowledge.
 - The company's intention was presumably to be able to reject some claims because of genetic predisposition to the condition.

Source - The Dark Side of Genetic Testing: Railroad Workers Allege Secret Testing, by Dana Hawkins, U.S. News and World Report, February 11 (19), 2001



So, How Do They Get My Data?

Beyond Phishing and Other Social
Engineering Means



Lack of Knowledge About Privacy Threats

- Users misplace valuable data items
- Users post many personal details on social network sites like Facebook, MySpace, Bebo etc
 - Can be combined with information from other sources to create profile



Carnegie Mellon University Heinz School Study of Facebook

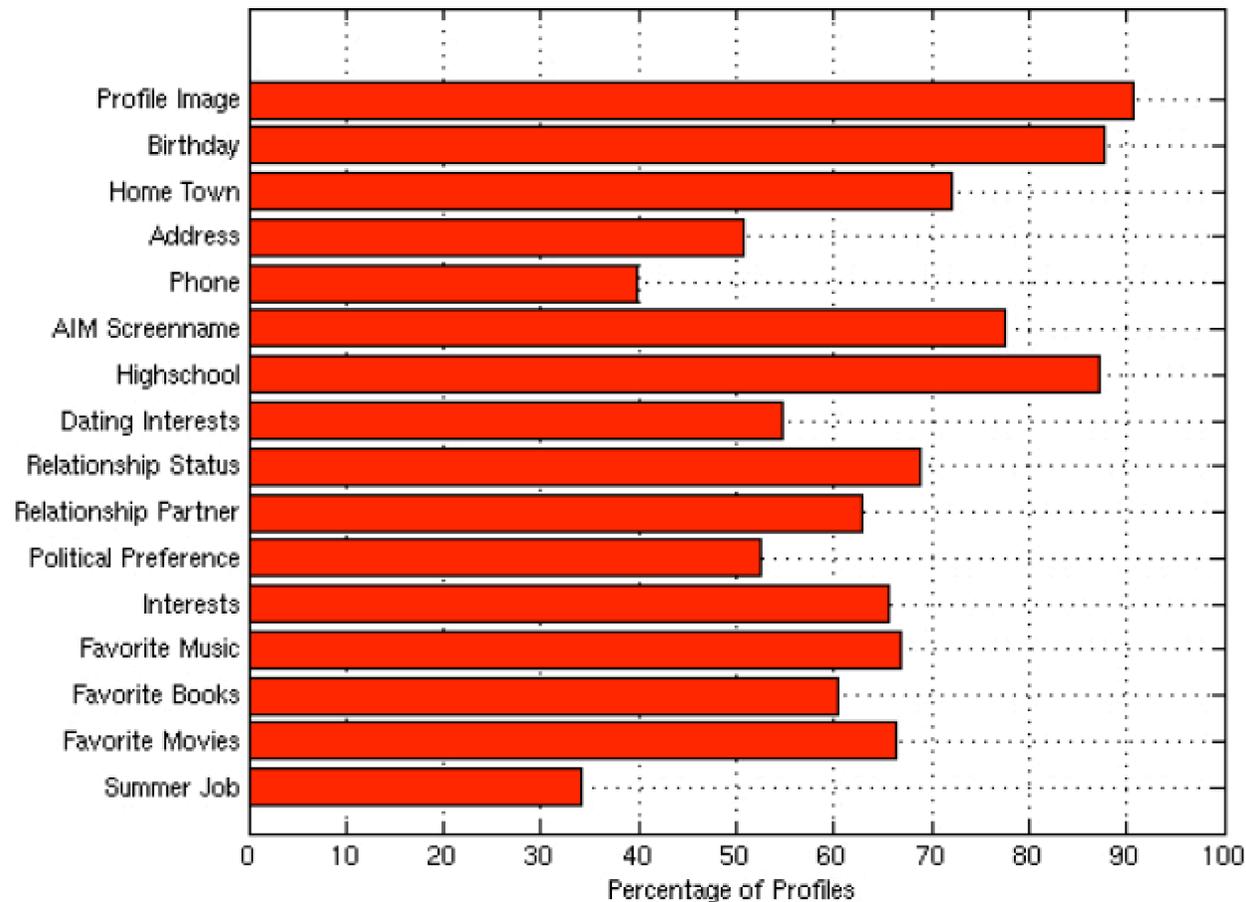


Figure 2: Percentages of CMU profiles revealing various types of personal information.

Workplace Monitoring

- 75% of employers monitor their employees website visit
 - Most computer monitoring equipment allows monitoring remotely without user's knowledge
- Almost all employers review employee email
 - Deleted emails are not really deleted
- 33% track keystrokes and time spent at the keyboard
- Currently there are very few laws regulating employee monitoring



Browser Chatter

- Browsers chatter about
 - IP address, domain name, organization,
 - Referring page
 - Platform: O/S, browser
 - What information is requested
 - URLs and search terms
 - Cookies
- To anyone who might be listening
 - End servers
 - System administrators
 - Internet Service Providers
 - Other third parties
 - Advertising networks
 - Anyone who might subpoena log files later



Monitoring on the Internet – What Your Browsing Reveals

Privacy.Net Browsing Analysis Results



<p>How to hide my IP address About 99% of hacking attacks uses the IP address. Hide your IP now. www.HideYourIPAddress.net</p>	<p>Fibre Channel Resources Extend the Value of Fibre Channel w/FCoE- Free Video, Papers, Webcast www.Brocade.com</p>	<p>Internet Access Service High-speed ADSL + free calls to UK Only ADSL in France just for expats www.teleconnect.fr</p>
--	--	---

Ads by Google

The [Privacy.net](#) Analyzer

This site analyzes the privacy of your Internet connection and shows some of the information web sites can know about you when you visit. The information can be used to display web content based on things such as country of origin and web browser.

[Click here to read a description of the tests \(opens new window\)](#)

You Are Visiting From:
128.93.62.86 is from France(FR) in Western Europe
Host name: dhcp-rocq-86.inria.fr

<p>Cookie Test</p> <p>No Cookie from this site is on your system from prior visits.</p> <p>You linked from here</p> <p>http://network-tools.com/analyze/</p> <p>Your Browser Type and Operating System:</p> <p>Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.5; en-US; rv:1.9.1.7) Gecko/20091221 Firefox/3.5.7</p> <p>All information sent by your web browser when requesting this web page:</p> <p>Connection: keep-alive Keep-Alive: 300 Content-Length: 607 Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Charset: UTF-8,* Accept-Encoding: gzip,deflate Accept-Language: en-us,en;q=0.5 Cookie: bhCookieSaveSess=1; bhCookieSess=1; Privacy.net_Last_Visit=1/18/2010; Privacy.net=Privacy+Analysis; bhawkplt=plt_state=tested&plt_stm=1263815352253&plt_url=null Host: analyze.privacy.net Referer: http://analyze.privacy.net/test.asp?RequestCookies=&Requestdate=&refer=http://network-tools.com/analyze/ User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.5; en-US; rv:1.9.1.7) Gecko/20091221 Firefox/3.5.7</p> <p>Firewall Test</p> <p>The following ports were checked: 16771, 80 Out of the above ports, the following are open and permitting outbound traffic: 16771,80</p> <p>Firewall status: PRESENT</p>		
<p>Browser Type and Version</p> <p>Browser: Firefox Fullversion: 3.5.7 Gecko: True GeckoBuildDate: 20091221 Crawler: False</p>	<p>Display and Layout</p> <p>Width: 1440 WidthAvail: 1100 Height: 900 StyleSheets: True</p>	<p>System Details</p> <p>Platform: MacOSX Win16: False WinInstallerMinVer: 0</p>

<p>Browser Security</p> <p>Session Cookies Not Accepted Persistant Cookies Accepted JavaScriptEnabled: True VBScriptEnabled: False JavaEnabled: True ActiveXEnabled: False SSL: True SSLActive: False SSLKeySize: 128 SSLEnabled: True Firewall: True OpenPorts: 16771,80 PopupsBlocked: True ImagesEnabled: True HighSecurity: False</p> <p>Connection Details</p> <p>Broadband: True ConnectionType: Firewall: True Proxy: False CompressGZip: True AOL: False MSN: False</p>	<p>PNG: True FontSmoothing: False FontColor: True FontSize: True Tables: True TableBGColor: True TableBGImage: True ColorDepth: 24 Frames: True IFrames: True</p> <p>Scripting Capabilities</p> <p>ActiveXControls: False ActiveXEnabled: False JavaScript: True JavaScriptEnabled: True JavaScriptVer: 1.8 JavaScriptBuild: VBScript: False VBScriptEnabled: False VBScriptBuild: XML: True MSXML: 0 XMLHttpRequest: True DHTML : True FileUpload: Yes</p>	<p>Plug-in Information</p> <p>Plugin Flash Version: 10.0 r22 Plugin Flash Version: 11.5.1 Plugin QuickTime Version: Installed (version 7.6.4) Plugin RealPlayer Version: 10.1.0.503 Plugin MediaPlayer Version: Installed but version not detected Plugin Flip4Mac installed</p> <p>Java Information</p> <p>JavaApplets: True JavaEnabled: True</p> <p>Wireless Device Information</p> <p>PDA: False WAP: False HDML: False</p> <p>Locale Information</p> <p>Country: FR Language: English User Language: en-us System Language: Time Zone Difference: 6 Browser Date and Time : Mon Jan 18 12:49:11 2010 Browser Date and Time ms: 1263815351981</p>
---	--	---

TraceRoute to 128.93.62.86 [dhcp-rocq-86.inria.fr]

Hop	(ms)	(ms)	(ms)	IP Address	Host name
1	7	2	3	192.168.255.1	-
2	12	6	6	67.222.132.1	router.dfw-datacenter.com
3	14	14	13	72.249.128.105	-
4	9	6	11	206.123.64.82	-
5	7	10	15	64.129.174.181	64-129-174-181.static.twtelecom.net
6	50	45	49	66.192.242.253	-
7	117	149	122	195.2.25.198	xe-3-1-0-xcr1.lnd.cw.net
8	186	128	128	195.2.21.210	-
9	132	127	128	195.2.9.198	xe-0-1-0.xcr1.prp.cw.net
10	123	137	137	195.2.9.189	xe-0-1-0.xcr1.par.cw.net
11	142	138	154	195.10.54.66	giprenater-gw.par.cw.net
12	148	140	146	193.51.189.38	-

13	141	140	139	193.51.189.210	te1-1-inria-rtr-021.noc.renater.fr
14	148	145	142	193.51.184.177	inria-rocquencourt-gj3-2-inria-rtr-021.noc.renater.fr
15	147	148	143	192.93.1.120	vs-lanroc-bb.inria.fr
16	Timed out	Timed out	Timed out		-
17	Timed out	Timed out	Timed out		-
18	Timed out	Timed out	Timed out		-
19	Timed out	Timed out	Timed out		-

Trace aborted.

Checking the domain name records of your connection:

whois query for inria.fr...

Results returned from whois.nic.fr:

```
%%
%% This is the AFNIC Whois server [clyde.nic.fr].
%%
%% complete date format : DD/MM/YYYY
%% short date format   : DD/MM
%% version              : FRNIC-2.5
%%
%% Rights restricted by copyright.
%% See http://www.afnic.fr/afnic/web/mentions-legales-whois_en
%%
%% Use '-h' option to obtain more information about this service.
%%
%% [67.222.132.194 REQUEST] >> -n inria.fr
%%
%% RL Net [#####] - RL IP [#####.]
%%
```

```
domain:  inria.fr
status:  ACTIVE
hold:    NO
holder-c: INDR18-FRNIC
admin-c:  DT5-FRNIC
tech-c:  GR1378-FRNIC
tech-c:  PB2340-FRNIC
zone-c:  NFC1-FRNIC
nsi-id:  NSL3778-FRNIC
registrar: RENATER
anniversary: 01/01
created:  01/01/1995
last-update: 11/03/2009
source:  FRNIC
```

```
ns-list:  NSL3778-FRNIC
nserver:  dns.inria.fr [193.51.208.13]
nserver:  nez-perce.inria.fr [192.93.2.78]
nserver:  dns.cs.wisc.edu
nserver:  dns.princeton.edu
nserver:  imag.imag.fr [129.88.30.1]
nserver:  ns2.nic.fr [192.93.0.4 2001:660:3005:1::1:2]
source:  FRNIC
```

registrar: RENATER
type: Isp Option 1
address: 151 Boulevard de l'hôpital
address: PARIS
country: FR
phone: +33 1 53 94 20 30
fax-no: +33 1 53 94 20 31
e-mail: domaine@renater.fr
website: http://www.renater.fr
anonymous: NO
registered: 01/01/1998
source: FRNIC

nic-hdl: DT5-FRNIC
type: PERSON
contact: Daniel Terrer
address: INRIA Sophia-Antipolis
address: 2004, route des Lucioles
address: B.P. 93
address: 06902 Sophia Antipolis Cedex
country: FR
phone: +33 4 92 38 77 22
fax-no: +33 4 92 38 76 02
e-mail: daniel.terrer@sophia.inria.fr
changed: 15/10/2000 migration-dbm@nic.fr
anonymous: NO
obsoleted: NO
source: FRNIC

nic-hdl: GR1378-FRNIC
type: ROLE
contact: GIP RENATER
address: GIP RENATER
address: Ensam
address: 151, boulevard de l'Hopital
address: 75013 Paris
country: FR
phone: +33 1 53 94 20 30
fax-no: +33 1 53 94 20 31
e-mail: rensvp@renater.fr
trouble: Information: http://www.Renater.fr/
trouble: abuse reports, ... mailto:CertSVP@Renater.fr
trouble: questions: mailto:RenSVP@Renater.Fr
admin-c: DV321-FRNIC
tech-c: FS65-FRNIC
tech-c: BT261-FRNIC
tech-c: MD5336-FRNIC
tech-c: SJ94-FRNIC
tech-c: ED168-FRNIC
tech-c: CT1053-FRNIC
tech-c: SEH1-FRNIC
tech-c: FXA1-FRNIC
changed: 08/11/2005 rensvp@renater.fr
anonymous: NO
obsoleted: NO
source: FRNIC

nic-hdl: INDR18-FRNIC

type: ORGANIZATION
contact: Institut National de Recherche en Informatique
address: et Automatique - Inria
address: Domaine de Voluceau
address: B.P. 105
address: 78153 le Chesnay
country: FR
phone: +33 1 39 63 55 11
fax-no: +33 1 39 63 53 30
e-mail: webmaster@inria.fr
changed: 02/12/2009 nic@nic.fr
anonymous: NO
obsoleted: NO
idstatus: ok
source: FRNIC

nic-hdl: PB2340-FRNIC
type: PERSON
contact: Philippe Balse
address: INRIA Sophia-Antipolis
address: 2004, route des Lucioles
address: B.P. 93
address: 06902 Sophia Antipolis Cedex
country: FR
phone: +33 4 92 38 79 34
fax-no: +33 4 92 38 76 02
e-mail: philippe.balse@sophia.inria.fr
notify: philippe.balse@sophia.inria.fr
changed: 15/10/2000 migration-dbm@nic.fr
anonymous: NO
obsoleted: NO
source: FRNIC

Checking domain configuration records. This includes where e-mail is processed for the domain:

127.0.0.1 xxx dhcp-rocq-86.inria.fr

Retrieving DNS records for dhcp-rocq-86.inria.fr...

