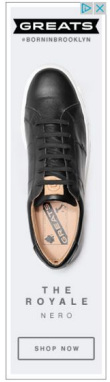
Sandboxing Trackers with Resource Blocking Lists

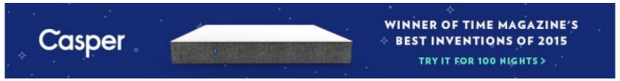
Steven Englehardt
@s_englehardt

Joint work with Tanvi Vyas and Eric Rescorla at Mozilla

Tracking Protection

≈





Manchester City 2-1 Sunderland: Former Manchester United defender Paddy McNair scores late own goal to gift first Premier League victory to Pep Guardiola

- Late Paddy McNair own goal handed Manchester City a win in Pep Guardiola's first match in charge
- An equaliser from Jermain Defoe had looked like denying Guardiola in the Premier League opener
- Sub McNair, signed from Manchester United this week, headed into his own net after 87 minutes
- New City boss had made an immediate impact at City by dropping Joe Hart and Yaya Toure

By ROB DRAPER FOR THE MAIL ON SUNDAY
PUBLISHED: 13:21 EST, 13 August 2016 | **UPDATED:** 15:41 EST, 13 August 2016

Share
1.2k shares
667 View comments

At the end, the Etihad Stadium roared with the kind of enthusiasm you might expect when greeting one of the world's finest and most iconic coaches. Poor Paddy McNair, brought on to safeguard the score, had just headed into his own goal within four minutes of his debut, and City finally had their breakthrough.

Jesus Navas crossed the ball, Vito Mannone flicked it away from the feet of Kelechi Iheanacho and McNair simply could not react quick enough to avoid nodding home from close range. The clock read 87 minutes and City fans sang with gusto, as though they finally believed a Messianic figure was about to lead them to the promised land. And so it will be recorded that the Pep Guardiola era began with a win

And, after the years of anticipation, it was really Guardiola on the touchline, finally overseeing a Premier League match. There was the familiar expensive, well-cut suit and the distinctive bald head, bobbing up and down as he waved his arms in excitement and exasperation in equal measure. On the pitch, the look was not quite so good.

Firefox Developer Edition automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share

Manchester City 2-1 Sunderland: Former Manchester United defender Paddy McNair scores late own goal to gift first Premier League victory to Pep Guardiola

- **Late Paddy McNair own goal handed Manchester City a win in Pep Guardiola's first match in charge**
- **An equaliser from Jermain Defoe had looked like denying Guardiola in the Premier League opener**
- **Sub McNair, signed from Manchester United this week, headed into his own net after 87 minutes**
- **New City boss had made an immediate impact at City by dropping Joe Hart and Yaya Toure**

By ROB DRAPER FOR THE MAIL ON SUNDAY
PUBLISHED: 13:21 EST, 13 August 2016 | **UPDATED:** 15:41 EST, 13 August 2016

Share 1.2k shares 667 View comments

At the end, the Etihad Stadium roared with the kind of enthusiasm you might expect when greeting one of the world's finest and most iconic coaches. Poor Paddy McNair, brought on to safeguard the score, had just headed into his own goal within four minutes of his debut, and City finally had their breakthrough.

Jesus Navas crossed the ball, Vito Mannone flicked it away from the feet of Kelechi Iheanacho and McNair simply could not react quick enough to avoid nodding home from close range. The clock read 87 minutes and City fans sang with gusto, as though they finally believed a Messianic figure was about to lead them to the promised land. And so it will be recorded that the Pep Guardiola era began with a win

And, after the years of anticipation, it was really Guardiola on the touchline, finally overseeing a Premier League

Firefox Developer Edition automatically sends some data to Mozilla so that we can improve your experience. Choose What I Share

Here's The Thing With Ad Blockers

We get it: Ads aren't what you're here for. But ads help us keep the lights on.
So, add us to your ad blocker's whitelist or pay $1 per week for an ad-free version of WIRED.
Either way, you are supporting our journalism. We'd really appreciate it.

Sign Up

Already a member? Log in

Can we sandbox trackers instead of block them?

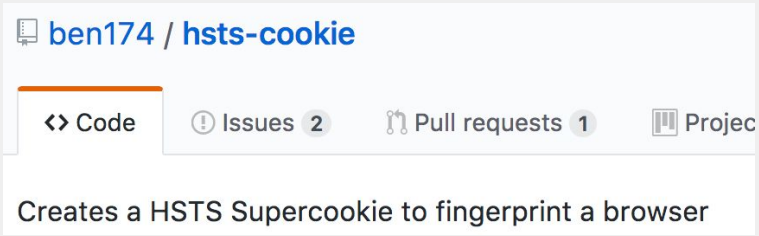
Can we sandbox trackers instead of block them?

