

Better Control of Your Data on the Web

Sid Stamm

<sid@mozilla.com>



PRIVACY IS HOT.

JULY 15, 2011 10:13 AM PDT

Appeals court: TSA must rethink airport body scans

by Declan McCullagh

Print E-mail

Recommend 369

Tweet 124

+1 32

Share

110 comments

The Transportation Security Agency violated federal law when installing **controversial full-body scanners** in U.S. airports without following proper procedures, a federal appeals court ruled today.

The D.C. Circuit Court of Appeals in Washington, D.C., rejected arguments from the Obama administration that the TSA was exempt from laws requiring federal agencies to file public and seek comments.

"It is clear that by producing an image of the unclothed passenger, (a full-body) scanner intrudes upon his personal privacy in a way a magnetometer does not," Judge Douglas Ginsburg for the three-judge panel wrote.

Ginsburg said he would not order TSA to immediately remove the scanners **air travelers last fall**—but instead instructed "the agency to study the issue."



Hacking into voicemail is easy, experts say

By Byron Acohido, USA TODAY

Updated 7/19/2011 1:48 PM

Comment 41

Recommend 111

Tweet 20



Reprints & Permissions

Three giant U.S. cellphone service providers do not require consumers to use voice mailbox PIN codes, making their customers vulnerable to the kind of hacks fueling the British tabloids scandal, security and privacy experts say.



AT&T, T-Mobile and Sprint allow subscribers to access voice messages without entering a Personal Identification Number.

This practice makes it trivial for an intruder to fully access the voice mailbox associated with any valid phone number, using a tried-and-true technique dubbed "caller ID spoofing."

The hack involves using a caller ID spoofing service, such

LIKE, REALLY HOT.

iPhone Stored Location in Test Even if Disabled

Article Video Stock Quotes Comments (80)

Email Print Save This

COMPUTERWORLD

Print Article Close Window

Smartphone apps: Is your privacy protected?

Are your apps putting your privacy at risk? We look at the dangers and solutions for Android, BlackBerry and iOS mobile platforms.

Preston Gralla, Al Sacco and Ryan Faas

July 7, 2011 (Computerworld)

Smartphone apps can do more than provide you with entertainment, information or useful services -- they can also invade your privacy.


Apps can trace your Web habits, look into your contact list, make phone calls without your knowledge, track your location, examine your files and more. They can also automatically send information such as location data to mobile ad networks.

In addition, apps can gather the phone number and the unique ID number of each type of phone: the Unique Device Identifier (UDID) on the iPhone, the International Mobile Equipment Identity (IMEI) number on the BlackBerry, and (depending on the make) the IMEI or the Mobile Equipment Identifier (MEID) on an Android phone.

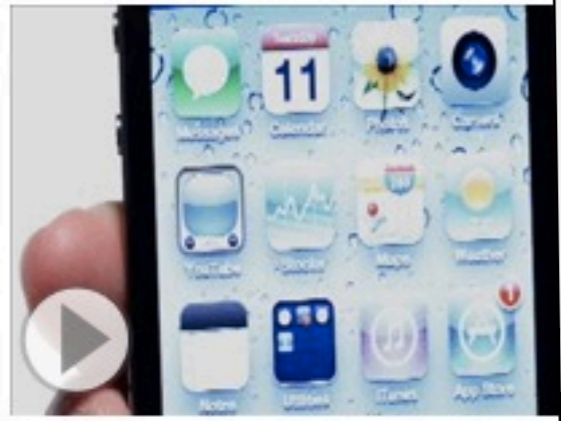
TECH BRIEFCASE

NEW APP

Search, store, and share IT white papers from across



By JENNIFER VALENTINO-DEVR
Apple Inc.'s iPhone is collecting and storing location data even if location services are turned off, according to a test conducted by researchers at the University of California, San Diego.
The location data appear to be collected even if location services are turned off on the user's phone and don't appear to be deleted when the phone is restarted, according to a request for comment.



LIKE,
I'M-NOT-EVEN-KIDDING
HOT.

Sites Feed Personal Details To New Tracking Industry

By JULIA ANGIN and TOM MCGINTY

The largest U.S. websites are installing new and intrusive consumer-tracking computers of people visiting their sites—in so Wall Street Journal investigation has found.