DNS servers

dns.inria.fr [193.51.208.13]
dns.princeton.edu
dns.cs.wisc.edu
nez-perce.inria.fr [192.93.2.78]
ns2.nic.fr
imag.imag.fr

Answer records

dhcp-rocq-86.inria.fr 1 A 128.93.62.86 3600s

Authority records

inria.fr 1 NS imag.imag.fr 3600s
inria.fr 1 NS dns.princeton.edu 3600s
inria.fr 1 NS ns2.nic.fr 3600s
inria.fr 1 NS dns.cs.wisc.edu 3600s

inria.fr 1 NS nez-perce.inria.fr 3600s
inria.fr 1 NS dns.inria.fr 3600s

Additional records

dns.inria.fr 1 A 193.51.208.13 3600s
imag.imag.fr 1 A 129.88.30.1 7200s
imag.imag.fr 1 28 [16 bytes] 7200s
nez-perce.inria.fr 1 A 192.93.2.78 3600s

Checking who manages your IP address:

whois query for 128.93.62.86...

Results returned from whois.arin.net:

OrgName: RIPE Network Coordination Centre
OrgID: RIPE
Address: P.O. Box 10096
City: Amsterdam
StateProv:
PostalCode: 1001EB
Country: NL

ReferralServer: whois://whois.ripe.net:43

NetRange: 128.93.0.0 - 128.93.255.255
CIDR: 128.93.0.0/16
NetName: RIPE-ERX-128-93-0-0
NetHandle: NET-128-93-0-0-1
Parent: NET-128-0-0-0-0
NetType: Early Registrations, Transferred to RIPE NCC
Comment: These addresses have been further assigned to users in
Comment: the RIPE NCC region. Contact information can be found in
Comment: the RIPE database at <http://www.ripe.net/whois>
RegDate: 2004-04-05
Updated: 2004-04-05

ARIN WHOIS database, last updated 2010-01-17 20:00
Enter ? for additional hints on searching ARIN's WHOIS database.

ARIN WHOIS data and services are subject to the Terms of Use
available at https://www.arin.net/whois_tou.html

Results returned from whois.ripe.net:

% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See <http://www.ripe.net/db/support/db-terms-conditions.pdf>

% Information related to '128.93.0.0 - 128.93.255.255'

inetnum: 128.93.0.0 - 128.93.255.255
netname: INRIA-NET
descr: Institut National de Recherche en Informatique et Automatique

descr: **Domaine de Voluceau, Rocquencourt**
descr: **BP 105, 78153 Le Chesnay CEDEX, France**
country: **FR**
admin-c: **PB63-RIPE**
tech-c: **DJ433-RIPE**
status: **ASSIGNED PI**
mnt-by: **RENATER-MNT**
changed: **ripe-dbm@ripe.net 19990706**
changed: **ripe-dbm@ripe.net 20040430**
changed: **rensvp@renater.fr 20050117**
source: **RIPE**

person: **Patrick BERTELLIN**
address: **Institut National de Recherche en Informatique et en Automatique**
address: **Domaine de Voluceau, Rocquencourt**
address: **BP 105, F-78153 Le Chesnay CEDEX, France**
phone: **+33 1 39 63 52 61**
fax-no: **+33 1 39 63 53 30**
e-mail: **Patrick.Bertellin@Inria.fr**
nic-hdl: **PB63-RIPE**
mnt-by: **RENATER-MNT**
changed: **rensvp@renater.fr 20011001**
changed: **rensvp@renater.fr 20060227**
source: **RIPE**

person: **Denis JOIRET**
address: **Institut National de Recherche en Informatique**
address: **et en Automatique**
address: **Domaine de Voluceau, Rocquencourt**
address: **BP 105, F-78153 Le Chesnay CEDEX, France**
phone: **+33 1 39 63 53 82**
fax-no: **+33 1 39 63 53 30**
e-mail: **Denis.Joiret@inria.fr**
nic-hdl: **DJ433-RIPE**
mnt-by: **RENATER-MNT**
changed: **rensvp@renater.fr 20000120**
changed: **rensvp@renater.fr 20060410**
source: **RIPE**

% Information related to '128.93.0.0/16AS2200'

route: **128.93.0.0/16**
descr: **RENATER**
descr: **Universite Pierre et Marie Curie**
descr: **4 place Jussieu 75252 PARIS CEDEX 05**
descr: **FRANCE**
origin: **AS2200**
mnt-by: **RENATER-MNT**
changed: **RenSVP@Renater.fr 19991008**
source: **RIPE**

The following is a list of all fonts installed on your computer:

Font detection requires IE 5 or higher.

[Click to Run The Test Again](#) (Don't use refresh)

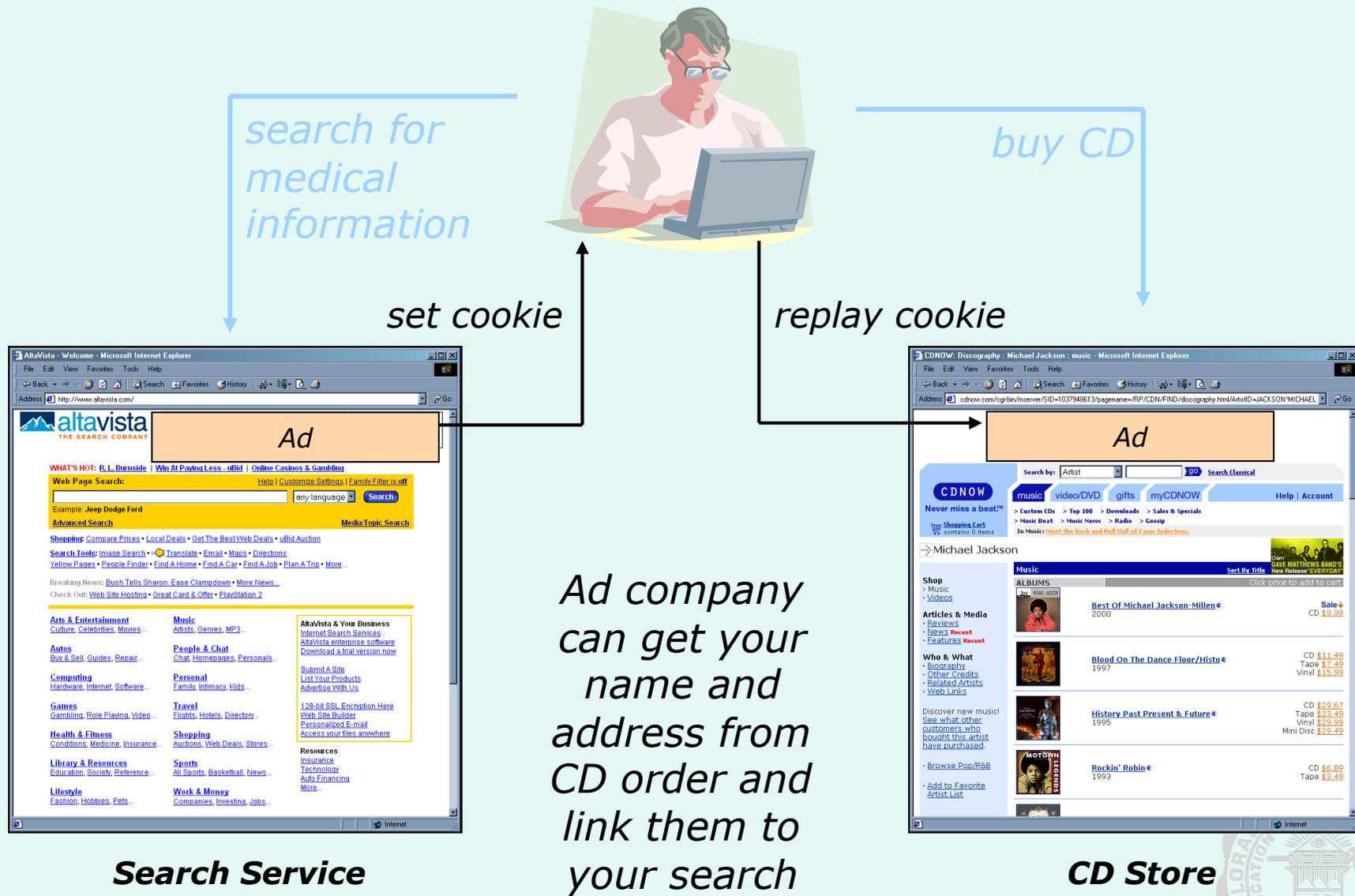
[Trace other computers on the Internet using Network-Tools.com](#)

Back to [Privacy.net](#)



This site is operated by [The Keyword Factory, LLC](#) of Ocean City, NJ ©2007 | [Contact This Web Site](#)

Linking With Cookies



Search Service

CD Store



On-line Privacy Concerns

- Data is often collected silently
 - Web allows large quantities of data to be collected inexpensively and unobtrusively
- Data from multiple sources may be merged
 - Non-identifiable information can become identifiable when merged
- Data collected for business purposes may be used in civil and criminal proceedings



Should We Be Worried?

Users given no meaningful choice
Few sites offer alternatives



Personal Information = Real Money to Companies

- In November 1999, DoubleClick purchased Abacus Direct, a company possessing detailed consumer profiles on more than 90% of US households.
- In mid-February 2000 DoubleClick announced plans to merge “anonymous” online data with personal information obtained from offline databases
- By the first week in March 2000 the plans were put on hold after complaints from privacy advocates
 - Stocks dropped from \$125 (12/99) to \$80 (03/00)



Privacy International's Privacy Ranking of Internet Service Companies



Consultation Report: Race to the Bottom? 2007

LEGEND

Privacy-friendly and privacy enhancing
Generally privacy-aware but in need of improvement
Generally aware of privacy rights, but demonstrate some notable lapses
Serious lapses in privacy practices
Substantial and comprehensive privacy threats
Comprehensive consumer surveillance & entrenched hostility to privacy

Company	Company administrative details	Corporate Leadership	Data Collection and Processing	Data Retention	Openness and Transparency	Responsiveness	Ethical Compass	Customer Control	Fair Gateways	Privacy Enhancing or Invading Innovations	Initial Assessment	Justification
Amazon	Webform access to email for those with privacy problems. No postal address given. Must be signed in as an account holder in order to complain.	Previously profiled and shared profiles of customers' purchasing habits. Signed up to Safe Harbor.	Privacy notice describes some of processing practices. Does not discuss what is done with 'clickstream' and 'cookie data', i.e. whether Amazon tracks usage, popularity, and then profiles.	No information readily available	Policy lacking in information about how information is used to profile customers.		Previously Amazon has been reluctant to introduce privacy measures. Firm seems to have responded to earlier problems.	Customers may close accounts, but only possible through an email sent to Amazon.	Offers the choice to use anonymous or pseudonymous profiles and even informs customers of a variety of PET tools. Amazon Prime accounts offer greater services for an annual fee. Not mandatory and other customers are not penalised.	No privacy enhancing innovations apparent though points to privacy services from other companies. No discussions of techniques to profile.	Notable lapses	Amazon has improved much over the years but consumers should be informed on how their clicking, reading, and purchase habits are profiled and used.
AOL	Contact only available via email at privacyquestions@aol.com (though with a separate email address for Californians, at CAPrivacyInfoAN@aol.com .)		Tracks user movements and use of resources. Monitors which e-mails you open and act upon. Monitors searches and how these searches were acted upon. Keeps a track of history of items purchased across AOL services. Supplements data from other firms. Collects IP address and geographic information. Researches use of AOL services, using cookies and web beacons.	No information readily available	Policy is relatively open about the fact that there is personal information processing but is lacking in information about how.		Leakage of search engine data was responded to poorly as though it was not privacy invasive. Investigations showed otherwise.	Closing account is possible but nothing is said about how long personal data is kept for afterwards.	Account-only access in many areas of site. Differentiates between different users (e.g. Apple users are prevented from viewing view video content).	No information readily available, though does use web beacons to track users activities.	Substantial Threat	No privacy enhancing innovations apparent though points to privacy services from other companies.
Apple	Apple Computer, 1 Infinite Loop, MS60-DR, Cupertino, California, USA, 95014 Privacy policy last updated in 2004. Numerous email addresses given based on geographic region including privacy@apple.com and privacyeurope@apple.com	Weak. Repeated statements in policy like: "As is true of most Web sites..." Relatively quiet on information processing issues. Member of Trust-e. Part of Safe Harbor.	Opt-out process available. Shares data with other companies to "manage and enhance customer data". Collects clickstream data. Does not consider IP address as personal information. Also collect 'clickthrough' data. Ministore collected list of music on home computers.	No specification of the deletion period. Does not consider itself responsible for data posted in forums, as a result is unlikely to anonymise or delete at any time.	Very little information is available. Vague privacy policy with an optimistic tone on data collection, but does not explain whether there is any profiling and marketing activities?		Kept quiet on the potential watermarking of DRM-free iTunes songs. They did respond eventually to the 'ministore' controversy. Subject access requests are said to be available according to the policy, by email.	May opt-out of some services. May not access free iTunes services without registering.	Certain features of the Apple website will not be available once cookies are disabled.	Profiles use of music in 'Ministore'. Mentions privacy enhancing precautions, but no information on technologies. Uses cookies and "other technologies" to track users. Uses "pixel tags" to identify whether individuals have read emails.	Substantial Threat	Vague privacy policy does not address the advanced level of services offered by Apple. Could be quite promising if Apple was more open. Good that firm offers access to data subjects. Responsiveness has been poor to date.
BBC	Data Protection Officer, MC3 D1, Media Village, 201 Wood Lane, London, W12 7TQ and email at dpa.officer@bbc.co.uk		Use cookies to track movements. Uses Nielsen and SageMetrics cookies to track readership.	Declares in some cases how long personal information is kept.	Privacy policy is relatively explicit about each cookie, describing in detail.		No evidence yet. Charge 10 GBP for access to records.	Explains how to opt-out of cookies.		No information readily available	Generally privacy aware	Rare in its openness about processing, what for, and how to access data and manage cookies.
Bebo	Customer Support, Bebo, Inc. 142 Tenth Street, San Francisco, CA 94103, USA	Co-operates with Child Online Exploitation Police in UK, after encountering problem cases.	Name, email address, IP address, age, hobbies, and interests and other content, such as photos. Does not consider IP addresses as personal information.	No information readily available	Inconsistencies in privacy policy. Lacks detail.		Responded to concerns about privacy problems (linked with child safety) but ensuring access is limited to certain age groups.	Can end membership. Can limit information available to people.	Company decides who can contact users based on their age.	No information readily available	Notable lapses.	Prior problems has led to some innovation. Lack of information is problematic. User control increasing.