Not completely :(

Stateful Tracking

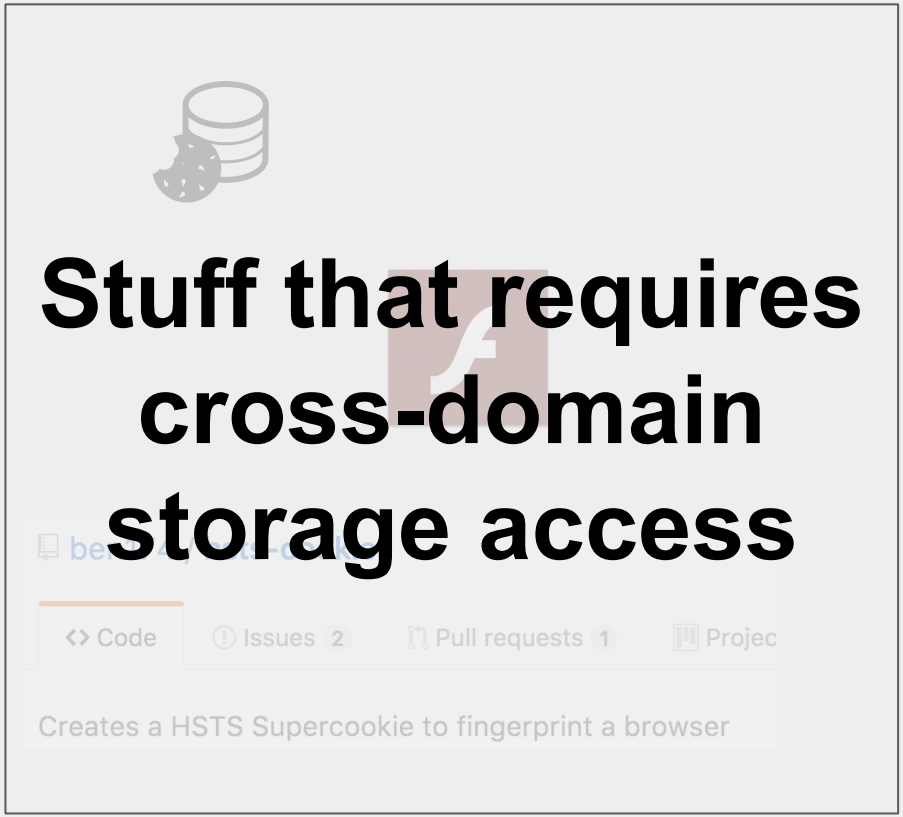
Stateless Tracking

Stateful Tracking



Stateless Tracking

Stateful Tracking



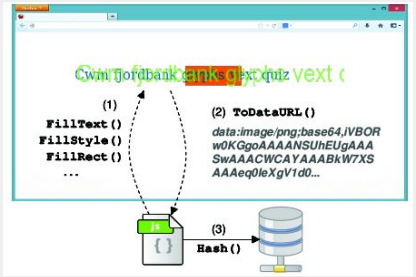
Stateless Tracking

Stateful Tracking

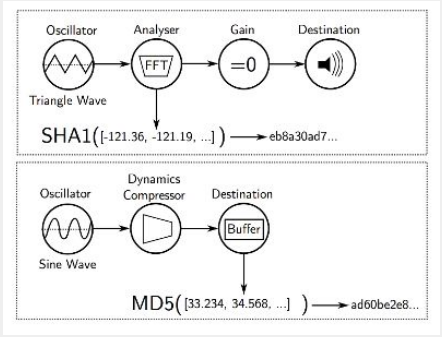
Stuff that requires cross-domain storage access

Stateless Tracking

Canvas



Audio

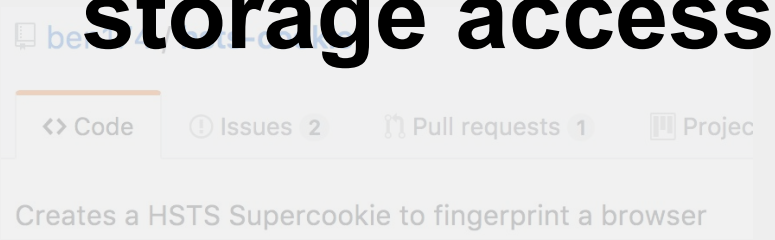


Font

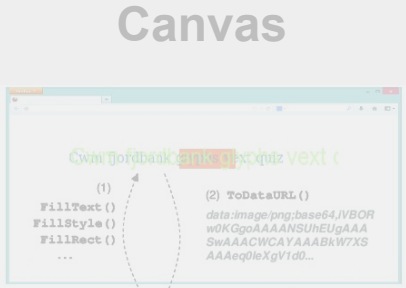
Image source: http://www.lalit.org/lab/javascript-css-font-detect/

