Better Control of Your Data on the Web

Sid Stamm
<sid@mozilla.com>
PRIVACY IS HOT.
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 said.

Ginsburg said he would not order TSA to immediately cease using the scanners, but instead instructed "the agency to seek an order providing interim relief that adheres to the law."...

Hacking into voicemail is easy, experts say

By Byron Acohido, USA TODAY

Updated 7/19/2011 1:48 PM

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 as...
LIKE, REALLY HOT.
By JENNIFER VALENTINO-DEVEAU

Apple Inc.'s iPhone is collecting and storing location data even when the feature is turned off, according to a test conducted by the company.

The location data appear to be collected without user approval and don't appear to be related to specific apps that are trying to use the user's phone and don't appear to be designed to respond to a request for comment.

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 also 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. Personal information that apps gather...
LIKE,
I’M-NOT-EVEN-KIDDING
HOT.
Sites Feed Personal Details To New Tracking Industry

By JULIA ANGWIN and TOM MCGINTY

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

You

Websites

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, but let their makers collect data about the websites people are visiting.

These so-called social widgets, alongside products that let users visit those sites even when they're not there, are gaining in popularity.

These widgets are popular with developers and the past year. Facebook Inc. and Twitter Inc. appear to be the most visited websites on the web.

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

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 users 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, 2011 4:11 PM ET

ANALYSIS

Eric Schmidt and I have at least one thing in common: we both find facial recognition software creepy.

In an onstage interview at a conference in Washington last week, Schmidt said: "I think that it's not just the obvious abuse of privac----" He broke off and pointed to the members of the audience, who were seated in rows of chairs. "It's the subtle abuse of privacy," he said. "The ability to use this data in ways that you might not have predicted might be quite chilling."

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

July 25, 2011 8:19 AM  |  1 COMMENT

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
I’m gonna go hide.
LOCAL SNOOPS
Private Browsing Mode
Have you heard of private browsing mode?

- Yes: 63%
- No: 26%
- Not sure: 11%
Have you ever used private browsing mode?

- Yes: 70%
- No: 27%
- Not sure: 3%
Why do you use private browsing mode?

- I don't want my browser history to record where I've been: 77.6%
- I don't want cookies from a website on my computer: 57.9%
- I share a computer with others and I don't want them to see what I've been doing: 41.4%
- I don't want the owners of the site to know how I got there: 36.8%
- I don't want my Internet Service Provider to have a record of the sites I've visited: 28.5%
But SSL is broken. :(
FINGERPRINTING
Panopticlick
How Unique — and Trackable — Is Your Browser?
Percent of Your Computer’s Abilities used by Web Sites

- YouTube
- Google Docs
- eBay
- Nintendo Emulator
TRACKING
[[ live demo... I hope ]]
Collusion: http://collusion.toolness.org
SITE HISTORY
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.
Let's get more paranoid for a minute...
DATA TRADING
PRIVACY PERCEPTION GAP
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

<table>
<thead>
<tr>
<th>General</th>
<th>Accounts and Import</th>
<th>Labels</th>
<th>Filters</th>
<th>Forwarding and POP/IMAP</th>
<th>Chat</th>
<th>Web Clips</th>
<th>Labs</th>
<th>Offline</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Themes</strong></td>
<td><strong>Buzz</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### 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.

### Buttons

- 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.”


(really... why?)
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
[ this slide intentionally left blank ]