Company	Company administrative details	Corporate Leadership	Data Collection and Processing	Data Retention	Openness and Transparency	Responsiveness	Ethical Compass	Customer Control	Fair Gateways	Privacy Enhancing or Invading Innovations	Initial Assessment	Justification
eBay	eBay Inc. Attn: Legal - Global Privacy Practices, 2145 Hamilton Avenue, San Jose, California 95125; and via a customer form	Member of Trust-e.	Information collection from other companies included.	No information readily available	Remarkable level of information about how data is shared.	Very responsive to privacy concerns: changed practice to allow for customer account deletion.		Can opt out of marketing and advertising. Can reject cookies though may have some effects.	Can gain access to much information without authenticating.	Uses web beacons. A lot of the cookies are only session cookies. Anonymised or de-identified information is shared.	Generally privacy aware	Good responsiveness. Web beacons and lack of information on retention detracts from score.
Facebook	156 University Avenue, Palo Alto, CA 94301; and privacy@facebook.com	Member of Trust-e. Signed up to safe harbor.	Earlier concerns about data matching, data mining and transfers to other companies. Collects data from 'other sources', including newspapers, blogs, instant messaging services, and other users of the Facebook service through the operation of the service (e.g. 'photo tags').	No information readily available	Basic privacy policy.	Has responded to some (of many) concerns about security and privacy.	Purports to have two principles: 1. you have control over personal information. 2. you have access to info others want to share. But track history indicates otherwise.	Unable to fully opt out of controversial 'news feed' services. Cookies can be blocked. Many are session cookies. Profiles are only accessible based on privacy settings, though name and profile-photo is available to all.	In 2005 a number of profiles were downloaded to prove weak security. Does not accept liability for security.	No information readily available	Substantial Threat	Problematic track history. Uses data from 'other sources', and has not maintained strong security mechanisms. Does not inform on measures being taken now to protect data.
Friendster	No specific privacy contact point. General address is given as Friendster, Inc. 568 Howard Street San Francisco, CA 94105 Fax: (415) 618-0074		Itemises information types collected through consent and without consent (e.g. IP address). Promises not to share personally identifiable information with third parties. Third party cookies are possible.	No information readily available	Open privacy policy, though vague at times.			User may chose to share with 'friends', 'friends of friends', and 'anyone', including non-Friendster members. Some profile information is shared with everyone.	Rejecting cookies may prevent access to website.	Access to personal information is said to be limited even to employees.	Notable lapses	Insufficient information to draw compelling conclusions. Lack of main point of contact is problematic.
Google	Privacy Matters, c/o Google Inc, 1600 Amphitheatre Parkway, Mountain View CA 94043 (USA). Policy not updated since 2005.	Rejected access to data by U.S. Justice Department for research purposes. Member of Safe Harbor.	Describes data collected. IP addresses are not considered personal information. They do not believe that they collect sensitive information. Do sometimes track links clicked upon. Shares information with consent, or to companies (subsidiaries, affiliated companies, trusted businesses or persons).	Unclear but has stated 18-24 months as eventual outcome. Log history is retained after this period.	Vague, incomplete and possibly deceptive privacy policy. Document fails to explain detailed data processing elements or information flows.	Generally poor track record of responding to customer complaints. Ambivalent attitude to privacy challenges (for example, complaints to EU privacy regulators over Gmail).	Privacy mandate is not embedded throughout the company. Techniques and technologies frequently rolled out without adequate public consultation (e.g. Street level view).	Customers have a right to amend personal details held by Google but does not allow search history to be removed. Most services do not permit user access to specific or aggregated disclosure or tracking data.	Opt-out possible for some services. Some services may not work well without cookies. May access essential resources without account but when account is created it is sticky.	Will utilise Doubleclick's "Dynamic Advertising Reporting & Targeting" (DART) advanced profiling system.	Hostile to Privacy	Track history of ignoring privacy concerns. Every corporate announcement involves some new practice involving surveillance. Privacy officer tries to reach out but no indication that this has any effect on product and service design or delivery.
Hi5	General Counsel, hi5 Networks, Inc., 455 Market St., Suite 910, San Francisco, CA 94105, USA.		Collects gender, date of birth, and ZIP. Track users with cookies and by IP addresses. Also tracks users movements on site by monitoring click-through data.	No information readily available	Relatively blatant about some processing but unnecessarily vague about others.		Poor. Clicking on Privacy Policy opens up a pop-up window advertisement!	User can identify what information is available to members vs. non-members. Can view other users' profiles without notifying that user. Can opt-out of receiving some information. May delete account.	All visitors can see public content on server (do not need to be registered).	No information readily available	Substantial Threat	Preposterous use of advertising technique (pop-up window) when clicking on privacy policy. Point of contact being a General Counsel leaves little confidence in responsiveness.

Company	Company administrative details	Corporate Leadership	Data Collection and Processing	Data Retention	Openness and Transparency	Responsiveness	Ethical Compass	Customer Control	Fair Gateways	Privacy Enhancing or Invading Innovations	Initial Assessment	Justification
Last.fm	No contact information given for specific access on privacy, though user is suggested to use 'feedback page'.		Email address is not required to register. Pseudonymous listening habit data will be available to other users. May sell or licence lists, but not personal data. No personal information collected regarding transactions with third sites. Monitors which songs listened to, whether skipped, etc., recommendations to other users Does not process PII relating to record collection Does not collect ZIP, post code, city or country unless user explicitly shares. Regards IP addresses as anonymous.	No information readily available	Thorough privacy policy.			Appear to be willing to issue a new user name or password if account anonymity has been destroyed.	Can identify users and what they are listening to without authenticating. Session cookies only. Turning off cookies will inhibit 'a significant proportion' of access.	Appears to collect only aggregate data when possible.	Generally privacy aware	More openness on how to appeal would help case. Explicit use of anonymised data is promising, though more detail on how this is done technologically would increase confidence.
LinkedIn	LinkedIn Corporation, Attn: Privacy Policy Issues, 2029 Stierlin Court, Mountain View, CA 94043 or privacy@linkedin.com	Members of Trust-e and Safe Harbor.	Claim that email addresses of friends that user includes are only used for inviting those friends, and sending reminders. Use cookies and web beacons. Permits third-party cookies and beacons. Shares information with other companies "for specific services".	May close account and then data may be deleted (but not necessarily).	Privacy policy outlines some situations where information is used but could be more explicit.			Some level of user control over information, e.g. friends' information is not accessible to others without permission. Can opt-out of public profile. May close account but only via email.	Users within three degrees of a network can see profile information. Only direct connections can see email address. Public profile is viewable by non-users.	"Any sensitive information that you provide will be secured with all industry standard protocols and technology" Use web beacons to profile and advertise by general profile, e.g. business managers in Texas.	Notable lapses	Use of email addresses of non-users and beacons is questionable. Accessibility of personal profiles could be better managed. Can close account but only via email.
LiveJournal	privacy@livejournal.com		Describes how and why information is collected, including IP addresses. IP addresses may be given to other journal owners within LiveJournal. However IP addresses are not considered sensitive for marketing.	Allows account closure, though keeps some information.	Clear and simple privacy policy. Have a procedure for data security breaches.			Account closure is possible.		Uses "physical, electronic, and procedural safeguards".	Generally privacy aware	More clarity about privacy enhancing innovations is needed. Lax attitude towards IP addresses is problematic. Good to have procedure on data breaches.
Microsoft	Microsoft Privacy, Microsoft Corporation One Microsoft Way Redmond, WA 98052	Established elaborate privacy reporting and awareness regime throughout the company. Developed the "laws of identity". Member of Safe Harbour and Trust-e.	May combine personal information derived from a spectrum of MS services. Shares information to partners (subsidiaries, affiliated companies, trusted businesses or persons). Permits third party advertisers to deploy cookies.	No information readily available	Lacks adequate detail of retention periods, data flows and targeting techniques. When pushed, has been open about some privacy problems.	Improved level of responsiveness to privacy concerns and customer feedback, though continues to be dominated by a PR imperative.	Privacy has now been embedded throughout all stages of the design process for MS products, though patchy management, oversight and reporting results in notable failures such as WGA.	Easily accessible and navigable account management pages. Little information available on accessing or deleting hidden data (logs etc).	MS Passport is used across services, though not required for some services and level of 'stickiness' is insufficiently tested.	Extremely poor privacy design of Windows Genuine Advantage (WGA) and Passport. Strong privacy design and principles in CardSpace.	Serious Lapses	More information on retention is required. Policy is too basic despite application to a number of services. Have embedded privacy into many product and service designs, but terrible track record, including recent WGA debacle.

Company	Company administrative details	Corporate Leadership	Data Collection and Processing	Data Retention	Openness and Transparency	Responsiveness	Ethical Compass	Customer Control	Fair Gateways	Privacy Enhancing or Invading Innovations	Initial Assessment	Justification
Myspace	8391 Beverly Blvd, #349, Los Angeles, CA 90048, privacy@myspace.com		Explicit in collecting name, email address, and age; other profile data including but not limited to: personal interests, gender, age, education and occupation. Considers IP addresses as non-identifying information, to track usage, and to share with third parties. Data is recorded for security and monitoring purposes. May opt-out of receiving service information. Email addresses are kept, particularly for invitations, though recipients of invitations can contact Myspace to have email address removed. Allow cookies and third party cookies.	No information readily available		Public profiles are no longer mandatory.	Tried to require subpoenas before handing over information to law enforcement authorities (on suspected sex offenders).	Users may block the receiving of Myspace invitations by emailing Myspace with a subject 'block'.	Email addresses and user names are limited in their disclosure.	No information readily available	Notable lapses	A mixed bag, with some strong protections and a lot of ambiguities. Problematic interpretation of IP addressing data. Invitation recipients can opt-out. Account deletion is unclear.
Orkut	Privacy Matters, c/o Google Inc. 1600 Amphitheatre Parkway, Mountain View CA 94043 (USA)		Must have a Google Account, including email address. Possible profile information: gender, age, occupation, hobbies, and interests, plus other content, such as photos	Can delete account, completed within 48 hours. Retain contents of messages for indeterminate amount of time.	Very limited privacy policy.		Ethical challenges in blocking site from access in Iran.	Invitees can choose to not receive invites.	Must have a Google Account.	No information readily available	Serious Lapses	No Orkut-specific privacy contact information. Limited privacy policy. Account deletion good sign. Checkered history in cooperating with governments. Requires registration to view information, but registration applies across Google services.
Reunion.com	Reunion.com, Inc., Attn: Privacy Policy Officer, 2118 Wilshire Blvd. Box 1008, Santa Monica, CA 90403-5784		Collects at a minimum, name, birth date, gender, email address and zip code. Uses real names. Company will contact users. May "engage third parties to perform analysis or data processing of our databases that involves access to this information in order to better provide you with the services for which you joined" Shares information with other sites. Tracks movements on site and with partner sites.	No information readily available	Changes to policy are announced but if user continues to use site, they have consented to the changes. May transfer information if firm is purchased.		Poor. Admonished by businesses community for misleading advertising practices to bring in new registrants.		Not accepting cookies will limit access.	Does protect email privacy through a relay system. Use "technical, administrative and physical safeguards" to protect security of personal information.	Substantial Threat	Promising for use of email relaying. Data sharing is dangerously vague. Tracking usage is problematic. Historical ethics problems.

Company	Company administrative details	Corporate Leadership	Data Collection and Processing	Data Retention	Openness and Transparency	Responsiveness	Ethical Compass	Customer Control	Fair Gateways	Privacy Enhancing or Invading Innovations	Initial Assessment	Justification
Skype	15, rue Notre Dame, L-2240 Luxembourg, Luxembourg and/or Skype Communications S.A though no explicit address given for privacy concerns.		Registration not required. Invitation email addresses are deleted immediately upon sending invitation. No communications from skype other than messages about faults. Shared with third parties for provision of services. Cookies do not contain identifying information. Third party cookies exist.	Vague. At least deals with the issue in part in the privacy policy without committing in detail. Though for traffic data, commits to "erase Traffic Data, or make Traffic Data anonymous, as soon as it is no longer needed for the purpose of the transmission of the communication or for billing purposes, unless applicable law permit otherwise."	No way to know if there are back doors in the software. Right to review data, correct, and delete personal data, via email delete@skype.com Thorough privacy policy, but no contact information for accountability.	Responded to concerns about DRM and reading motherboard information.	Poor. Co-operated with Chinese government.		Do not need to register to use Skype Software, but registration may be needed for particular services. Blocking cookies may inhibit personalised services.	User profile data not stored centrally on server. Takes 'appropriate organizational and technical measures'; authorised employees only. Will take "appropriate technical measures to protect the confidentiality of the Communications Content via its Skype Software and VoIP Services"	Notable lapses	Good promises on deleting invitation email addresses. Lack of contact details is problematic. Lack of openness about software capabilities is problematic. Deletion of traffic data is good statement though less ambiguity about role of laws would help.
Wikipedia	No explicit contact, but policy says it was approved by Board.		Can operate under pseudonym, but if not, then logs IP addresses for public view. Recommends using pseudonym. IP addresses are stored and can be seen by server administrators and advanced users. Data is combined to investigate abuse.	Raw logs are normally discarded after two weeks. Unable to remove accounts. Deleted 'content' is not in fact deleted.	Clear privacy policy, but no main point of contact.				Fully accessible without authenticating.	Session cookies only, and temporary log-in cookies that expire every 30 days.	Generally privacy aware	Lacking in some information, such as contact details. Good statement on retention policy, though unless there is a contact, this is unverifiable.
Windows Live Space	Microsoft Privacy, Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052 - 425-882-8080, and webform is available.	Signed up to Trust-e and Safe Harbor.	IP addresses not treated as personal information. Customised links are used to identify users. Voice messenger service requires signing up with Verizon. Tracks all requests for maps. Locations are logged when service is used online.	No information readily available	Unclear about what information is used for and how long it is used for.		Poor. Co-operated with Chinese government. Unclear policy statement about future co-operation. Recent research hints at profiling based on search requests. Disclosed search data to U.S. Department of Justice for research purposes.	User can designate who has access to which calendar data.	Anyone may review calendar information that is published for public access.	May use beacons to track messages sent by MS to determine whether opened or read. Beacons also used by third parties to aggregate statistics.	Substantial Threat	Problematic use of personal information, without clear statements about retention. Uses almost every means to identify users and track movements.
Xanga	Contactable through webform for email interaction.		Username, password, email address, date of birth. Email and birthdate are not necessarily disclosed if user wishes. Profile information is optional. For invitations, Xanga may send multiple invitations by email. Email addresses can be blacklisted to receive no further invitations. Logs IP data. Targets advertisements based on profile and past activities. Third party cookies are possible as well. May transfer data if company is purchased.	If account is shut down, Xanga site no longer accessible. Data may be archived, but offline.	Presumes consent by non-U.S. users.			By default information is shared widely, though can be controlled. Can control comments on your section of the site, and whether someone can be blocked from commenting.	Information available to non-registered users. Blocking cookies may limit access.	Footprints' service allow users to watch visitors on his or her own site (username or geographic information based on IP address).	Serious Lapses	Invitation process could be better managed. Treatment of IP data is vague. Profiling is mentioned but more clarity is required. Information should not be shared by default. May limit information collected.

