



Privacy Badger

Take a Bite Out of Tracking



Noah Swartz
noah@eff.org
[@swartzcr](https://twitter.com/swartzcr)



Electronic Frontier Foundation

- Non-Profit defending civil liberties in the digital world
- Impact litigation, activism, technology
- Projects like HTTPS Everywhere, Let's Encrypt, Panoptick and Privacy Badger
- I am a staff technologist at EFF
 - I'm a programmer; I can't answer your legal questions



What We Are Going to Talk About

- Browser Tracking — It's a Bigger Problem Than You May Think
- Why Online Privacy Matters
- Who Is Tracking Us
- How Are They Doing It
- What Can We Do To Stop It



Third Parties Are Everywhere

- Images & CSS can be cached on CDNs
- Fonts, maps, videos, widgets
- Analytics engines
- Social media share buttons
- And obviously - Ads



Your Browsing Is Being Tracked

- How third parties track you
 - Unique ID cookies, canvas fingerprinting, tracking pixels, 'super cookies', and more!
- This is big business — A Multi-Billion Dollar Industry



Panoptick

How Unique — and Trackable — Is Your Browser?

Your browser fingerprint **appears to be unique** among the 5,678,435 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys **at least 22.44 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	13.23	9591.95	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/43.0.2357.65 Safari/537.36
HTTP_ACCEPT Headers	6	64.14	text/html, */* gzip, deflate en-US,en;q=0.8
Browser Plugin Details	13.86	14865.01	Plugin 0: Chromium PDF Viewer; ; mhjfbmdgcfjbbpaeojfohoefgiehjai; (; application/pdf; pdf). Plugin 1: Chromium PDF Viewer; Portable Document Format; internal-pdf-viewer; (Portable Document Format; application/x-google-chrome-pdf; pdf).
Time Zone	4.52	22.94	420
Screen Size and Color Depth	6.9	119.78	2560x1440x24
System Fonts	2.24	4.72	No Flash or Java fonts detected
Are Cookies Enabled?	0.43	1.34	Yes
Limited supercookie test	0.85	1.8	DOM localStorage: Yes, DOM sessionStorage: Yes, 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 panoptick@eff.org.

Learn about **Panoptick** and **web tracking**.

The Panoptick **Privacy Policy**.

Learn about the **Electronic Frontier Foundation**.





Who is tracking you online?



Some Key Players in the Industry





Third Party Trackers

- Non-consensual
 - You don't opt in to an agreement with them
- Ubiquitous
- Hard to avoid
- Strong financial incentive



But I Like Targeted Ads!

- You have no control over how your information is stored/used
- Third parties have no obligation to anonymize or store temporarily
- Data can be stolen or sold
- Misuse of ad targeting

THE WALL STREET JOURNAL.

[Subscribe Now](#)

WHAT THEY KNOW

Websites Vary Prices, Deals Based on Users' Information

f i ® s t m x ñ d @ ¥
PEER-REVIEWED JOURNAL ON THE INTERNET

Digital inclusion and data profiling

by Seeta Peña Gangadharan



Third Party Tracking is Also Useful For Spies

Sections

The Washington Post

Search



The Switch

NSA uses Google cookies to pinpoint targets for hacking

future tense

THE CITIZEN'S GUIDE TO THE FUTURE

DEC. 13 2013 5:02 PM

How the NSA Piggy-Backs on Third-Party Trackers

By Edward Felten and Jonathan Mayer



2

FEATURED NEWS

Secret 'BADASS' Intelligence Program Spied on Smartphones



69



Micah Lee

Jan. 26 2015, 9:12 a.m.



TOP SECRET//COMINT//ORCON/REL TO USA, AUS, CAN, GBR, NZL

Cookies!

TOP SECRET//COMINT//ORCON/REL TO USA, AUS, CAN, GBR, NZL



TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

What can cookies be used for?

- Cookies can be used to identify a single machine from hundreds of other users on the same proxy IP address
- The Yahoo B cookie is a “machine specific cookie”

```
f61468b596u4b  
b=4  
B d=GtdIgXBpYEQvWQEG:VnWhazdPNw-  
g=9e  
i=80SsR4OwqEO5oGGF2kTh
```

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL



Why Should You Care About Privacy?