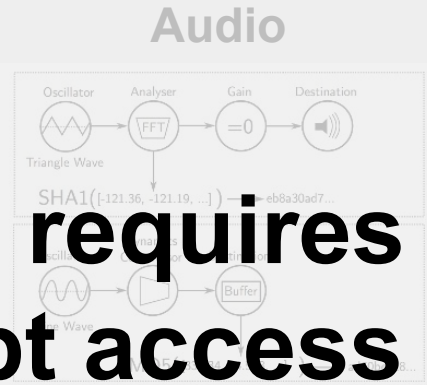
Stateful Tracking

Stuff that requires cross-domain storage access



Stateless Tracking





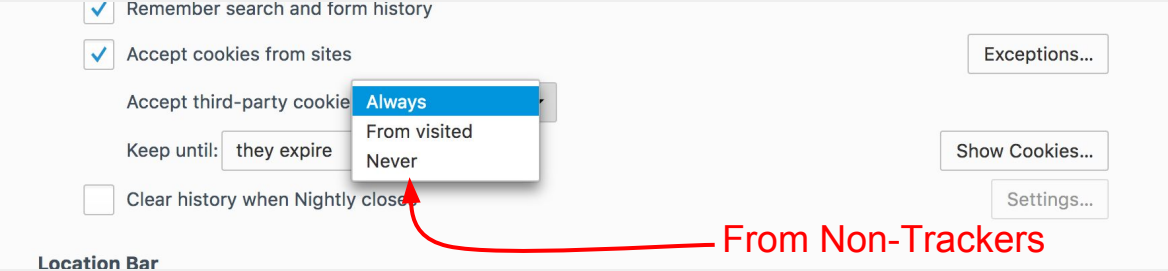
Stuff that requires Javascript access

Image source: http://www.lalit.org/lab/javascript-css-font-detect/

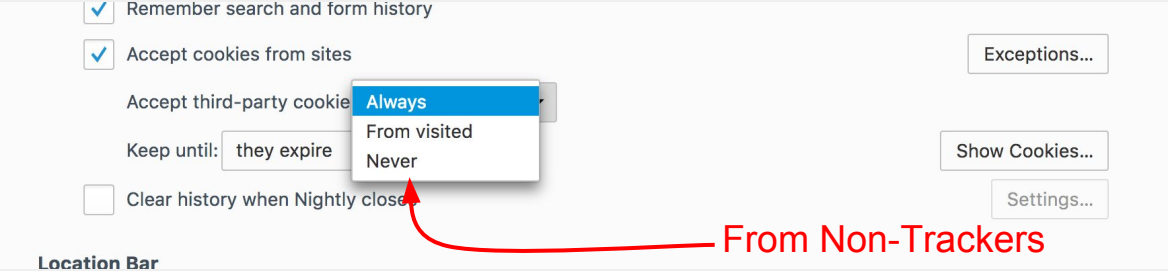
	First-party Context	Third-party Context (iframes)
Stateful		
Stateless		

	First-party Context	Third-party Context (iframes)
Stateful	SOP already provides protection	
Stateless		

