



## iOS 9.3.3: Apple Device Update Can Code Vulnerability, Reports Say

The update will fix a software bug in Apple products that allows hackers to access devices via an image in a text message, outlets reported, citing Cisco Talos, a research and security group.

Technology

## iPhone bug allows hackers to steal passwords with just a text message – update now to protect yourself



The flaw has been fixed for users who update their software. CREDIT: BLOOMBERG

# iOS 9.3.3 from July 18

2

- [According to researcher Tyler Bohan at cybersecurity firm Cisco Talos](#), older versions of iOS and OS X contain an exploit that could theoretically allow a media file like a photo or video to defeat built-in software security measures and take over your device. The malformed media file could arrive as an email, iMessage, webpage, or other apps.
- For those who are curious, here's a technical explanation of the hack. The problem lies in how older versions of Apple's device software handle media. **A malformed multimedia file, like a photo sent via email or text, could trigger one of several bugs in the software's playback engine that subsequently cause it to "lose control of how it handles its memory space."** This happens when your device processes the image to create a thumbnail for you to view. From that point, unfortunately, the sky's the limit. A hacker could take over your device and access your private information.
- Typically, iOS prevents malicious code from operating outside of prescribed boundaries, but an attacker could potentially gain elevated privileges by applying secondary exploits. And Mac OS X, unlike iOS, imposes no such limitations, so an ill-meaning programmer could install unwanted apps on an infected computer, send personal information contained within it to a remote server, or commandeer it for a [denial-of-service attack](#).

# USER TRACKING AND BROWSER PRIVACY

Dr. Benjamin Livshits

# Third Party Content on SFGate



Subscribe to the weekend  
Save 40%

A Brilliant Opening at San Francisco Centre

**TIFFANY & CO.**  
LEGENDARY FOR 175 YEARS

# SFGate

Monday Sep 17, 2012 4:55 PM PT

63°F San Francisco, CA (change)  
Partly Cloudy  
Today 50/65 Tue. 54/61  
5 Day Forecast Traffic

sfgate.com Web Search by YAHOO! Businesses

Sign In | Register

Home News Sports Business Entertainment Food Living Travel Columns Shopping Cars Jobs Real Estate Index WEEKLY AD

Don't Miss: Cindy Sherman at SFMOMA | Opera with my daughter | 'Death and the Civil War' | Name 'Moneyball' sequel? | Weird wheels | Fight over Kate pics



**Entitled victims for Obama?**  
Leaked video: Romney disparages the 47% who pay no income tax.  
▪ Romney joke: Latino wannabe?



**Height of luxury living**  
SoMa high-rise, home to Joe Montana, named a top-10 residential building in world.



**Getting a peek at wildlife**  
Hidden cameras at Point Reyes capture more than 20 species - with some surprises. Photos

**Skydiver plunges to his death**  
Napa County man killed in Byron after pulling his chute.

**S.F. power plan may skirt PG&E**



Supes to consider legislation to secure a contract with Shell to provide 100 percent renewable power to San Franciscans.

**MORE NEWS**

Shaun White charged with vandalism 4:00 p.m.  
Tweeters mock mag's #MuslimRage cover 3:46 p.m.  
Are bikinis appropriate for little girls? 4:16 p.m.  
Burned bear cub moved to Idaho sanctuary 3:27 p.m.  
Homeowners assn. members face violence 3:45 p.m.  
Body found in Mission District IDd 3:30 p.m.  
Veteran 'General Hospital' actor dies 2:53 p.m.



**TIFFANY & CO.**  
LEGENDARY FOR 175 YEARS

**49ers INSIDER** DIGITAL MAGAZINE  
Hard-hitting coverage of all 49ers games  
>> Download NOW San Francisco Chronicle SFGate.com

Most Read | Most Commented | Most Emailed

# Overview



- Website creators were mostly responsible for their content themselves
- Today content is aggregated from a lot of different sources
- Third party content seems to come for free but...

There's a hidden price tag! But where?

# SFGate's Privacy Policy: the Fine Print...

.....

## **2. Web Site Usage Information**

### **(i) Cookies**

We may use "cookies" to keep, and sometimes track, information about you. Cookies are small data files that are sent to your browser or related software from a Web server when you visit it and are stored on your computer's hard drive for record keeping purposes. Cookies track where you travel on our Web Site and what you look at and purchase. They may store the information in your shopping cart, and/or your username and password. A cookie may enable us to relate your use of our Web Site to other information about you, including your Personal Information. These purposes serve to improve and personalize your experience on our Web Site.

You may occasionally get cookies from our advertisers, which is standard in the internet industry. We do not control these cookies, and these cookies are not subject to our privacy policies.

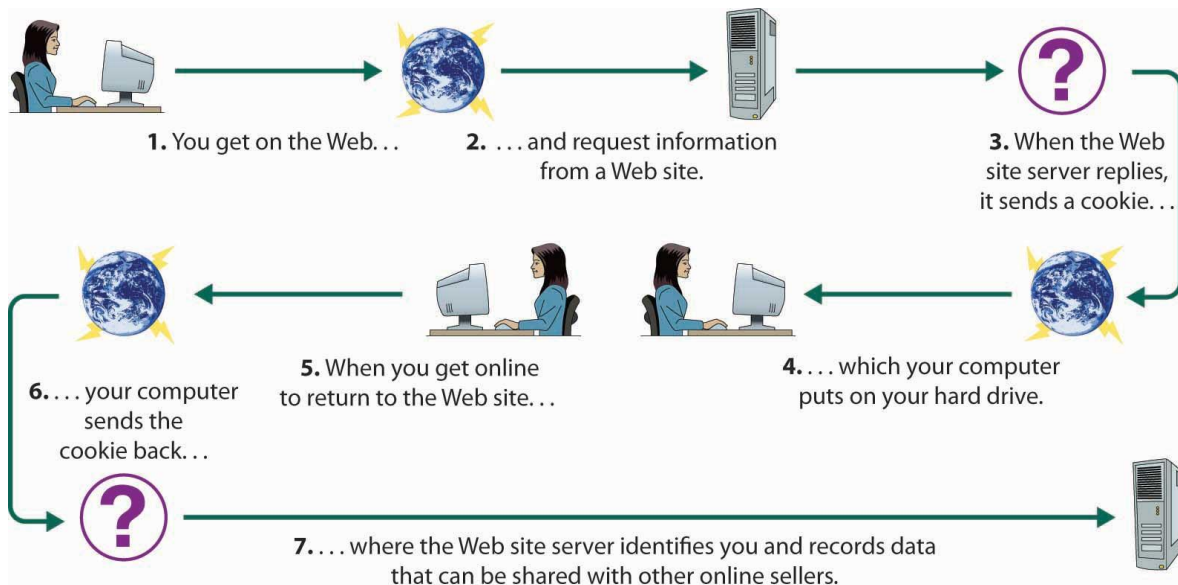
Most Web browsers can be set to inform you when a cookie has been sent to you and provide you with the opportunity to refuse that cookie. Additionally, if you have a Flash player installed on your computer, your Flash player can be set to reject or delete Flash cookies. However, refusing a cookie may, in some cases, preclude you from using, or negatively impact the display or function of, the Web Site or certain areas or features of the Web Site.



# Cookie-based Tracking

# Cookies and Privacy

- A key topic in Web application privacy in the last several years
- The majority of focus is on **cookie-based tracking**



# Lots and lots of advertising companies

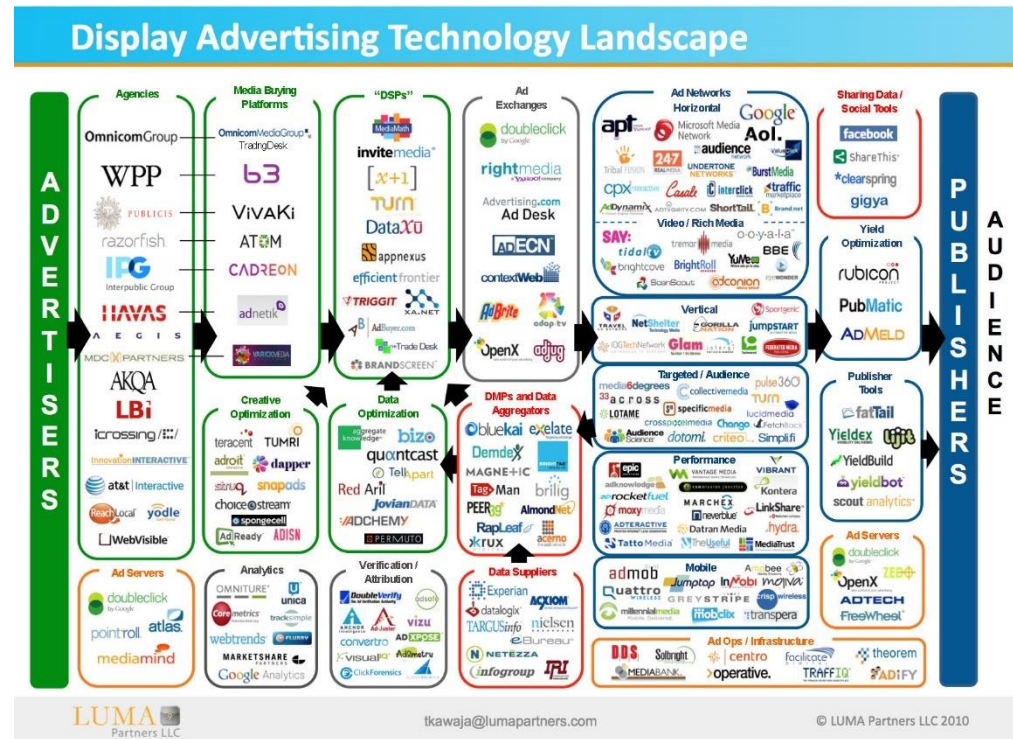
a.com

b.com

c.com

...

z.com



# Cookies on a popular news site

Breaking News and Opinion

www.huffingtonpost.com

May 12, 2012

THE HUFFINGTON POST

THE INTERNET NEWSPAPER: NEWS BLOGS VIDEO

Elements Resources Network Scripts Timeline Profiles

Session Storage

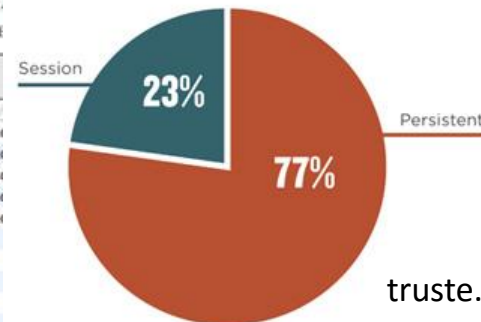
Cookies

- www.huffingtonpost.com
- ads.tw.adsonar.com
- at.atwola.com
- platform.twitter.com
- cdn.tacoda.at.atwola.com
- js.adsonar.com
- ad.yieldmanager.com
- plusone.google.com
- static.ak.facebook.com
- s-static.ak.facebook.com
- cdn.at.atwola.com
- www.facebook.com

