



Privacy Tricks for Activist Web Developers

Micah Lee
@micahflee
micah@eff.org

GPG: 5C17 6163 61BD 9F92 422A C08B B4D2 5A1E 9999 9697

Web Developer at
Electronic Frontier Foundation
<https://www.eff.org/>

Download slides from <https://bit.ly/privacytricks>



Privacy Tricks for Activist Web Developers

Who learns your surfing habits?

Website	Companies with access to visitor data
HOPENumberNine.net	Google, Twitter
OccupyOakland.org	Google, Twitter, Facebook, ShareThis
InternetDefenseLeague.org	Google, Twitter, Facebook, Heroku
Adbusters.org	Google, Twitter, YouTube, PayPal
AnonNews.org	Google, Creative Commons, Flattr, CryptoCC
news.Infoshop.org	Google, PayPal, WePay, Constant Contact, Counterpunch



What's in an HTTP request?

- User-Agent: browser, OS, architecture, language, etc.
- Referrer: where you came from
- Other identifying headers: Accept, Accept-Encoding, Accept-Language, DNT, etc.
- Cookies (possibly tracking you)
- Also: IP address, timestamp
- If it's a 3rd party script: browser plugins, screen resolution, etc.

This info gets sent for each page load, image, css or js file, and Ajax request. Most of it gets logged.



When do you give this information to third parties?

- Facebook Like buttons
- Twitter widgets
- Google Analytics
- Embedded YouTube videos
- PayPal buttons
- Any `<script>`, ``, `<iframe>`, etc. tags that loads something from a remote server



Privacy Tricks for Activist Web Developers

Who doesn't leak visitor data

Website

Hackmeet.org

EFF.org

Riseup.net

Indymedia.org

TorProject.org

Noisebridge.net

HackBloc.org

AnarchistNews.org

From EFF's privacy policy:

We do occasionally allow our website to interact with other services, like social networking, mapping, and video hosting websites. **It is our policy not to include third-party resources when users initially load our web pages**, but we may dynamically include them later after giving the user a chance to opt-in.



Privacy Tricks for Activist Web Developers

But who cares if they know what
browser I use?

How Unique – and Trackable – is Your Browser?

<https://panopticklick.eff.org/>

It takes surprisingly few pieces of information to
uniquely identify anyone in the world

<https://www.eff.org/deeplinks/2010/01/primer-information-theory-and-privacy>



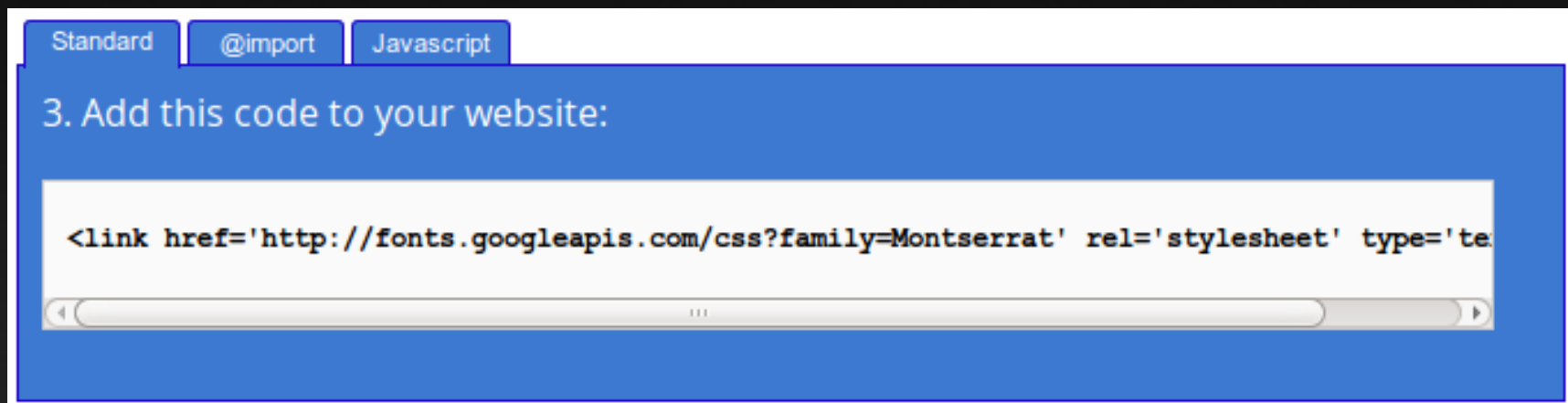
What third parties can do

- Log everything
 - Give these logs to law enforcement
 - Accidentally give these logs to hackers
- Track your visitors
 - Even if users disable third party cookies, there's enough data to build fingerprints
 - Sell this data to advertisers