1. Make a new third-party cookie blocking mode

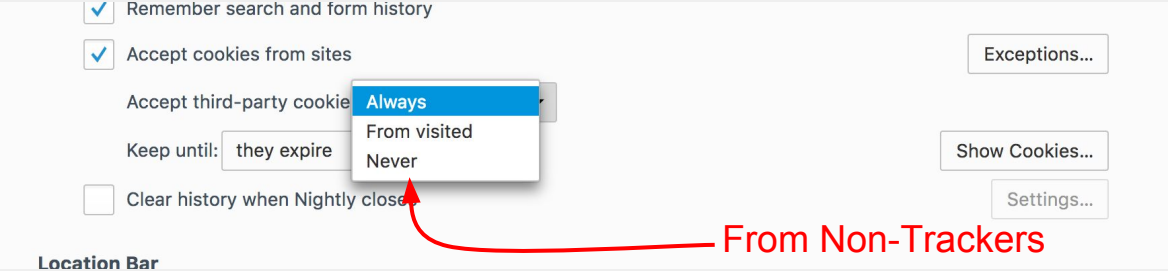


1. Make a new third-party cookie blocking mode



+ No stateful tracking in 3rd party iframes

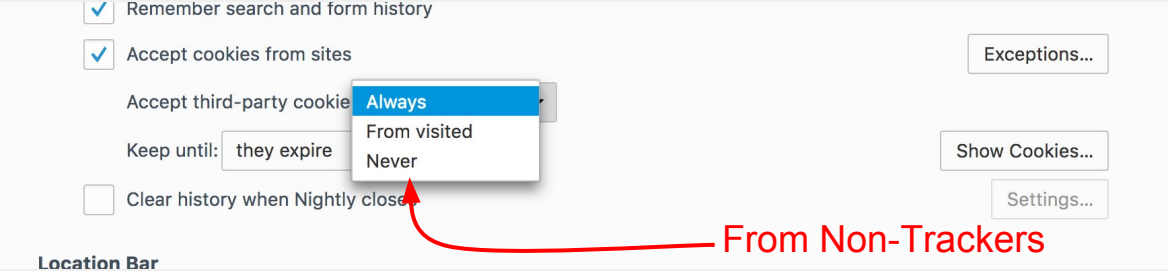
1. Make a new third-party cookie blocking mode



+ No stateful tracking in 3rd party iframes

+ No cookies with <script src…> embeds

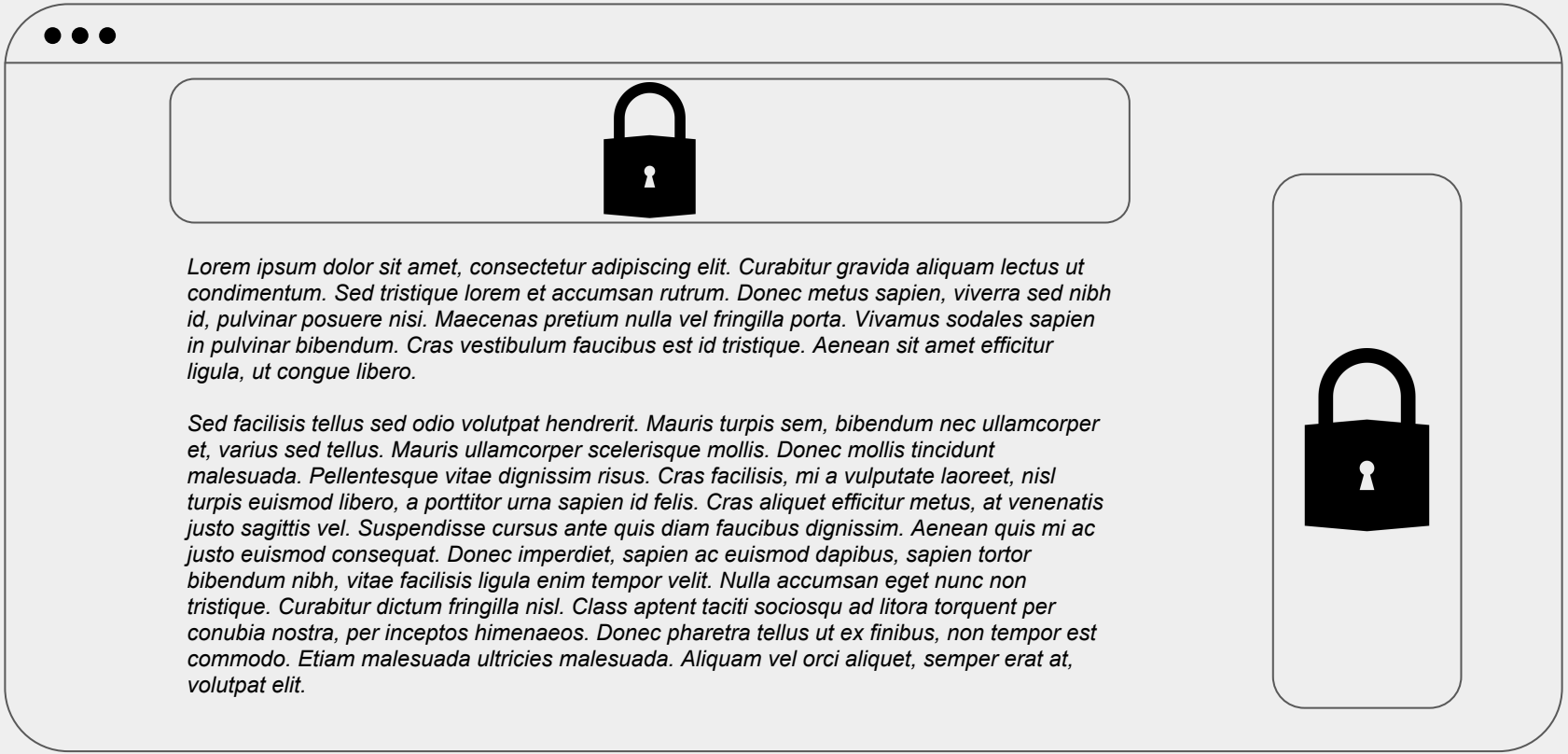
1. Make a new third-party cookie blocking mode