On the Web, Children Face Intensive Tracking

the Web's Cutting Edge, Anonymity in Name Only

'Like' Button Follows Web Users

By AMIR EFRATI

Internet users tap Facebook Inc.'s "Like" and Twitter Inc.'s "Tweet" buttons to let their makers collect data about the websites people are visiting.



Getty Images

Facebook and other sites say they don't use the tools to track users.

These so-called social media widgets appear alongside products on websites visited those sites even though a study done for The Wall Street Journal

These widgets are popular on the past year. Facebook and Twitter are the most-visited websites in the world, Google Inc. appears to be

The widgets, which are used to help websites track user behavior

What They Know About You

By JENNIFER VALENTINO-DEVRIES

A few online marketers will show you what they know about you – or think they know.

Google Inc., Microsoft Corp., Yahoo Inc. and others have created "preference managers" that let you see, and change, the interests they've assigned to you based on your browsing behavior. The companies acted partly in response to concerns about the privacy of the people they're tracking.



Google's foray into face recognition raises privacy concerns

Newly acquired PittPatt software could add facial recognition elements to Google+, YouTube, image searches

CBC News Posted: Jul 26, 2011 3:40 PM ET | Last Updated: Jul 26,

ANALYSIS



Dan M. Spark

profile. algorithm also cre

Eric Schmidt and I have at common: we both find facial software creepy.

In an onstage interview at

Facebook's Privacy Malfunction Exposed Your Private Videos To All Your Friends

JULY 25, 2011 8:19 AM TRAVIS WILSON 1 COMMENT

Like Be the first of your friends to like this.

Online-privacy tools fail to prevent tracking, study warns

BY MIKE SWIFT, MCCLATCHY-TRIBUNE NEWS SERVICE JULY 22, 2011

SAN JOSE, Calif. - A new study by Stanford University researchers has found many online advertising companies continue to follow people's Web activity even after users believe they have opted out of tracking.

The preliminary research has sparked renewed calls from privacy groups and Congress for a do-not-track law to allow people to opt out of tracking, like the do-not-call list that limits telemarketers.

While some online advertisers acknowledged the problem, an industry trade group criticized the study by "a Stanford graduate student" and said self-regulation by the industry was better than a new law.

"I think industry self-regulation is a joke," shot back U.S. Rep. Jackie Speier, D-Calif, who has proposed legislation allowing the Federal Trade Commission to regulate online tracking. "It's precisely why we need the FTC to regulate them. For those who say, 'Privacy, get over it,' I absolutely reject that."

Stanford's research looked at 65 online advertising companies, including big companies such as Google, Yahoo, Microsoft and AOL and smaller, lesser-known companies such as x+1, eXelate and BlueKai. It found that half the companies continued tracking even after consumers opted out. In online

er Facebook privacy [Tweet](#) 2
osed. Not that it matters much that our videos
e revealed to those friends we did not share
r a little over a week, and showed your friends
description, and the people that were tagged
ed. Trying to click on the video on resulted in
facebook or is not visible due to privacy

nd in a video, and they ask why? Or as
a video description didn't show anything
ne awkward questions: "So, why can't I see
?"

by glitch corrected, a new commitment on
acted. This has happen too many times, and