TRICK: Copy Google webfonts to your own server



<https://fonts.googleapis.com/css?family=Montserrat>:

```
@font-face {  
  font-family: 'Montserrat';  
  font-style: normal;  
  Font-weight: 400;  
  src: local('Montserrat Regular'),  
  local('Montserrat-Regular'),  
  url('https://themes.googleusercontent.com/static/fonts/montserrat/v2/zhcZ-_WihjSQC0oHJ9TCYBsxEYwM7FgeyaSgU71cLG0.woff') format('woff');  
}
```

Your local stylesheet:

```
@font-face {  
  font-family: 'Montserrat';  
  font-style: normal;  
  Font-weight: 400;  
  src: local('Montserrat Regular'),  
  local('Montserrat-Regular'),  
  url('fonts/montserrat.woff') format('woff');  
}
```




TRICK: Use plain HTML links as share buttons

Don't use the share code social media sites give you. Make image links instead.

- https://twitter.com/home?status=TWITTER_STATUS
- <https://www.facebook.com/share.php?u=URL>
- https://identi.ca/notice/new?status_textarea=IDENTICA_STATUS
- <http://sharetodiaspora.github.com/?title=TITLE&url=URL>



How do I include a Twitter button?

Twitter's code:



```
<a href="https://twitter.com/micahflee" class="twitter-follow-button"
data-show-count="false">Follow @micahflee</a>
<script>!function(d,s,id){var js,fjs=d.getElementsByTagName(s)[0];if(!
d.getElementById(id))
{js=d.createElement(s);js.id=id;js.src="//platform.twitter.com/widgets.js";fjs.pare
ntNode.insertBefore(js,fjs);}}(document,"script","twitter-wjs");</script>
```

Loads requests from: platform.twitter.com, p.twitter.com, r.twimg.com, cdn.api.twitter.com, and knows who users are if logged in