- You May Want to Read Things That Are Controversial or Embarrassing For Research or Just General Interest
- Data Which May Be Embarrassing When Put Together
 - A search for health insurance quotes and then looking up a disease on Web MD for example
- Chilling Effects



How Can Online Tracking be Stopped?



How About Incognito Browsing?

- Only untrackable between sessions
- Hard to retain first party info
- Vulnerable to fingerprinting
 - And some super cookies
- Tor Browser
 - Not a general purpose solution
 - Hard for the layperson
 - Tor network couldn't handle the load of all web users



What About Ad Blockers?

- By default only block ads, not necessarily trackers
- Blacklist means they're always behind
- Arms race problem
- Not always trustworthy
 - Ghostery sells information to advertisers
 - Other ad blockers will get paid off to unblock ads



Policy Work — Do Not Track

- **W3C**[®] standard
- Opt in to DNT – advertisers will not track you
 - Really they only don't tell you they are tracking you
- Not as strong as it could be
- Low level of adoption
- Not a real privacy preserving option



Digital Advertiser Alliance



- Advertisers have proposed to self regulate
- DAA members offer an 'opt out'
 - Only required to not show target ads
 - No requirements on what data they can and can not collect/store
- Not legally binding
- Still only limited adoption



A Combination of Tech and Policy



Privacy Badger 1.0

New Browser Plugin Blocks Spying Ads and Invisible Trackers.



Privacy Badger in it's natural habitat





Privacy Badger

- Browser Plugin – Chrome/Firefox
- Open Source – GPLv3
- Focuses on completely blocking trackers
- Tries to solve the arms race problem
 - Uses an algorithm instead of a blacklist
 - Can cause false positives and false negatives
 - Allows advertisers a way out



How Does Privacy Badger Work?

- Send a DNT=1 header
- Watch for requests to third party domains
- If a third party domain sets a high entropy cookie*, add it to a list of potential trackers
- If the tracker is seen on multiple sites -
block it
 - Or anonymize your browser but still load the content



Privacy Badger on NYT.com

The screenshot shows the Privacy Badger extension interface. At the top, it says "Privacy Badger detected 0 trackers on this page. These sliders let you control how Privacy Badger handles each tracker." Below this, there are three icons: a red circle with a slash, a cookie with a red 'x', and a green checkmark. A list of domains is shown with sliders indicating their status:

Domain	Status
a1.nyt.com	Blocked (Green)
i1.nyt.com	Blocked (Green)
i2.nyt.com	Blocked (Green)
int.nyt.com	Blocked (Green)
s1.nyt.com	Blocked (Green)
static01.nyt.com	Blocked (Green)

At the bottom, there are two buttons: "Disable Privacy Badger for This Site" and "Report Broken Site".



How Does Privacy Badger Work?

- Entropy in Information Theory
 - The information contained in a message, usually in units such as bits.
 - A 2 bit message would have 2 bits of entropy or 1 in 4
- Low entropy cookie:
 - `lang=es; /*About 8 bits of entropy or 1 in 255 */`
- High entropy cookie:
 - `utmz=32c3e3f09a23 /* About 48 bits of entropy */`
 - Approximately 1 in 281.5 trillion



How Does Privacy Badger Work?

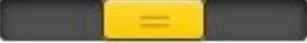
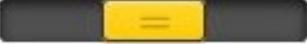
- Occasionally a tracker can't be blocked without creating significant problems for the user
 - Youtube, Google Maps, AWS, Paypal, etc.
- For these we block cookies
 - HTTP and Javascript
 - HTML5 Supercookies
 - Canvas fingerprinting



Privacy Badger on BoingBoing.net

 **Privacy Badger**  

Privacy Badger detected 9 **trackers** on this page. These sliders let you control how Privacy Badger handles each tracker.