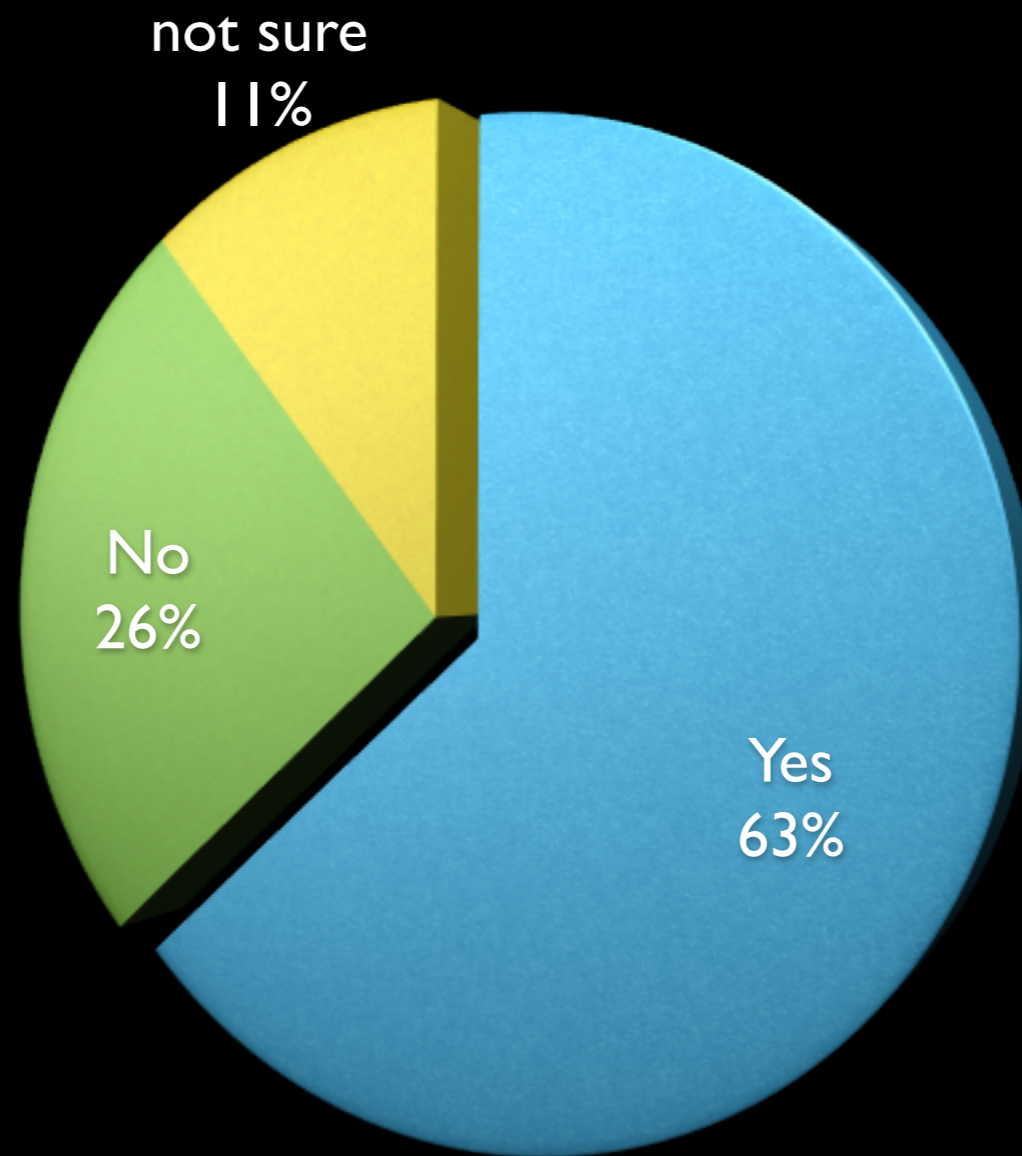


I'm gonna go hide.