Privacy Tricks for Activist Web Developers

TRICK: Copy a Twitter button without including their script

```
<a href="https://twitter.com/micahflee" style="box-sizing: border-box; height: 20px; max-width: 100%; position: relative; background-color: #F8F8F8; background-image: -webkit-gradient(linear,left top,left bottom,from( white),to( #DEDEDE)); background-image: -moz-linear-gradient(top, white, #DEDEDE); background-image: -o-linear-gradient(top, white, #DEDEDE); background-image: -ms-linear-gradient(top, white, #DEDEDE); background-image: linear-gradient(to top, white, #DEDEDE); border: #CCC solid 1px; -webkit-border-radius: 3px; border-radius: 3px; color: #333; font-weight: bold; text-shadow: 0 1px 0 rgba(255, 255, 255, .5); -webkit-user-select: none; user-select: none; cursor: pointer; overflow: hidden; display: inline-block; vertical-align: top; zoom: 1; outline: none; text-decoration: none; white-space: nowrap; text-align: left; font: normal normal normal 11px/18px 'Helvetica Neue',Arial,sans-serif;" target="_blank"><i style="position: absolute; top: 50%; left: 2px; margin-top: -5px; width: 16px; height: 13px; background: transparent 0 0 no-repeat; background-image: url('data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAAC0AAAAoCAYAAABq13MpAAAGcklEQVRYw+2YXUyTVxjHz4vJLiZGd7MtXi2LkZtdELM7lyzOG7Nk2RJvL8iujBiNV2JcMA0fwqCFEGCAfJRC+SyltqWFgnwULIKAWB3y0VrAttQWC1ZC0i6ePc8LL74tVD6ly2KTf87J6Tnv+3uf8zzP+WAAwEhMIj8h1MViEs0Jlqi+we5oJFjGCX3D9X+fmKTmq/f/rzkrLX5fzkmNPhLVqW2DQ1Ify9eFAZ8kafUsURMX+qCo1BYry3oILKcflMQb2N3Wzqhk48xn6YbLuwJ01cQeydAvURkWONtk5UoGgKsaXRPw03LarVHsjvRmXhm+6pHV3h4YdDp0gE7D5XUJPo6QyzLfwKscgZY1UtgChuwkjH4t0hpQPP4Nn430GeU/TcJ4sif5iV2V/NL6P/H81oT0IUvUvPs04AyeNVG9ehw4xTP4oubZ268VFiP2jd4Y9Hufw8TKJoAgufT2RZZikJ8s7JMzXTQw1QKwhtdrZY0Likd9Azm1G6gpc0z8VzdFHC1E8AV9gKXYdCI3eWc9q96Tj0DnHEBu0bXa6J60yvgtC740Tw3jf0Sgtzj89JhK6tyAKt2Ag9f+AxY8SgPyQMLUs5hd/hut/5MH3mp3z3H6eeBa7ADV/4UuNx04DINw1GyZkLMw/MhTut8BywCj2mb9wvAqdBNOz5ldJ1zlbemygusdn5NVBeA8b/Tart/D8CMYVrjjteNeo81v1rljF7gdC7gVNPakUeAdwuaAb17MzS6yTdGmzPoWWJLXLG8Go9We1aDLCTwnRskA27zXqCfuP0Xj9ZNBHgwQWE6acP4Nu9m6FxFzn7tmbWEg2Zpg670U1rXUpB1xVbW0sjKF/YCTQHU5X5rjmn3+IP8djthMJaNe+6EHuBfmub8jefapZ5NbtHk8TuX/1HsEziXetJz5rc+11BMxw7Bsc+3bS99oUH/bgGRYCL/o93Hp7gK07B6zzqwF342L7jWgaP3A03jzxrGTJzm5dausIVrlP/tU22KD+FhFJ1djJfma4/mbdf6vbZrgz6bb0TN6IvFgGU9cvcLL0jqI6WA5bp10RbTurDe4vhR1594bTT74aA3ghEVJxL575cHBLuhC3rr+bPN06aj0kdG54tj26UB79w6A9s0+oMpKk0j5zKb0rksk48reLiW6mjFE00j1U+2elbK7P7nNCNh0+dhQZ0LSa0u3U8dttmT0vsKv5DQ0u2gx0wLqz88eu2RTbwZxX412y1ehwnN1mES1sE6RdKjkneaTg8b+kD0Efoj9P8WWiKRbHnmo/bExMQbWEqwjBPawvU/V0jk5GQ9gmxagdLS0qzZ2dmQm5sLWVlZkKJ6e3pmamjQD5eWIQ8vLcjtBpaSkyAUrIlxsQUEBKJVKqK6uhsrKSigrK4Pi4uLA48eP4yM03dfXZyovLweCzMjIWCT4e/fuySsqKkCtVknJyYnF1tXVwdjY2K7PiB8Eurs01FpTUw01tbVA8AgM2MZDERAgsvgez4gHD22325UqlWqVrEmqr6/nJVhZsDSW/v288NatW++9sFkPcjm6po9EdcFdqbX9+3Zs0LbUYrGMazSaVbFlxckPgqGhIfNegfGLsRjwS1SGA6bAz8/P52eZRHV0Vyu5KyUA9IIRQYMGBwfT9Xr9kti6YivrdLr9nBEZBvHNvLw8ykIEvunCRiaTJRQVFQ65aUNDAY+qU/CTuyLwWyyNm86IDoejsa0jwxPqFkaj0b+8vLyvMyIaJV6hUPAxk50TA2g5DcJvuAv0ZD1lqtB30wxTbLW1tfEXNhvTkpsUJM/MzPQJKY6+UhjU3d3tWgfe75HrVE9PzxxFCr2jsLAQpFIppdlh/ABJVVXVECWCrWYZPCafesPEnxHRYube3l4b5mAbWsU2ir/FxcUD0y0iv8ahpb0UN0L6pJRaULIC5BY0A2TVUGgyII5xRuSM6Ha7LyJkgMDEuV+YfnG7WDQzDx48sERqwxTtdDrNFB9bwYUTBSN0+p2I7fImJyFpOF8PNTc37wic+hgMhqALm0isaNEIY6KvdsfQ5BoTEx0q/8J++ioFOAV7S0tLWItT0yWF0Aubi00fM0j042JlwgAMhFvMMJNteWFzqKC0j8Cc3Il7cR/t0SnVUZCFLiaYk1empqbCXtgctoUTC0+iQ5eYRUuv0EJC0ZhaTvtaldXl2dkZGTbC5tIuMa+L2z+BexZXK+0BaruAAAAAE1FTkSuQmCC')";></i><span style="padding: 0 3px 0 19px; white-space: nowrap; display: inline-block; vertical-align: top; zoom: 1; color: #333; font-weight: bold; text-shadow: 0 1px 0 rgba(255, 255, 255, .5); cursor: pointer; text-align: left;">Follow @micahflee</span></a>
```




TRICK: Copy a Twitter button without including their script

- There's no need for 3rd party scripts
- By copying and pasting styles, it's not too difficult to create the same look
- That giant block of base64 was a data URI image of Twitter's logo
- Instead of a Twitter pop-up window, just a privacy-friendly link to <https://twitter.com/#!/micahflee>



