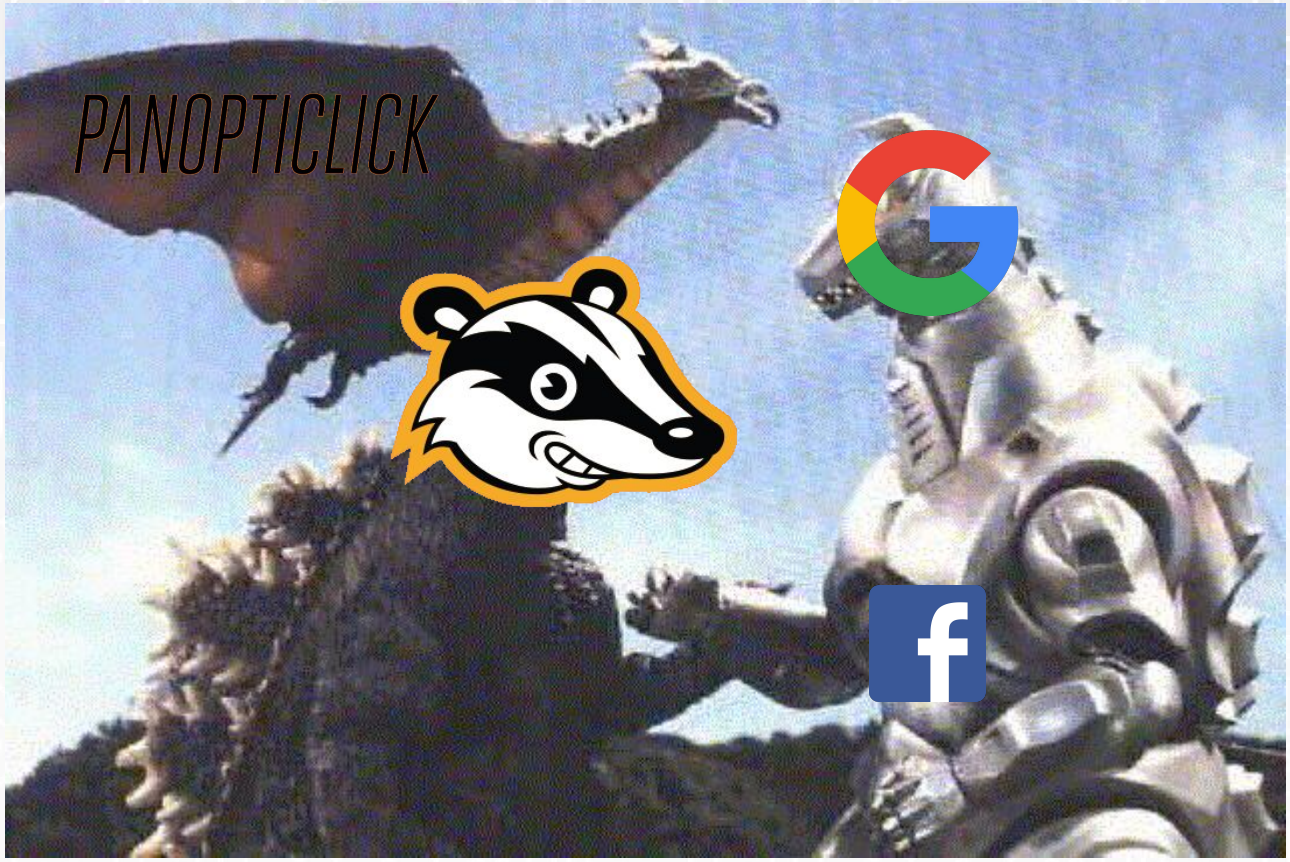
Privacy Badger & Panopticlick vs. The Trackers (Round One)



William Budington - @legind - bill@eff.org
Cooper Quintin - @cooperq - cjq@eff.org

Whois

Whois

What is EFF?

"What Binge On does, it includes a proprietary technology and what the technology does is not only detect the video stream but select the appropriate bit rate to optimize to the video, the mobile device. That's part A of my answer. Part B of my answer is, who the fuck are you, anyway, EFF? Why are you stirring up so much trouble, and who pays you?" - John Legere

Q: Who the fuck are you, anyway, EFF?

Legal Work

Coders' Rights Project

Q: Why are you stirring up so much trouble?

Activism


NSA
ILLEGAL
SPYING
BELOW
StandAgainstSpying.org
GREENPEACE


TELL CONGRESS:
CFAA Is Broken – Don't Make It Worse

MAY 28, 2015 | BY NATE CARDOZO AND EVA GALPERIN

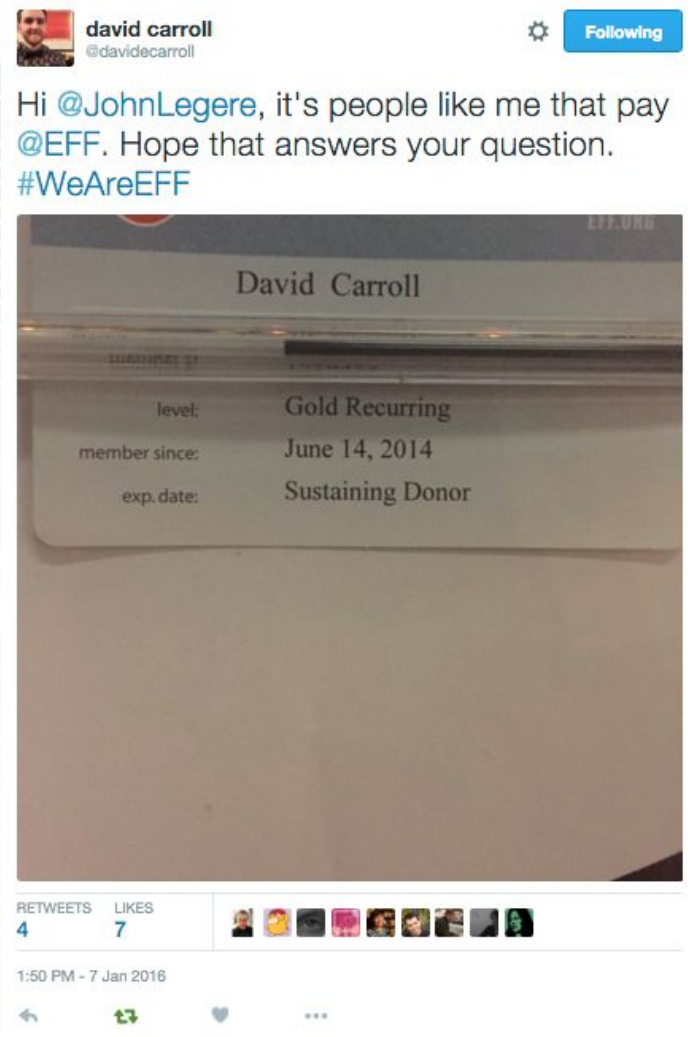
What Is the U.S. Doing About Wassenaar, and Why Do We Need to Fight It?

On May 20, 2015, the U.S. Department of Commerce's Bureau of Industry and Security (BIS) published its proposed implementation of the December 2013 changes to the Wassenaar Arrangement. What follows is a long post, as we're quite troubled by the BIS proposal. In short, we're going to be submitting formal comments in response, and you should too.

What is the Wassenaar Arrangement?