Company	Company administrative details	Corporate Leadership	Data Collection and Processing	Data Retention	Openness and Transparency	Responsiveness	Ethical Compass	Customer Control	Fair Gateways	Privacy Enhancing or Invading Innovations	Initial Assessment	Justification
Yahoo!	Yahoo! Inc. Customer Care - Privacy Policy Issues, 701 First Avenue, Sunnyvale, CA 94089, (408) 349-5070	Trust-e and safe harbor.	<p>registration process can be combined with data from other sources (business partners and other companies). Information collected: name, email, birthdate, gender, ZIP code, occupation, industry, personal interests. May also ask for social security for financial services. Collects transaction data, including information about use of financial products. Collects and stores information including IP addresses and cookies related data. Data can be shared for marketing purposes. Data will be transferred if acquired. Cookies (and third party cookies) are used, as are web beacons. Opt-out of marketing</p>	<p>May delete account but some information retained, for 90 days. Log files are used — after they are used they are stored (but said to be inaccessible). No further information on searches.</p>	<p>Overly broad and vague policy.</p>	<p>Did not go out of its way to respond to ethical concerns.</p>	<p>Poor. Cooperates with governments with disclosure of information, including Chinese government. Disclosed search data to U.S. Department of Justice for research purposes.</p>		<p>Registration not necessary for some services.</p>	<p>Use 'physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information' Also limit access to employees.</p>	Substantial Threat	<p>Vague privacy policy prevents us from understanding the dynamics of data processing. Using information from other sources is highly problematic. Account closure possibility is good (and honest statement about retention is relatively positive). Lack of information on search and IP data is problematic. Poor track record.</p>
YouTube	Contact only available through a contact form.		<p>Video, image, or other content posted are not considered personal information. Use both session and persistent cookies, as well as web beacons. Monitors and tracks IP logs. IP data not considered personal data. Data used to monitor marketing effectiveness and track actions (e.g. entries). Share personal information with subsidiaries, affiliated companies, or other businesses and persons.</p>	<p>Media files, once uploaded, can not be modified. No information on deletion of other data.</p>	<p>Use of site is considered consent to U.S. law (no safe harbor). Data can be purchased in event of sale.</p>	<p>Has a policy for data breaches.</p>			<p>Blocked cookies may inhibit service.</p>	<p>Web beacons used to track usage, and uses gifs in emails to track users. "[U]ses commercially reasonable physical, managerial, and technical safeguards to preserve the integrity and security of your personal information"</p>	Serious Lapses	<p>Considering the size of YouTube and its owners, the vague information about sharing of personal information with affiliated companies leaves much to be desired. Tracking email reading habits is problematic. Videos are not considered personal information. Explicit statement that 'consent' is presumed in transborder data flows is questionable.</p>

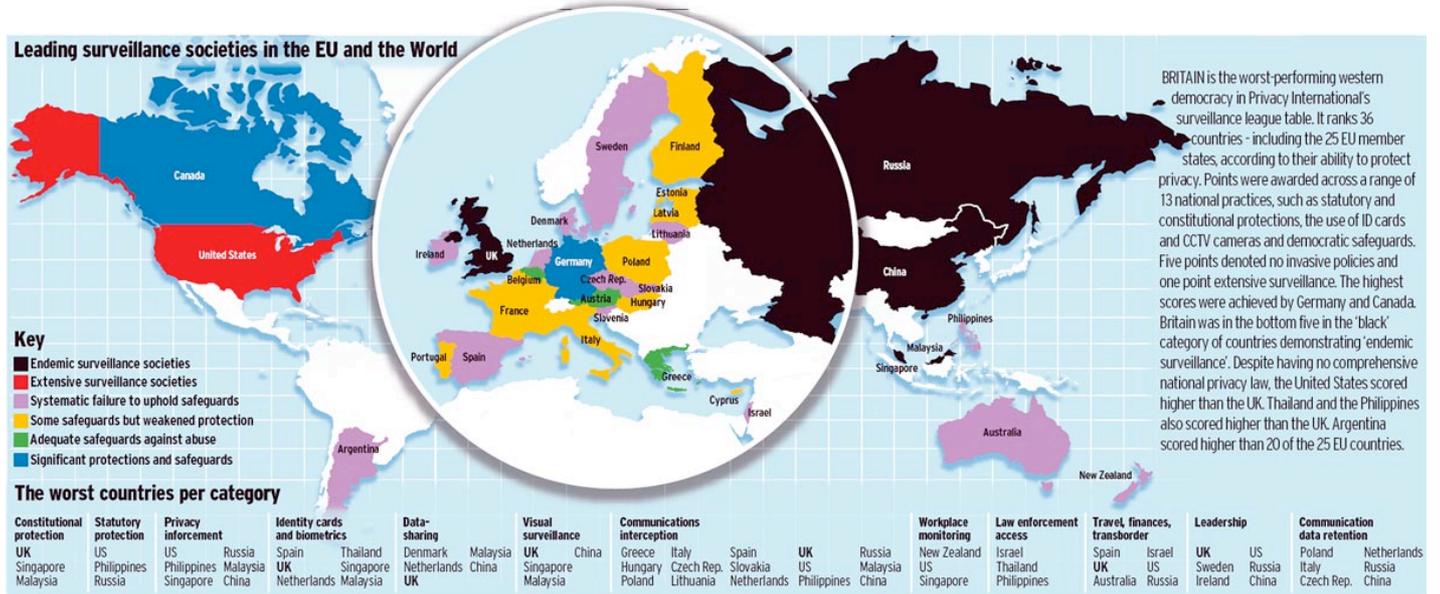
Ranking Countries for Their Privacy Protection and Surveillance Levels





Leading surveillance societies in the EU and the World 2006

02/11/2006



Graphic from the Daily Telegraph, November 2, 2006.

Privacy International																
National Privacy Ranking 2006 - European Union and Leading Surveillance Societies																
	Constitutional protection	Statutory protection	Privacy Enforcement	Identity Cards and Biometrics	Data-sharing	Visual surveillance	Comms interception	Workplace monitoring	Law enforcement access	Comms Data retention	Travel, finances, transborder	Leadership	Democratic safeguards	Total	Ranking	
GERMANY	4	4	4	4	4	4	4	4	3	4	4	4	4	3.9		
BELGIUM	4	4	3	2	-	-	2	4	3	2	4	4	3	4	3.2	
AUSTRIA	2	4	3	2	4	3	2	4	2	4	3	4	4	3.2		
GREECE	4	3	4	3	-	3	1	-	3	-	-	-	4	3.1		
HUNGARY	4	4	4	4	-	2	1	-	3	-	3	2	3	3.0		
FRANCE	3	2	4	2	2	4	3	4	2	2	4	2	4	2.9		
POLAND	4	4	3	2	4	4	1	-	3	1	2	4	3	2.9		
PORTUGAL	4	3	3	3	-	-	2	3	-	-	-	2	4	2.9		
CYPRUS	3	3	3	3	-	-	3	-	-	-	-	2	3	2.9		
FINLAND	3	3	3	2	2	-	3	2	-	3	3	2	4	2.7		
ITALY	4	-	4	3	-	3	1	4	2	1	2	2	3	2.6		
LUXEMBOURG	3	2	3	3	-	-	2	-	-	-	2	3	2	2.6		
LATVIA	3	3	3	2	-	-	3	-	-	-	2	2	3	2.6		
ESTONIA	3	3	3	2	-	-	2	-	3	-	-	2	3	2.6		
MALTA	2	4	3	-	-	-	2	-	2	-	-	2	3	2.6		
DENMARK	4	2	2	4	1	3	2	-	2	2	-	2	4	2.5		
CZECH REP.	4	-	4	2	-	2	1	2	2	2	2	3	4	2.5		
IRELAND	2	3	4	3	3	2	3	3	2	1	2	1	4	2.5		
SLOVENIA	4	3	4	2	2	3	1	3	2	2	2	2	3	2.5		
SLOVAKIA	4	3	3	2	-	-	2	-	2	2	2	2	3	2.5		
LITHUANIA	4	3	3	-	-	2	1	2	-	3	2	2	3	2.5		
SPAIN	3	3	4	1	-	-	1	3	2	2	1	2	4	2.4		
NETHERLANDS	3	4	2	1	1	2	1	3	2	3	2	2	4	2.3		
SWEDEN	3	2	2	3	2	2	2	2	2	1	2	1	4	2.2		
UK	1	2	2	1	1	1	1	2	2	2	1	1	3	1.5		
Non-EU countries																
CANADA	4	4	4	4	3	3	3	3	3	5	3	4	4	3.6		
ARGENTINA	4	4	3	-	2	-	2	3	2	2	3	4	4	3.0		
NEWZEALAND	2	3	3	3	-	-	1	2	2	3	2	2	4	2.5		
AUSTRALIA	2	3	2	3	2	2	2	3	2	4	1	2	3	2.4		
ISRAEL	3	3	3	2	2	2	2	-	1	2	1	2	3	2.2		
US	3	1	1	3	2	2	1	1	2	4	1	1	4	2.0		
THAILAND	3	2	2	1	-	2	2	-	1	3	-	2	1	1.9		
PHILIPPINES	3	1	1	2	-	-	1	-	1	3	2	-	3	1.9		
SINGAPORE	1	2	1	1	2	1	1	1	1	3	2	1	1	1.4		
RUSSIA	3	1	1	2	2	-	1	-	1	1	1	1	1	1.4		
MALAYSIA	1	2	1	1	1	1	1	-	1	3	1	2	1	1.3		
CHINA	2	2	1	2	1	1	1	-	1	1	2	1	1	1.3		
Worst Countries per category	UK, SINGAPORE, MALAYSIA	US, PHIL, RUSSIA	US, PHIL, SINGAPORE, RUSSIA, MALAYSIA, CHINA	SPAIN, UK, NL, THAILAND, SINGAPORE, MALAYSIA	DENMARK, NL, UK, MALAYSIA, CHINA	UK, SINGAPORE, MALAYSIA, CHINA	GREECE, HUNGARY, POLAND, ITALY, CZECH REPUBLIC, LITHUANIA, SPAIN, SLOVENIA, NL, UK, NEW ZEALAND, US, PHIL, SINGAPORE, RUSSIA, MALAYSIA, CHINA	US, SINGAPORE	ISRAEL, THAILAND, PHIL, SINGAPORE, RUSSIA, MALAYSIA, CHINA	POLAND, ITALY, CZECH, NL, SINGAPORE, CHINA	SPAIN, UK, AUSTRALIA, ISRAEL, US, RUSSIA, MALAYSIA	UK, SWEDEN, IRELAND, US, SINGAPORE, CHINA	THAILAND, SINGAPORE, RUSSIA, MALAYSIA, CHINA	CHINA, MALAYSIA, RUSSIA, UK		
Grade	5	no invasive policy or widespread practice/leading in best practice														
4	comprehensive efforts, protections, and safeguards for privacy															
3	some safeguards, relatively limited practice of surveillance															
2	few safeguards, widespread practice of surveillance															
1	extensive surveillance/leading in bad practice															
Final Score	4.1-5.0	Consistently upholds human rights standards														
3.6-4.0	Significant protections and safeguards															
3.1-3.5	Adequate safeguards against abuse															
2.6-3.0	Some safeguards but weakened protections															
2.1-2.5	Systemic failure to uphold safeguards															
1.6-2.0	Extensive surveillance societies															
1.1-1.5	Endemic surveillance societies															

Related:

- [PHR2005 - Forward](#)
- [PHR2005 - Acknowledgements and Front Matter](#)
- [PHR2005 - Executive Summary](#)
- [PHR2005 - Overview of Privacy](#)
- [PHR2005 - Highlights](#)
- [PHR2005 - Glossary and International Resources \(PDF\)](#)
- [Leading surveillance societies in the EU and the World 2007](#)
- [PHR2005 - Country Reports](#)
- [PHR2005 - Threats to Privacy](#)
- [Privacy International and EPIC launch Privacy and Human Rights 2005 global study](#)
- [Publication of the first international privacy rankings](#)

[<< Back](#)

Email us at privacyint@privacy.org.
Call on +44 (0)208.123.7933.
[Privacy Policy](#) - [About PI](#) - [Support PI](#)

What Can We Do About It? Privacy Enhancing Technologies

Educating Users to Privacy Threats



Anti-Phishing Phil

- http://cups.cs.cmu.edu/antiphishing_phil/

An interactive game that teaches users how to identify phishing URLs, where to look for cues in web browsers, and how to use search engines to find legitimate sites

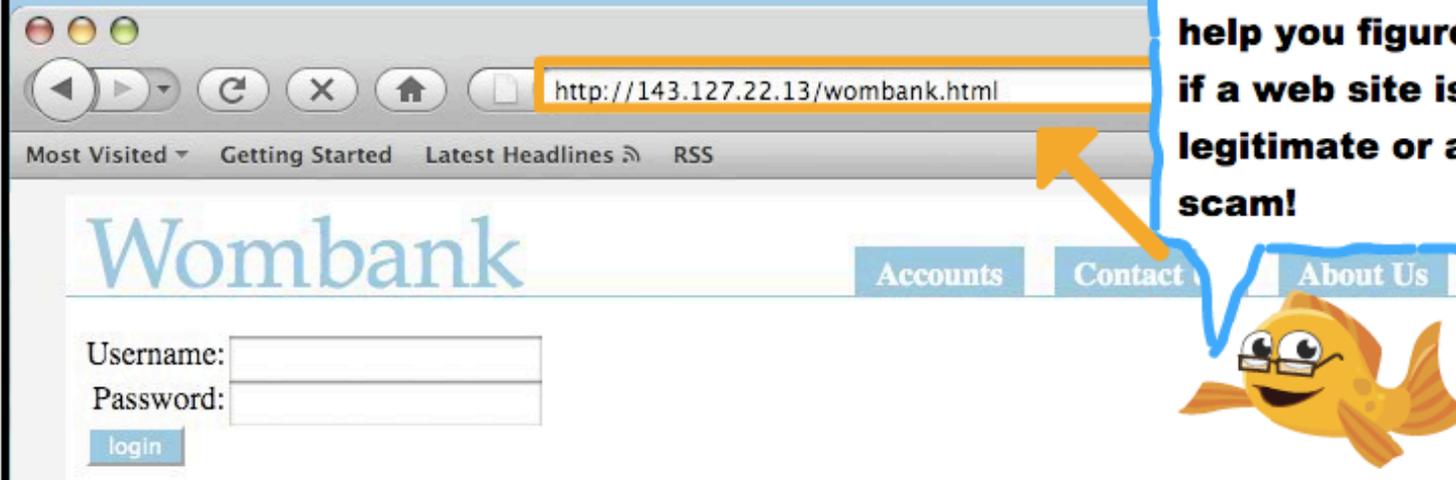


Anti-Phishing Phil

How to Avoid Online Scams

Don't ignore the URL!

Looking at the address bar can help you figure out if a web site is legitimate or a scam!



PLAY!