Application Cache

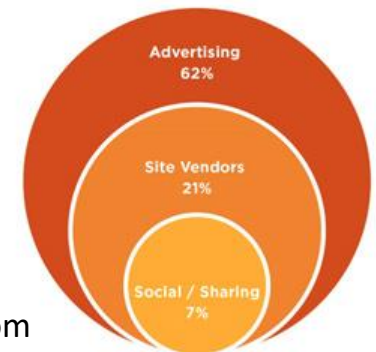
| Name     | Value                | Domain      |
|----------|----------------------|-------------|
| guest_id | XXXXXXXXXXXXXXXXXXXX | .twitter.co |
| twll     | XXXXXXXXXXXXXXXXXXXX | .twitter.co |
| __utma   | XXXXXXXXXXXXXXXXXXXX | .twitter.co |
| __utmz   | XXXXXXXXXXXXXXXXXXXX | .twitter.co |
| pid      | XXXXXXXXXXXXXXXXXXXX | .twitter.co |

Cookie Persistence



truste.com

Third Party Type



# Today, a Visit to Huffingtonpost.com results in...

DATA GATHERED SINCE  
MAR 2, 2015

YOU HAVE VISITED  
1 SITE

YOU HAVE CONNECTED V  
79 THIRD PART

All Sites

| Type        | Prefs | Website           |
|-------------|-------|-------------------|
| Third Party |       | turn.com          |
| Visited     |       | huffingtonpost.es |
| Third Party |       | tidaltv.com       |
| Third Party |       | atwola.com        |
| Third Party |       | amgdt.com         |
| Third Party |       | doubleclick.net   |
| Third Party |       | gravity.com       |
| Third Party |       | aolcdn.com        |
| Third Party |       | google.com        |

|             |                       |
|-------------|-----------------------|
| Third Party | scorecardresearch.com |
| Third Party | facebook.com          |
| Third Party | huffpost.com          |
| Third Party | googlesyndication.com |
| Third Party | twitter.com           |
| Third Party | gstatic.com           |
| Third Party | weborama.fr           |
| Third Party | grvcdn.com            |
| Third Party | 2mdn.net              |
| Third Party | stickyadstv.com       |
| Third Party | bluekai.com           |
| Third Party | 360yield.com          |

|             |                       |
|-------------|-----------------------|
| Third Party | mathtag.com           |
| Third Party | audienceiq.com        |
| Third Party | adnxs.com             |
| Third Party | pubmatic.com          |
| Third Party | contextweb.com        |
| Third Party | smartclip.net         |
| Third Party | liverail.com          |
| Third Party | demdex.net            |
| Third Party | huffingtonpost.com    |
| Third Party | epimg.net             |
| Third Party | quantserve.com        |
| Third Party | googletagservices.com |

# A fundamental underlying question

---

□ **Why profile the user?**

# Inference based on cookies

## Carrie Isaac

Based on a single click, the tracking company [x+1] placed Carrie Isaac in Nielsen's "White Picket Fences" segment.

### What They Got Right

- Young parent from Colorado Springs
- Lives on about \$50,000 a year, white collar
- Attended some college
- Shops at Wal-Mart, rents videos for her kids

### What They Got Wrong

- Doesn't speak Spanish
- Doesn't watch cable TV
- Drives a Honda Odyssey minivan, not a Nissan Frontier truck

### The Credit Cards

Based on [x+1]'s assessments, Capital One showed Ms. Isaac two cards designed for "People with Average Credit"

- The interest rate is 0% until April 2011, and then goes up to 19.8%, with no annual fee.

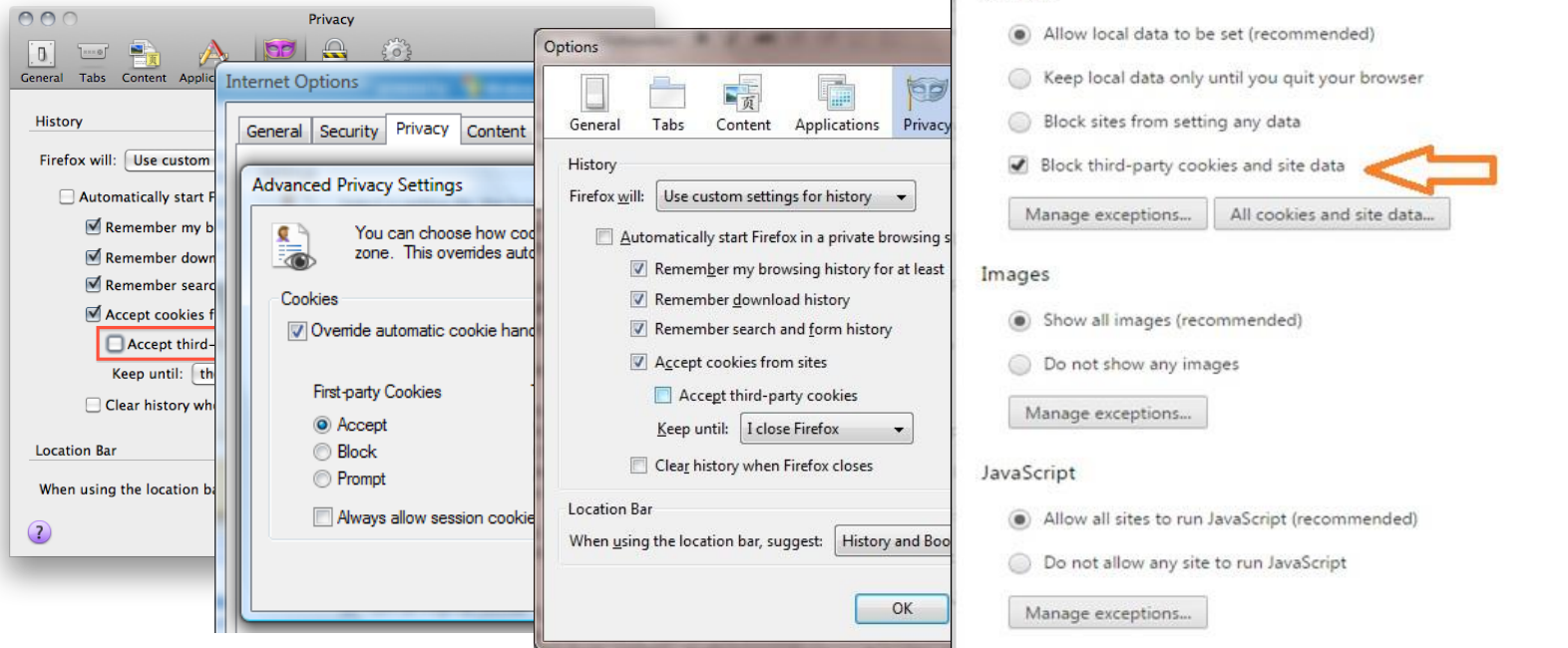
```
Referrer:
http://www.capitalone.com/creditcards/?linkid
=WWW_1009_CARD_A25A3_HOME_H1_01_T_CB1
Cookie: X1ID=CG-00000000175923535; 0179638=0;
C335690=0@0; M62795-52786=1;
ru4.uid=21310#52156694988912556#2745049666;
ru4.CAP=CHP:UMT0:EXP5:1279057272840;
ru4.1584=1#2697#0#2697=ad-2697-
0051111279057272837%7C2697%7Cpt-2697-031%7Cp1
-2697-1313%7Cad-2697-005%7Cpt-2697-031%7Con%7
C6134%7Cexperiment%7C8%7Cnone%7Ccontrol%7C126
9034887%7Cpt-2697-031%2526mountain%25255E070%
25255Ecolorado%252Bsprin%25257E%25255E0%2526a
fternoon%25255Eqwest.net%25255E518%2526%252B-
%25255E1%25255E%25255E0%2526high%25255E
%25255E5%25255E3%25255E%252B-%25260%2
5255E752%25255E%25255E0%25255E0%25255E0%2526T
2%25255EF3%25255E70%25255Eco%25255Etown%25255
E1%25255E%252B-%25255E0%25255E0%2526tue%25255
E4%25255E2%25255E4%25255E3%25255Eu%25255E%252
B-%25255E0%25255E0%2526qwest%2526midscale%252
55Esome%252Bcollege%25252Fcollege%252Bgrad%25
55E9%252632%25255E00%25255E28%25255ET2%25255
E70%25255E7%25255Enet%25255E0%25255E0%25255E0
%25255E%25255En%25255E%252B-%2
```



Ad tracking company [x+1] made predictions about users based on just one website click

(from WSJ)

# Block third-party cookies

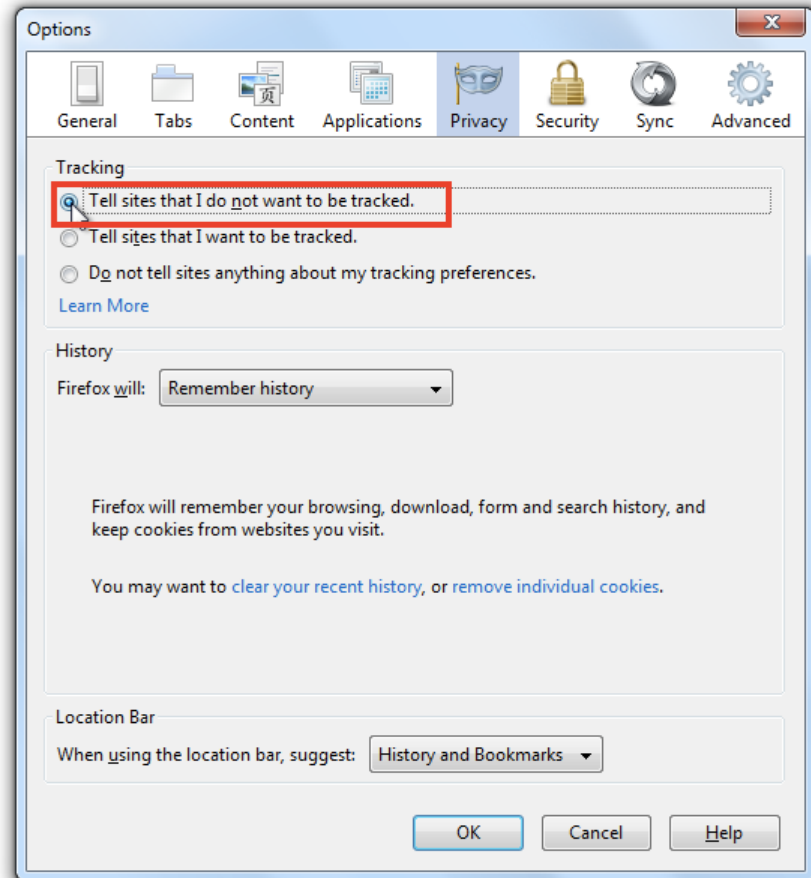
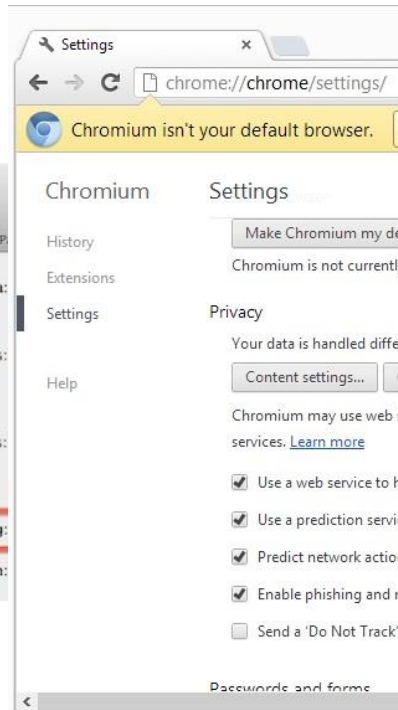
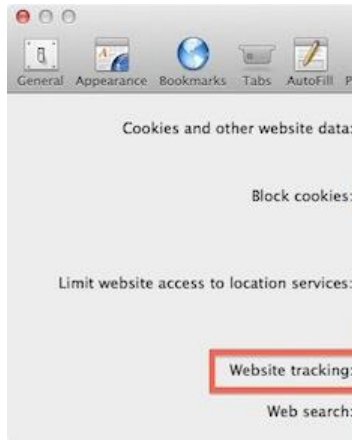