Privacy Tricks for Activist Web Developers

TRICK: Load your Twitter feed from the server, not the client



GLOBAL CENSORSHIP CHOKEPOINTS

Tracking Censorship through Copyright Proposals Worldwide

- HOME
- ABOUT
- ALL COUNTRIES

About Global Chokepoints

Global Chokepoints is an online resource created to document and monitor global proposals to turn Internet intermediaries into copyright police. These proposals harm Internet users' rights of privacy, due process and freedom of expression, and endanger the future of the free and open Internet. Our goal is to provide accurate empirical information to digital activists and policy makers, and help coordinate international opposition to attempts to cut off free expression through misguided copyright laws, policies, agreements and court cases. Scroll down to see a list of countries currently featured for threatening free expression through copyright censorship. **Learn more.**

Our site is created and maintained by free speech advocates worldwide. Want to help us grow? **Contact us.**

Countries

Belgium	Chile	Colombia	European Union
---------	-------	----------	----------------

Twitter Updates

@EFF: The Oatmeal creator is fighting a bizarre lawsuit targeting his online speech. EFF is on it. <https://t.co/ydUqKk1a>
1 min 50 sec ago

@EFF: Can Apple refuse to sell a laptop to an Iranian citizen? The answer is complicated. <https://t.co/8nWcoMdb>
42 min 23 sec ago

@EFF: We asked Dr. Richard Stallman to comment on the state of software patents. Check out his response & add comments: <https://t.co/c6bgYkvE>
54 min 46 sec ago

@Numerama: LOL entre dans le dictionnaire Le Robert illustré: L'édition 2013 du Robert illustré accueille de nouveaux ter... <http://t.co/L95TvszJ>
55 min 29 sec ago

@Numerama: Document : la sécurisation du vote électronique aux législatives: Numerama publie le projet de "Guide de confi... <http://t.co/igTuyeUO>
55 min 34 sec ago

@Numerama: Kim Dotcom arrive sur Twitter et se dévoile:



TRICK: Load your Twitter feed from the server, not the client

How do you access the feed?

- Twitter API:
<https://dev.twitter.com/>
- JSON URL to Twitter feed:
https://twitter.com/statuses/user_timeline/micahflee.json

```
$tweets_json = file_get_contents('https://twitter.com/statuses/
user_timeline/micahflee.json');
$tweets = json_decode($tweets_json);
foreach($tweets as $tweet) {
    echo("<p>".htmlspecialchars($tweet->text)."</p>");
}
```



Privacy Tricks for Activist Web Developers

TRICK: Proxy Ajax requests to avoid sending data to third parties

The screenshot shows the top section of the Humble Indie Bundle V website. At the top left is the text "the Humble Indie Bundle V" in a stylized red font. To the right of this is a green button with the text "Support EFF". Below the title, there are two sections: "Time remaining" and "Bundles sold". The "Time remaining" section features a clock icon and a digital timer showing "00:00:00:00". The "Bundles sold" section features a bundle icon and a digital counter showing "396411".

the Humble Indie Bundle V

Support EFF

Time remaining

00:00:00:00

Bundles sold

396411



TRICK: Proxy Ajax requests to avoid sending data to third parties

- Make scripts send Ajax requests to your own server, `proxy.php?q=querystring_to_proxy`
- ```
<?php /* proxy.php */
echo(file_get_contents('http://service_to_proxy' . $_GET['q']));
```
- It's more complicated than this:
  - If you get much traffic, you'll need aggressive caching
  - You might need to copy request/response headers from original Ajax requests





# Privacy Tricks for Activist Web Developers

## TRICK: Let users “opt-in” before including third-party scripts

**STOP CYBER SPYING**  
**A WEEK OF ACTION AGAINST #CISPA**

CISPA—the Cyber Intelligence Sharing & Protection Act—would cut a loophole in all existing privacy laws allowing the government to suck up data on everyday Internet users. We can't let that happen.

The House of Representatives voted to approve CISPA, but it's not over yet! Urge your Senators to stand up for user privacy and oppose cybersecurity bills.

Use our interactive tool to Tweet at your US Senators. Show them all the unnecessary personal info this cyber spying bill will collect on everyday Internet users.

ZIP Code **FIND MY REPS** [I don't have a US zip code](#)  
[I'm not on Twitter](#)

Infographic courtesy of [Lumin Consulting](#).

**Live Tweets from the Campaign Against CISPA**

**Click here to show me the Tweets!**

You'll get some data from Twitter (like a cookie) and Twitter will get some data from you (like the fact that you saw these tweets).