Privacy Enhancing Technologies

Knowing Privacy Policies



Platform for Privacy Preferences (P3P)

- Allows websites to express their privacy practices in a machine as well human readable way
- Can be retrieved automatically by P3P enabled web browsers and interpreted
 - Users can be made aware of privacy practices
 - Enables automated decision making based on these practices

<http://www.w3.org/P3P/>

PrivacyFinder – Privacy Enhanced Search Engine

- <http://www.privacyfinder.org>

PrivacyFinder is a privacy-enhanced search engine. Once you state your privacy preferences (low, medium, high, or custom), the search results are ordered based on how their computer-readable privacy policies comply with your preferences. A red bird indicates that the site has conflicts with your preferences while a green bird indicates compliance. The absence of any bird means that a valid computer-readable privacy policy, known as a P3P policy, could not be located.



Privacy Enhancing Technologies

Anonymizing Protocols for Communication

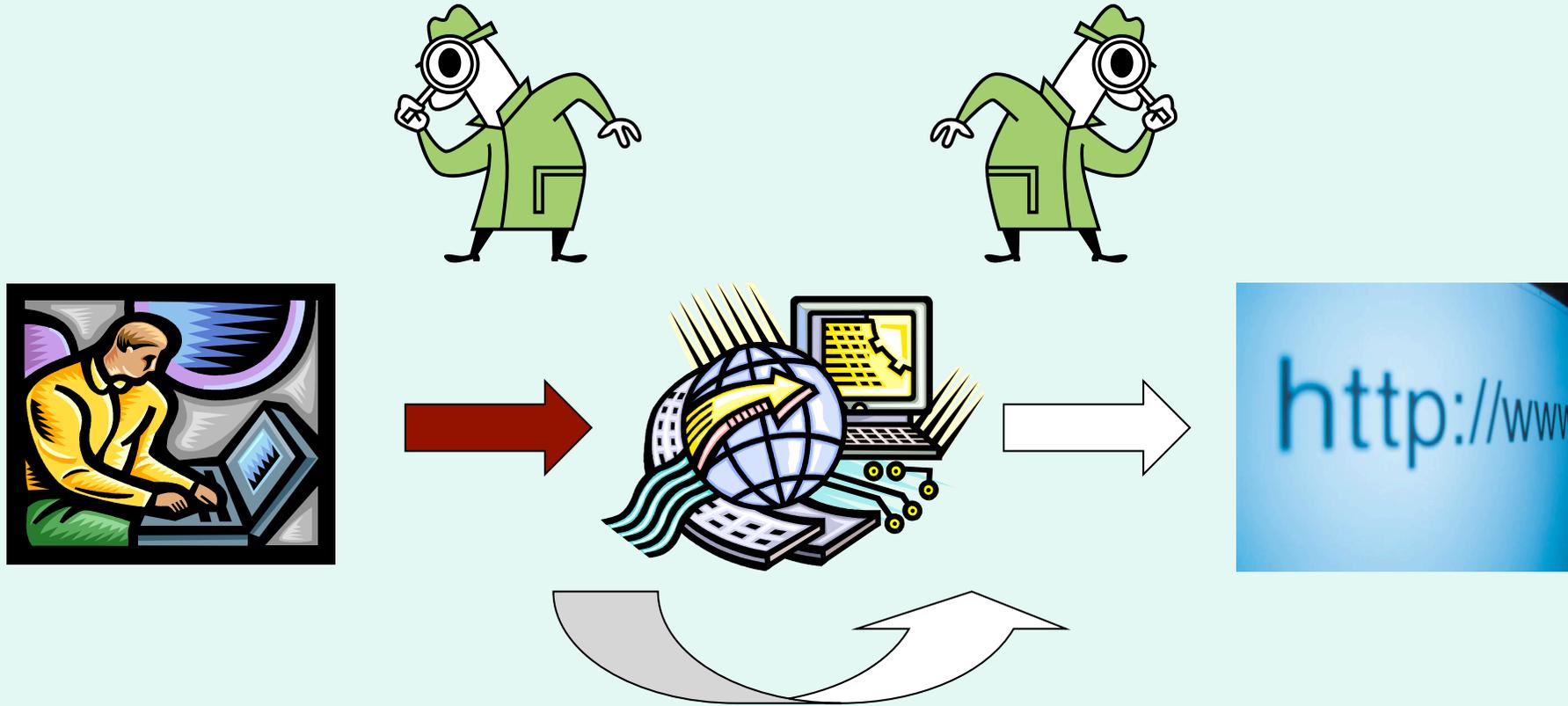


Anonymizing Protocols

- Makes it difficult from someone to trace back a message to its source
- Prevents
 - Linkability
 - Traceability
- Examples
 - Anonymizing Proxy
 - Mix Networks and Onion Routing
 - Tarzan, Tor, I2P
 - Anonymous sharing
 - Freenet

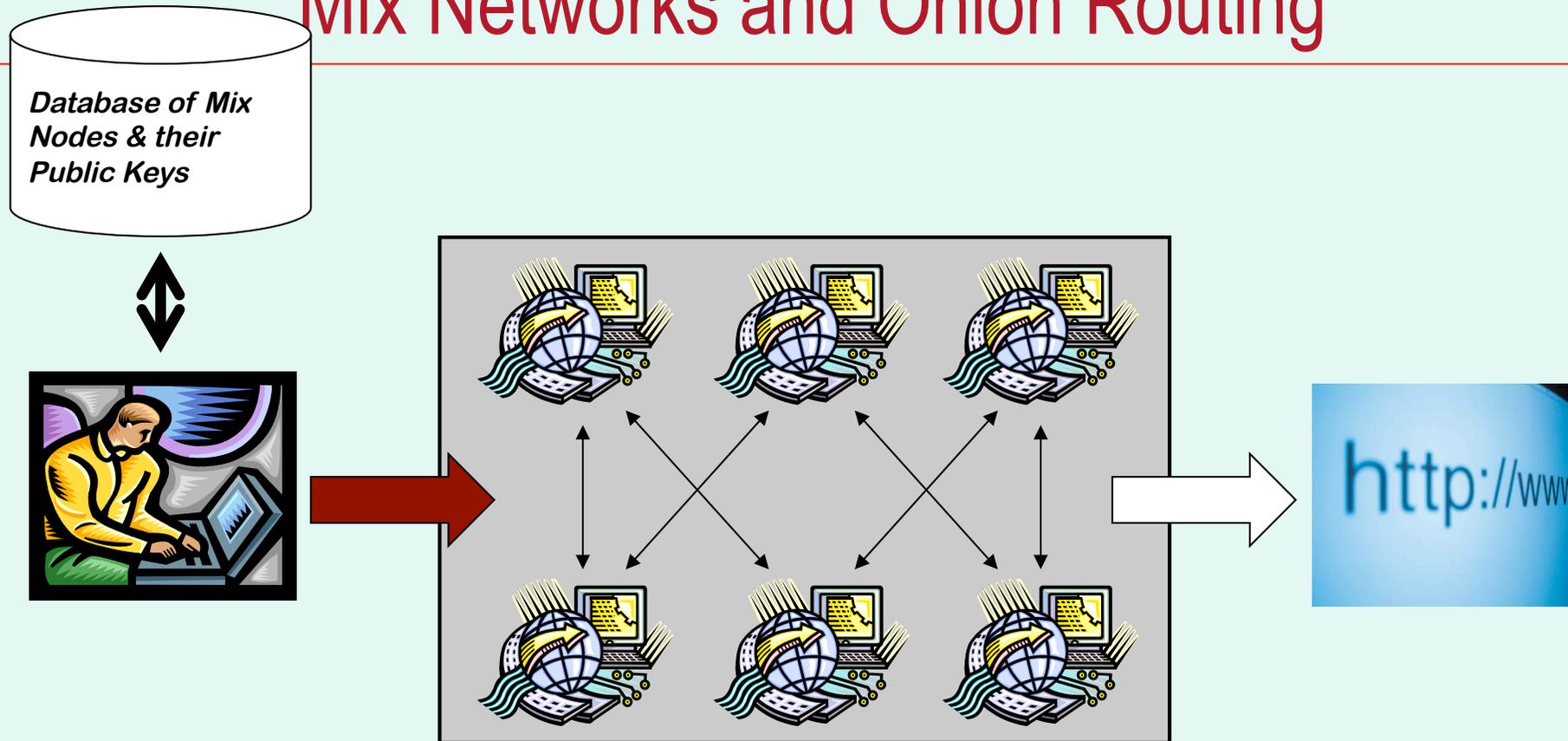


Anonymizing Proxy



Traffic Analysis Breaks Anonymity

Mix Networks and Onion Routing



Layered encryption: $E\left[E\left[E\left[E\left[M, K_{pub}^1\right], K_{pub}^2\right], K_{pub}^3\right], K_{pub}^4\right]$

Prevent edge analysis by introducing cover traffic

Tor – Working Mix Network

- From the Tor project website (<http://www.torproject.org>)

Tor is a toolset for a wide range of organizations and people that want to improve their safety and security on the Internet. Using Tor can help you anonymize web browsing and publishing, instant messaging, IRC, SSH, and other applications that use the TCP protocol. Tor also provides a platform on which software developers can build new applications with built-in anonymity, safety, and privacy features.



Browsing with Tor

Privacy.net Browser Privacy Results with Tor



How to hide my IP address	Search and Navigation	Google Website Optimizer
About 99% of hacking attacks uses the IP address. Hide your IP now. www.HideYourIPAddress.net	Site Search And Navigation Software Improve Relevancy Of Search Results Search and Navigation	Testen Sie, welche Landing Page die meisten Conversions erzielt. Gratis www.Google.com/WebsiteOptimizer

Ads by Google

The [Privacy.net](#) Analyzer

This site analyzes the privacy of your Internet connection and shows some of the information web sites can know about you when you visit. The information can be used to display web content based on things such as country of origin and web browser.

[Click here to read a description of the tests \(opens new window\)](#)

You Are Visiting From:

192.251.226.206 is from Germany(DE) in Western Europe

No host name is associated with this IP address or no reverse lookup is configured.

Error:Timed out

<p>Cookie Test</p> <p>No Cookie from this site is on your system from prior visits.</p> <p>Your Browser Type and Operating System:</p> <p>Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.0.7) Gecko/2009021910 Firefox/3.0.7</p> <p>All information sent by your web browser when requesting this web page:</p> <p>Connection: keep-alive Content-Length: 414 Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Charset: UTF-8,* Accept-Encoding: gzip,deflate Cookie: bhCookieSaveSess=1; bhCookieSess=1; Privacy.net_Last_Visit=1/18/2010; Privacy.net=Privacy+Analysis; bhawkplt=plt_state=tested&plt_stm=1263815853323&plt_url=null Host: analyze.privacy.net Referer: http://analyze.privacy.net/test.asp?RequestCookies=&Requestdate=&refer= User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.0.7) Gecko/2009021910 Firefox/3.0.7</p> <p>Firewall Test</p> <p>The following ports were checked: 16771, 80 Out of the above ports, the following are open and permitting outbound traffic: 16771,80</p> <p>Firewall status: PRESENT</p>		
<p>Browser Type and Version</p> <p>Browser: Firefox Fullversion: 3.0.7 Gecko: True GeckoBuildDate: 2009021910 Crawler: False</p> <p>Browser Security</p> <p>Session Cookies Not Accepted</p>	<p>Display and Layout</p> <p>Width: 1100 WidthAvail: 1100 Height: 700 StyleSheets: True PNG: True FontSmoothing: False FontColor: True FontSize: True</p>	<p>System Details</p> <p>Platform: WinXP Win16: False WinInstallerMinVer: 2</p> <p>Plug-in Information</p> <p>Plugin Flip4Mac installed</p>

Persistant Cookies Accepted JavaScriptEnabled: True VBScriptEnabled: False JavaEnabled: False ActiveXEnabled: False SSL: True SSLActive: False SSLKeySize: 128 SSLEnabled: True Firewall: True OpenPorts: 16771,80 PopupsBlocked: True ImagesEnabled: True HighSecurity: False Connection Details Broadband: False ConnectionType: Firewall: True Proxy: False CompressGZip: True AOL: False MSN: False	Tables: True TableBGColor: True TableBGImage: True ColorDepth: 24 Frames: True IFrames: True Scripting Capabilities ActiveXControls: False ActiveXEnabled: False JavaScript: True JavaScriptEnabled: True JavaScriptVer: 1.8 JavaScriptBuild: VBScript: False VBScriptEnabled: False VBScriptBuild: XML: True MSXML: 0 XMLHttpRequest: True DHTML : True FileUpload: Yes	Java Information JavaApplets: True JavaEnabled: False Wireless Device Information PDA: False WAP: False HDML: False Locale Information Country: DE Language: English User Language: en-us System Language: Time Zone Difference: 5 Browser Date and Time : Mon Jan 18 11:57:33 2010 Browser Date and Time ms: 1263815853320
---	---	--

TraceRoute to 192.251.226.206

Hop	(ms)	(ms)	(ms)	IP Address	Host name
1	5	5	6	192.168.255.1	-
2	6	8	9	67.222.132.1	router.dfw-datacenter.com
3	12	14	6	72.249.128.105	-
4	9	11	17	8.9.232.73	xe-5-3-0.edge3.dallas1.level3.net
5	16	12	17	4.69.145.179	ae-82-80.ebr2.dallas1.level3.net
6	54	54	56	4.69.137.122	ae-3.ebr4.newyork1.level3.net
7	73	56	65	4.69.134.114	ae-64-64.csw1.newyork1.level3.net
8	47	54	43	4.69.134.65	ae-61-61.ebr1.newyork1.level3.net
9	121	115	135	4.69.137.77	ae-44-44.ebr2.london1.level3.net
10	132	121	112	4.69.139.106	ae-2-52.edge4.london1.level3.net
11	133	113	148	195.50.122.2	-
12	168	129	129	84.16.14.165	-
13	143	136	140	84.16.9.102	-
14	144	148	145	195.71.158.21	rmwc-frnk-de01-so-2-1-0-0.nw.mediaways.net
15	143	151	139	195.71.254.78	rmwc-gtso-de01-ge-0-0-0-0.nw.mediaways.net
16	149	147	143	195.71.12.59	xmws-gtso-de01-vlan-2.nw.mediaways.net
17	Timed out	Timed out	Timed out		-
18	Timed out	Timed out	Timed out		-
19	Timed out	Timed out	Timed out		-
20	Timed out	Timed out	Timed out		-

Trace aborted.

Checking who manages your IP address:

whois query for 192.251.226.206...

Results returned from whois.arin.net:

OrgName: RIPE Network Coordination Centre
OrgID: RIPE
Address: P.O. Box 10096
City: Amsterdam
StateProv:
PostalCode: 1001EB
Country: NL

ReferralServer: whois://whois.ripe.net:43

NetRange: 192.251.226.0 - 192.251.226.255
CIDR: 192.251.226.0/24
NetName: RIPE-ERX-192-251-226-0
NetHandle: NET-192-251-226-0-1
Parent: NET-192-0-0-0-0
NetType: Early Registrations, Transferred to RIPE NCC
Comment: These addresses have been further assigned to users in
Comment: the RIPE NCC region. Contact information can be found in
Comment: the RIPE database at <http://www.ripe.net/whois>
RegDate: 2005-02-28
Updated: 2005-02-28

ARIN WHOIS database, last updated 2010-01-17 20:00
Enter ? for additional hints on searching ARIN's WHOIS database.