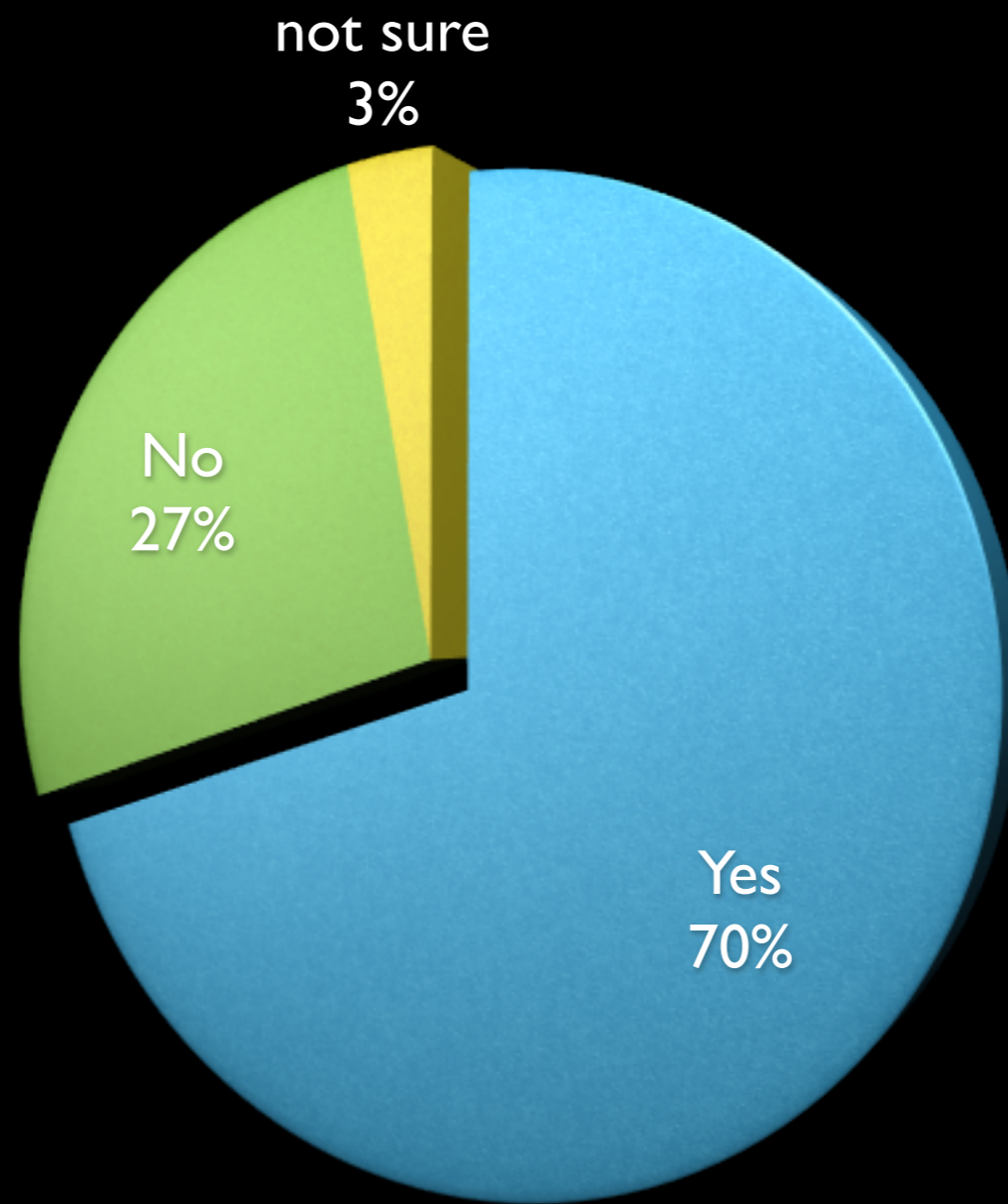
LOCAL SNOOPS



Private Browsing Mode

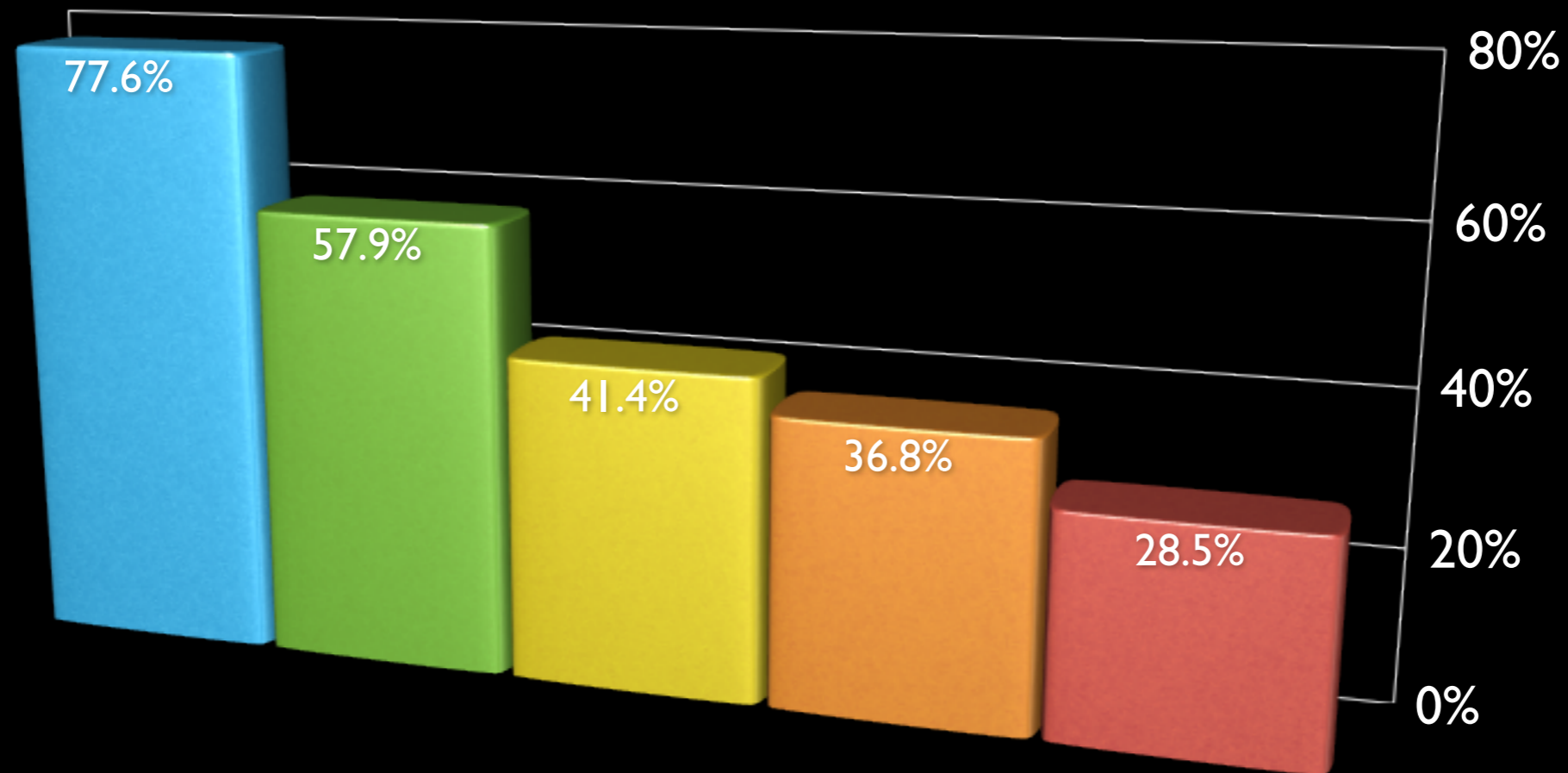


Have you heard of private browsing mode?



Have you ever used private
browsing mode?

- I don't want my browser history to record where I've been
- I don't want cookies from a website on my computer
- I share a computer with others and I don't want them to see what I've been doing
- I don't want the owners of the site to know how I got there
- I don't want my Internet Service Provider to have a record of the sites I've visited



Why do you use private browsing mode?