# Do-NOT-TRACK initiative

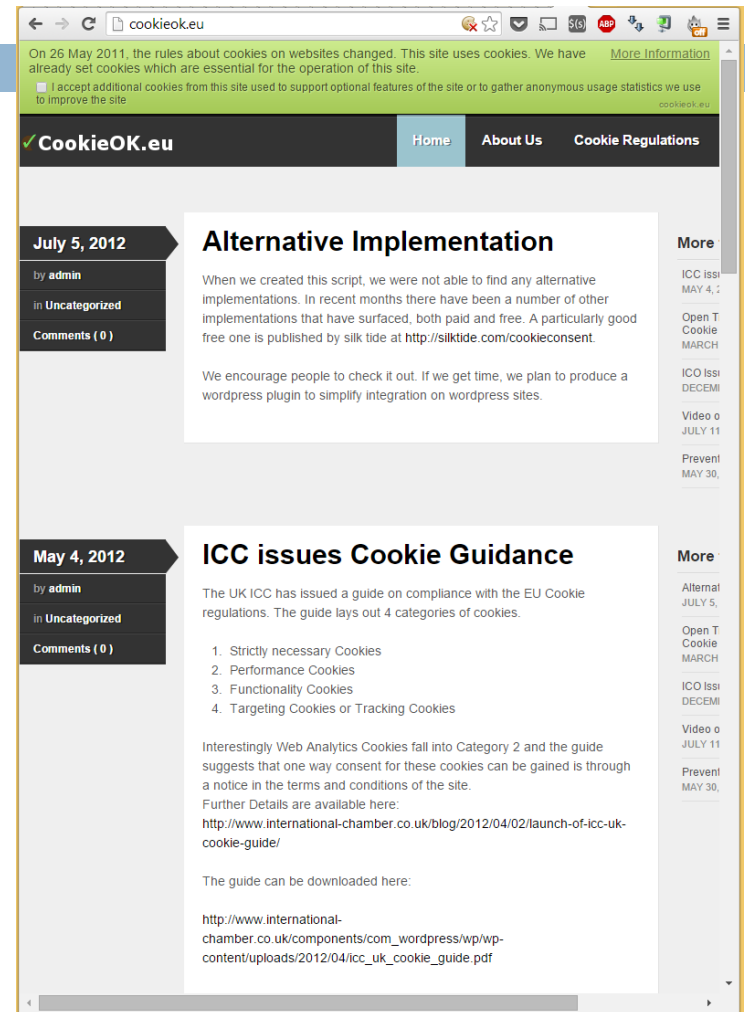
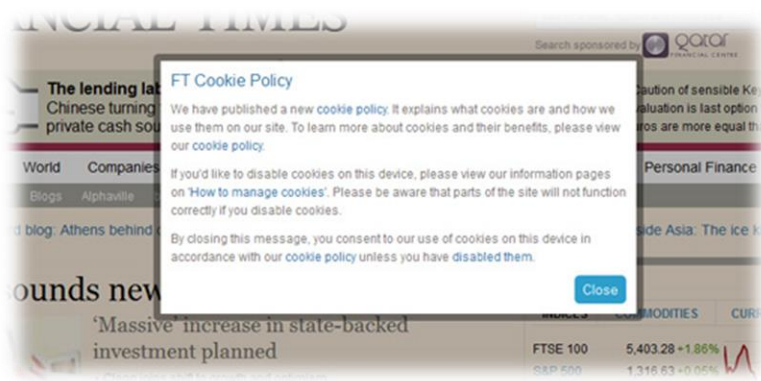
-88 AT&T

3:18 PM

85%



# EU cookie regulations



# NoT everybody is fond of the cookie law



DATA CENTRE SOFTWARE NETWORKS SECURITY BUSINESS HARDWARE SCIENCE BOOTNOTES

## Want to avoid another cookie law mess? Talk to EU bods next time

'Dear ICO, sue us ... We're sick of you and this ridiculous cookie law'



11 Sep 2012 at 08:19, OUT-LAW.COM

49 7 63

UK businesses should actively involve themselves in the debate over changes to EU law if they want to avoid problems stemming from the way those laws are drafted, an expert has advised.

Technology law specialist Luke Scanlon of Pinsent Masons, the law firm behind Out-Law.com, said that businesses can help law makers avoid putting "burdensome" requirements on them if they make their views on plans to reform EU law heard.

Scanlon was commenting after a UK software firm stripped its websites of "cookies solutions" and called on the UK's Information Commissioner's Office (ICO) to "sue" it for non-compliance with the Privacy and Electronic Communications Regulations (PECR). SilkTide created a [dedicated website](#) promoting its non-compliance where it announced that it was "tired" of the ICO and "the ridiculous cookie law".

## Europe's Web-Cookie Warnings Are a Waste, Report Says

ARTICLE

COMMENTS (2)

COOKIES EUROPEAN UNION REGULATION WEB BROWSERS

Email Print Facebook Twitter Google+ LinkedIn

By CHASE GUMMER



Jean-Claude Juncker, new president of the European Commission, has written to a colleague to urge a review of the cookie policy. — Agence France-Presse/Getty Images

Internet cookie notifications are costing European taxpayers a mint while offering netizens no real benefit, a new report by a Washington-based think tank says.

Web surfers in many European countries are greeted with banners and pop-up notifications about browser cookies when they click on a website for the first time.

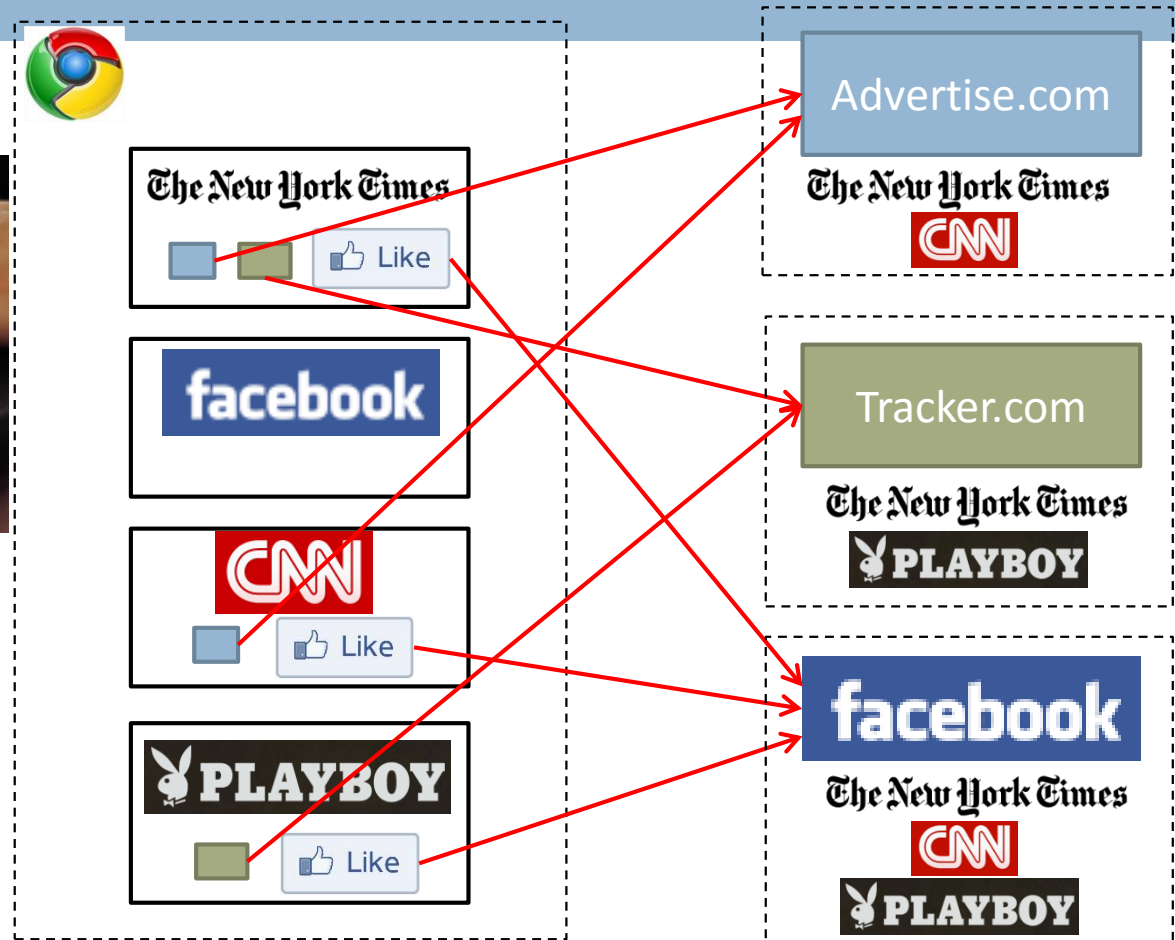
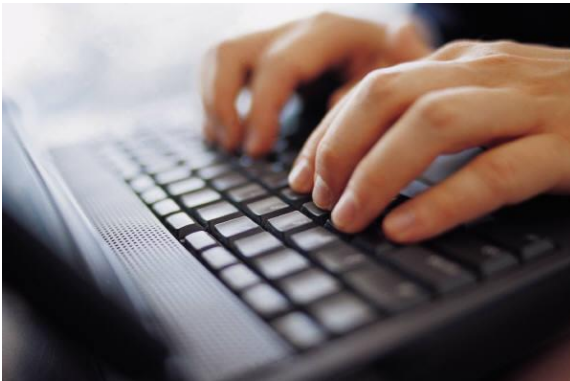
Cookies are small packets of data sent from the site to a user's browser, allowing sites to monitor user behavior on the Web, even after a person has left the site.

In 2009, the European Union sought new regulations as part of an "e-privacy" directive, seeing cookies as a potential threat to privacy, because users often don't know they're being tracked.

The regulation was supposed to be implemented into national law by the individual EU states, but only the U.K., Denmark and Estonia did so by the rollout deadline of May 26.