ARIN WHOIS data and services are subject to the Terms of Use
available at https://www.arin.net/whois_tou.html

Results returned from whois.ripe.net:

% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See <http://www.ripe.net/db/support/db-terms-conditions.pdf>

% Information related to '192.251.226.200 - 192.251.226.207'

inetnum: 192.251.226.200 - 192.251.226.207
netname: BLUTMAGIE
descr: Olaf Selke
remarks: Inquiries/Abuse: abuse@blutmagie.de
remarks: Inquiries/Abuse: for contact details see OS835-RIPE
country: DE
admin-c: OS835-RIPE
tech-c: OS835-RIPE
status: ASSIGNED PA
mnt-by: MNT-WUSEL
changed: wusel@uu.org 20080129
source: RIPE

person: Olaf Selke

address: Detmolder Strasse 109
address: 33397 Rietberg
phone: +495246801169
fax-no: +495246802169
nic-hdl: OS835-RIPE
changed: wusel@uu.org 20080123
mnt-by: MNT-WUSEL
source: RIPE

% Information related to '192.251.226.0/24AS6805'

route: 192.251.226.0/24
descr: Kai Siering
origin: AS6805
mnt-by: MDA-Z
changed: ingo.stampe@mediaways.net 20000407
source: RIPE

The following is a list of all fonts installed on your computer:

Font detection requires IE 5 or higher.

[Click to Run The Test Again](#) (Don't use refresh)

[Trace other computers on the Internet using Network-Tools.com](#)

Back to [Privacy.net](#)

Web Spider Software Extract web content and metadata from websites into your database www.newprosoft.com	Stop Bad Bots Spot your users from the web robots Identify bad crawlers, scrapers www.atlbl.com/webcrawlers.html	GoogleSearchAppliance New Kayxo Connector for GSA ` and Microsoft Exchange Server kayxo.com/KayxoConnector
--	---	--

Ads by Google

This site is operated by [The Keyword Factory, LLC](#) of Ocean City, NJ ©2007 | [Contact This Web Site](#)

Anonymous Communication

- Not easy to use and administer
- Most rely on a majority of entities being trusted
- Susceptible to collusion among some subsets of entities
- Susceptible to some types of traffic analysis
- Scalability
- Ease of Adaptation



Privacy Enhancing Technology

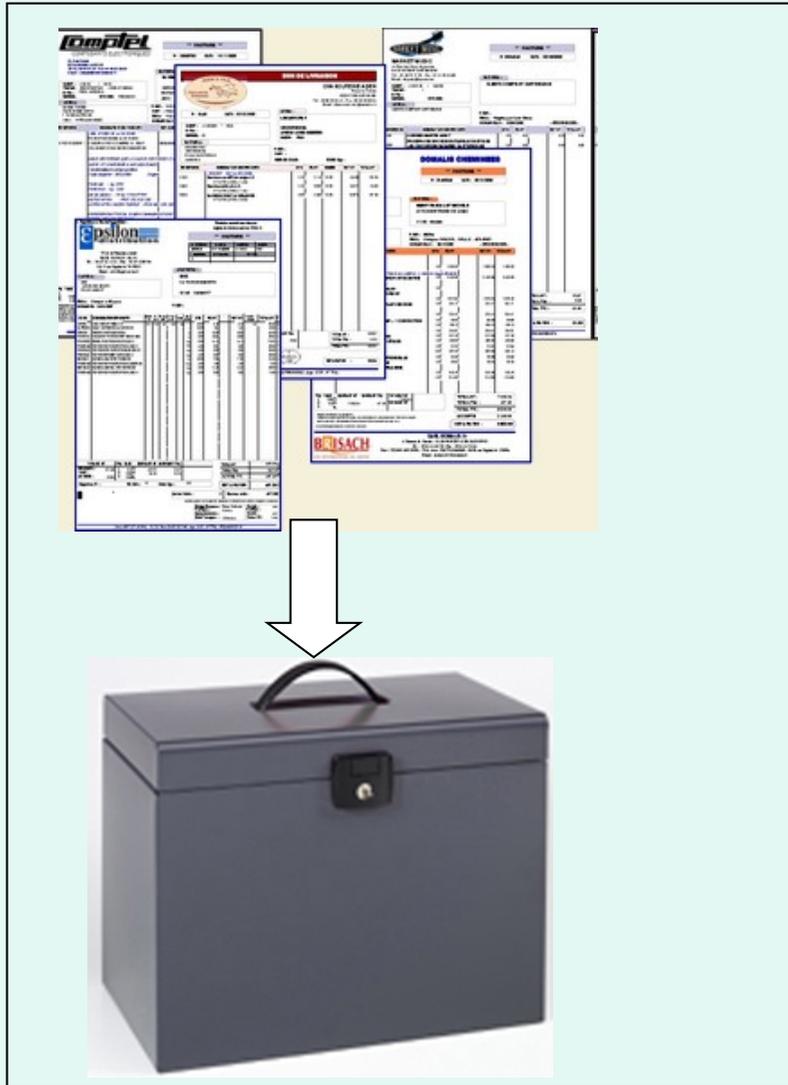
Personal Data Servers

@

SMIS.INRIA



Paper Based Personal Data

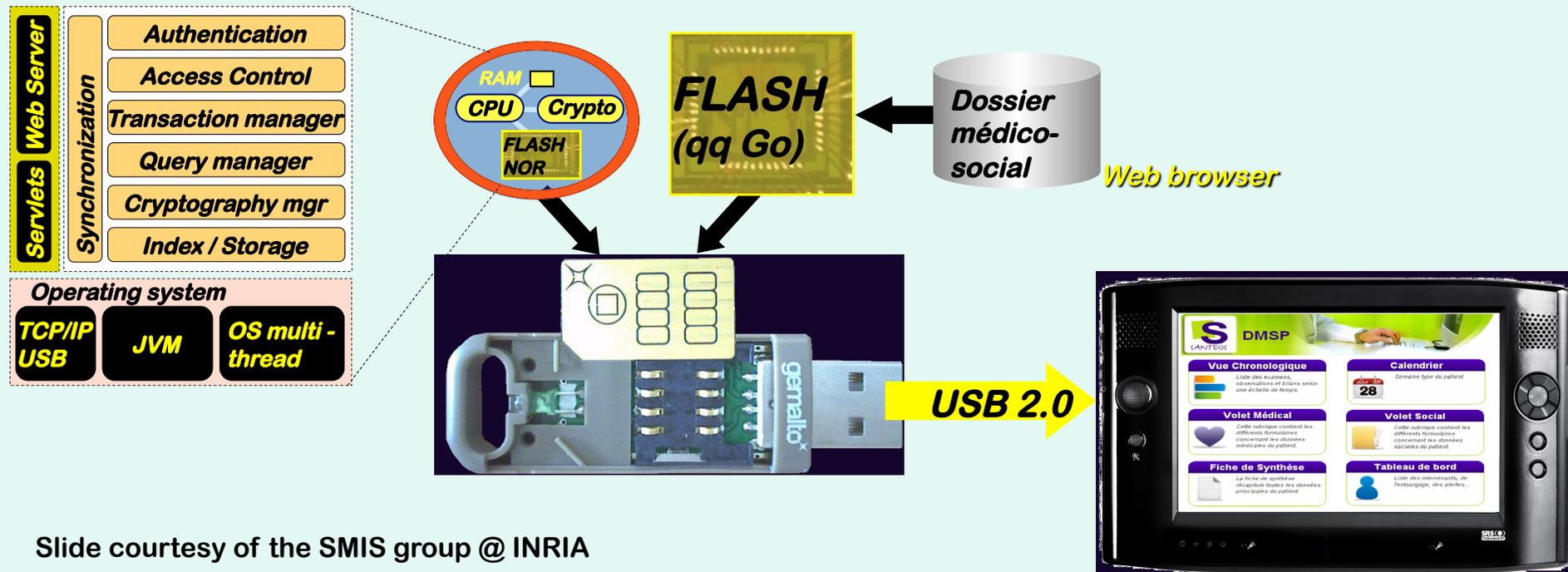


- Yesterday
 - Many paper based personal data
 - Invoices, bank, salary form, ...
 - Diplomas, official forms, ...
 - Health folder, insurance, ...
- Today
 - More and more electronic versions
 - e-invoice, e-health, e-government, ...
 - And new forms of data
 - Bookmarks, navigation history, location tracking ...
- → Need to store those data while ensuring important properties !!!
 - Availability: 24/24, 7/7, from everywhere
 - Durability
 - Query facilities
 - Security (confidentiality, controlled sharing)

Slide courtesy of the SMIS group @ INRIA

Baseline = Secure Portable Token

- Embed the traditional chain of software in secure hardware
 - Web server – Application – DBMS – Database



Slide courtesy of the SMIS group @ INRIA

Personal Data Servers (PDS)

- Store data under strong trusted hardware-guaranteed protection on SPTs
- Do not share unless absolutely needed
- Share only what is needed to be shared
- User can specify personal preferences for
 - Data sharing
 - Date usage
 - Date retention
- Ability to audit access to personal data



Data Dissemination can be Useful Too

- Personally identifiable information collected whenever a user
 - creates an account
 - submits an application
 - signs up for newsletter
 - participates in a survey
 - ...
- Data sharing and dissemination is often useful and may be done
 - to study trends or to make useful statistical inference
 - to share knowledge
 - to outsource the management of data
 -



Privacy Enhancing Technology

Microdata Disclosure Control



The Anonymity Problem

SSN	Name	DOB	Sex	ZIP	Disease
123456789	W. Carter	04/12/67	F	80542	<i>hypertension</i>
234567891	P. Jack	04/21/67	F	80541	<i>obesity</i>
345678912	B. Robert	09/27/63	M	80535	<i>chest pain</i>
456789123	D. Young	03/13/63	M	80539	<i>obesity</i>
567891234	J. Lin	09/27/63	M	80539	<i>hypertension</i>
678912345	K. Martin	03/18/64	F	80538	<i>short breath</i>
789123456	F. Clark	10/22/64	F	80539	<i>short breath</i>
891234567	J. Young	04/21/69	F	80549	<i>chest pain</i>
912345678	R. Smith	04/22/69	F	80541	<i>short breath</i>

Name	DOB	Address	Sex	ZIP
...
J. Young	4/21/69	600 Welker Av. Mead, CO	F	80549
...

Privacy breach: J. Young who lives at 600 Welker Av., Mead, CO suffers from chest pain.



Preserving Privacy: k-Anonymity

- The released data should be indistinguishably related to no less than a certain number, k , of respondents
- The respondents must be indistinguishable with respect to a set of attributes (quasi-identifiers)
- k-Anonymity requires that every combination of values of quasi-identifiers in the released table must have at least k occurrences
 - Enforced using generalization and suppression

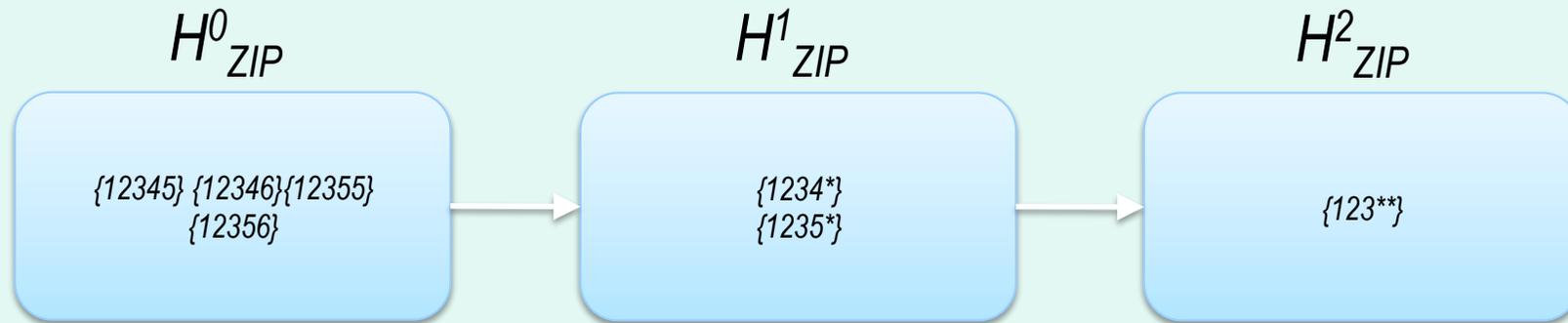


Generalization and Suppression

- Generalization: the values of a given attribute are replaced by more general values
 - ZIP codes 80521 and 80523 can be generalized to 8052*
 - Date of birth 12/04/64 and 12/10/64 can be generalized to 64 or 12/64
- Suppression: remove the information altogether
 - Suppression reduces the amount of generalization necessary to satisfy the k-anonymity requirement