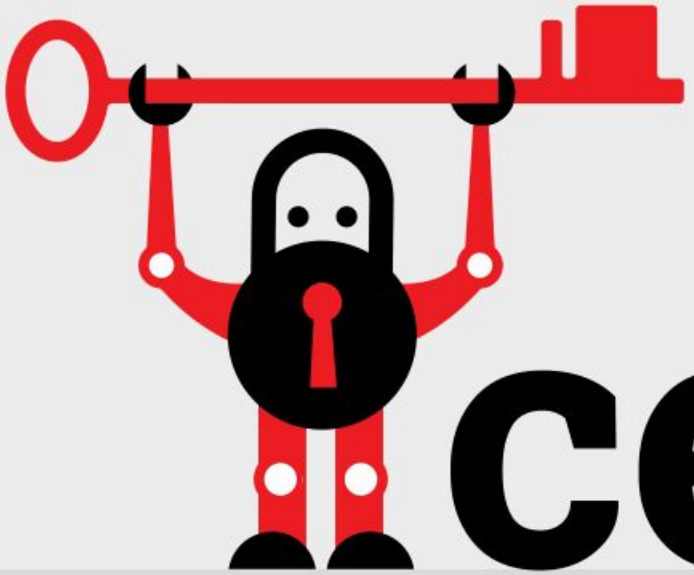
The Wassenaar Arrangement is a multi-national agreement intended to control the export of certain "dual-use" technologies. It's a voluntary agreement among 41 participating states that mostly regulates

Q: Who pays you?




John Legere
@JohnLegere
Following
Let me be clear- I know who the @EFF is. I'm sure they do a lot of great things for a lot of consumers, but innovation can be controversial!

Technology



certbot

Automatically enable HTTPS on your website.

Surveillance on the Web

July 15, 1999

Fresh From Your Browser's Oven

By GLENN FLEISHMAN

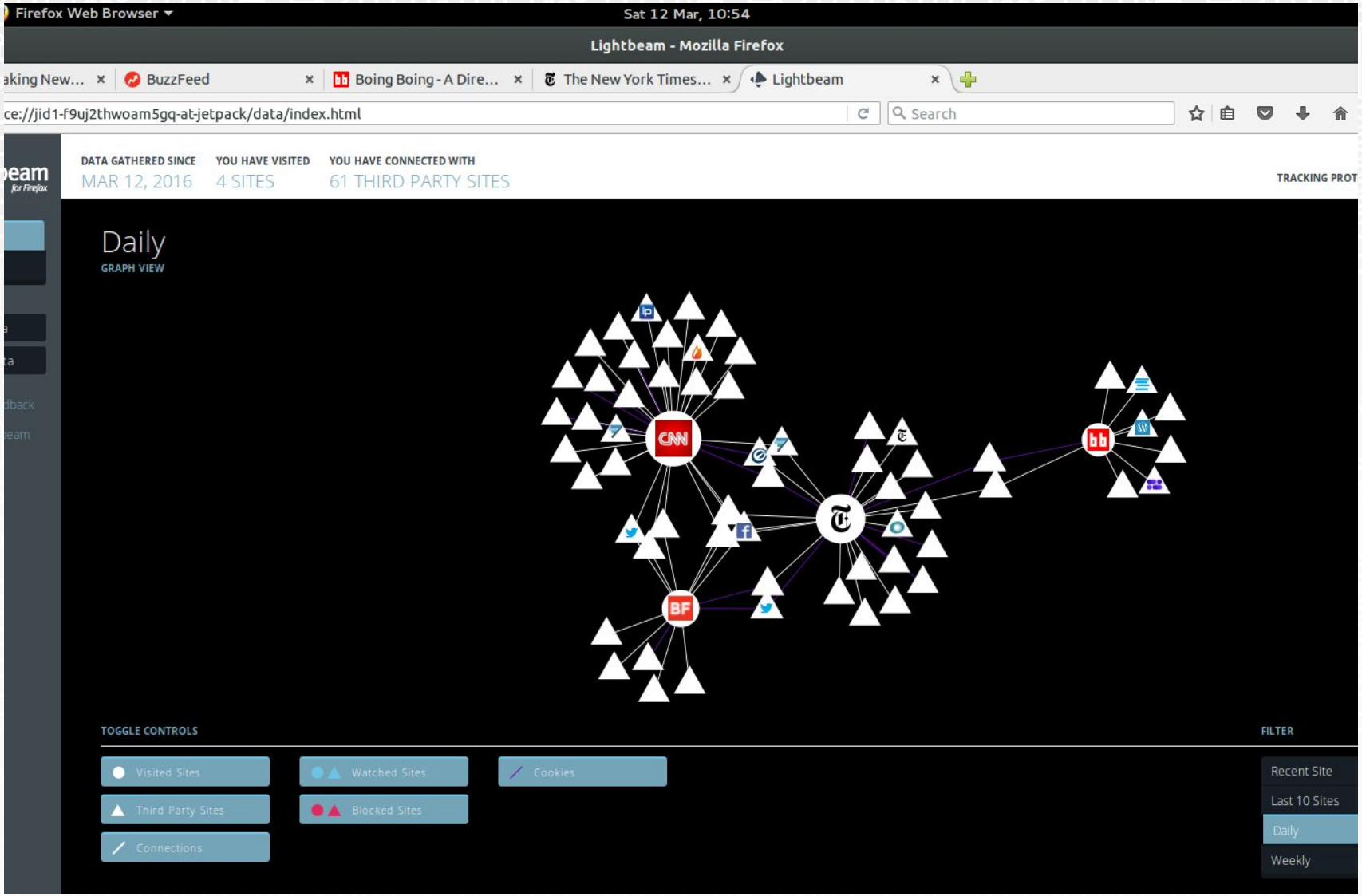
YELL people that you're going to track their every move on a Web site, store that information in files and analyze it later, associating it with personal data they gave the site earlier, and the response might be, "Back off, Big Brother!"

But that is not a paranoid vision of personal-data piracy. It's simply what happens when, as you browse the Web, you (or your browser, without your knowledge) accept a "cookie," a short bit of text that a Web site can store on a user's machine. In other words, it happens every day, millions and millions of times.

The term cookie has been used by computer scientists for a long time, but its origin is murky. A Web site uses a cookie to recognize return visitors. It can be no more than 4,096 characters long, but it is often as short as 10 or 20 characters.

Cookies can let users avoid tediously typing in their user names and passwords at sites that require them. (But you wouldn't want to let a cookie to keep track of your password for a site where someone could do real damage to your bank account, like at a stock trading site.) And cookies help shopping sites keep track of a limited amount of information, like the contents of a shopping basket or a mailing address.

Third Party Tracking



Why Focus on Third Party Trackers?

- Non-consensual
- Ubiquitous
- Hard to avoid
- Strong financial incentive

This is Big Business – A Multi Billion Dollar Industry

Some Key Players in the Industry

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.

July 15, 1999

Fresh From Your Browser's Oven

By GLENN FLEISHMAN

YELL people that you're going to track their every t information in files and analyze it later, associating it with personal data they gave the site t be, "Back off, Big Brother!"

But that is not a paranoid vision of personal-data p s when, as you browse the Web, you (or your browser, without your knowledge) accept a " t a Web site can store on a user's machine. In other words, it happens every day, m

The term cookie has been used by computer in is murky. A Web site uses a cookie to recognize return visitors. It can be no ma as short as 10 or 20 characters.