# Third-Party Web Tracking

18

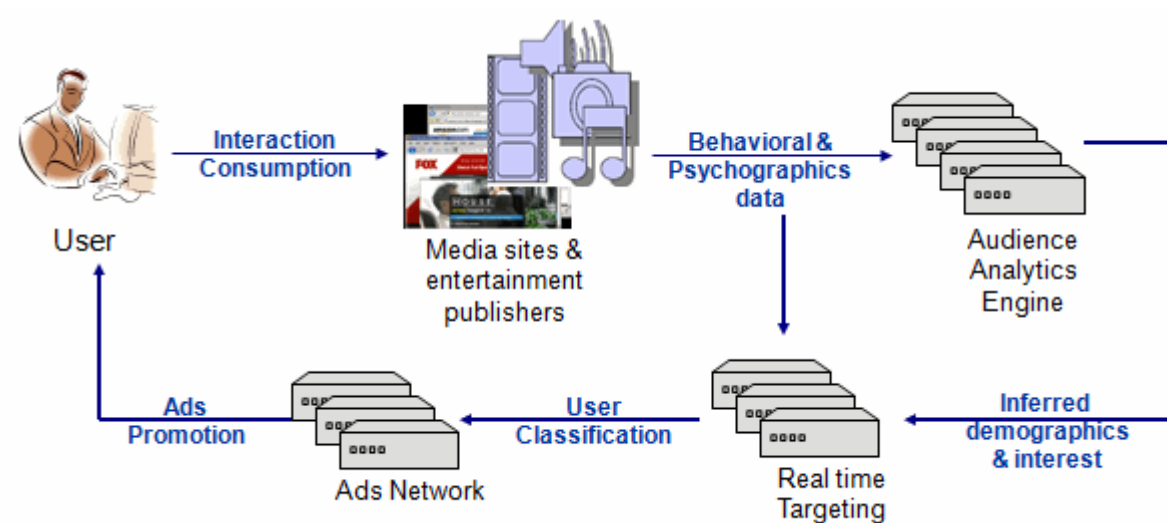


(Hypothetical tracking relationships only.)

Bigger browsing profiles  
= increased value for trackers  
= reduced privacy for users

# The Advertising Ecosystem

19

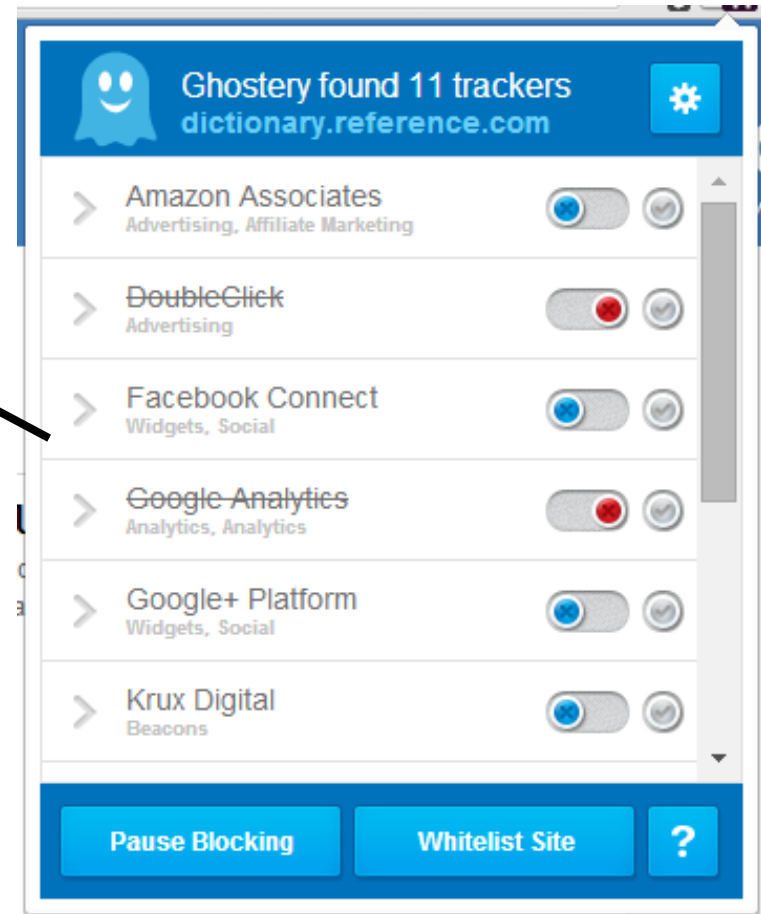


The user is “being sold” to advertisers by content companies

# Scale of Tracking

20

| Site                | Exposure Index | Trackers |
|---------------------|----------------|----------|
| dictionary.com      | Very High      | 234      |
| merriam-webster.com | High           | 131      |
| comcast.net         | High           | 151      |
| careerbuilder.com   | High           | 118      |
| photobucket.com     | High           | 127      |
| msn.com             | High           | 207      |
| answers.com         | Medium         | 120      |
| yp.com              | Medium         | 89       |
| msnbc.com           | Medium         | 117      |
| yahoo.com           | Medium         | 106      |
| aol.com             | Medium         | 133      |
| wiki.answers.com    | Medium         | 72       |
| cnn.com             | Medium         | 72       |
| about.com           | Medium         | 83       |
| cnet.com            | Medium         | 81       |
| verizonwireless.com | Medium         | 90       |
| imdb.com            | Medium         | 55       |
| live.com            | Medium         | 115      |
| att.com             | Medium         | 58       |
| walmart.com         | Medium         | 66       |
| bbc.co.uk           | Medium         | 45       |
| ebay.com            | Medium         | 42       |
| ehow.com            | Medium         | 55       |
| amazon.com          | Medium         | 38       |
| espn.com            | Medium         | 61       |



# What Do Trackers Think?

21



## Google web history

### Today

- ☐ Searched for [collecting web browsing histories](#)  
[About Google Search History - Accounts... - google.com](#)
- ☐ Searched for [collecting web histories](#)
- ☐ Searched for [collecting web histories](#)
- ☐ Searched for [what do advertisers know about me](#)  
[This Is Who Facebook Thinks You Are |... - time.com](#)  
[The Wall Street Journal Asks: What Do... - eff.org](#)  
[I'm Being Followed: How Google—and... - theatlantic.com](#)  
[Who Do Online Advertisers Think You Are?... - nytimes.com](#)
- ☐ Searched for [ghostery](#)

# Implications?

22

**Getting Different Deals Online**  
A Journal examination found online retailers adjusted prices by a shopper's location, among other factors

**Staples.com**  
SnapSafe Titan safe

HIGHER PRICE  
**\$1,199.99**

DISCOUNT PRICE  
**\$1,099.99**

DIFFERENCE:  
**9.1%**

**Homedepot.com**  
A 250-foot spool of electrical wiring



Six pricing groups, including:

|         |                     |
|---------|---------------------|
| \$70.80 | in Ashtabula, Ohio  |
| \$72.45 | in Erie, Pa.        |
| \$77.87 | in Monticello, N.Y. |

**RosettaStone.com**



**A 20% DISCOUNT**

...for buying multiple levels of German lessons, when test-shopping from the U.S. or Canada. But not from the U.K. or Argentina.

Photos: l to r: SnapSafe; Home Depot; Rosetta Stone Source: WSJ testing The Wall Street Journal

- Personalization can lead you down a road to a kind of informational determinism in which what you've clicked on in the past determines what you see next — a Web history you're doomed to repeat.
- You can get stuck in a static, ever-narrowing version of yourself — an endless you-loop

# Target Scandal

23

## How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did

+ Comment Now + Follow Comments

Every time you go shopping, you share intimate details about your consumption patterns with retailers. And many of those retailers are studying those details to figure out what you like, what you need, and which coupons are most likely to make you happy. [Target](#), for example, has figured out how to data-mine its way into your womb, to figure out whether you have a baby on the way long before you need to start buying diapers.



- In Target's case, it all comes down to your **Guest ID** number tied your credit card, name, and other info, which saves all kinds of data about what you buy.
- ian Andrew mined that data and saw patterns in it, for example — women on baby registries buy larger amounts of unscented lotion around the beginning of their second trimester. Bam! Send'em some coupons for other baby items.

# How Does the Information Leak?

- HTTP Referrer (Use POST Requests!)
- document.title
- UserID in URLS (e.g Facebook)
- Scripts included in body of website can read the whole page!
- Some first parties deliberately make information available
  - (Homedepot, Wall Street Journal)

# What Information is Gathered?

- Location
- Interests
- Purchases
- Employment status
- Sexual orientation,
- Financial challenges
- Medical conditions

....and much more.....

# Users Don't Seem to Like It

Survey results indicate a strong dislike of "targeted marketing"...

- No advertising based on tracking!  
(2009 Phone Survey Turow et al 87%)
- Behavioral targeting should be illegal!  
(2010 Poll USA Today Gallup 67%)
- "not okay" with behavioral advertising! (2012 Phone Survey Pew Research 68%)

# Google Ad Preferences

27

## Google Ads Preferences

**Opt out**  
Opt out if you prefer ads not to be based on interests and demographics.

When you opt out, Google disables this cookie and no longer associates interest and demographic categories with your browser.

**Your cookie**  
Google stores the following information in a cookie to associate your ads preferences with the browser you are currently using:

```
id=22f4eaac2c010080 | t=1318500183 | et=730 | cs=bqos07qp
```

Visit the [Advertising and Privacy page](#) of our [Privacy Center](#) to learn more.

# So is This Legal - In the US?

- FTC prevent "unfair" or "deceptive" behaviour - tracking related to "deceptive" behaviour
- First violation small (if any) payment, subsequent violation gets monetary penalties
- 2011 three(!) enforcement actions
- Advertising industry's self-regulatory programs concentrates on use of data

# And What About the EU?

- 2002 ePrivacy directive only "strictly necessary" and "explicitly requested" information, "opt out" (almost no implications)
- 2009 amendment to "opt in" (no enforced compliance)
- 2012 consent must be explicit, penalties up to 2% of revenue
- Notion of "essential" cookies - a lot of room for interpretation....

# Opt Out Cookies I

Recently on SFGATE..

The screenshot shows the top section of the SFGATE website. At the top is a large yellow and blue banner for TransUnion. On the left, a baseball with the number '832' is shown next to the text 'Get your FREE Credit Score'. A hand cursor icon points to the word 'Get'. In the center, there is an illustration of a baseball player running. On the right, a red circular button says 'CLICK HERE'. Further right, there is a small 'AdChoices' icon and the TransUnion logo. Below the banner is a weather section for San Francisco, CA, showing a temperature of 63°F and 'Partly Cloudy' conditions. It also includes a 5-day forecast and a traffic link. Below the weather section is a navigation bar with links to various sections: Entertainment, Food, Living, Travel, Columns, Shopping, Cars, Jobs, Real Estate, Index, and a 'WEEKLY AD' button. At the bottom, there is a list of featured articles: 'Opera with my daughter', 'Death and the Civil War', 'Name Moneyball sequel?', 'Weird wheelks', and 'Fight over Kate pics'.

Get your **FREE Credit Score** **CLICK HERE** AdChoices TransUnion®

63°F San Francisco, CA (change)  
Partly Cloudy  
Today 50/65 Tue. 54/61 5 Day Forecast Traffic

ate.com Web Search by YAHOO! Businesses Sign In | Register

Entertainment Food Living Travel Columns Shopping Cars Jobs Real Estate Index WEEKLY AD

| Opera with my daughter | 'Death and the Civil War' | Name 'Moneyball' sequel? | Weird wheelks | Fight over Kate pics

# Opt Out Cookies II



EVIDON™

## How Data Powers Your Experience

You can opt out of any or all of the companies listed below. Opting out does not mean you will stop seeing ads. It means that the company you opt out of will no longer use your data to target ads to you.