Domain Generalization Hierarchy

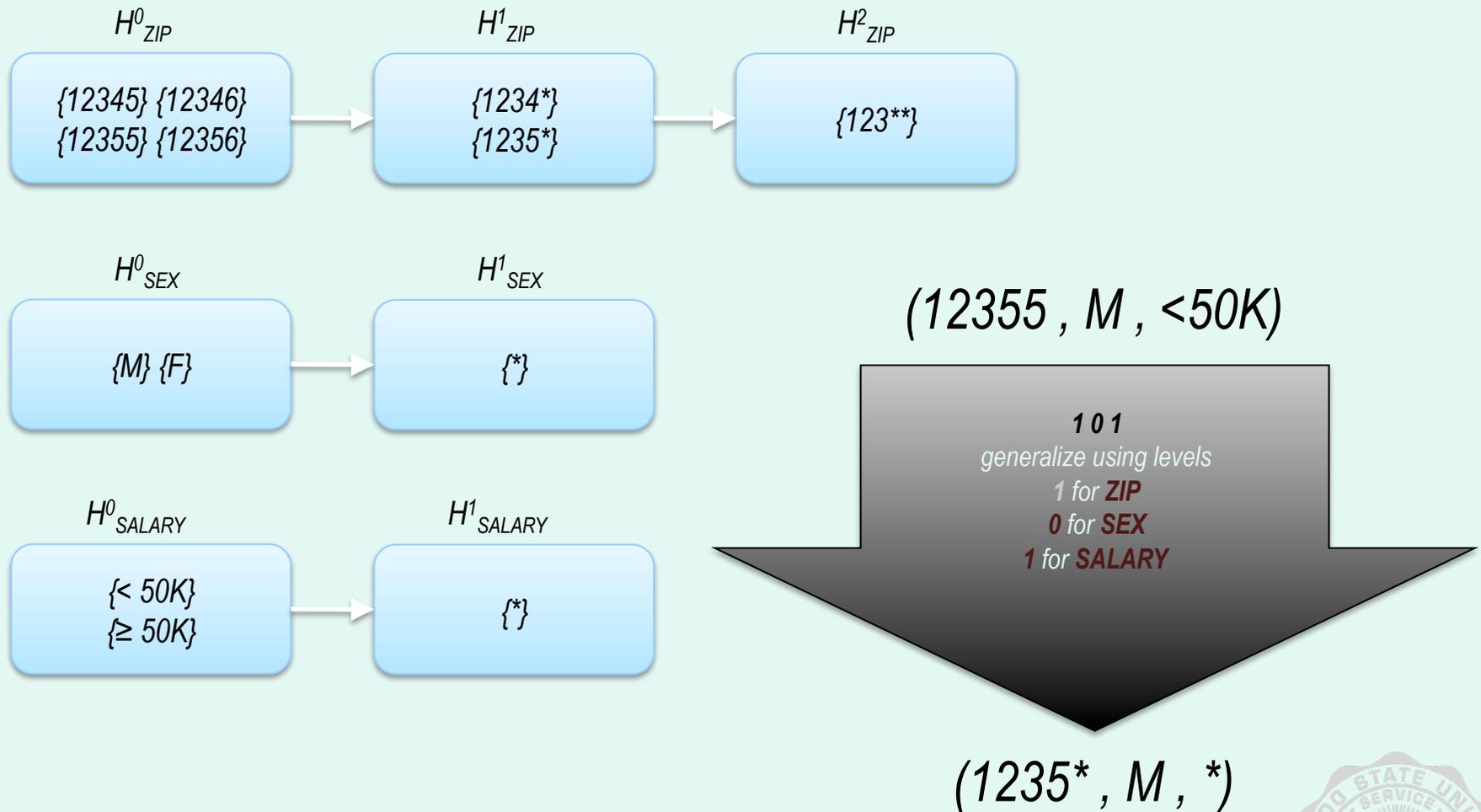


0 full specialization
full generalization

H generalization level
attribute name



Anonymizing a Tuple



Privacy by k -Anonymity

SSN	Name	DOB	Sex	ZIP	Disease
123456789	W. Carter	04/12/67	F	80542	<i>hypertension</i>
234567891	P. Jack	04/21/67	F	80541	<i>obesity</i>
345678912	R. Robert	09/27/63	M	80535	<i>chest pain</i>
456789123	D. Young	03/13/63	M	80539	<i>obesity</i>
567891234	J. Lin	09/27/63	M	80539	<i>hypertension</i>
678912345	K. Martin	03/18/64	F	80538	<i>short breath</i>
789123456	F. Clark	10/22/64	F	80539	<i>short breath</i>
891234567	J. Young	04/21/69	F	80549	
912345678	R. Smith	04/22/69	F	80541	

Generalization: group attribute (quasi-identifier) values into larger domains

SSN	Name	DOB	Sex	ZIP	Disease
		67	F	8054*	<i>hypertension</i>
		67	F	8054*	<i>obesity</i>
		63	M	8053*	<i>chest pain</i>
		63	M	8053*	<i>obesity</i>
		63	M	8053*	<i>hypertension</i>
		64	F	8053*	<i>short breath</i>
		64	F	8053*	<i>short breath</i>
		69	F	8054*	<i>chest pain</i>
		69	F	8054*	<i>short breath</i>

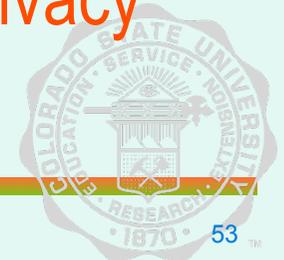
equivalence class

k -Anonymity: size of every equivalence class is at least k

2-anonymous

Other Models of Microdata Disclosure Control

- Other models are proposed around the privacy issues identified by k-anonymity
 - l-diversity and t-closeness
 - Mondrian multidimensional k-anonymity
 - k-type anonymizations
 - (α, k) -anonymity, p-sensitive k-anonymity, (k, l) -anonymity
 - Anatomy, personalized privacy, skyline privacy
- All existing anonymity models are minimalistic view models
 - privacy of a table is characterized by the minimum privacy level of all individuals



Privacy Research @ Colorado State University



Major Research Initiatives

- Optimal microdata disclosure with focus on data publisher's dilemma and biased privacy
- Identifying trustworthy data recipients
- Location privacy models and techniques
- Network trace data anonymization
- Privacy preserving protocols
 - Trust negotiation
 - E-commerce
 - E-voting



Optimal Microdata Disclosure

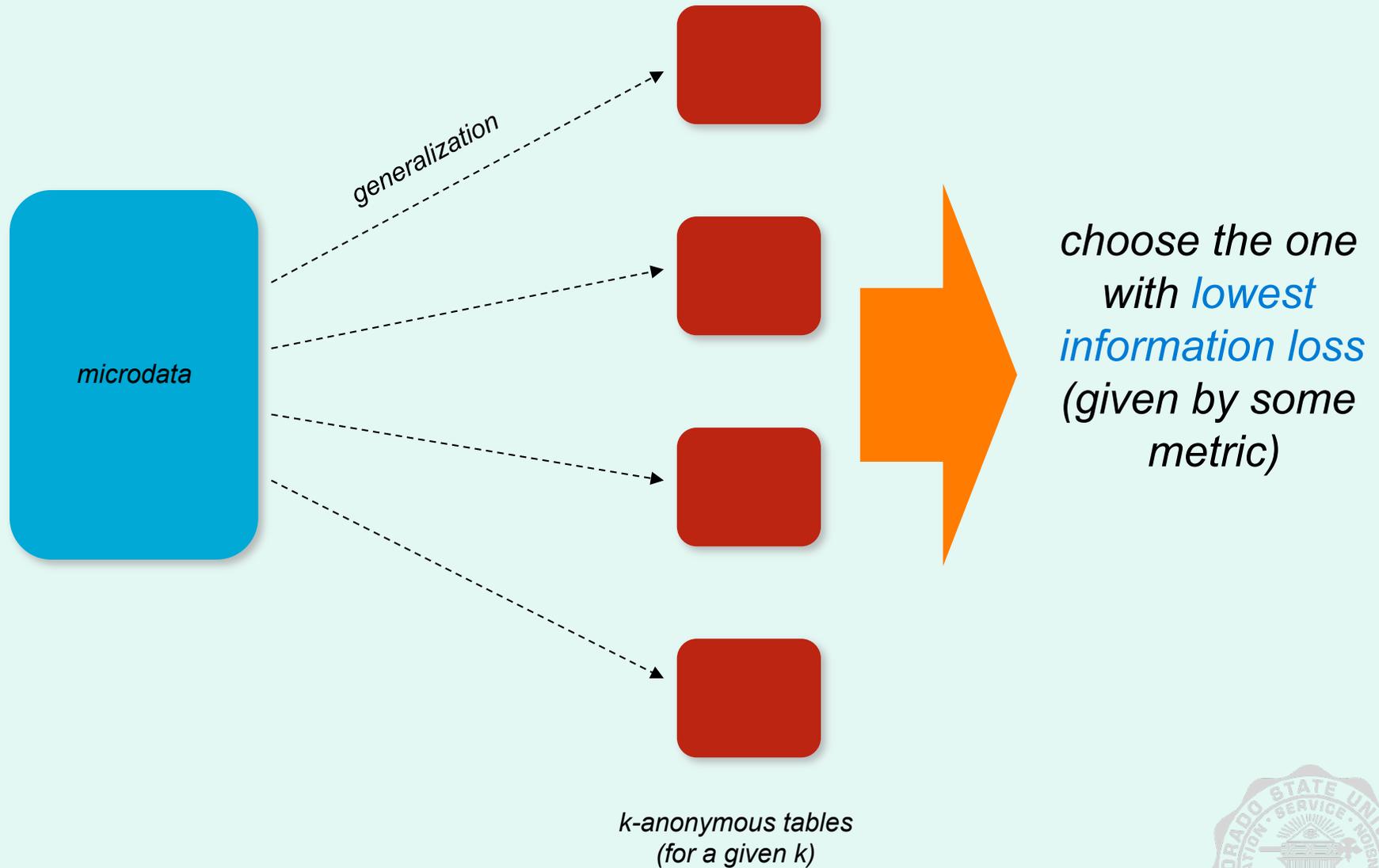


Too Much Sanitization

- May reduce the quality of the data to such extent that it may not be useful anymore
- What is too much?
 - Need to assess the degree of data disclosure
 - Need to assess the quality of data resulting from disclosure control



Preserving Data Utility



Problem – Data Publisher’s Dilemma

- A data publisher must weigh in the the risk of publicly disseminated information against the statistical utility of the content
 - How to decide what a good value of k is?
 - How to assure that higher k values or lower information loss is not possible in the neighborhood of a chosen value?



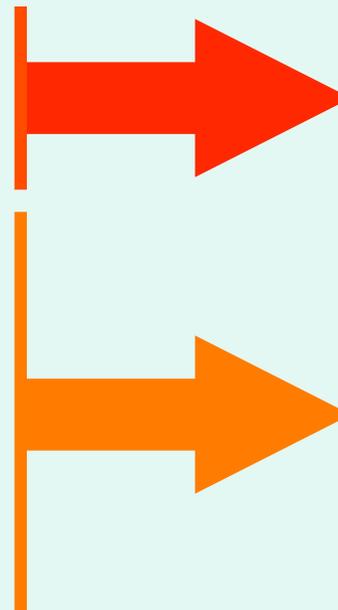
Problem – Biased Privacy

- k-anonymity only specifies a minimum privacy level present for all individuals in the microdata
- Individual privacy levels can be very different for different individuals

Probability of breach

Race	DOB	Sex	ZIP
asian	64	F	805**
asian	64	F	805**
asian	64	F	805**
asian	63	M	805**
asian	63	M	805**
black	64	F	805**
black	64	F	805**
white	64	F	805**
white	64	F	805**

2-anonymized table



1/3

1/2



Current Research Focus

- Multi-objective analysis
 - to resolve the data publisher's dilemma
- Quantification of anonymization bias
 - bias may be infused to cater to personal privacy requirements
- Fair comparison of anonymization techniques in the presence of bias
- Alternative characterization of privacy
 - privacy from an individualistic viewpoint
- Optimization framework for alternative privacy models

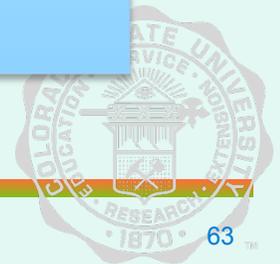
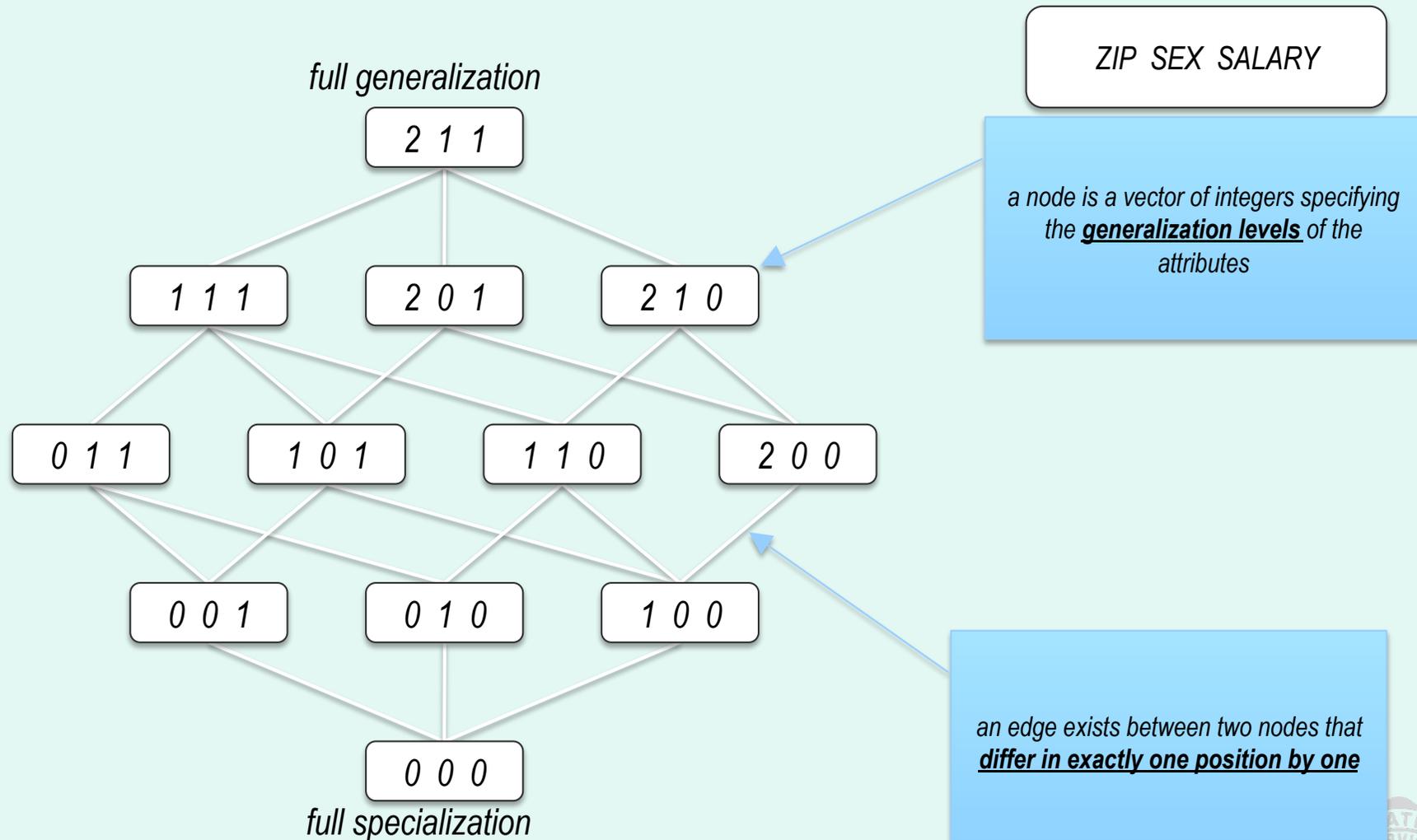
Most Recent Work

- Identify Pareto-optimal generalizations and report to data publisher for trade-off analysis