Cookies can let users avoid tediousl quire them. (But you wouldn't want to let a ie to l real d ge to your bank account, like at a s unt of information, like the con

FREEDOM TO TINKER

research and expert commentary on digital technologies in public life

If You're Going to Track Me, Please Use Cookies

JULY 7, 2009 BY ED FELTEN

Web cookies have a bad name. People often complain — with good reason — about sites using cookies to track them. Today I want to say a few words in favor of tracking cookies.

[Technical background: An HTTP "cookie" is a small string of text. When your web browser gets a file from a site, the site can send along a cookie. Your browser stores the cookie. Later, if the browser gets another file from the same site, the browser will send along the cookie.]

What's important about cookies, for our purposes, is that they allow a site to tell when it's seeing the same browser (and therefore, probably, the same user) that it saw before. This has benign uses — it's needed to implement the shopping cart feature of e-commerce sites (so the site knows which cart is yours) and to remember that you have logged in to a site so you don't have to log in over and over.

The dark side of cookies involves "hidden" sites that track your activities across the web. Suppose you go to A.com, and A.com's site includes a banner ad that is provided by the advertising service AdService.com. Later, you go to B.com, and B.com also includes a banner ad provided by AdService.com. When you're reading A.com and your browser goes to AdService.com to get an ad, AdService.com gives you a cookie. Later, when you're reading B.com and your browser goes back to AdService.com to get an ad, AdService.com will see the cookie it gave you earlier. This will allow AdService.com to link together your visits to A.com and B.com. Ad services that place ads on lots of sites can link together your activities across all of those sites, by using a "tracking cookie" in this way.

What Happened?

Samy Kamkar

Combination of all persistence mechanisms = Evercookie

EXAMPLE

Cookie found: *uid* = 974

Click to create an evercookie. Don't worry, the cookie is a random number between 1 and 1000, not enough for me to track you, just enough to test evercookies.

Click to create an evercookie

userData mechanism: undefined
cookieData mechanism: **974**
localData mechanism: **974**
globalData mechanism: undefined
sessionData mechanism: **974**
windowData mechanism: **974**
pngData mechanism: **974**
etagData mechanism: **974**
cacheData mechanism: **974**
dbData mechanism: **974**
lsoData mechanism: **974**
slData mechanism: undefined

Now, try deleting this "uid" cookie anywhere possible, then

Click to rediscover cookies

or

Click to rediscover cookies WITHOUT reactivating deleted cookies

Fingerprinting


```
1  GET /
2  Host: commons.wikimedia.org
3  User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_
   64; rv:40.0) Gecko/20100101 Firefox/40.0
4  Accept: text/html,application/xhtml+xml,applicat
   ion/xml;q=0.9,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  DNT: 1
8  Referer: https://commons.wikimedia.org/wiki/Cate
   gory:Fonts
9  Cookie: WMF-Last-Access=06-Dec-2015; GeoIP=US:CA
   :Oakland:37.83:-122.22:v4; CP=H2; commonswikimwu
   ser-sessionId=a8f3987a024fdea3
10 Connection: keep-alive
11 Cache-Control: max-age=0
                                    7,1           All
```

Panopticlick 1.0 (Jan 2010)

Panopticlick

How Unique — and Trackable — Is Your Browser?

Your browser fingerprint **appears to be unique** among the 6,176,561 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys **at least 22.56 bits of identifying information.**

Browser Characteristic	bits of identifying information	one in *x* browsers have this value	value
User Agent	12.76	6916.64	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Ubuntu Chromium/45.0.2454.101 Chrome/45.0.2454.101 Safari/537.36
HTTP_ACCEPT Headers	10.97	2004.08	text/html, */* gzip, deflate en-US,en;q=0.8,de;q=0.6
Browser Plugin Details	13.22	9546.46	Plugin 0: Chromium PDF Viewer; ; mhjfbmdgcfjbbpaeojofohoefgiehjai; (; application/pdf; pdf). Plugin 1: Chromium PDF Viewer; Portable Document Format; internal-pdf-viewer; (Portable Document Format; application/x-google-chrome-pdf; pdf). Plugin 2: Chromoting Viewer; This plugin allows you to securely access other computers that have been shared with you. To use this plugin you must first install the Chrome Remote Desktop webapp.; internal-remoting-viewer; (; application/vnd.chromium.remoting-viewer;). Plugin 3: Widevine Content Decryption Module; Enables Widevine licenses for playback of HTML

Calculating Entropy

Entropy: a mathematical quantity which allows us to measure how close a fact comes to revealing a person's identity uniquely.

Surprisal: a quantity measuring how unexpected a new piece of information is, which allows us to recalculate entropy.

$$\Delta S = -\log_2(\Pr(X=x))$$

Starsign $\Delta S = -\log_2(\Pr(\text{Starsign}=\text{Capricorn})) = -\log_2(1/12) = 3.58$ bits

Birthday $\Delta S = -\log_2(\Pr(\text{DOB}=\text{Jan 2}) = -\log_2(1/365) = 8.51$ bits

Metrics

A mixture of **headers** & **javascript-detection** to measure your browser characteristics

Headers:

- User-Agent
- HTTP Accept
- Cookies

Javascript:

- Plugins
- Timezone
- Screen Resolution / Color depth
- Fonts & Supercookies

ELECTRONIC FRONTIER FOUNDATION

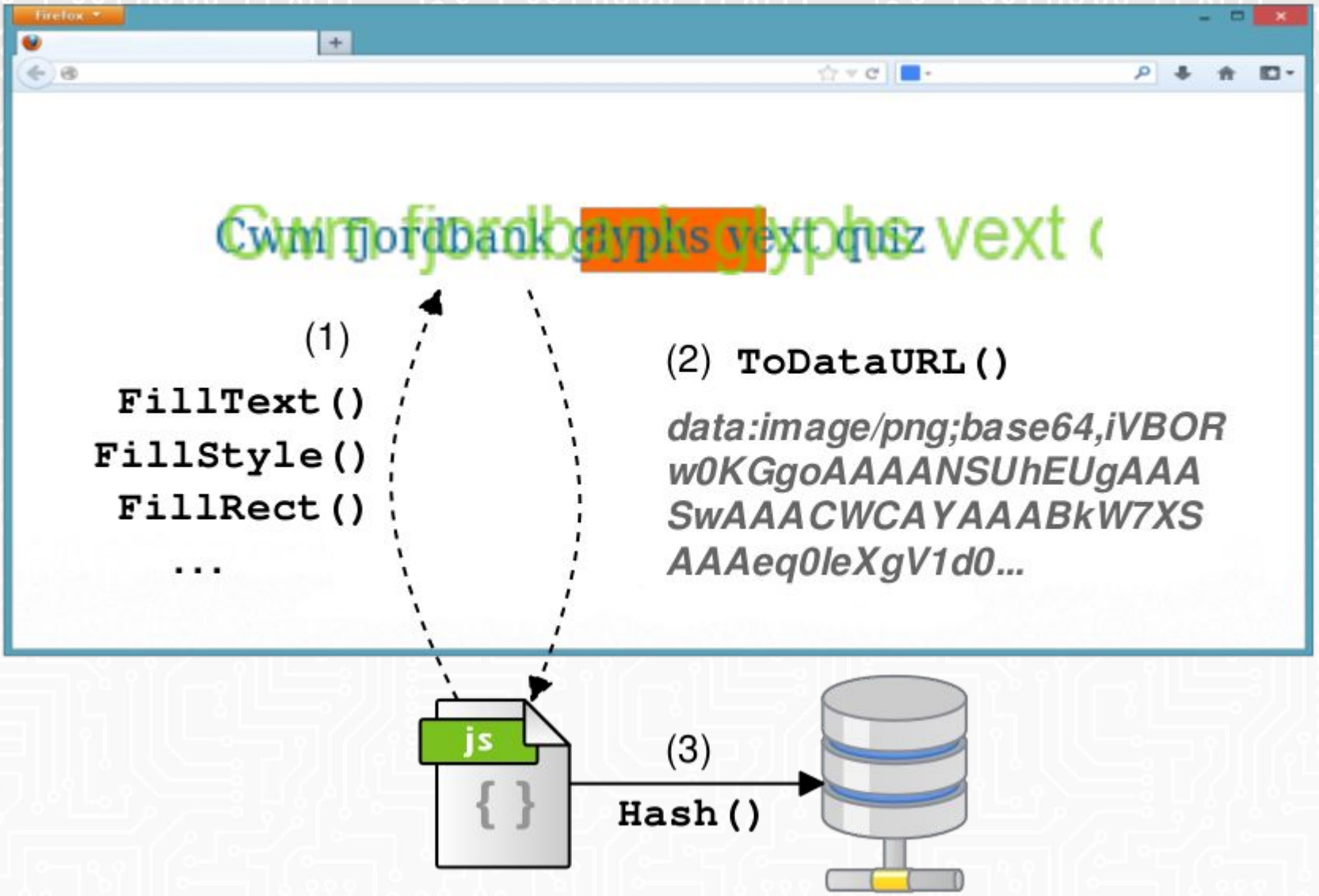
How Unique Is Your Web Browser?

Peter Eckersley*

Electronic Frontier Foundation,
pde@eff.org

Abstract. We investigate the degree to which modern web browsers are subject to "device fingerprinting" via the version and configuration information that they will transmit to websites upon request. We implemented one possible fingerprinting algorithm, and collected these fingerprints from a large sample of browsers that visited our test side, panopticlick.eff.org. We observe that the distribution of our fingerprint contains at least 18.1 bits of entropy, meaning that if we pick a browser at random, at best we expect that only one in 286,777 other browsers will share its fingerprint. Among browsers that support Flash or Java, the situation is worse, with the average browser carrying at least 18.8 bits of identifying information. 94.2% of browsers with Flash or Java were unique in our sample.

By observing returning visitors, we estimate how rapidly browser fingerprints might change over time. In our sample, fingerprints changed quite rapidly, but even a simple heuristic was usually able to guess when a fin-

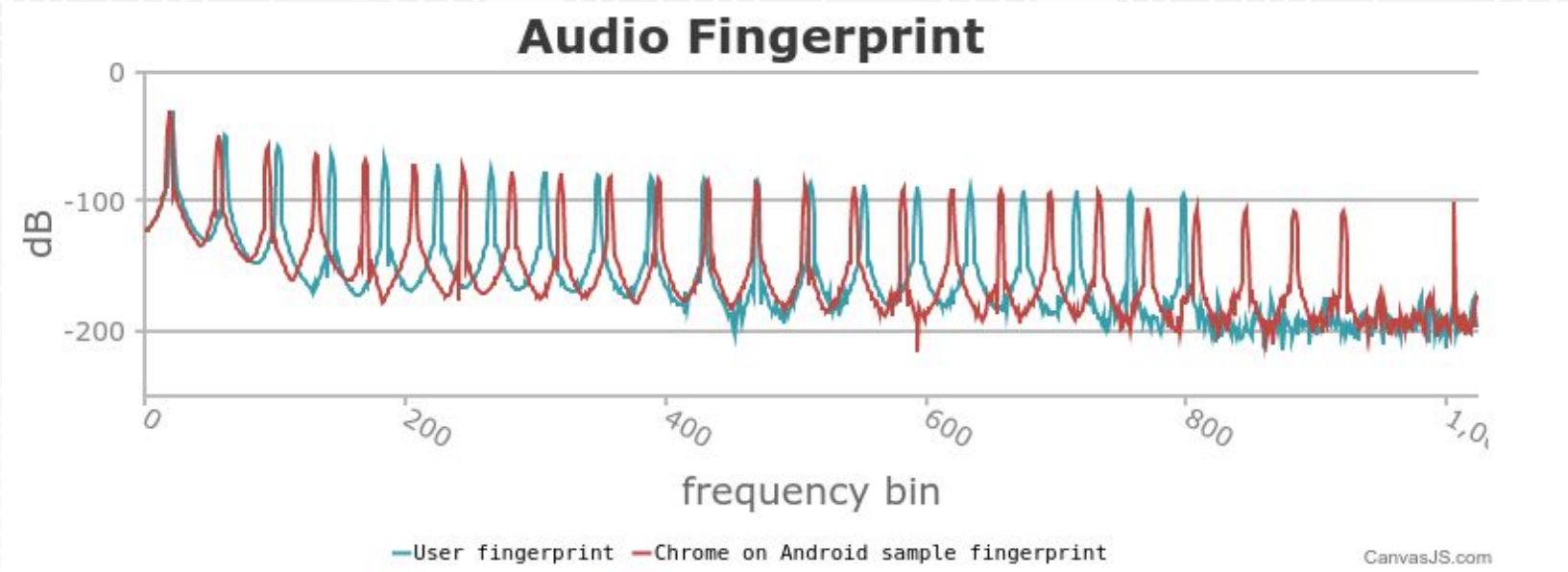

(1)
FillText()
FillStyle()
FillRect()
...
(2) ToDataURL()

w0KGgoAAAANSUhEUgAAA
SwAAACWCAYAAABkW7XS
AAAeq0leXgV1d0...
js
{ }
(3)
Hash()


CanvasFingerprintBlock
Blocked 1 potential HTML canvas fingerprinting attempt on this page
Prevented a script on https://panopticlick.eff.org from capturing the following 2000px × 200px canvas:
Cwm fjordbank glyphs vext quiz, 😀
Cwm fjordbank glyphs vext quiz, 😀

AddThis®

LIGATUS


Audio Fingerprint
0
-100
-200
dB
0
200
400
600
800
frequency bin
User fingerprint
Chrome on Android sample fingerprint
CanvasJS.com

SilverPush


atlas
by Facebook


Ve are nihilists, Mr Lebowski,
Ve do not believe in ze private web!

I Like Targeted Ads!

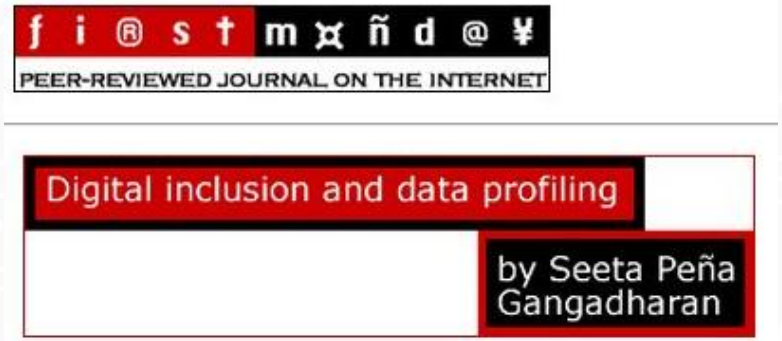
- You have no control over how your information is stored/used
- Third parties have no obligation to anonymize or store temporarily
- Data can be stolen or sold
- Misuse of ad targeting


THE WALL STREET JOURNAL.