[Show help](#)

Select All ☐

| Ad companies:          | Manage | Opt-out                    |
|------------------------|--------|----------------------------|
| Acxiom (Relevance-X)   |        | <a href="#">go to site</a> |
| BlueKai                |        | <input type="checkbox"/>   |
| Collective             |        | <input type="checkbox"/>   |
| Datalogix              |        | <input type="checkbox"/>   |
| DoubleClick            |        | <input type="checkbox"/>   |
| IXI Corp               |        | <input type="checkbox"/>   |
| Nielsen MyBestSegments |        | <input type="checkbox"/>   |
| Polk Automotive        |        | no opt-out provided        |

# Opt Out cookies III

- Fight fire with fire? Set Cookies to prevent other cookies from being set
- Manual updating - useability?
- Expiration?
- Clear cookies (and opt-out cookies)
- Can be undone by third party itself - opt out from behavioral targeting doesn't include the user is not tracked anymore!

# Google Analytics

33



Select a language ▼

## Google Analytics Opt-out Browser Add-on

To provide website visitors the ability to prevent their data from being used by Google Analytics, we have developed the Google Analytics opt-out browser add-on for the Google Analytics JavaScript (ga.js, analytics.js, dc.js).

If you want to opt-out, download and install the add-on for your web browser. The Google Analytics opt-out add-on is designed to be compatible with Chrome, Internet Explorer 8-11, Safari, Firefox and Opera. In order to function, the opt-out add-on must be able to load and execute properly on your browser. For Internet Explorer, 3rd-party cookies must be enabled. Learn more about the opt-out and how to properly install the browser add-on [here](#).

**Get Google Analytics Opt-out Browser Add-on**

Available for Microsoft Internet Explorer 8-11, Google Chrome, Mozilla Firefox, Apple Safari and Opera.

[Learn more about Google Analytics Privacy »](#)

# Private Browsing

34

- Private Browsing allows you to browse the Internet without saving information about which **sites** and **pages** you've visited

- Historically speaking, web browsers store information such as browsing **history, images, videos** and text within **cache**.
- In contrast, privacy mode can be enabled so that the browser does not store information for sessions. You can still browse the Internet, but all data that is stored is deleted after date. You can also disable the cookies and Flash cookies.
- It is still possible to identify frequented websites by associating the IP address with the user on the server end.

What about browser **extensions**?

Should they be **supported** in private browsing mode?

# Do Not Track HTTP header

DNT = “DNT” “:” BIT

1 => opt out of tracking

0 => opt in to tracking

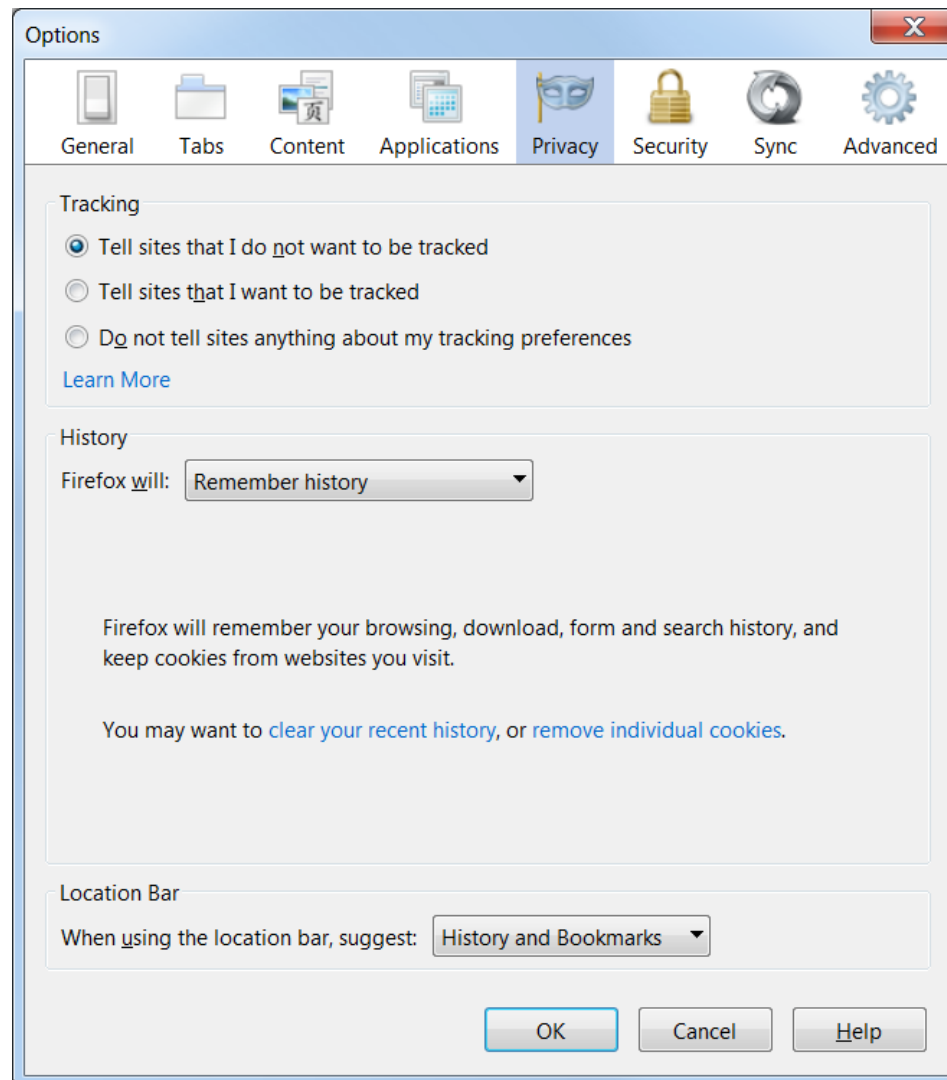
absent => no expressed preference

# User Agent Requirements

- ❑ MAY include a DNT header in any HTTP request
- ❑ SHOULD provide a user interface
- ❑ MAY adopt no-expressed-preference or opt-out by default
- ❑ MUST NOT transmit opt-in without user consent

# Firefox UI

37



# Second and Third Parties

Opt out: a server acting in a **third-party** capacity **MUST NOT track** a user or user agent unless subject to an **exception**.

- A third party is a functional entity with which the user does not reasonably expect to share data.
- E.g., ad networks, analytics providers, social plug-in providers

Tracking includes collection, retention, and use of all data related to the request and response.

# Exceptions

- ❑ Explicit user consent for tracking
- ❑ Third-party tracking **exclusively** on behalf of first party
- ❑ Data **unlinkable** to a user or UA
- ❑ Logging:
  - ▣ Single site logs: 2 weeks
  - ▣ Logs for ad fraud: 1 month
  - ▣ Logs for security: 6 months
  - ▣ Logs for financial fraud: 6 months

# Server Requirements

- Server SHOULD echo request header

```
GET /thirdpartycontent.html HTTP/1.1
Host: thirdparty.example.com
```

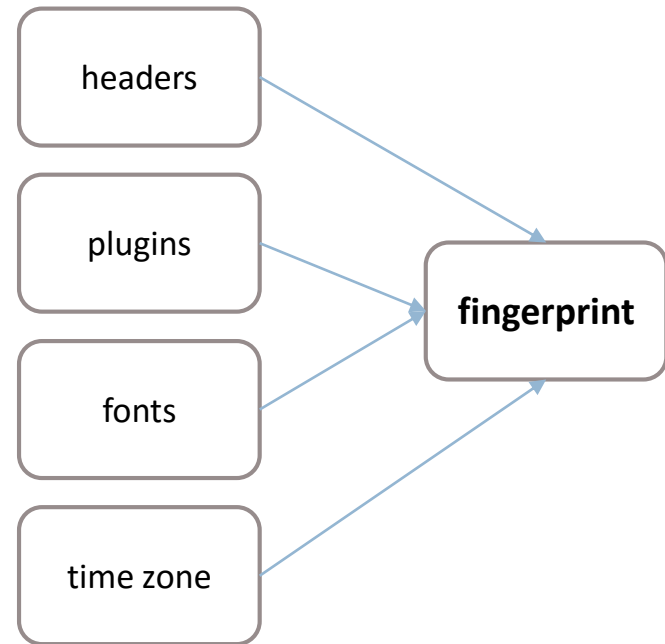
```
DNT: 1
HTTP/1.1 200 OK
Date: Mon, 7 March 2011 01:23:45 GMT
Server: Apache/2.2.17 (Unix)
Content-Length: 123
Connection: close
Content-Type: text/html; charset=UTF-8
DNT: 1
```



# Stateless tracking

# Stateless Fingerprinting

- Emerges around 2010 as a project from the EFF
- Since then, has been replicated in various settings, including by academic researchers
- In the last two years we have seen active fingerprinting from several large advertising targeting companies: BlueCava, Iovation, and ThreatMetrix



# Panopticlick

- Of the 470,000-plus users who had participated at that point in his public [Panopticlick](#) project, **84 percent** of their browsers produced unique fingerprints
- 94 percent if you count those that supported Flash or Java)

Panopticlick – Mozilla Firefox

Panopticlick

https://panopticlick.eff.org/index.php?action=log&js=yes

## Panopticlick

How Unique – and Trackable – Is Your Browser?

Your browser fingerprint **appears to be unique** among the 4,979,774 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys **at least 22.25 bits of identifying information**.

The measurements we used to obtain this result are listed below. You can read more about our methodology, statistical results, and some defenses against fingerprinting in [this article](#).

Help us increase our sample size: [📧](#) [🔗](#)

| Browser Characteristic      | bits of identifying information | one in x browsers have this value | value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------|---------------------------------|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User Agent                  | 12.61                           | 6232.51                           | Mozilla/5.0 (X11; Linux x86_64; rv:35.0) Gecko/20100101 Firefox/35.0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| HTTP_ACCEPT Headers         | 6.34                            | 80.98                             | text/html, */* gzip, deflate de,en-US;q=0.7,en;q=0.3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Browser Plugin Details      | 11.02                           | 2073.18                           | Plugin 0: Gnome Shell Integration; This plugin provides integration with Gnome Shell for live extension enabling and disabling. It can be used only by extensions.gnome.org; libgnome-shell-browser-plugin.so; (Gnome Shell Integration Dummy Content-Type; application/x-gnome-shell-integration; ). Plugin 1: Shockwave Flash; Shockwave Flash 11.2 r202; libflashplayer.so; (Shockwave Flash; application/x-shockwave-flash; swf) (FutureSplash Player; application/futuresplash; spl)                                                                                                                                                                              |
| Time Zone                   | 2.6                             | 6.08                              | -60                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Screen Size and Color Depth | 3.85                            | 14.46                             | 1920x1080x24                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| System Fonts                | 20.66                           | 1659924.67                        | URW Gothic, Serto Jerusalem, Estrangelo TurAbdin, Nimbus Roman, DejaVu Sans Mono, Century SchoolBook URW, Chancery URW, Nimbus Sans, Estrangelo Nisibin, Bookman URW, Estrangelo Nisibin Outline, Dingbats, Cantarell, DejaVu Sans Light, Estrangelo Talada, Nimbus Sans Narrow, Palladio URW, East Syriac Ctesiphon, DejaVu Serif Condensed, Nimbus Mono, DejaVu Sans Condensed, DejaVu Sans, Serto Malankara, Standard Symbols L, Serto Urho, DejaVu Serif, Estrangelo Antioch, Serto Kharput, Estrangelo Edessa, Serto Jerusalem Outline, Estrangelo Midyat, East Syriac Adiabene, Serto Batman, Estrangelo Quenneshrin, Serto Mardin, Goha-Tibeb Zemen (via Flash) |
| Are Cookies Enabled?        | 0.44                            | 1.35                              | Yes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Limited supercookie test    | 3.23                            | 9.36                              | DOM localStorage: No, DOM sessionStorage: No, IE userData: No                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

Thanks to [browserspy.dk](#) for the font detection code, and to [breadcrumbs](#) for supercookie help.