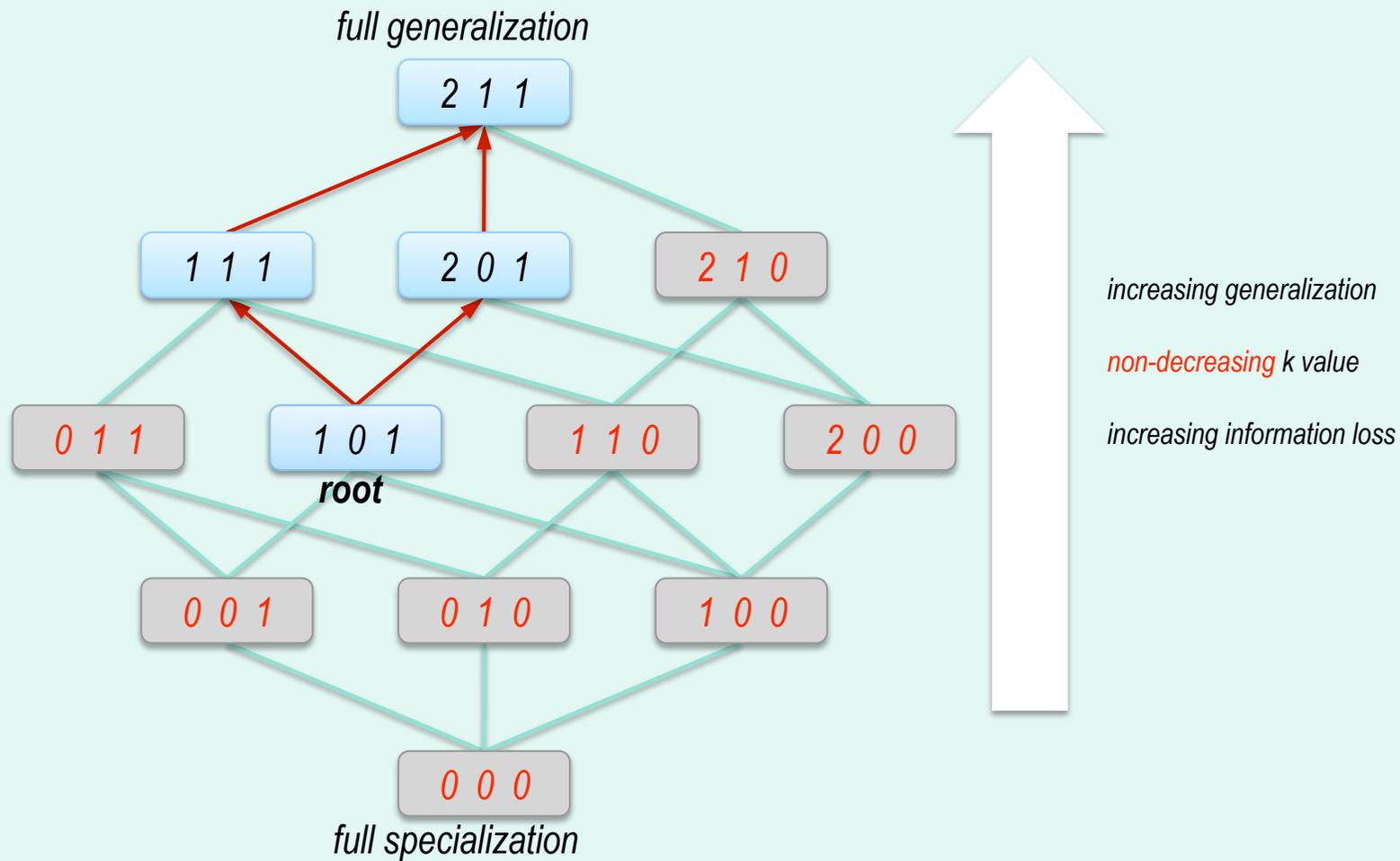
**Data publisher gets optimal k-value – information loss pairs.
Can now decide which one to choose**



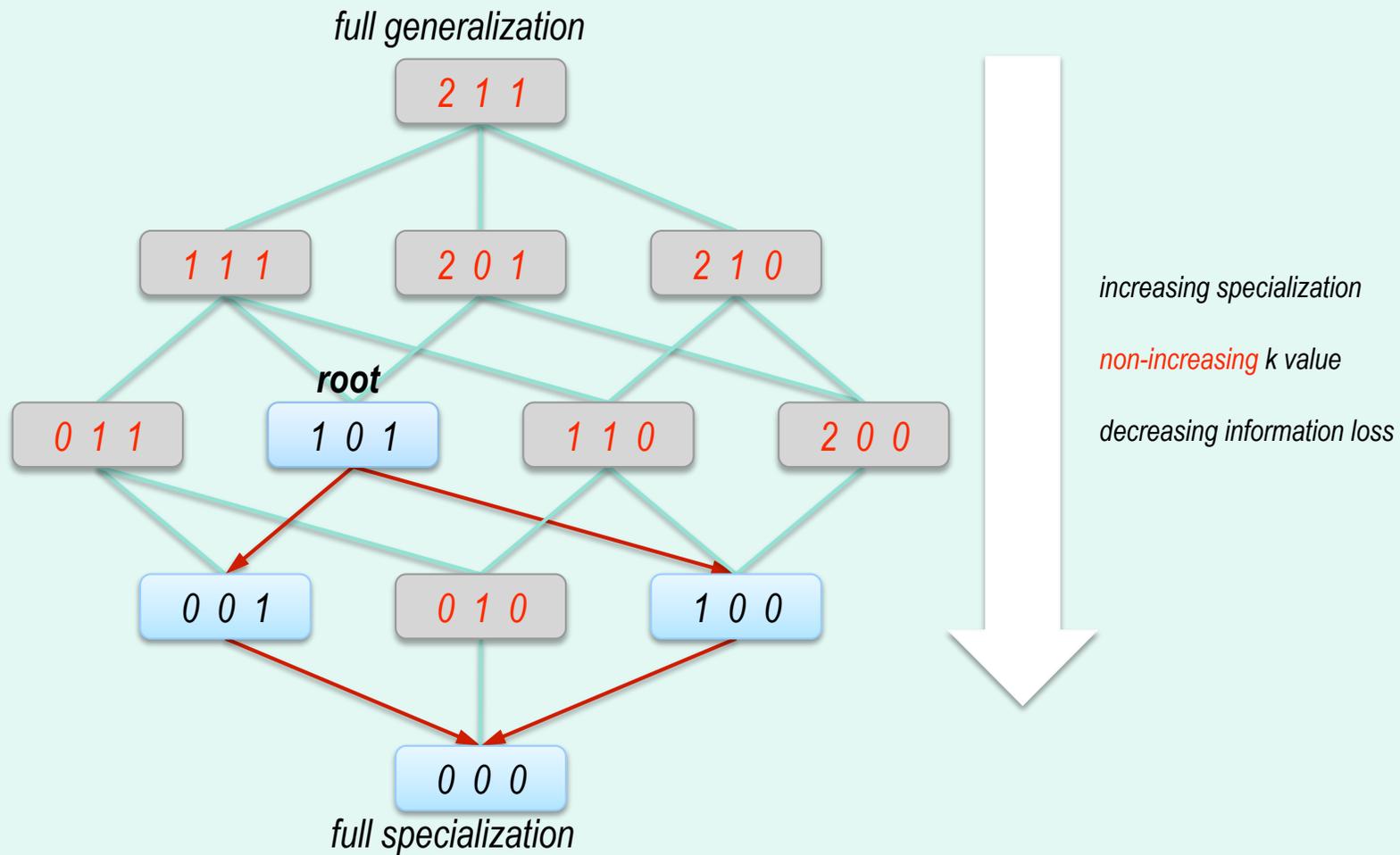
Domain Hierarchy Lattice



Generalization Graph



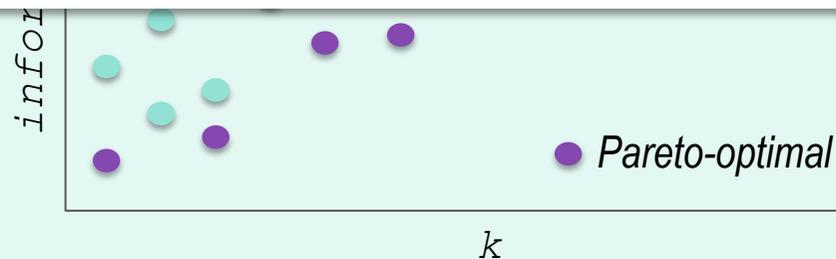
Specialization Graph



Pareto-Optimal Node in Generalization Graph

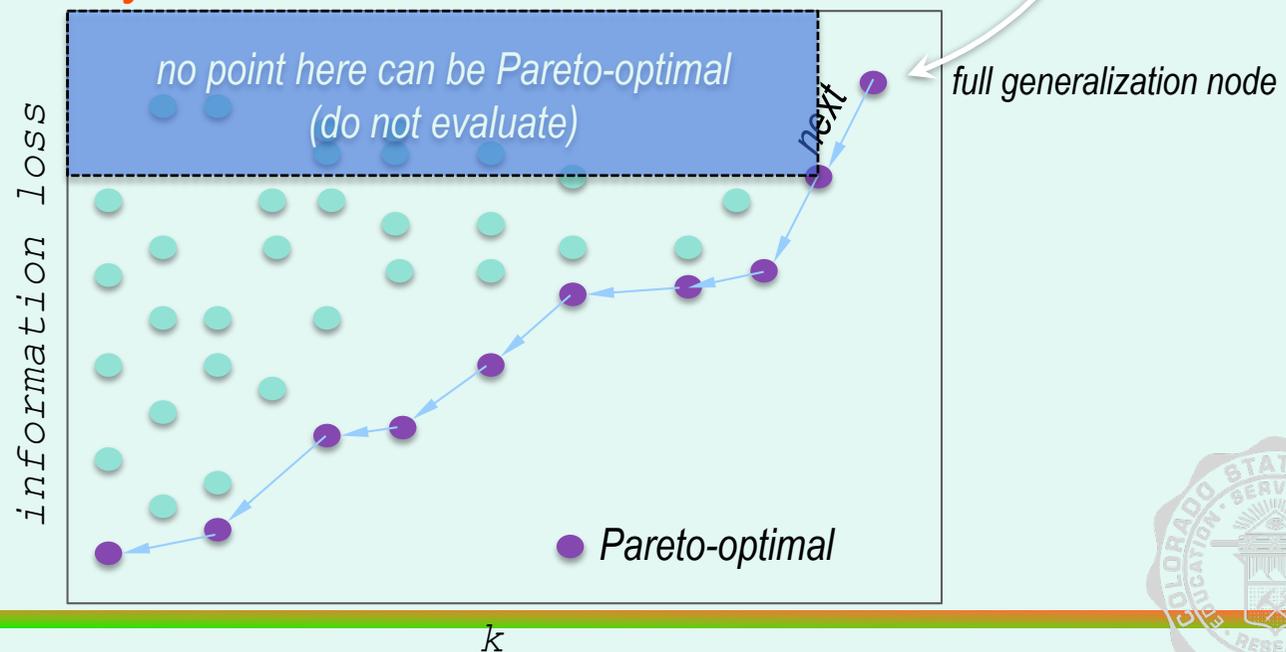
- Node N is Pareto-optimal iff there is no other node M such that
 - $k_M \geq k_N$ and $loss_M < loss_N$, or

Identify the Pareto-optimal nodes in a domain hierarchy lattice without evaluating (computing k and $loss$) every node



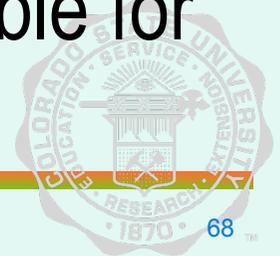
POkA

- **Pareto-Optimal k-Anonymization**
 - start from a known Pareto-optimal node
 - prune nodes that cannot be Pareto-optimal
 - move to the *next* Pareto-optimal node
 - repeat from newly found node



Identifying Trustworthy Data Recipients

- Pareto optimal anonymization produces a set of optimal privacy level, information loss pairs
- No guarantees that data recipients are not malicious and hence misuse data
- Evaluate trustworthiness of data recipients to handle data properly
 - Previous experience with data recipient
 - Properties of data recipient
 - Recommendation for data recipient
- Use specific privacy level (from optimal set) suitable for recipient



Conclusions



So Where Are We?

- Privacy survey indicates concern among Internet users
 - Increasingly people say they are concerned about online privacy (80-90% of Net users)
 - 27% of Net users have abandoned online shopping carts due to privacy concerns
 - 64% of Net users decided not to use a web site or make an online purchase due to privacy concerns
 - 34% of Net users who do not buy online would buy online if they didn't have privacy concerns
- Improved privacy protection is factor most likely to persuade more users and previous non-Net users to go online



So Where Are We?

- Often users are left with little choice but to accede
 - However, user can benefit from conscious decision
 - Other times there are tools to help user (at least partially)
 - User should know what these tools can or cannot do
- More research needed in privacy enhancing technologies



Thank You

THANK YOU



Privacy Research @ CSU

Data Anonymization for Network Traces



Use of Public Trace*

	SIG 06	IMC 06	SIG 07	IMC 07
Total papers	37	34	35	38
Used a traffic trace	9	15	10	15
Used a public trace	2	1	6	1
Used a private trace	8	14	6	14

*Source: Jelena Mirkovic, *Privacy-Safe Network Trace Sharing via Secure Queries*, NDS '08.



Trace Data Requirements

- Pseudonym Consistency: useful for traffic matrix estimation, connection characterization, etc.
- Header Information: required in analyzing the effects of packet loss and reordering in TCP dynamics
- Transport Protocol: useful for studying round trip times, reassembly and fragmentation
- Port Numbers: protocol classification schemes



Sensitive Information

- Infrastructure: topology, capacities, hardware, etc.
- Participation: no. of customers, volume of traffic, web server hits, etc.
- Identity: IP address
- Data: payloads



Fundamental Difference with Microdata Disclosure Control

- A tuple in a microdata relate to a single individual
- Sensitive information are certain attributes that are part of the data itself
- Anonymity models quantify privacy of an individual
- Preliminary attempts to quantify loss
- A tuple in a trace is just a part of a bigger communication sequence
- Sensitive information is also inferential, derivable by combining information in the attributes
- No privacy model yet
- No privacy quantification yet
- No quantification of information loss



Attacks on Sanitized Traces

- Web page attack: identify web pages based on number and length of objects
- Clock skew attack: identify a host by calculating the skew between the packet sender's clock and some reference clock
- Link layer attack: identify network topology
- Clustering attack: use address clustering to detect subnets of IPs
- Behavior attack: use behavior models of popular, known servers



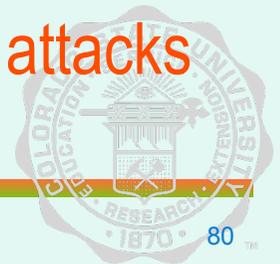
Data Anonymization Techniques Used for Traces

- Suppression: outright removal
- Fixed Transformation: constant substitution
- Variable Transformation: replace an IP address with different pseudonym values based upon application layer protocol
- Typed Transformation: prefix-preserving address anonymization



Techniques Used (cont'd)

- Share data with only **trusted parties** - legal binding (PREDICT model)
 - Who to trust and how much too trust
- Do not publish data; instead publish an access portal to the data
 - Access data using a query language
 - Access is restricted by a privacy policy implemented as part of the language interpreter
 - Publisher's can modify the policy : balance privacy and utility trade-off according to needs
 - Usefulness of the data is limited by the capabilities of the query language
 - Too much freedom in the language can lead to inference attacks in unknown ways



Our Research in Trace Data Anonymization

- Characterize privacy levels
 - A binary approach is not sufficient
 - Introduce ambiguity in attacker inference
- Is there a way to quantify the information content of a trace?
 - Data usefulness classification
 - Levels of anonymization: the more you do, the more you lose
 - But remember, we need a “one for all” anonymization; multiple versions may be dangerous
- Develop policy model for trace data dissemination
 - Integrate trust into policy model



Grand Vision

- A trace anonymization tool
 - Query the user to determine requirements
 - Determine anonymization possibilities
 - Estimate value of anonymized trace data
 - Maximize utility of anonymized trace data to user