Subscribe Now

WHAT THEY KNOW

Websites Vary Prices, Deals Based on Users' Information



Rewire

INVESTIGATIONS ABORTION

Anti-Choice Groups Use Smartphone Surveillance to Target 'Abortion-Minded Women' During Clinic Visits

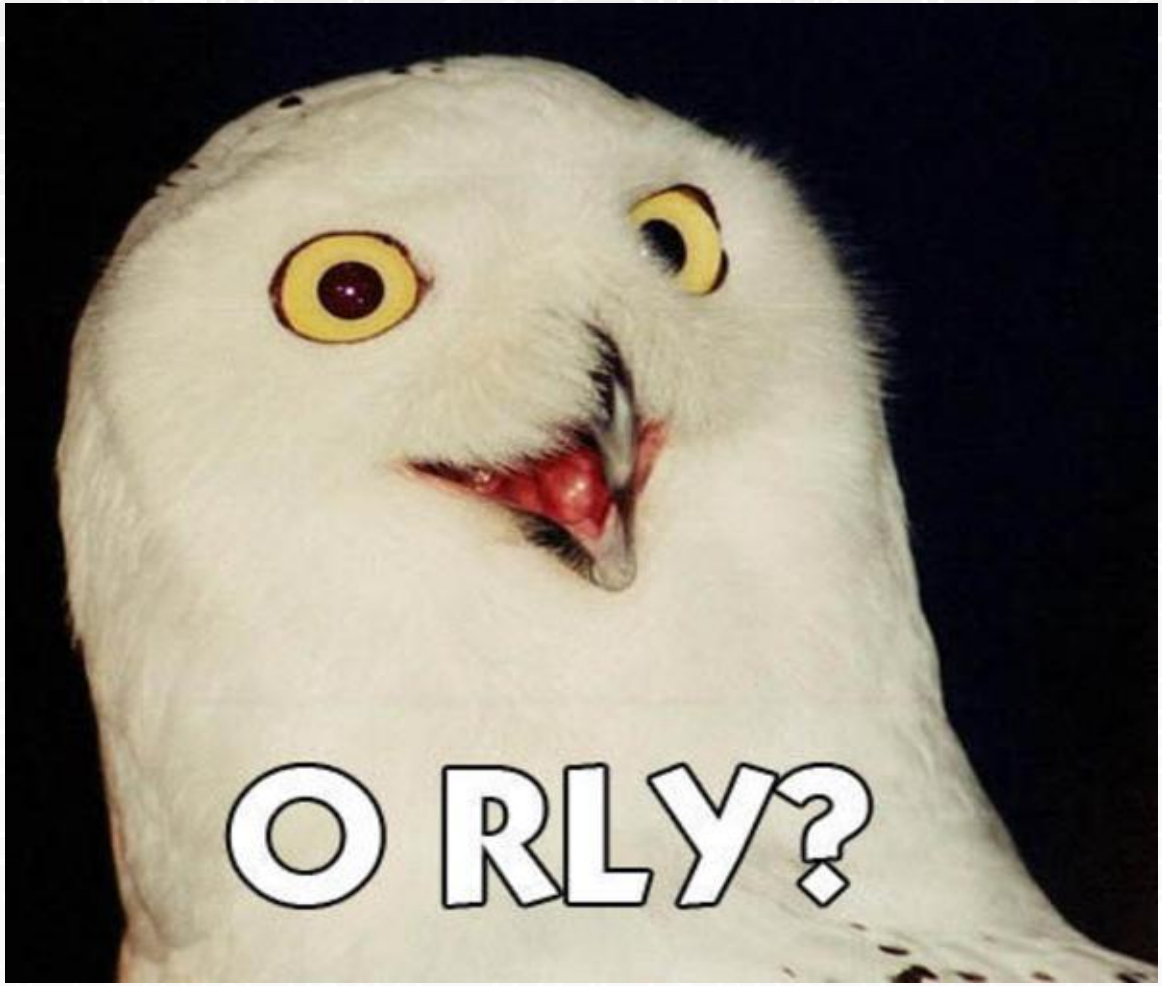
May 25, 2016, 6:52pm Sharona Coutts

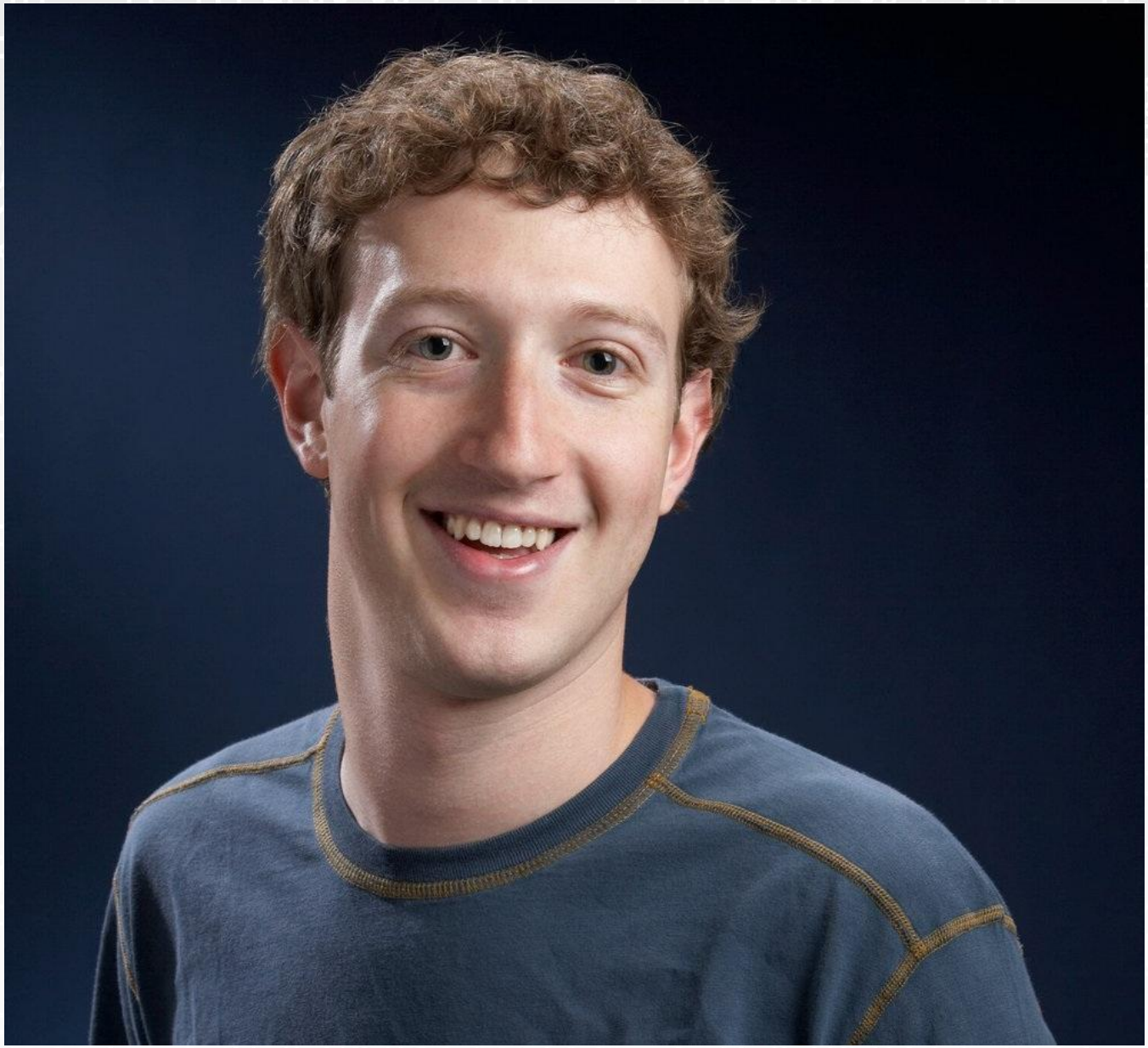
Women who have visited almost any abortion clinic in the United States have seen anti-choice protesters outside, wielding placards and chanting abuse. A Boston advertiser's technology, when deployed by anti-choice groups, allows those groups to send propaganda directly to a woman's phone while she is in a clinic waiting room.