+ No stateful tracking in 3rd party iframes
+ No cookies with <script src…> embeds
+ Less breakage than other cookie blocking

	First-party Context	Third-party Context (iframes)
Stateful	SOP already provides protection	Selective 3rd-party cookie blocking
Stateless		

2. Block cookies and use iframe sandbox



Lorem ipsum dolor sit amet, consectetur adipiscing elit. Curabitur gravida aliquam lectus ut condimentum. Sed tristique lorem et accumsan rutrum. Donec metus sapien, viverra sed nibh id, pulvinar posuere nisi. Maecenas pretium nulla vel fringilla porta. Vivamus sodales sapien in pulvinar bibendum. Cras vestibulum faucibus est id tristique. Aenean sit amet efficitur ligula, ut congue libero.

Sed facilisis tellus sed odio volutpat hendrerit. Mauris turpis sem, bibendum nec ullamcorper et, varius sed tellus. Mauris ullamcorper scelerisque mollis. Donec mollis tincidunt malesuada. Pellentesque vitae dignissim risus. Cras facilisis, mi a vulputate laoreet, nisl turpis euismod libero, a porttitor urna sapien id felis. Cras aliquet efficitur metus, at venenatis justo sagittis vel. Suspendisse cursus ante quis diam faucibus dignissim. Aenean quis mi ac justo euismod consequat. Donec imperdiet, sapien ac euismod dapibus, sapien tortor bibendum nibh, vitae facilisis ligula enim tempor velit. Nulla accumsan eget nunc non tristique. Curabitur dictum fringilla nisl. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Donec pharetra tellus ut ex finibus, non tempor est commodo. Etiam malesuada ultricies malesuada. Aliquam vel orci aliquet, semper erat at, volutpat elit.

2. Block cookies and use iframe sandbox

+ No fingerprinting in iframes

+ Restrict plugin use, modal dialogs, top-level navigation, etc

2. Block cookies and use iframe sandbox

+ No fingerprinting in iframes

+ Restrict plugin use, modal dialogs, top-level navigation, etc

Not enough trackers are embedded in iframes.

71% of third-party scripts on top homepages will still be able track on 90%+ of pages

10% of third-party scripts on top homepages have a reduction in tracking by 50% or more

	First-party Context	Third-party Context (iframes)
Stateful	SOP already provides protection	Selective 3rd-party cookie blocking
Stateless		Reduced JS feature set (extend iFrame sandbox)

3. Block active content and sandbox iframes

Built a prototype to test this...