EAVESDROPPING

But SSL is broken. :(



FINGERPRINTING

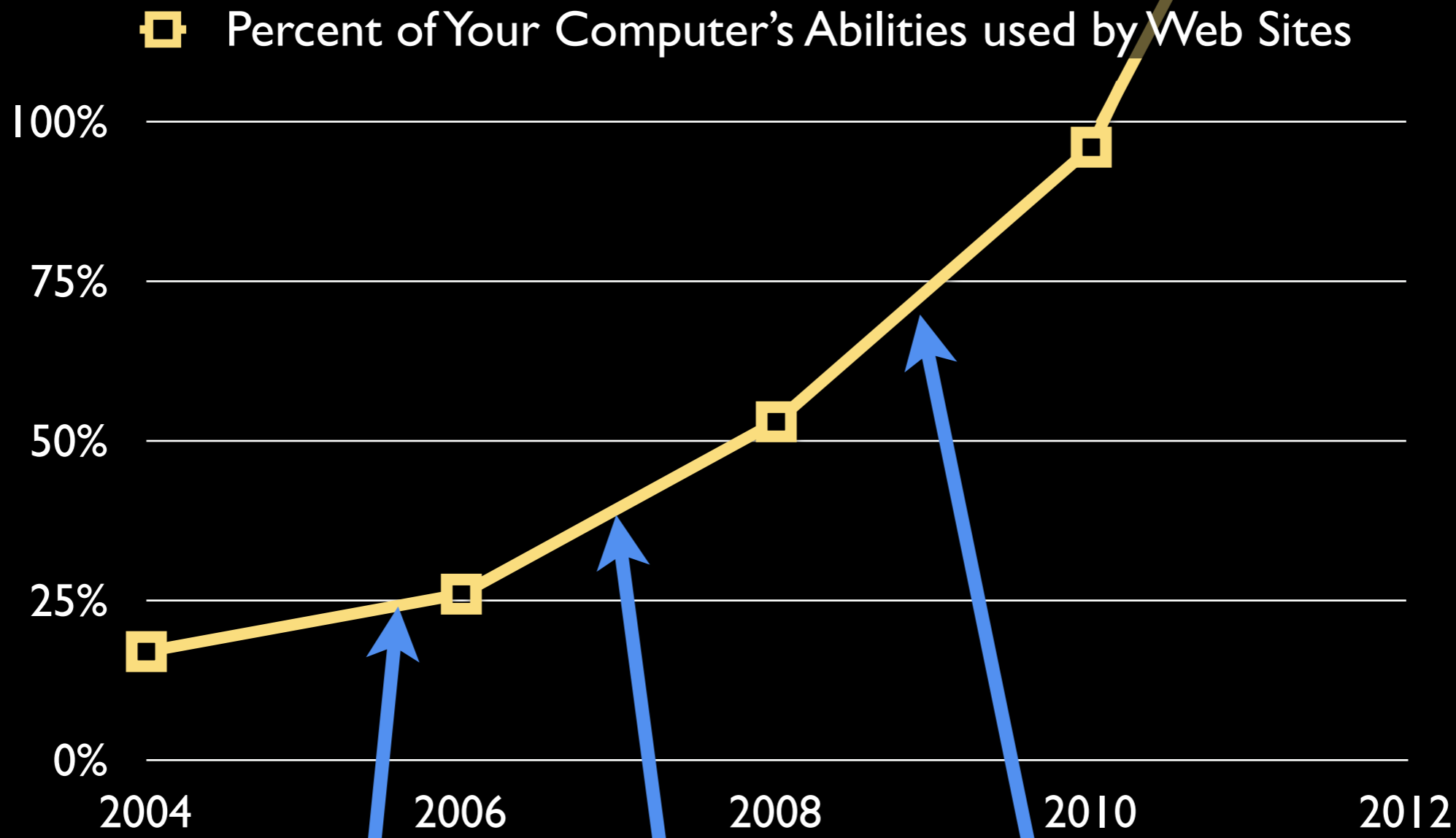


A research project of the **Electronic Frontier Foundation**

Panoptick

How Unique — and Trackable — Is Your Browser?

