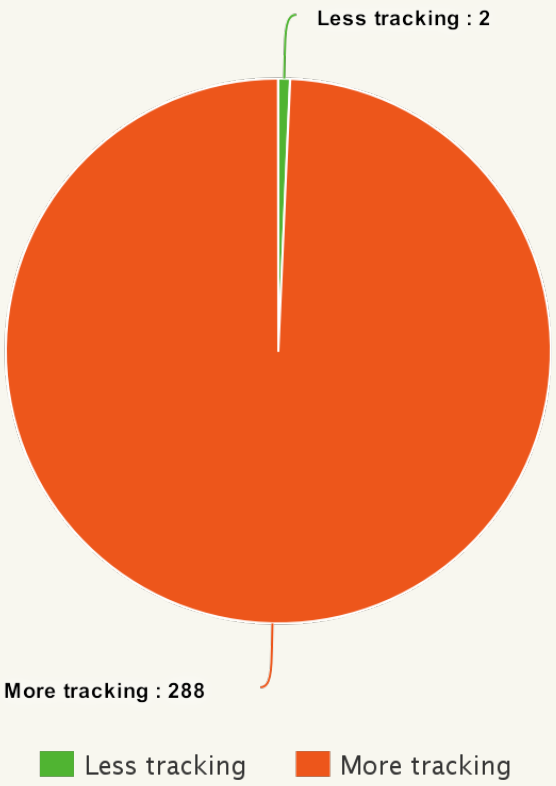
Privacy and the Web –
Are you doing what it takes?

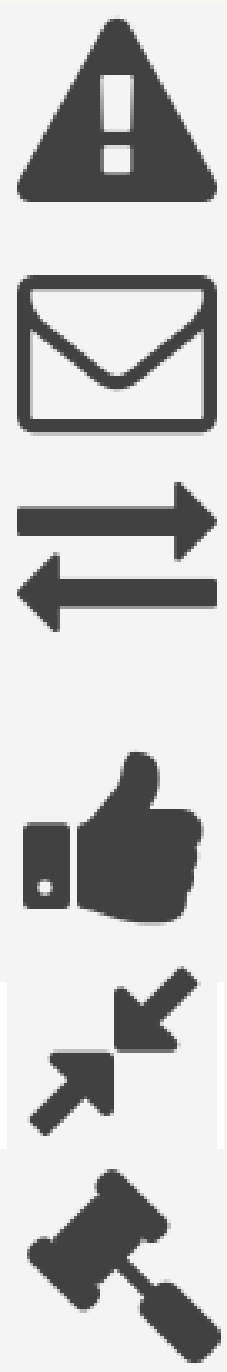
Amelia Andersdotter & Anders Jensen-Urstad

WordCamp Europe 2016, Vienna, June 25

dataskydd.net

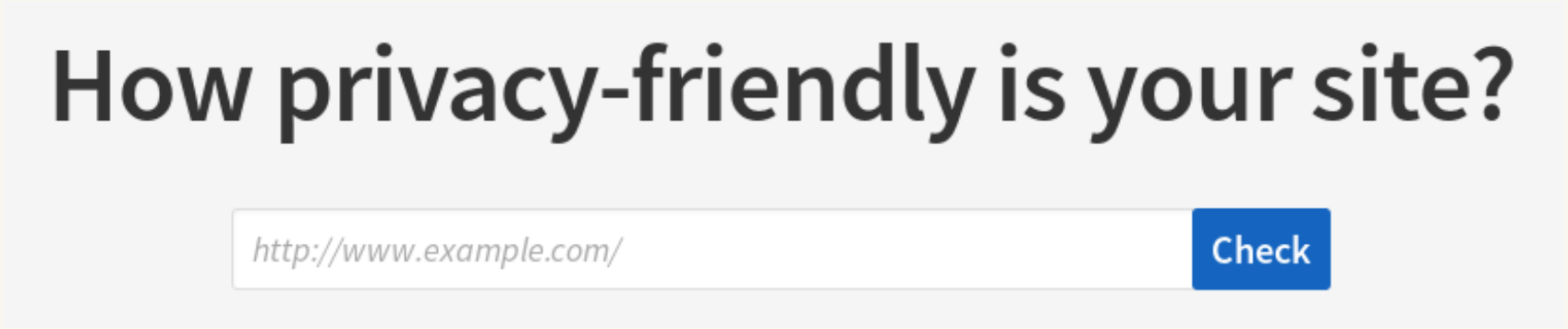
A small recap of the year...