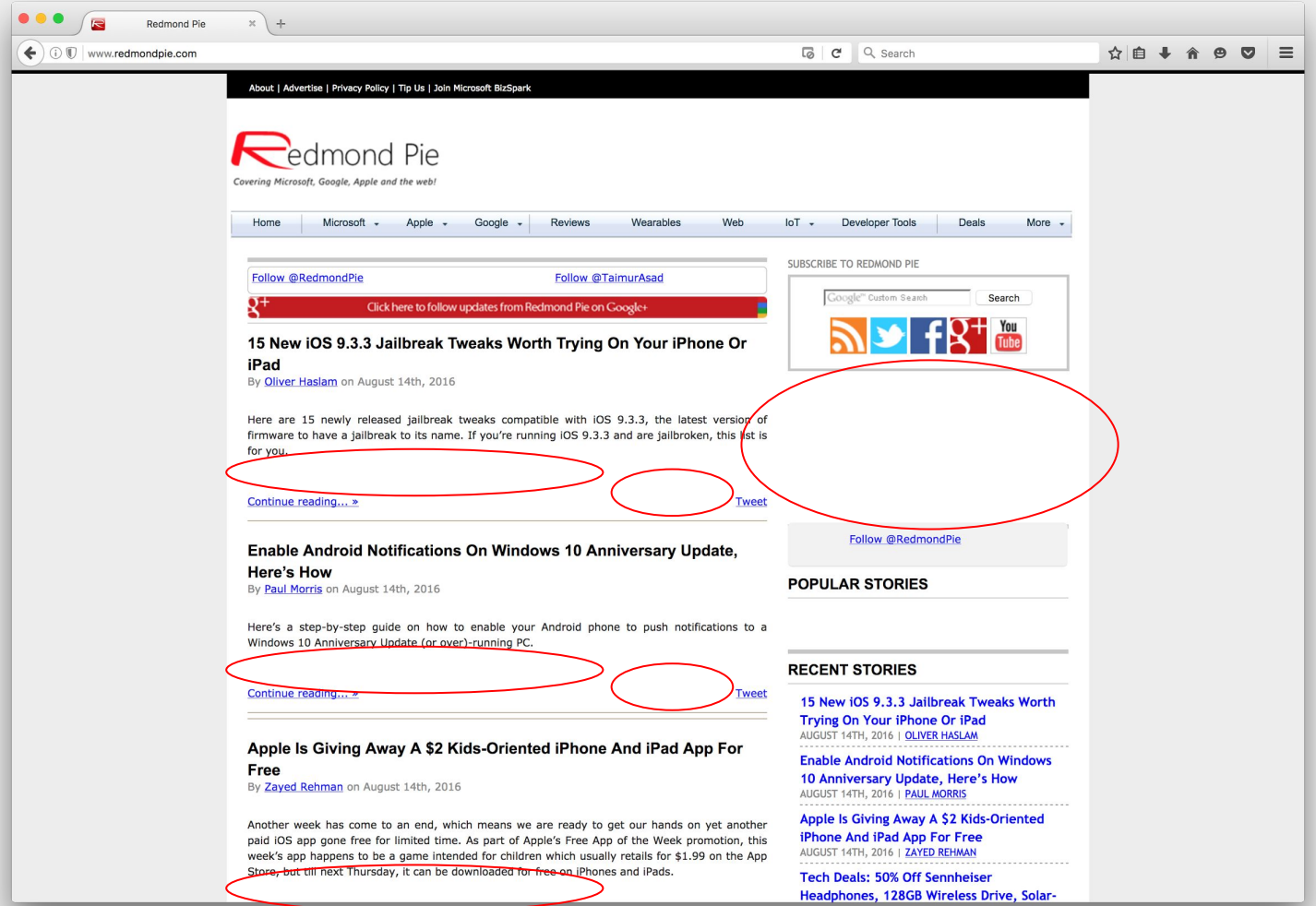
3. Block active content and sandbox iframes

Built a prototype to test this...

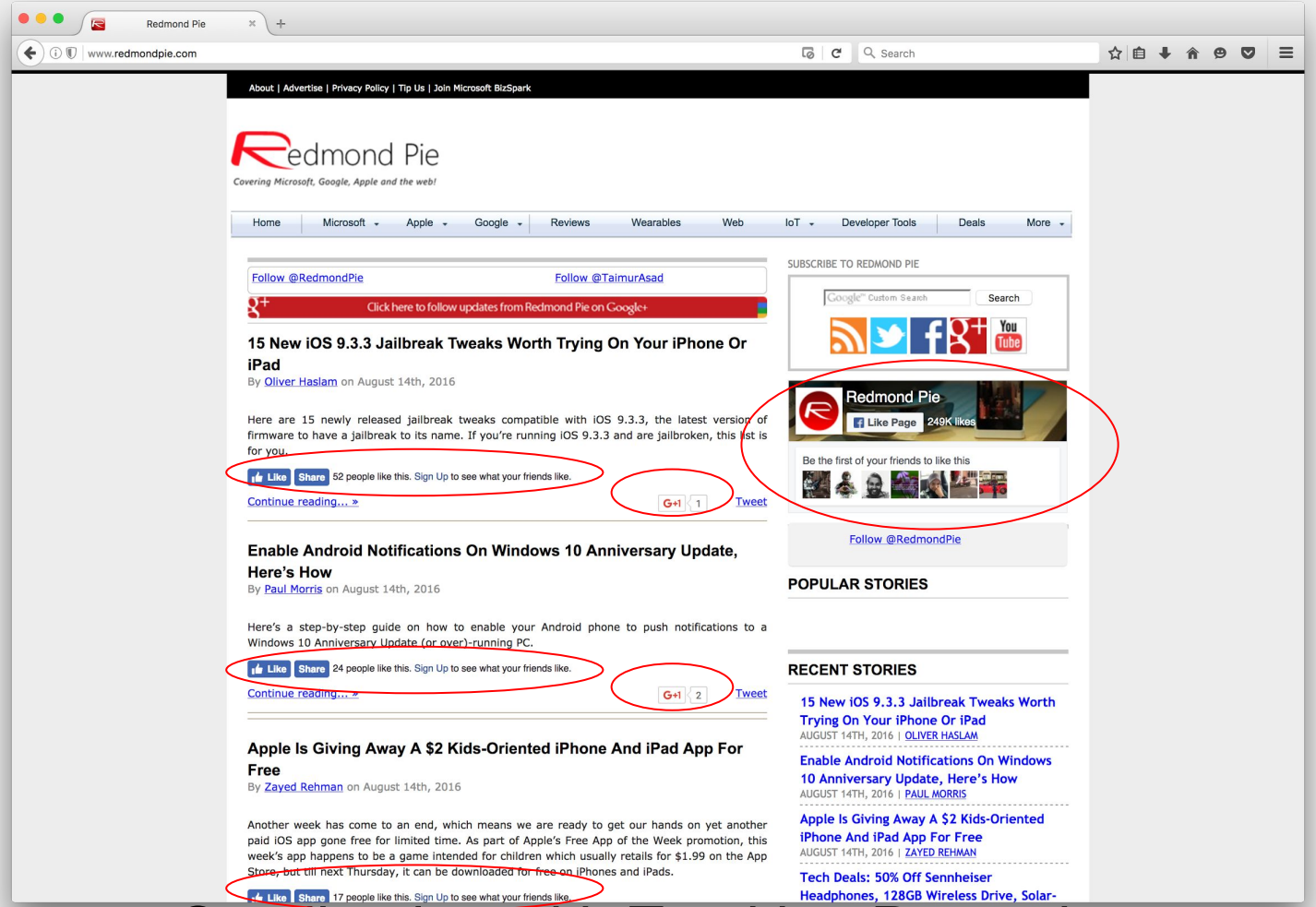
breakage is still too high!