<https://cyberspying.eff.org>



# Privacy Tricks for Activist Web Developers

## TRICK: Let users “opt-in” before including third-party scripts

# STOP CYBER SPYING

## A WEEK OF ACTION AGAINST #CISPA

**CISPA—the Cyber Intelligence Sharing & Protection Act—would cut a loophole in all existing privacy laws allowing the government to suck up data on everyday Internet users. We can't let that happen.**

**The House of Representatives voted to approve CISPA, but it's not over yet! Urge your Senators to stand up for user privacy and oppose cybersecurity bills.**


Use our interactive tool to Tweet at your US Senators. Show them all the unnecessary personal info this cyber spying bill will collect on everyday Internet users.

**FIND MY REPS**

[I don't have a US zip code](#)  
[I'm not on Twitter](#)


Infographic courtesy of [Lumin Consulting](#).

### Live Tweets from the Campaign Against CISPA




wandering\_nt\_1st .@senatorburr Does the NSA really need to know I post in online political forums? #CongressTMI Stop #CISPA [eff.org/r.1X2](http://eff.org/r.1X2)  
yesterday · reply · retweet · favorite


1 new tweet




wandering\_nt\_1st .@SenatorHagan Does the NSA really need to know I post in online political forums? #CongressTMI Stop #CISPA [eff.org/r.1X2](http://eff.org/r.1X2)  
yesterday · reply · retweet · favorite



dblue02 Save the Internet from US Spies! Tell @Microsoft @IBM @Facebook to stop #CISPA, take action @Avaaz #CongressTMI [bit.ly/HQInfX](http://bit.ly/HQInfX)  
yesterday · reply · retweet · favorite



bookbound7 .@senatorburr Does the CIA really need to know what RSS feeds I read? #CongressTMI Stop #CISPA [eff.org/r.1X2](http://eff.org/r.1X2)

 Join the conversation

<https://cyberspying.eff.org>





# Privacy Tricks for Activist Web Developers

TRICK: Let users “opt-in” before including third-party scripts



Clicking this loads remote content from  
threatened.globalvoicesonline.org, maps.google.com,  
maps.gstatic.com, google.com, chart.apis.google.com,  
chart.googleapis.com



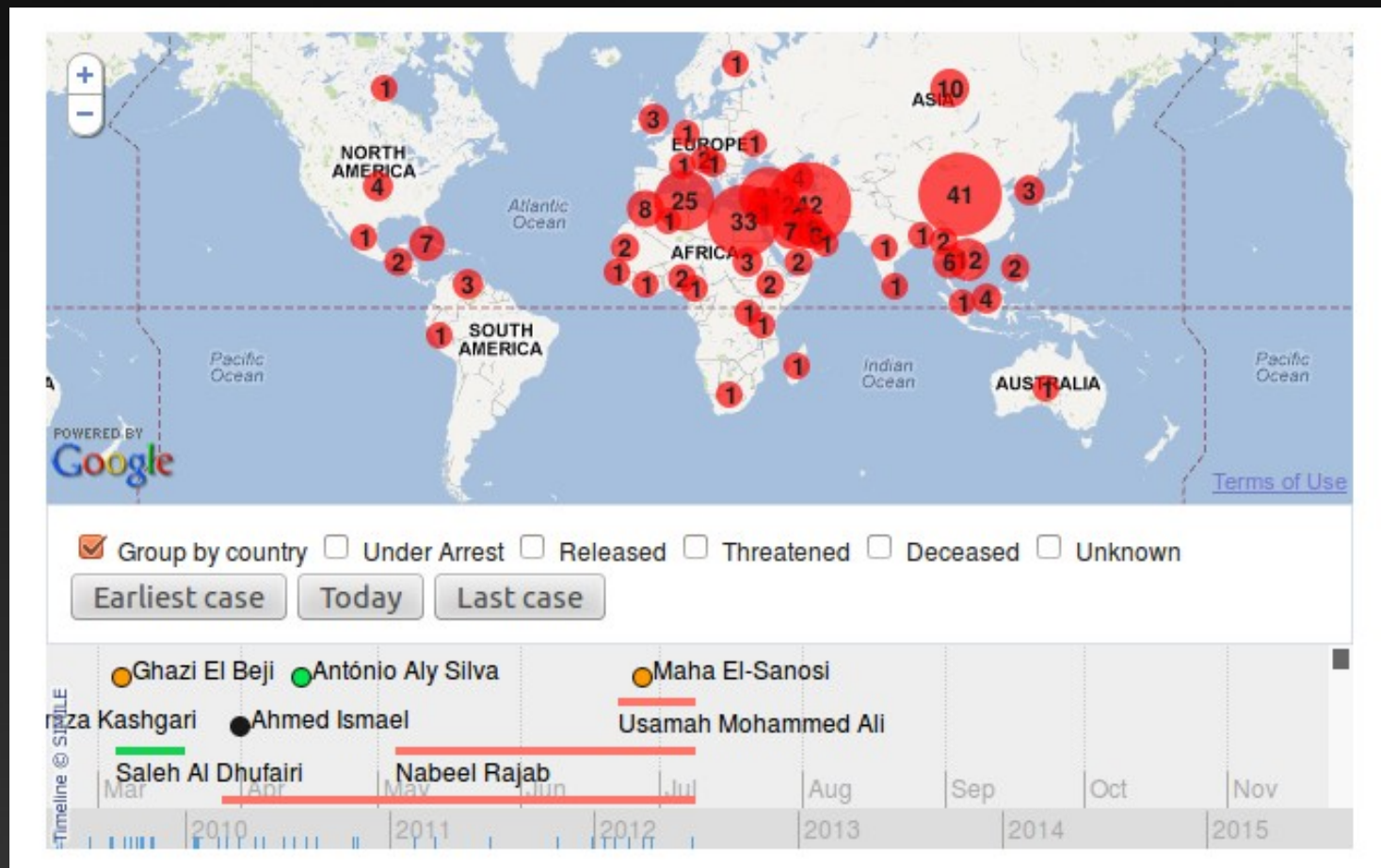
As activists and ordinary citizens around the world are increasingly making use of the Internet to express their opinions and connect with others, many governments are increasing their surveillance and censorship capabilities and taking legal or extrajudicial