Geo-fencing technology can be deployed by anti-choice groups to send propaganda directly to a woman's phone while she is in a clinic waiting room.

Kiva Bay for *Rewire*

Privacy Is Dead!





TECH

More: Mark Zuckerberg

Mark Zuckerberg Just Spent More Than $30 Million Buying 4 Neighboring Houses For Privacy

ALYSON SHONTELL

OCT. 11, 2013, 7:42 AM 155,015 47

Mark Zuckerberg just made an unusual purchase.

Well, four purchases.

Facebook's billionaire founder bought four homes surrounding his current home near Palo Alto, Mercury News reports. The houses cost him more than $30 million, including one 2,600 square-foot home that cost $14 million. (His own home is twice as large at 5,000 square-feet and cost half as much.)

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
- Geo-targeting for Political Reasons
- Chilling Effects

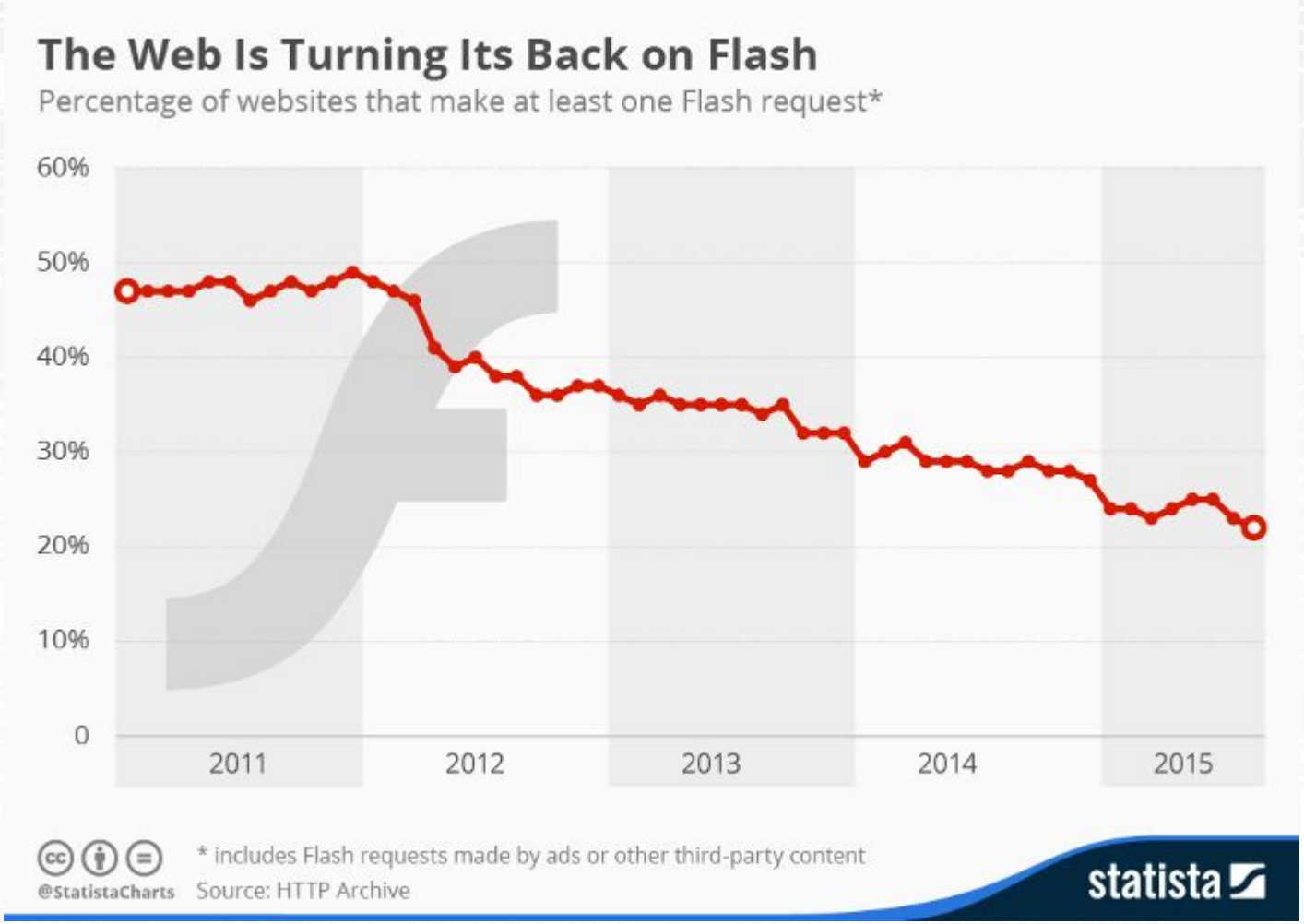
Privacy lets us make mistakes, play with ideas, and grow as individuals—it gives us the space to discover who we are.

Don’t Give Up HOPE (XI)!

The Good, the Bad, and the Ugly

Past Efforts to Stop Tracking

The Good


The Web Is Turning Its Back on Flash
Percentage of websites that make at least one Flash request*
60%
50%
40%
30%
20%
10%
0
2011
2012
2013
2014
2015
* includes Flash requests made by ads or other third-party content
@StatistaCharts
Source: HTTP Archive
statista

The Good

- Tor Browser
  - Great Tracking Protection
  - Not Always Easy to Use
  - Patches Coming Back to Firefox
- Firefox Tracking Protection
- Open WPM
- More Research!