3. Block scripts and sandbox iframes

- Google, Facebook, Twitter all require or recommend first-party script access
- 2 out of 10,000 sites iframe Doubleclick
- 209 out of 10,000 sites iframe Facebook



Blocking with Tracking Protection



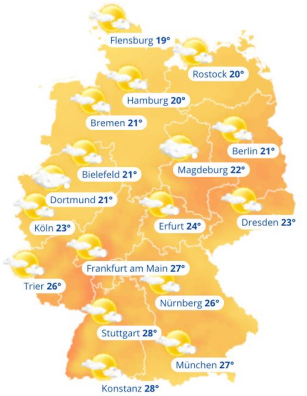
Sandboxing with Tracking Protection

wetter.com: Wetter, Wetter...

www.wetter.com

Search

Menü | wetter.com | Suche nach Ort oder PLZ



Höchstwerte heute

Guten Abend!

Ihr Wetter für heute in

Berlin

bis 21°C
leicht bewölkt

Zur Tagesvorhersage

Aussichten

Heute ist es im Norden und zum Teil auch in der Mitte teilweise bewölkt und vor allem in Richtung Küste sind einzelne Schauer möglich. In der Südhälfte scheint hingegen häufiger die Sonne und es wird sehr warm. Abgesehen von einzelnen gewittrigen Schauern an den Alpen bleibt es meist trocken.

weiterlesen

Aktuelle Themen

NEU - Alle Wetternews per WhatsApp

Grillfreunde aufgepasst!