<https://www.eff.org/issues/bloggers-under-fire>



# Privacy Tricks for Activist Web Developers

TRICK: Let users “opt-in” before including third-party scripts



<https://www.eff.org/issues/bloggers-under-fire>



## TRICK: Let users “opt-in” before including third-party scripts

```
<div id="widget">
 <div id="widget-opt-in" style="cursor:pointer">Click here to opt-in to the
 widget, if you're ok with https://blahblah/ tracking you</div>
</div>
```

```
<script>
var embed_code = '<script src="https://blahblah/widget.js"></script>';
$('#widget-opt-in').click(function(){
 $('#widget').html(embed_code);
});
</script>
```



## Don't store more than you need

- Who might get this data?
  - Law enforcement
  - Spies or military
  - Unauthorized employees
  - Hackers



## TRICK: Disable IP address logging with Apache

- Here is Apache's default log format (/etc/apache/apache2.conf):  
`LogFormat "%h %l %u %t \"%r\" %>s %b" common`
- Make your own:  
`LogFormat "- %l %u %t \"%r\" %>s %b" noip`
- Then use it (/etc/apache/sites-enabled/\*):  
`CustomLog /var/logs/apache2/access.log noip`



## TRICK: Encrypt your IP addresses and throw away the key

- **Cryptolog:** `sha256(random_tmp_salt+IP_addr)`
- You can still tell the difference between unique visitors and pageviews
- Under Development: <https://git.eff.org/?p=cryptolog.git;a=summary>
- Makes this:  
`192.168.1.118 - - [12/May/2011:17:58:07 -0700] "GET / HTTP/1.1" 200 430`
- Look like this:  
`UkezVh - - [12/May/2011:17:58:07 -0700] "GET / HTTP/1.1" 200 430`





## TRICK: Encrypt your IP addresses and throw away the key

- `git clone https://git.eff.org/public/cryptolog.git/`
- Using cryptolog as an Apache filter:  
`CustomLog "| /usr/bin/cryptolog -w /logs/cryptolog-access.log" common`
- Using cryptolog with another filter, like cronolog:  
`CustomLog "| /usr/bin/cryptolog -c /usr/bin/cronolog\\ /logs/cryptolog-access-%Y-%m-%d.log" common`
- Sorry about the sloppy open source project. Some day there will be a website, mailing list & bug tracker.
- See also: *mod\_log\_iphash* [https://github.com/franzs/mod\\_log\\_iphash](https://github.com/franzs/mod_log_iphash)



## TRICK: Hide identifying data from PHP with \$\_SERVER

- In Wordpress add to wp-config.php
- In Drupal add to sites/default/settings.php

```
$_SERVER['HTTP_REFERER'] = 'https://web/';
$_SERVER['HTTP_USER_AGENT'] = 'web browser';
$_SERVER['REMOTE_ADDR'] = '127.0.0.1';
$_SERVER['REMOTE_HOST'] = 'localhost'
```



## TRICK: Hide non-public stuff behind HTTP basic authentication

If you want to keep the riff-raff out, put this in your Apache config or .htaccess:

```
AuthName "Are you allowed in?"
AuthType Basic
AuthUserFile /path/to/htpasswd
Require valid-user
AllowOverride All
```



## Piwik: Privacy Friendly Analytics

**Piwik** # Open source web analytics

Piwik is downloadable, Free/Libre (GPLv3 licensed) real time web analytics software. It provides you with detailed reports on your website visitors; the search engines and keywords they used, the language they speak, your popular pages, and much more.