Good news: *(Say what?!)*

A new data protection regulation.



https://webbkoll.dataskydd.net

Swedish municipalities *(in Swedish)*:
https://dataskydd.net/kommuner

Funding: Internetfonden / The Internet Foundation IIS

Three paradigms for privacy

The right to be left alone (1870s)

The right to keep things to yourself. To be secret and unrevealed.

Three paradigms for privacy

The right to be left alone (1870s)

The right to keep things to yourself. To be secret and unrevealed.

The right to privacy as control (1970s)

The origin of data protection laws: rules for transparency and accountability even after information is revealed.

Three paradigms for privacy

The right to be left alone (1870s)

The right to keep things to yourself. To be secret and unrevealed.

The right to privacy as control (1970s)

The origin of data protection laws: rules for transparency and accountability even after information is revealed.

The right to identity and identity development (2000s)

The opportunity to develop one's own personality without undue interference.

Data leakage to ISPs, schools, work, etc.

Data leakage to adjacent websites.

Data leakage to advertisers, CDNs, font providers, etc.

"All browsing activity should be considered private and sensitive."

— HTTPS://HTTPS.CIO.GOV/

"Pervasive monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible."

— INTERNET ENGINEERING TASK FORCE, RFC 7258, "PERVASIVE MONITORING IS AN ATTACK"

"We're in a world where if your adversary can see your traffic ... and your traffic is unencrypted, that is an attack vector – not an information leak. This is key: unencrypted traffic is a vulnerability."

— NICHOLAS WEAVER, "THE GOLDEN AGE OF BULK SURVEILLANCE", USENIX ENIGMA 2016

GitHub battles “largest DDoS” in site’s history, targeted at anti-censorship tools

HTTP hijacking used to redirect Baidu search engine traffic into a massive DDoS.

by **Sebastian Anthony** - Mar 30, 2015 1:19pm CEST

Share Tweet Email 61

GitHub, the largest public code repository in the world, is currently battling against the largest and most gnarly distributed denial of service (DDoS) attack in the site's history. The attack started on Thursday morning (March 26) and has continued unabated since then, evolving several times to circumvent

Meet “Great Cannon,” the man-in-the-middle weapon China used on GitHub

Powerful weapon could easily be used to inject malware attacks into traffic.

by **Dan Goodin** - Apr 10, 2015 6:32pm CEST

Share Tweet Email 61

(Ars Technica)

www.openbsd.org

Search

Hardware Platforms
Security Crypto
Events Papers Innovations

Getting OpenBSD
Buy CDs/Shirts/Posters
Download

Getting Source
AnonCVS
CVSync
CVS on Web
Daily Changelog

OpenBSD Resources

Only two remote holes in the default install, in a heck of a long time!

The OpenBSD project produces a **FREE**, multi-platform 4.4BSD-based UNIX-like operating syste
Our efforts emphasize portability, standardization, correctness, proactive security and integrate
cryptography. As an example of the effect OpenBSD has, the popular OpenSSH software comes fr

view-source:http://www.openbsd.org/

Search

```
1 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
2 <html>
3 <head><link href="http://wifi.norwegian.com/unb/unb.css"
  rel="stylesheet" type="text/css">
4 <script type="text/javascript" src="http://wifi.norwegian.com
  /unb/jqr44-1.8.3.js"></script>
5 <script type="text/javascript">var r44_btime=new Date();var
  r44_smu_time=1455916733.232</script>
6 <script type="text/javascript" src="http://wifi.norwegian.com
  /unb/unb.js"></script>
7
8     <title>OpenBSD</title>
```

Chromium > Chromium Security >

Deprecating Powerful Features on Insecure Origins

Mozilla Security Blog

APR 30 2015

Deprecating Non-Secure HTTP

Chromium > Chromium Security >

Marking HTTP As Non-Secure

Geolocation API removed from unsecured origins in Chrome 50

Let's Encrypt

Data leakage to ISPs, schools, work, etc.

Data leakage to adjacent websites.

Data leakage to advertisers, CDNs, font providers, etc.

"Note: Because the source of a link may be private information or may reveal an otherwise private information source, it is strongly recommended that the user be able to select whether or not the Referer field is sent."

— RFC 1945, HYPERTEXT TRANSFER PROTOCOL–HTTP/1.0, 10.13, MAY 1996

Referrer Policy, W3C draft

```
<meta name="referrer" content="no-referrer">
```

Data leakage to ISPs, schools, work, etc.

Data leakage to adjacent websites.

Data leakage to advertisers, CDNs, font providers, etc.