The Bad (Or Just Less Effective)

- Incognito Mode
  - Not meant to be used to stop tracking
  - Doesn't Block Fingerprinting
  - Doesn't Block Some Supercookies
- Adblockers
  - Most do not block trackers—especially invisible ones—by default
  - Questionable business models
- W3C's Do Not Track Policy
  - No Enforcement Mechanism / Low Compliance

The Ugly

Digital Advertisers Alliance

- Ad Choices
  - Advertisers have proposed to self regulate
  - DAA members offer an 'opt out'
  - Only required to not show targeted ads
  - No requirements on what data they can and can not collect/store
  - Not legally binding
  - Doesn’t address security concerns
  - Still only limited adoption

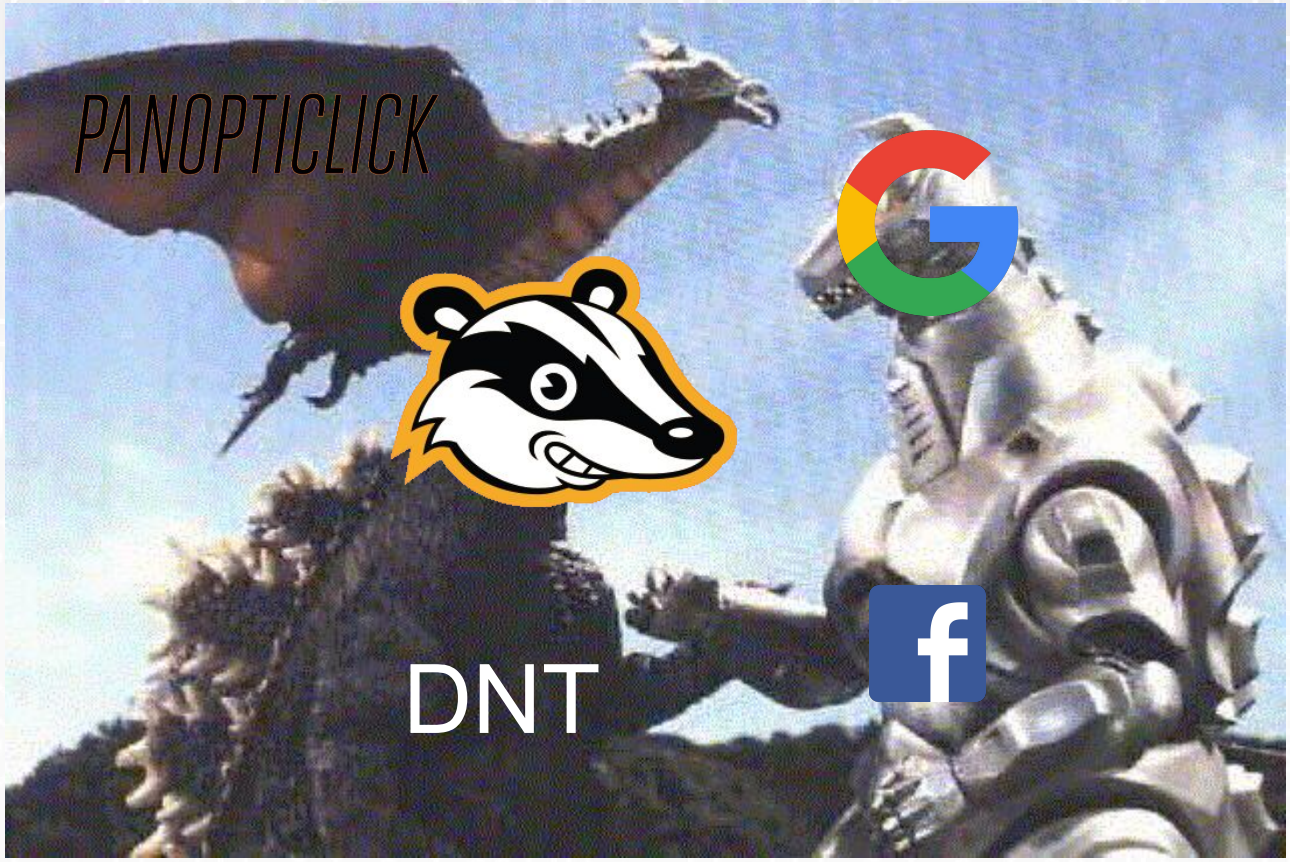
The Ugly

Interactive Advertising Bureau

- DEAL: The adblocker blocker
  - Doesn't address privacy concerns
  - Doesn't address security concerns
  - Annoying for users
  - More like "DEAL with it" amirite?
- LEAN: Non-Obnoxious Ads
  - Still doesn't address privacy concerns
  - Only minimally addresses security concerns

None of these really addressed all the concerns we had at EFF. And we like combining technology, law, and activism, so....

Privacy Badger, Panopticlick, and Do Not Track to the Rescue!



Privacy Badger In It's Natural Habitat

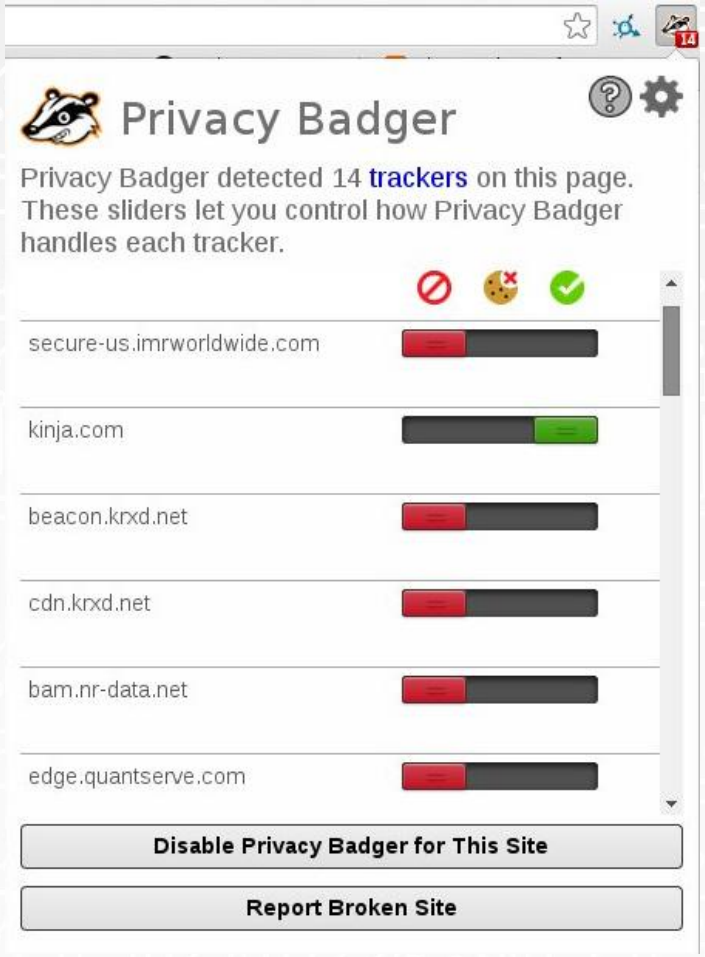
Privacy Badger

- Browser Extension
- Free Open Source Software
- Focuses on completely blocking trackers at the source
- Uses an algorithm instead of a blacklist
- Allows honest actors a way out

How Does Privacy Badger Work?

- Tells sites you do not wish to be tracked
- Looks for third parties as your browse the web
- If a third party is seen on several different domains...
- ...and it appears to be tracking you...
- It gets blocked!