Belastung durch Beifuß-Pollen

Anzeige

Anzeige

Empfehlungen der Redaktion

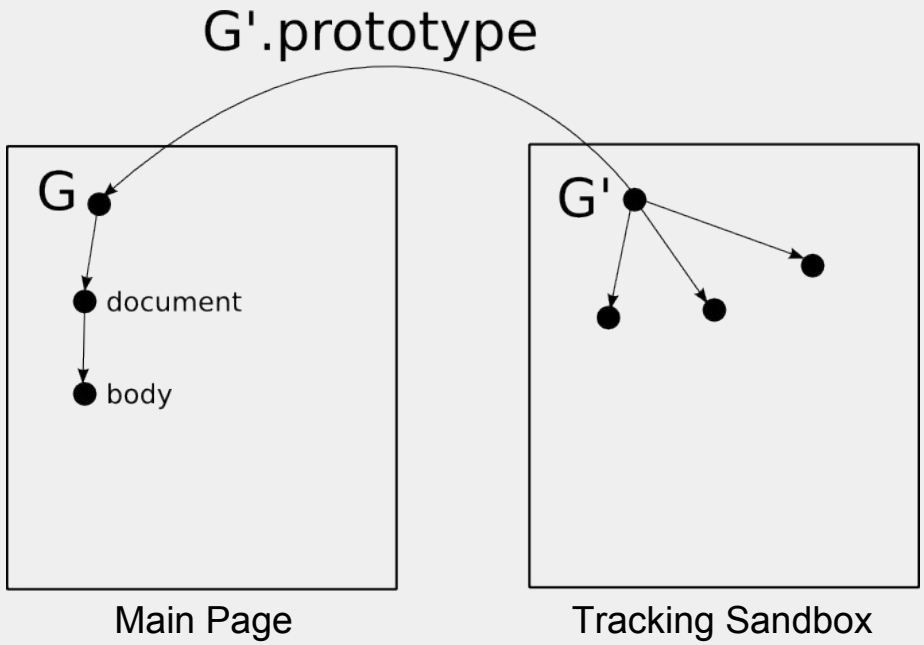
Nach oben

Blocking with Tracking Protection

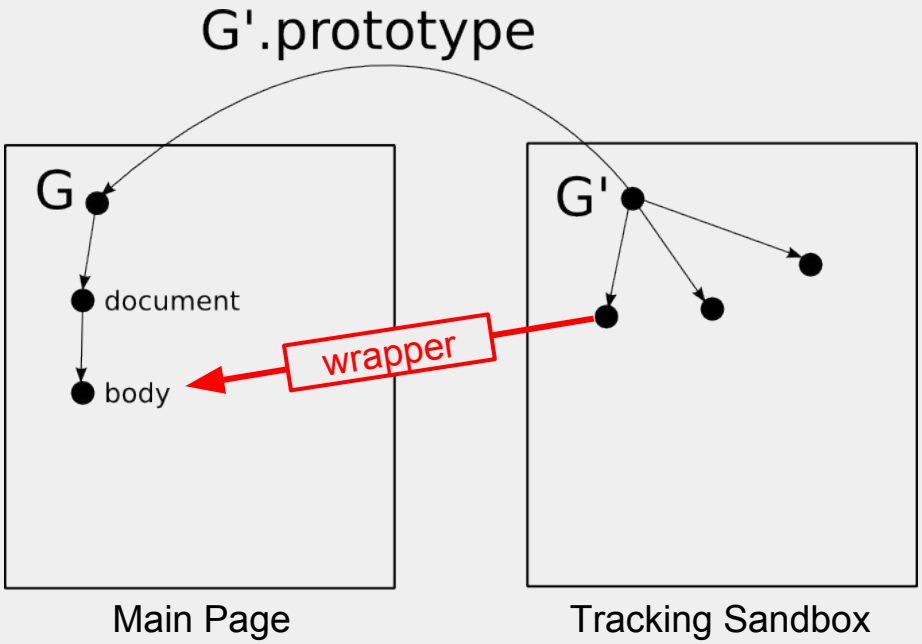
Sandboxing with Tracking Protection

	First-party Context	Third-party Context (iframes)
Stateful	SOP already provides protection	Selective 3rd-party cookie blocking
Stateless	:(	Reduced JS feature set (extend iFrame sandbox)

4. Sandbox active content and sandbox iframes



4. Sandbox active content and sandbox iframes



Define *tracking wrappers* for interactions across the sandbox boundary

What do Google scripts do?

What do Google scripts do?

```
<iframe
        onload = ...
        id = "aswift_0"
        width = "300"
        height = "250"
>< /iframe>
```

What do Google scripts do?

```
<iframe
      onload = ...
      id = "aswift_0"
      width = "300"
      height = "250"
>< /iframe>
```

```
var i = this.id,
      s = window.google_iframe_oncopy,
      h = s & amp; & amp;
s.handlers, h = h & amp; & amp;
h[i], w = this.contentwindow, d;
d = w.document
if (h & amp; & amp; d & amp; & amp;
`     ...
      w.location.replace(h)
      }
}
```

Tracking scripts require inline javascript access

- Google iframes with `onload` -- 10% of sites
- Iframes with `javascript:` src urls -- 20% of sites
- Insert inline scripts into first-party -- 18% of sites

Sandboxing Javascript is infeasible

- Breakage still too high
- Requires support for inline javascript
  - Inline function rewriting
  - Function reflection from sandbox to main page
- **Sandbox design will change as scripts change**

A Path Forward: Only block first-party context fingerprinting scripts, sandbox everything else.

- How to detect?
  - Blocklist building through crawling
  - Real time classifier in browser

- Crowdsource fingerprinting detection in scripts