Results for **edition.cnn.com**

Input URL: http://cnn.com/

Final URL: http://edition.cnn.com/

Insecure	Referrers leaked	72 Cookies	194 Third-party requests	67 Third-parties contacted

Pinboard
@Pinboard

Following

At this point people without ad and script blockers are like those poor kids born without an immune system

RETWEETS	LIKES
87	117

6:38 PM - 10 Jun 2016

Google Analytics Solutions

MaxCDN

Google Fonts

DISQUS

Google Maps

Like Share

google-webfonts-helper

IcoMoon App

PIWIK
Open Analytics Platform

OpenStreetMap

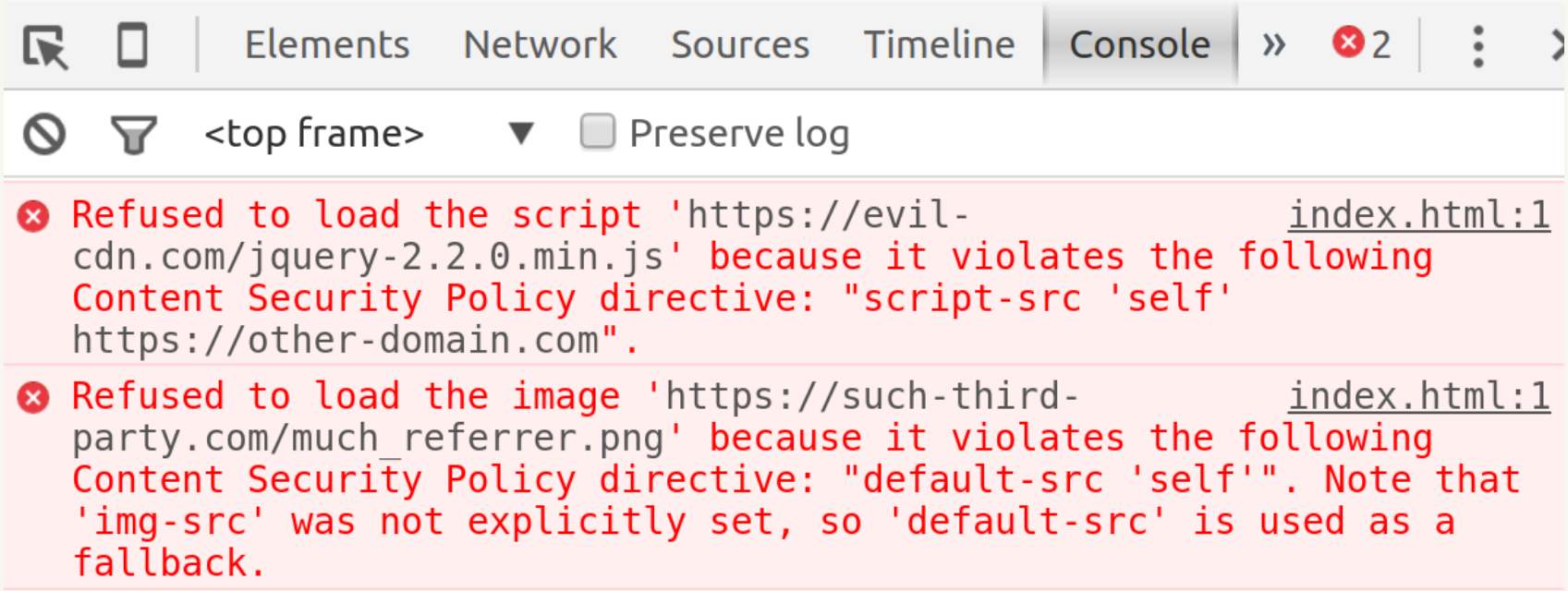
Nextcloud

Like Tweet +1

Alternatives: `https://dataskydd.net/wceu2016`

Content Security Policy

```
Content-Security-Policy: default-src 'self';
script-src 'self' https://other-domain.com
```



Check & build: `https://report-uri.io/home/tools`

Going forward...

Visualizations of website privacy analysis results?

Similar mappings of public sector in other EU countries?

Join us & implement data protection!

Thank you!

Slides, links, etc.: `https://dataskydd.net/wceu2016`

Amelia Andersdotter
@teirdes
amelia@andersdotter.cc
ameliaandersdotter.eu

Anders Jensen-Urstad
@ndrsju
anders@unix.se
anders.unix.se

P.S. Talk to us in the HappinessBar after the talk!
(Halle G foyer)

dataskydd.net