Privacy badger on Gawker.com



Privacy Badger on BoingBoing.net

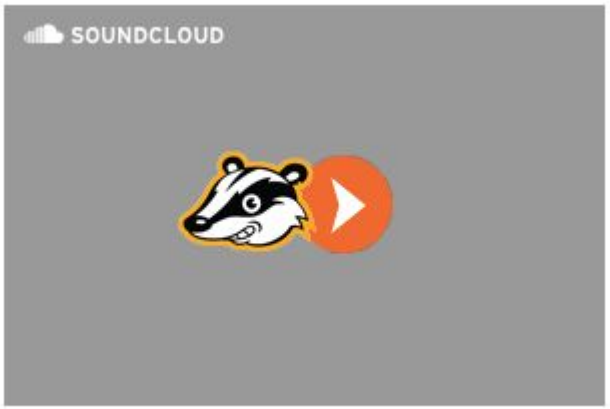
User Choice!


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



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

The Policy Side — A New DNT

- EFF has written a new do not track policy
- Document which states that users sending DNT will not be tracked
- Posted at a well-known location on your website
- We think that the FTC can take action against someone who posts this and violates it.

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 can be anonymized and aggregated for analytics

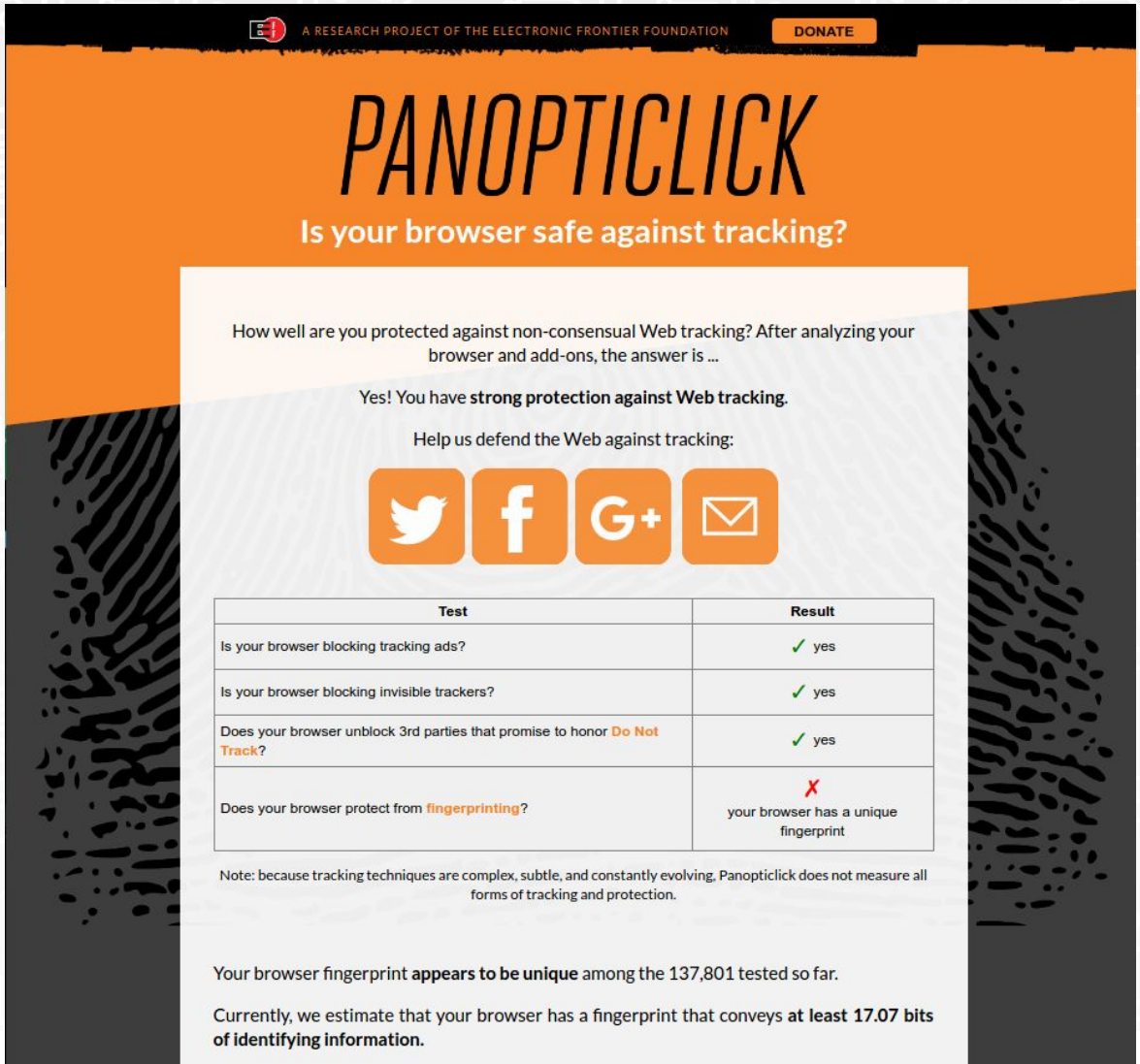
The Policy Side — A New DNT

- Sites adopting it get automatically whitelisted by Privacy Badger and other participating tracking protection software
- Blocking sites that don't respect DNT creates an incentive to respect DNT
- Carrot and the stick

The Policy Side — A New DNT

- Right now we have a policy up
  - https://www.eff.org/dnt-policy
- Adopted by:
  - Duck Duck Go
  - Adzerk
  - Mixpanel
  - Medium
  - Disconnect
  - And more!

Panopticlick 2.0 (Dec 2015)



New Features

- Tracker Blocking Protection test
- Ad Blocking Protection test
- Open-Sourced Codebase Rewrite
- 6 new fingerprinting metrics
- Fingerprinting tests epoched

Results

- The test has been run over 800,000 times.
- We've seen over 15,500 unique IPs start protecting themselves.

Results

yayponiez

Future Plans

Panopticlick

- Opening up the data
- Additional tracking tests
- Testing framework for blockers

Panopticlick

- Opening up the data
- Additional tracking tests
- ~~Testing framework for blockers~~

Privacy Badger / DNT

- Heuristic Improvements
- Reduce false positives
- Detect and block more types of supercookies
- Detect and block more types of fingerprinting
- More DNT adoption!

What Must Be Done

How You Can Help

- Use Privacy Badger
- Use Panopticlick
- Adopt DNT
- Submit a bug report / pull request
- Donate to EFF!

We Still Need Better Tools in the Browser

- Built in tracking protection
  - This is already happening!
- Double keyed cookies and supercookies
- Browsers hardened against fingerprinting
- Better controls for blocking and clearing supercookies

We also need new business models for the web

- Memberships
- Donations
- Crowd Funding
- Micropayments
- Non-Intrusive Advertising

Third party tracking is still a huge problem on the web, but the situation isn't hopeless.

Don’t be a privacy nihilist, be a privacy vegan!

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.

Thank You!

https://eff.org/privacybadger
https://panopticlick.eff.org
https://github.com/EFForg

Follow: @cooperq && @legind && @privacybadger

Acknowledgements: Peter Eckersley, Garrett Robinson, Yan Zhu, Jeremy Gillula, Gunes Acar, Franzi Roesner, Noah Schwarz, Hugh D'Andrade, Rob Cutmore, Blake Griffith, Dan Auerbach, Alexei Miagkov, The HOPE Crew, OpenWPM, Open source contributors, All Our Haters...

cjq@eff.org: 75FB 9347 FA4B 22A0 5068 080B D0EA 7B6F F0AF E2CA
bill@eff.org: 977A 04EC 512A 9D0D B4A5 6E0E CDCA E8ED 6842 C592