Piwik is a free software alternative to Google Analytics, and is already used on more than 320,000 websites.

Piwik is a PHP/MySQL software program that you download and install on your own web server. At the end of the five minute installation process you will be given a JavaScript tracking code. Simply copy and paste this tag to any websites you wish to track (or use an existing plugin to do it automatically for you) and access your analytics reports in real time.

<http://piwik.org>



## Piwik: First Party Analytics

- You can run it on your own server
- It can do analytics for multiple sites
- You don't have to give Google any data
- Customizable with plugin architecture
- Supports anonymizing IP addresses, deleting old logs, DoNotTrack
- Mobile apps



# Privacy Tricks for Activist Web Developers

## TRICK: Prevent Piwik from tracking browser plugins, resolution, etc.

```
<!-- Piwik →
<script type="text/javascript">
var pkBaseURL = (("https:" == document.location.protocol) ? "https://anon-stats.eff.org/" :
"http://anon-stats.eff.org/");
document.write(unescape("%3Cscript src='" + pkBaseURL + "piwik.js' type='text/javascript'%3E%3C/script%3E"));
</script><script type="text/javascript">
try {
var piwikTracker = Piwik.getTracker(pkBaseURL + "piwik.php", 1);
piwikTracker.trackPageView();
piwikTracker.enableLinkTracking();
} catch(err) {}
</script><noscript><p></noscript>
<!-- End Piwik Tracking Code -->
```

```
<!-- Piwik Image Tracker →

<!-- End Piwik -->
```

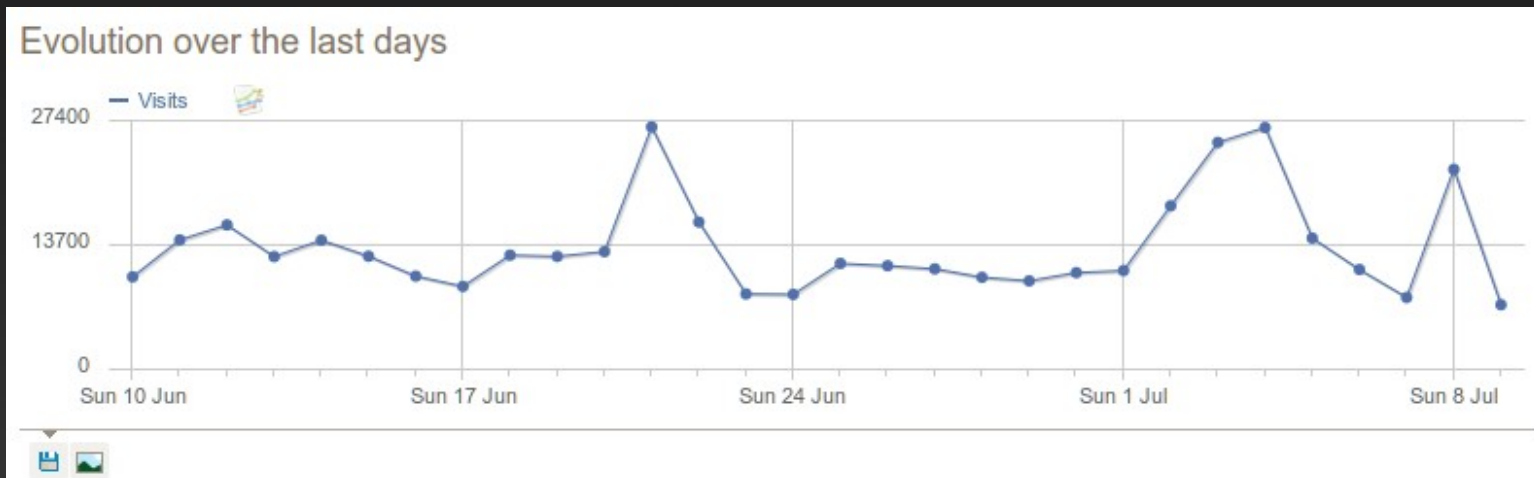


# Privacy Tricks for Activist Web Developers

Keep in mind: When using 3rd party resources, you give them this data

| Browser                                                                                             | Visits ▼ |
|-----------------------------------------------------------------------------------------------------|----------|
|  Chrome            | 50610    |
|  Firefox           | 36337    |
|  Safari            | 31634    |
|  Internet Explorer | 13823    |
|  Opera             | 5330     |

| Operating system                                                                               | Visits ▼ |
|------------------------------------------------------------------------------------------------|----------|
|  Windows 7  | 48348    |
|  Mac OS     | 22306    |
|  Windows XP | 18903    |
|  Linux      | 13372    |
|  Android    | 9517     |