[Frequently asked questions.](#)

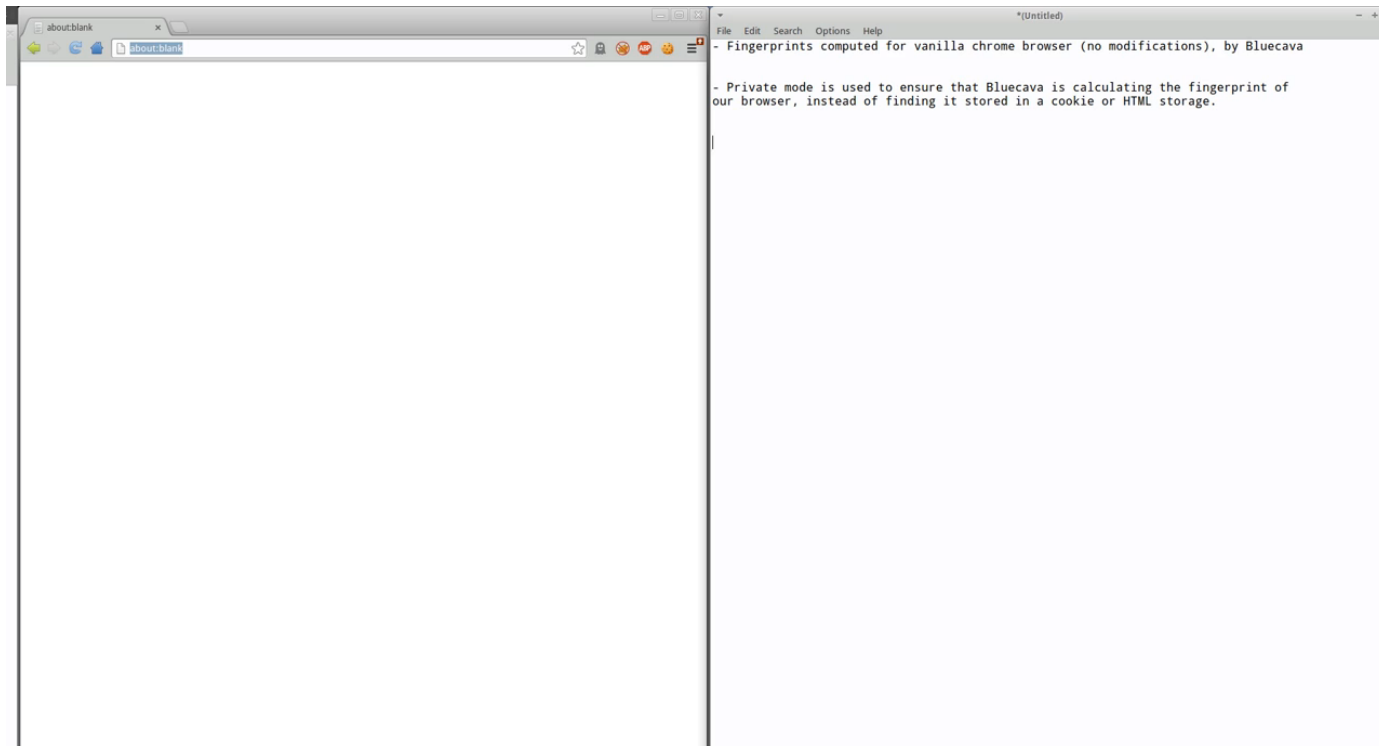
Send other questions or comments to [panopticlick@eff.org](mailto:panopticlick@eff.org).

# fingerprint.js: Fingerprinting lib on github

```
Fingerprint.prototype = {
  get: function(){
    var keys = [];
    keys.push(navigator.userAgent);
    keys.push(navigator.language);
    keys.push(screen.colorDepth);
    if (this.screen_resolution) {
      var resolution = this.getScreenResolution();
      if (typeof resolution !== 'undefined'){ // headless browser
        keys.push(this.getScreenResolution().join('x'));
      }
    }
    keys.push(new Date().getTimezoneOffset());
    keys.push(this.hasSessionStorage());
    keys.push(this.hasLocalStorage());
    keys.push(!window.indexedDB);
    //body might not be defined at this point or removed programmatically
    if(document.body){
      keys.push(typeof(document.body.addBehavior));
    } else {
      keys.push(typeof undefined);
    }
  }
}
```

```
keys.push(typeof(window.openDatabase));
keys.push(navigator.cpuClass);
keys.push(navigator.platform);
keys.push(navigator.doNotTrack);
keys.push(this.getPluginsString());
if(this.canvas && this.isCanvasSupported()){
  keys.push(this.getCanvasFingerprint());
}
if(this.hasher){
  return this.hasher(keys.join('###'), 31);
} else {
  return this.murmurhash3_32_gc(keys.join('###'), 31);
}
},
```

# Blue Cava Fingerprinting in Action



# Current state of fingerprinting?

- Results in *Cookieless monster* showed that 159 of [Alexa's](#) 10,000 most-visited websites track their users with such fingerprinting software.
- Also found that more than 400 of the million most popular websites on the Internet have been using JavaScript-only fingerprinting, which works on Flash-less devices such as the iPhone or iPad.
- Users continue to be fingerprinted even if they have checked “Do Not Track” in their browser’s preferences
- But it’s a little hard to say how much is really going on in practice
- Fingerprinting is designed to remain pretty invisible
- At the same time, we should expect more in this space because of cookie-based tracking becoming problematic



privaricator

# Insight of PriVaricator

- Most prior research focuses on making fingerprints not unique
- For example, they make navigator.userAgent to always be Firefox
- They strip revealing headers, etc.
- Typically this is done via browser extensions
- What is the effect of that?
- The focus on user **uniqueness** is misguided
- What matters is fingerprint **linkability**
- Making fingerprints non-deterministic also makes them hard to link across browsing sessions
- It's often easier to **randomize** the fingerprint than to keep in the same

# Use “pluggable” Randomization Policies

- We explore a space of **randomization policies** designed to produce unique fingerprints
  - Change the way the browser represents certain important properties (**offsetHeight** used to measure the presence of fonts) and **plugins**, to the JavaScript environment
  - Creatively misrepresenting — or lying — about these values introduces an element of non-determinism, which generally makes fingerprints **unlinkable** over visits
  - Producing practically **impossible** combinations of, say, browser headers and the navigator object, can actually **reduce** user privacy
- Blatant lying is *not* such a good idea
- Can significantly degrade user experience by, for instance, by presenting Firefox-optimized sites to users of IE, leading to visual discrepancies or calls into missing APIs

# A good randomization policy should...

---

- 1) produce unlinkable fingerprints; and
- 2) not break existing sites

# Extension to the privacy mode

- ❑ Browsers today already come with a private mode
- ❑ Designed to combat stateful (cookie-based) fingerprinting
- ❑ PriVaricator adds protection against stateless fingerprinting
- ❑ Built on top of Chromium and can be integrated directly into the browser
- ❑ Deploying it as an extension is not a such a good idea because it may make the user **more** identifiable, not less

# What to misrepresent?

Need to balance fingerprinting prevention with breaking existing sites

For example, navigator.userAgent is a *bad* thing to misrepresent

Likely to lead to a lot of site breakage

plugins

fonts

| Fingerprinting provider | Script name              | Plugin enumeration | Screen properties | Uses canvas | Access to offsetWidth | Access to offsetHeight |
|-------------------------|--------------------------|--------------------|-------------------|-------------|-----------------------|------------------------|
| BlueCava                | BCAC5.js                 | ✓                  | ✓                 | ✗           | 63                    | 63                     |
| Perferencement          | tagv22.pkmin.js          | ✓                  | ✓                 | ✗           | 155                   | 155                    |
| CoinBase                | application-9a3a[...].js | ✓                  | ✓                 | ✗           | 592                   | 197                    |
| MaxMind                 | device.js                | ✓                  | ✓                 | ✗           | 261                   | 27                     |
| Inside graphs           | ig.js                    | ✓                  | ✓                 | ✗           | 1,050                 | 48                     |

# Space of randomization policies

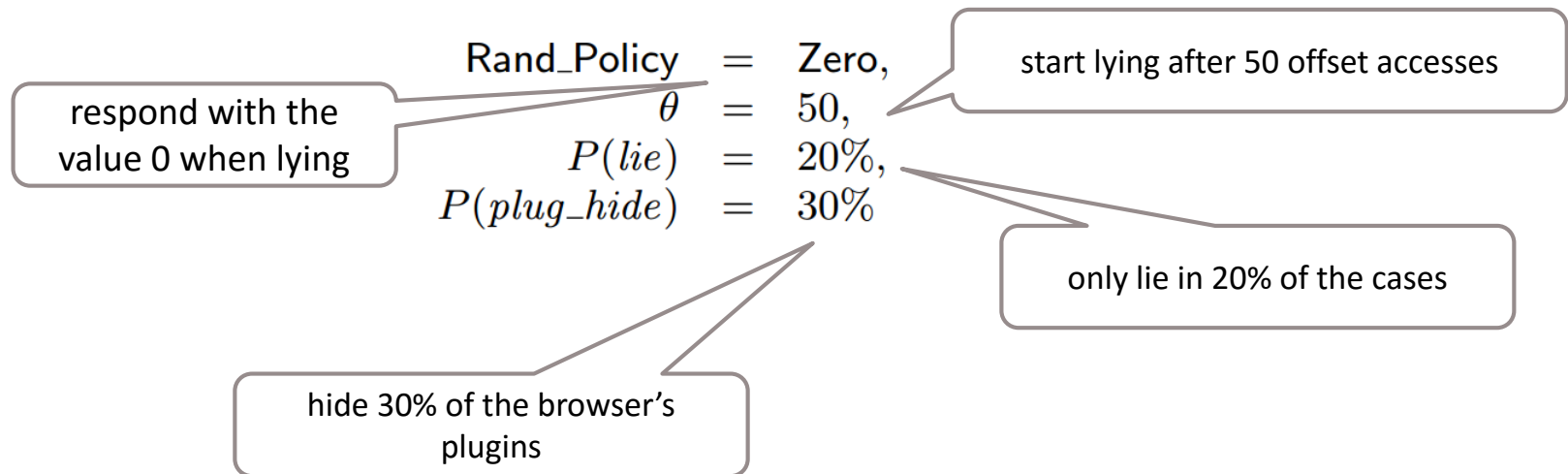
## Policies for offset measurements

- For the values of **offsetHeight**, **offsetWidth**, and **getBoundingClientRect** in PriVaricator, we propose the following numeric randomization policies
- - a) Zero
  - b) Random(1..100)
  - +/- 5% noise
- The policies are parametrized by the *lying threshold* (denoted as  $\theta$ ) and a *lying probability* (denoted as  $P(lie)$ ).
- $\theta$  controls how fast PriVaricator starts lying, *i.e.*, after how many accesses to **offsetWidth** or **offsetHeight** values, will the policy kick in