Tracker	Control
i.creativecommons.org	   
apis.google.com	
fonts.gstatic.com	
licensebuttons.net	



Privacy badger on Gawker.com

The screenshot shows the Privacy Badger extension interface. At the top, it says "Privacy Badger detected 14 trackers on this page. These sliders let you control how Privacy Badger handles each tracker." Below this, there are three icons: a red circle with a slash, a yellow circle with a red 'x', and a green checkmark. A list of trackers is shown with sliders indicating their status:

Tracker Domain	Status
secure-us.imrworldwide.com	Blocked (Red)
kinja.com	Allowed (Green)
beacon.krxd.net	Blocked (Red)
cdn.krxd.net	Blocked (Red)
bam.nr-data.net	Blocked (Red)
edge.quantserve.com	Blocked (Red)

At the bottom of the interface, there are two buttons: "Disable Privacy Badger for This Site" and "Report Broken Site".



How Does Privacy Badger Work?

- Users can see and adjust what is blocked, greylisted and allowed
- Can disable privacy badger entirely for certain sites if they wish.
- Can opt back in to third parties for certain uses (e.g. Disqus, Youtube comments)



User Choice!

Privacy Badger

Enable Privacy Badger for This Site

Report Broken Site

google-analytics.com



googleadservices.com



fonts.googleapis.com





How Does Privacy Badger Work?

- Social Widgets
 - Privacy Badger replaces them with locally sourced versions
 - Gives the option to turn them back on

**Loïc Nottet van outside
regelrechte kanshebbe
storm op iTunes**





**But what about third party sites
that legitimately do not wish to
track users?**



The Policy Side — A New DNT

- We just released DNT 1.0!
 - <https://www.eff.org/dnt-policy>
- Sites host it on a .well-known domain
- States that users sending DNT will not be tracked
- Blocking sites that don't respect DNT creates an incentive to respect DNT



The Policy Side — A New DNT

- User identifiers will be discarded
- Logs will not be kept longer than necessary
- Data can be kept for debugging or security
- Data won't be sold to sites that don't respect this DNT policy
- Sites adopting it get whitelisted by Privacy Badger
 - But won't override user settings



Privacy Badger detected 3 trackers on this page. These sliders let you control how Privacy Badger handles each tracker.

 **Privacy Badger**  

 do-not-tracker.org		
eviltracker.net		
trackersimulator.org		

Disable Privacy Badger for This Site

Report Broken Site



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

PanoptiClick

How Unique – and Trackable – Is Your Browser?

We tested your browser & addons. Do they protect you against non-consensual Web tracking?

Yes! You have strong protection against Web tracking

Test	Result
Is your browser blocking tracking ads?	✓ yes
Is your browser blocking invisible trackers?	✓ yes
Is your browser accepting Do Not Track commitments?	✓ yes





The Policy Side — A New DNT

- Drafted with Disconnect, adopted by:
 - Mixpanel
 - Medium
 - AdBlockPlus
- And hopefully more to come!



What Are You Waiting For? Get Privacy Badger!

EFF.org/pb

**INSTALL PRIVACY
BADGER**
AND ENABLE DO NOT TRACK

[Click here for Firefox version](#)





Still To Come...

- Better tracker detection algorithms
- Localization / UI
- Extension enumeration
- Mobile/Safari versions
- More DNT adoption from third parties



How You Can Help

- Use Privacy Badger
 - Report broken sites from inside Privacy Badger
- Submit a bug report / pull request
 - <https://github.com/EFForg>
- Respect users who send DNT header
- Donate to EFF!



We Still Need Better Tools

- **Browser Improvements**
 - Double Keyed Cookies
 - Harden browsers against fingerprinting
 - Better controls for blocking and clearing supercookies
- **Built-In Protection**
 - Firefox Tracking Protection
 - <http://monica-at-mozilla.blogspot.de/2015/05/tracking-protection-for-firefox-at-web.html>



Is advertising the best way to fund
the web? It's hard to say.



But if we are going to live with advertising, it *must stop* violating users' privacy without their consent.



Thanks! Questions?

noah@eff.org

Twitter: [@swartzcr](https://twitter.com/swartzcr)

<https://eff.org/privacybadger>

p.s. I have stickers

PGP: 9206 A6E0 F07C F141 663F 8B93 9C7A DED2 2966 0F56