## TRICK: Harden Piwik with HTTP basic authentication

```
<Directory "/path/too/piwik/htdocs/">
 AuthName "Are you allowed?"
 AuthType Basic
 AuthUserFile /path/too/piwik/htpasswd
 Require valid-user
 AllowOverride All
</Directory>
<Location /piwik.php>
 allow from all
 Satisfy Any
</Location>
<Location /piwik.js>
 allow from all
 Satisfy Any
</Location>
```

- The <Directory> block sets basic auth for all of Piwik
- The <Location> blocks make exceptions for /piwik.php and /piwik.js





## How to use HTTPS correctly

- **Always force HTTPS**
- **Use HSTS**
- **Use “secure”, “httponly” cookies**
- **Never include any http:// resources (mixed content)**
- **How to Deploy HTTPS Correctly**  
<https://www.eff.org/https-everywhere/deploying-https>
- **duraconf – A collection of hardened configuration files for SSL/TLS services**  
<https://github.com/ioerror/duraconf>



## TRICK: How to force HTTPS

Plop this into your Apache config or .htaccess:

```
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI} [L,R=permanent]
```



## TRICK: How to setup HTTP Strict Transport Security (HSTS)

- Tells modern browsers to only communicate to your server over HTTPS
- [https://developer.mozilla.org/en/Security/HTTP\\_Strict\\_Transport\\_Security](https://developer.mozilla.org/en/Security/HTTP_Strict_Transport_Security)

In PHP:

```
if(!empty($_SERVER['HTTPS'])) {
 header("Strict-Transport-Security: max-age=31536000; includeSubdomains");
}
```

In Apache:

```
LoadModule headers_module modules/mod_headers.so
Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"
```



## TRICK: Make your cookies “secure”, “httponly”

- Browsers will never send “secure” cookies over http, only https. **If user is tricked into visiting http link, session is still secure.**
- Cookies with the “httponly” flag are only readable on the HTTP layer, not accessible from JavaScript. **XSS bugs can't be used to steal “httponly” cookies.**
- `bool setcookie ( string $name [, string $value [, int $expire = 0 [, string $path [, string $domain [, bool $secure = false [, bool $httponly = false ]]]]] )`
- `setcookie("cookie_name", "cookie value", 0, "/", $_SERVER['HTTP_HOST'], true, true);`



## TRICK: Make CMS session cookies “secure”, “httponly”

- Session cookies set by WordPress, Drupal, etc. generally don't have “secure” and “httponly” flags set
- Before the session is started (wp-config.php, sites/default/settings.php), run this:
- `session_set_cookie_params(0, '/', $_SERVER['HTTP_HOST'], true, true);`



## Remote Administration

- Public key authentication is better than password authentication (see: HBGary hack)
- Use SSH or SFTP to transfer files
- **Never use FTP!**  
**It is old and insecure.**  
(Just search #FTP on Twitter to see how widely it's hated)



## TRICK: Make your site work better with privacy/security tools

- If possible, don't require Javascript (NoScript, accessibility issues) – this is becoming harder
- Don't use Flash: it doesn't work over Tor and is annoying, proprietary, obsolete, and is a major source of security holes
- Don't block proxy IPs to handle spam/abuse because legit users use these IPs too
- Use HTTPS correctly (secure cookies!), and force it all the time, so HTTPS Everywhere users won't need to write a rule
- Test your site with Tor Browser Bundle
- Don't use privacy-invasive third party services



## TRICK: Static HTML is *always* more secure than server-side code

- Most web-based security problems are from badly sanitized input (XSS, SQL injection, file inclusion, file viewing)
- Very few security problems come from web server exploits (Apache, nginx, etc.)
- If you don't need people logging into your site/commenting, don't use a CMS





# Privacy Tricks for Activist Web Developers

---

Thank You!

Micah Lee  
@micahflee  
micah@eff.org

GPG: 5C17 6163 61BD 9F92 422A C08B B4D2 5A1E 9999 9697

Download slides from:  
<https://bit.ly/privacytricks>

Happy hacking.