## Policies for plugins

- $P(\text{plug\_hide})$  the probability of hiding each individual plugin in navigator.plugins

# Sample Randomization policy



# Breakage concerns

Out of Alexa 10,000  
1.87% of scripts have 50+  
accesses when visited

but don't want to break  
spiegel.de

| Alexa Rank |  | Domain       | colorDepth |    |   |    | height | pixelDepth | width | Navigator |          |          |           |         |        |             | HTML element |         |                        |             |              |
|------------|--|--------------|------------|----|---|----|--------|------------|-------|-----------|----------|----------|-----------|---------|--------|-------------|--------------|---------|------------------------|-------------|--------------|
|            |  |              |            |    |   |    |        |            |       | mimeType  | platform | language | userAgent | appName | vendor | appCodeName | appVersion   | plugins | getBounding-ClientRect | offsetWidth | offsetHeight |
| 6,444      |  | bunte.de     | 0          | 1  | 0 | 1  |        |            |       | 0         | 0        | 2        | 8         | 0       | 0      | 0           | 0            | 1       | 2                      | 205,115     | 202,909      |
| 8,039      |  | nzz.ch       | 3          | 34 | 1 | 34 | 4      | 4          | 4     |           |          |          | 176       | 5       | 0      | 0           | 5            | 4       | 48                     | 187,881     | 187,349      |
| 191        |  | spiegel.de   | 2          | 4  | 0 | 4  | 0      | 0          | 0     |           |          |          | 15        | 3       | 0      | 0           | 1            | 4       | 7                      | 154,265     | 149,293      |
| 4,037      |  | wistia.com   | 1          | 2  | 0 | 2  | 0      | 0          | 3     |           |          |          | 81        | 0       | 0      | 0           | 0            | 0       | 0                      | 109,347     | 109,299      |
| 1,369      |  | zeit.de      | 0          | 4  | 1 | 4  | 0      | 0          | 2     |           |          |          | 8         | 3       | 2      | 0           | 0            | 5       | 1,318                  | 70,025      | 72,268       |
| 8,894      |  | menards.com  | 0          | 0  | 0 | 0  | 0      | 0          | 0     |           |          |          | 3,783     | 0       | 0      | 0           | 0            | 0       | 37                     | 43,877      | 38,715       |
| 4,754      |  | groupon.fr   | 0          | 0  | 0 | 0  | 0      | 0          | 0     |           |          |          | 1         | 0       | 0      | 0           | 0            | 0       | 15                     | 150,777     | 36,627       |
| 7,488      |  | xinmin.cn    | 0          | 0  | 0 | 1  | 0      | 0          | 0     |           |          |          | 70,380    | 0       | 0      | 0           | 3            | 0       | 4,426                  | 34          | 31,996       |
| 2,320      |  | celebuzz.com | 2          | 55 | 0 | 55 | 4      | 2          | 0     |           |          |          | 23        | 0       | 0      | 0           | 0            | 4       | 326                    | 27          | 27,779       |
| 1,370      |  | wetter.com   | 4          | 30 | 0 | 30 | 6      | 1          | 8     |           |          |          | 18        | 5       | 0      | 0           | 1            | 7       | 212                    | 2           | 21,764       |

most are ranked pretty low

82.3% of scripts have 0  
accesses to  
**offsetHeight**

# Policy implementation in the browser

## Strawman approach

- ❑ Instrumented access to navigator.plugins at the source level
- ❑ Try to intercept calls to **offsetWidth** and **offsetHeight** using DOM getters
- ❑ However, it's difficult to know which element will be measured
- ❑ **offsetWidth** and **offsetHeight** properties are not part of the HTMLElement prototype

## Real implementation

- ❑ Instrument access to the properties of interest
- ❑ Browser changes are, by nature, very local
- ❑ Our full prototype involves modifications to a total of seven files in the WebKit implementation of the Chromium browser, version 34.0.1768.0 (242762)
- ❑ 947 lines of code added/changed



evaluation

# Evaluation: dimensions



- Performance impact
- Effectiveness in breaking existing fingerprinters
- Minimizing breakage

# Slowdown? In the noise

| Browser      | JSBench |            | SunSpider |            | Kraken |             |
|--------------|---------|------------|-----------|------------|--------|-------------|
| Chromium     | 72.31   | $\pm 0.40$ | 139.20    | $\pm 1.00$ | 1,146  | $\pm 20.48$ |
| PriVaricator | 72.10   | $\pm 0.31$ | 138.70    | $\pm 0.49$ | 1,142  | $\pm 20.09$ |

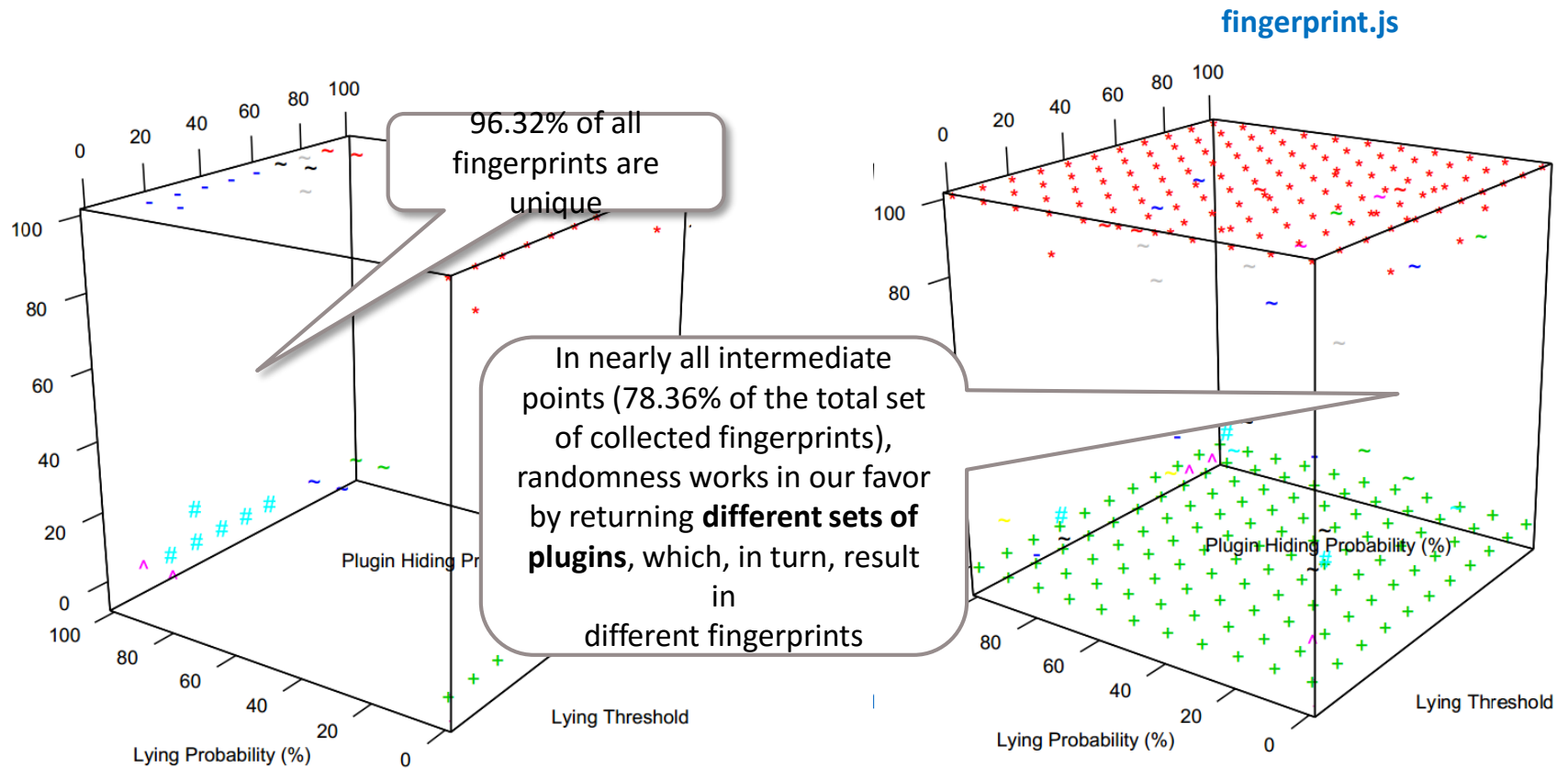
- Executed each suite five times, clearing the browser's cache in between runs
- The experiments were run on a desktop machine, running a recent Ubuntu Linux distribution, with an Intel Core i5-3570 CPU @ 3.40 GHz processor, and 8 GB of RAM

To calculate the upper bound of PriVaricator's overhead, we used the lying policy with the most computations ( $\pm 5\%$  Noise) configured with the worst (from a performance point of view) parameter settings, i.e.,  $\theta=0$  and  $P(lie)=100\%$

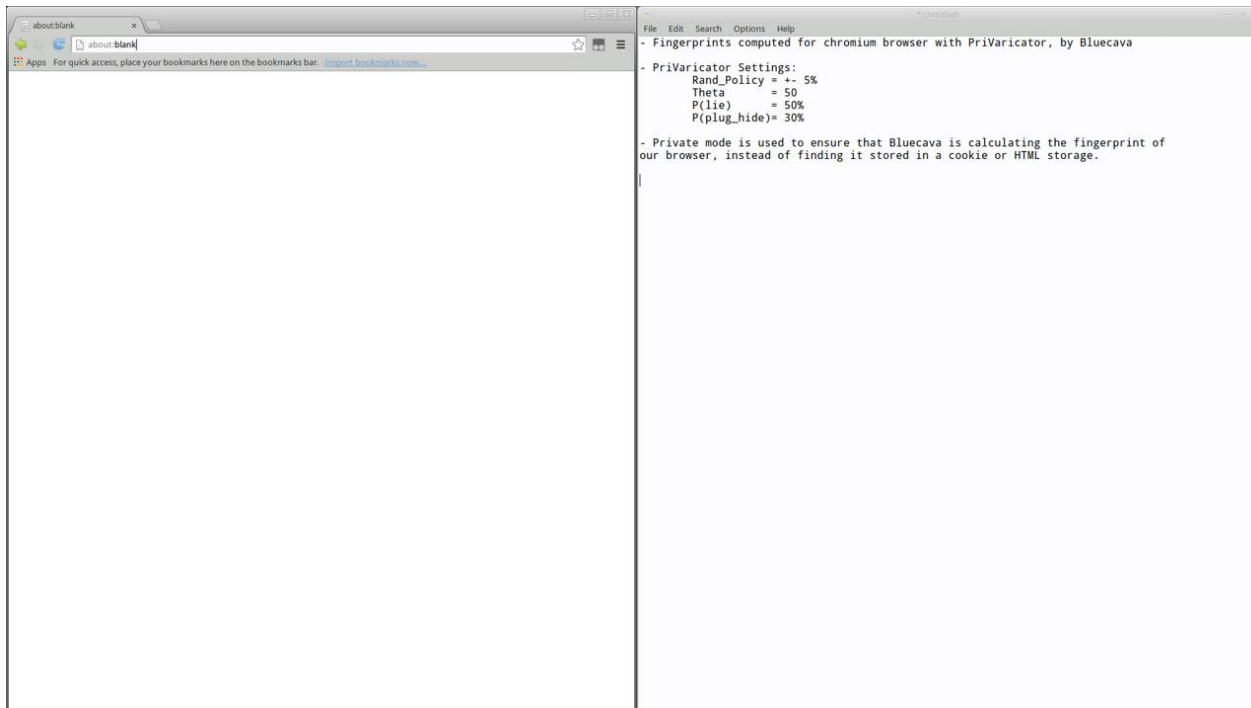
# Is it Effective?