CSS History Sniffing



eBay

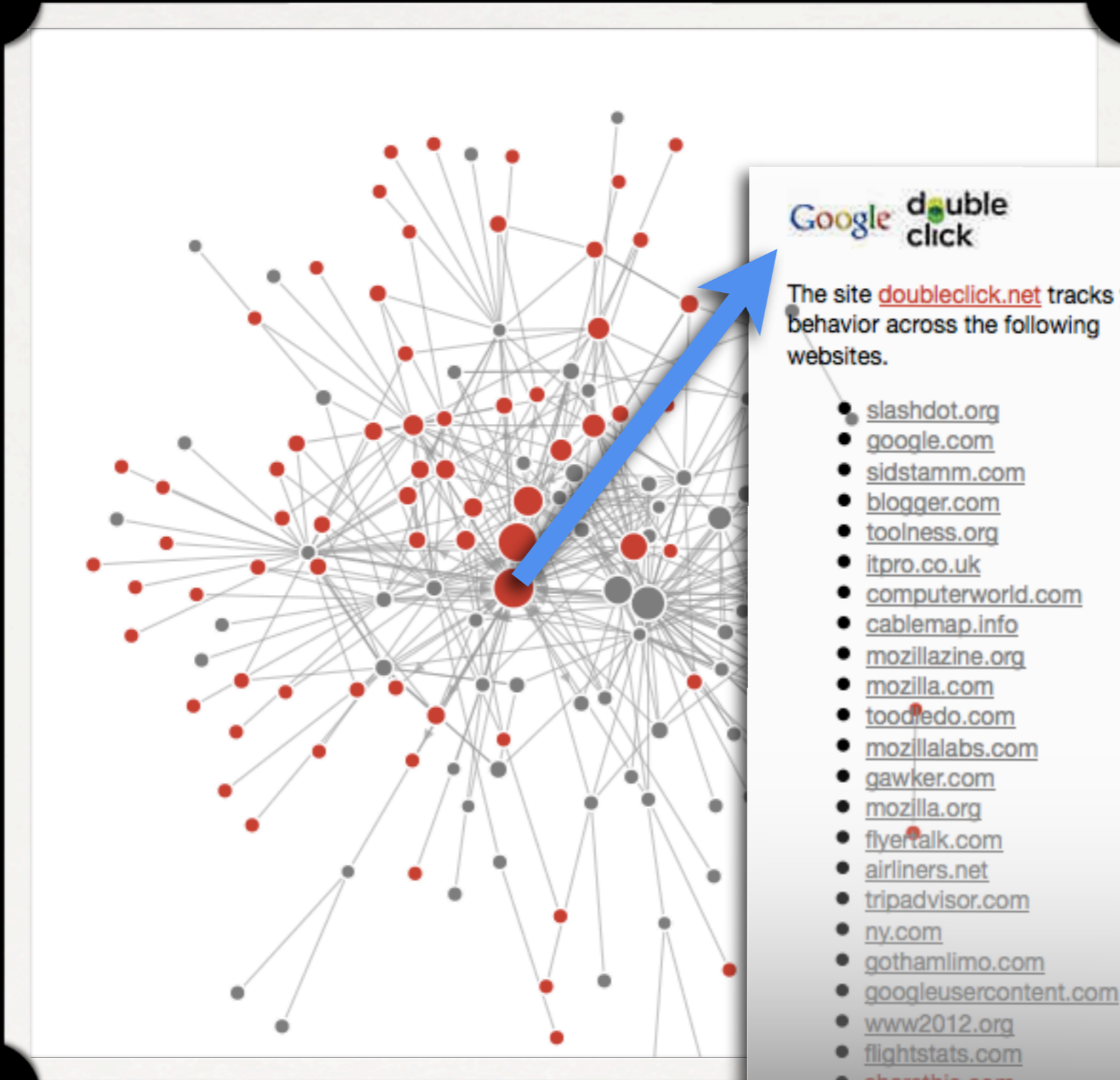
YouTube

Google Docs

Nintendo Emulator

TRACKING

[[live demo... I hope]]



Google double click

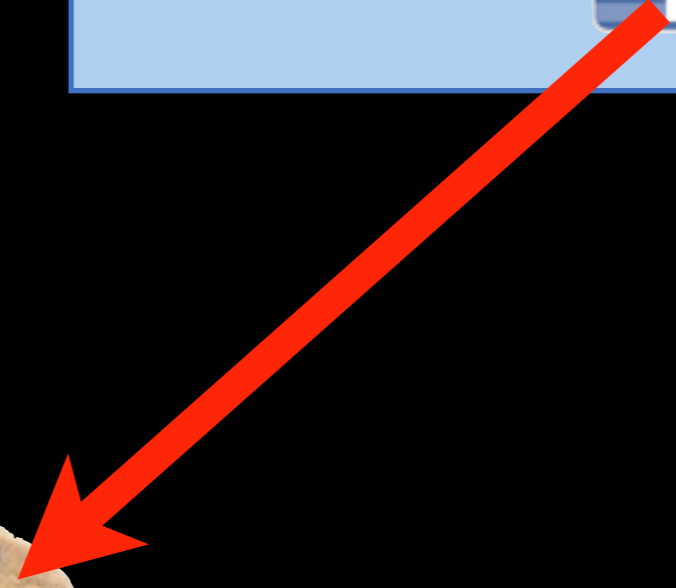
The site doubleclick.net tracks your behavior across the following websites.