- 1) BlueCava
  - <http://bluecava.com/opt-out>
  - Shows fingerprints such as 18B1-EBFC-A3F0-6D81-6DE8-D8DA-CA56-A22B
- 2) PetPortal
  - <http://fingerprint.pet-portal.eu>
  - Similarly, get a fingerprint
- 3) Coinbase
  - Obtained entirely client-side
  - Can be captured
  - MD5 applied to it and it's submitted via a cookie
- 4) fingerprintjs
  - That's the code we saw earlier
- To explore the space of possible policies in detail, we performed an automated experiment where we visited each fingerprinting provider 1,331 times, to account for  $11^3$  parameter combinations, where each parameter of our randomized policy
  - lying threshold
  - lying probability, and
  - plugin-hiding probability
- ranged from 0 to 100 in increments of 10

# Success of PriVaricator



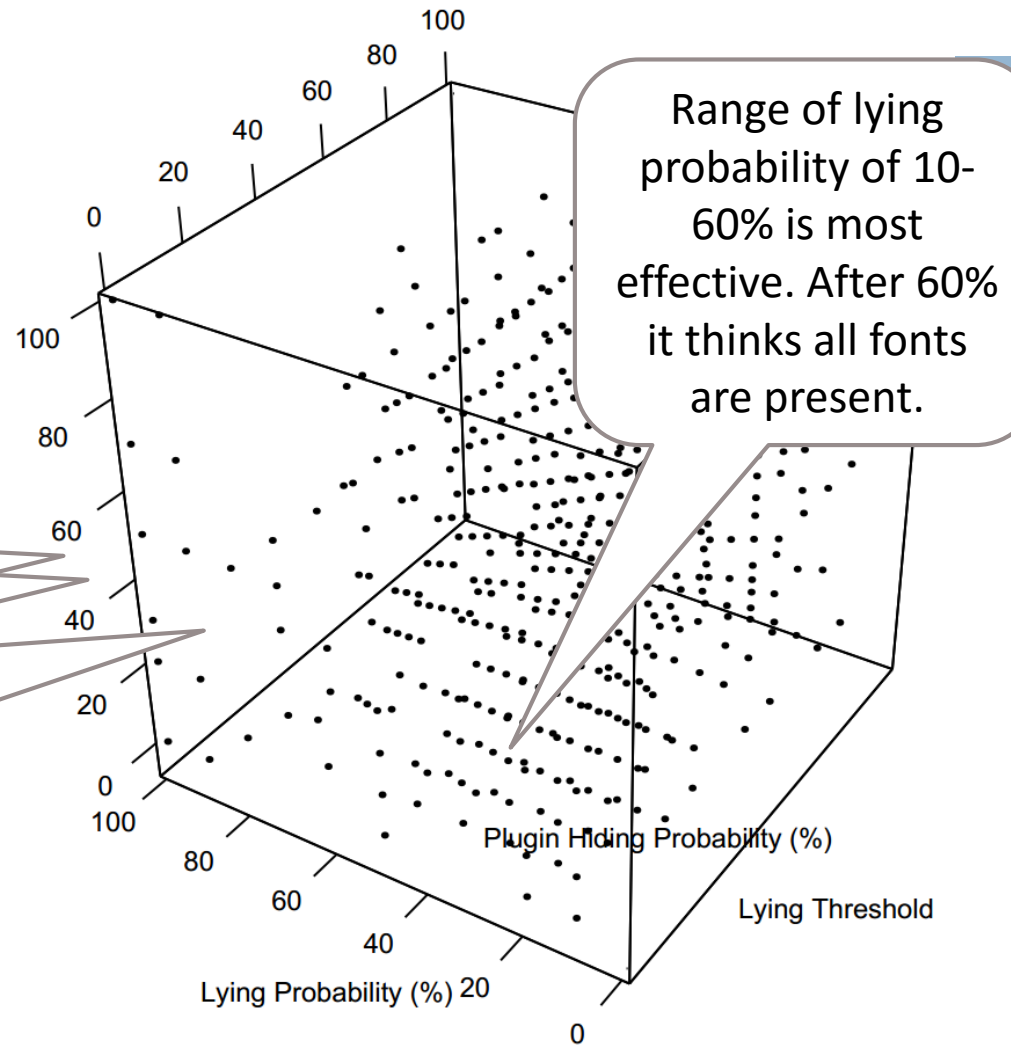
# PriVaricator stopping Blue Cava Fingerprinting



# PetPortal: most robust

Get unique fingerprints for “only” 37.83% of the 1,331 parameter combinations

succeeds more in tracking us than BlueCava, Coinbase, and fingerprintjs



# Measuring breakage

- When PriVaricator lies about these values like **offsetWidth** and **offsetHeight**, it creates a potential for **visual breakage**
- For example, by reporting that an element is smaller than it actually is, PriVaricator could cause the page to place it in a smaller container, hiding part of its content from the user.
- Numerically, we define *breakage* as the fraction of pixels that are different when a site is loaded with a vanilla browser (PriVaricator turned off) and with PriVaricator
- We instrumented Chromium to visit the main pages of the top 1,000 Alexa sites, for 48 different combinations of lying probability and lying threshold; these were the parameter combinations that resulted in unique fingerprints for PetPortal

# Measuring Breakage by Counting Pixels

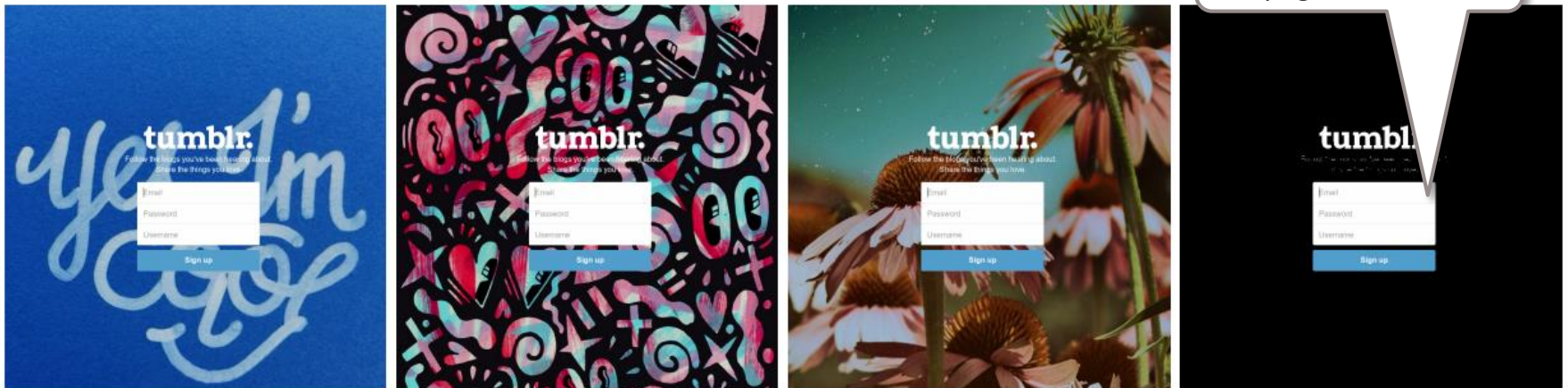
Need to separate breakage caused by PriVaricator from naturally dynamic web pages

Collected a new vanilla-browser screenshot every ten visits of a page, resulting in a total of five extra screenshots

We computed a visual mask of differences appearing on them, and used it when comparing a screenshot captured using a specific policy parameter combination, to the vanilla one

This mask can be applied to all PriVaricator screenshots to exclude the naturally varying parts of a page from comparisons.

Mask: unchanging  
page elements



# Examining breakage results

| Policy         | Min         | Mean | Max % |
|----------------|-------------|------|-------|
| Random(0..100) | 0.8%        | 1.5% | 2.3%  |
| Zero           | 0.4%        | 0.9% | 1.4%  |
| ± 5% Noise     | <b>0.4%</b> | 0.7% | 1.0%  |

Overall, the results of our breakage experiments show that the negative effect that PriVaricator has on a user's browsing experience is negligible.

- Manually reviewed the 100 screenshots with the largest breakage. In only 8 cases, the differences could be attributed to PriVaricator.
- In many cases, the sites would show an “in-page” pop-up asking the user to participate in a survey

Next to surveys, the reported breakage was due to missing or not-fully loaded ads, error-pages and image carousels

In one case, PriVaricator had caused a slight stretch of a site's background image. While this led to a large computed breakage, users would not notice the change if they could not compare the page with the original non-stretched version.

- We likely overestimated the breakage since most of the pages with the highest reported breakage turned out to be false positives.

# Challenges

## Transparency

- We do not claim to preserve transparency in PriVaricator; indeed, this is a tough property to maintain for just about any runtime protection mechanism
- A motivated fingerprinter could test for the presence of unexpected randomness, *e.g.*, by inquiring about the dimensions of an element 100 times
- A statistical attack may collect multiple readings and average them over a large number of samples, in an effort to approximate the real measurement

## Lie cache

- Setting up a “lie cache”, a mechanism where the browser would report the *same* false value for multiple inquiries about the same, unmodified element
- To break linkability, the lie cache should be reset at the beginning of every new private mode session, *i.e.*, when a user is opening a private mode tab or window of her browser.
- This would enhance the transparency at the cost of linkability within the same private mode session.

# Challenges

## Future fingerprinting vectors

- Just like with most defense mechanisms, more sophisticated attacks often are developed in response to them.

Note, however, that as long as either plugins or fonts are included as part of a user's fingerprint and relied upon to provide meaningful information to the fingerprinting party, the current version of PriVaricator is likely to provide adequate randomization

## Updating policies

- Fluid browser updates enable changing PriVaricator policies

Note that similar updates are shipped to other browser-hosted security mechanisms such as XSS filters, malware filters, and tracking protection lists (TPLs)

Extensions such as ad blockers also update their blacklists on a regular basis. As such, we feel that PriVaricator provides an extensible platform for stateless fingerprinting defenses

# Conclusions



- ❑ PriVaricator: an addition to the browser private mode
- ❑ Designed to combat stateless tracking or fingerprinting
- ❑ Negligible performance overhead
- ❑ Effective for a range of policy parameter values
- ❑ Breaks quite little (only a handful of sites) in our evaluation