- slashdot.org
- google.com
- sidstamm.com
- blogger.com
- toolness.org
- itpro.co.uk
- computerworld.com
- cablemap.info
- mozillazine.org
- mozilla.com
- toodledo.com
- mozillalabs.com
- gawker.com
- mozilla.org
- flyertalk.com
- airliners.net
- tripadvisor.com
- ny.com
- gothamlimo.com
- googleusercontent.com
- www2012.org
- flightstats.com
- sharethis.com
- nytimes.com
- ifkiat.com
- airportterminalmaps.com
- visitingdc.com
- turn.com
- brlio.com

Collusion: <http://collusion.toolness.org>

awesomenews.com

gamesite.com



awesomenews.com



gamesite.com



SITE HISTORY

The image shows a browser interface with a search bar at the top containing 'sidstamm.com'. Below the search bar is a list of site history entries: 'blog.sidstamm.com', 'research.sidstamm.com', and 'sidstamm.com'. The 'sidstamm.com' entry is highlighted with a blue bar. To the right of the history list is a 'Permissions for sidstamm.com' panel, which includes a '141 visits' counter and three settings: 'Store Passwords' set to 'Block', 'Share Location' set to 'Always Ask', and 'Set Cookies' set to 'Allow'. Each setting has a corresponding icon and a dropdown menu. At the bottom right of the permissions panel, there is a 'Remove' button.

sidstamm.com

blog.sidstamm.com

research.sidstamm.com

sidstamm.com

Permissions for sidstamm.com 141 visits

Store Passwords
Block
0 passwords are stored for this web site.

Share Location
Always Ask

Set Cookies
Allow
0 cookies are set for this web site. Remove

sidstamm.com

- blog.sidstamm.com
- research.sidstamm.com
- sidstamm.com**

Permissions for **sidstamm.com** 141 visits [Forget About This Site](#)



Store Passwords

Block

0 passwords are stored for this web site. [Manage Passwords...](#)



Share Location

Always Ask



Set Cookies

Allow

0 cookies are set for this web site. [Remove Cookies](#) [Manage Cookies...](#)



Open Pop-up Windows

Block



Maintain Offline Storage

Always Ask



You are connected to
paypal.com
which is run by
Paypal Inc.
San Jose CA, US
Verified by: VeriSign, Inc.



Your connection to this web site is encrypted to prevent eavesdropping.

[More Information...](#)

Lets get more paranoid
for a minute...

DATA TRADING

PRIVACY PERCEPTION GAP





DNT





DNT

???



???



HOW TO STAY GROUNDED



I. No Surprises





(this is a surprise)

2. Real Choice





Security Warning

The information you have entered is to be sent over an unencrypted connection and could easily be read by a third party.

Are you sure you want to continue sending this information?

Alert me whenever I submit information that's not encrypted.

Cancel

Continue

(this is not a real choice)

3. Sensible Defaults




Settings

[General](#) [Accounts and Import](#) [Labels](#) [Filters](#) [Forwarding and POP/IMAP](#) [Chat](#) [Web Clips](#) [Labs](#) [Offline](#)

[Keyboard Shortcuts](#) [Themes](#) **Buzz**

Display following lists: Show the list of people I'm following and the list of people following me on my public Google profile [Learn more](#)
 Do not show these lists on my public Google profile.

Buzz choices: Show Google Buzz in Gmail
 Do not show Google Buzz in Gmail
This will only hide the Buzz tab in Gmail. You'll still be able to use Buzz on your phone. Your connected sites will continue to create new posts in Google Buzz.

 **Disable Google Buzz**
This will disable Google Buzz in Gmail and delete your Google Profile and Buzz posts. It will also disconnect any connected sites and unfollow you from anyone you are following.

Save Changes

Cancel

(allowing by default is mean)

4. Limited Data



“Buy a toaster and you're asked for a postcode. Buy a television and you're asked for a home address - ostensibly to validate a warranty. Buy a mobile phone service and you're likely to have your driver's licence photocopied.”

<http://www.smh.com.au/money/planning/id-protection-at-crisis-point-20110308-1blep.html>

(really... why?)



Firefox Sync

apitome

(5. Third Parties Too)



OPEN QUESTIONS

How does data flow
about the web?

Who traded my data?

What does this site do
with my data?

What encourages
sites to be honest?

Create More Meaning
from Less Data

Better Control of Your Data on the Web

Sid Stamm

<sid@mozilla.com>



[this slide intentionally left blank]