

# Unsafe Harbors

## Data Protection Strikes Back

Amelia Andersdotter & Anders Jensen-Urstad

WordCamp Nürnberg 2016

[dataskydd.net](https://dataskydd.net)

Good news: *(Say what?!)*

A new data protection  
regulation.

*Why data protection?*

Because human rights.

## *Data protection*

A collection of tools for achieving privacy.

## *Data security*

When procedures work as foreseen.



## FIVE PRINCIPLES

Right to *know* 

Right to *consent*

User-centric

Data minimization

Effective sanctions

## FIVE PRINCIPLES

Right to *know*

Right to *consent* 

User-centric

Data minimization

Effective sanctions

## FIVE PRINCIPLES

Right to *know*

Right to *consent*

User-centric 

Data minimization

Effective sanctions

## FIVE PRINCIPLES

Right to *know*

Right to *consent*

User-centric

Data minimization 

Effective sanctions



## FIVE PRINCIPLES

Right to *know*

Right to *consent*

User-centric

Data minimization

Effective sanctions 🦋

# Our work – *why websites?*

- 💡 Simple solutions
- 💡 Public sector: no need to rewrite laws to make protection possible

# Common website privacy problems

- 🦋 Inventing end-user obligations
- 🦋 Letting curiosity get the better of you
- 🦋 Doing things the way they've always been done

# *Legislative status*

- ☞ ~~Safe Harbor~~ R.I.P. Instead: “Privacy Shield”?
- ☞ General Data Protection Regulation (GDPR)
- ☞ Law Enforcement Data Protection Directive
- ☞ ePrivacy Directive
- ☞ EU court jurisprudence; right to be forgotten

*So what to do?*

Encrypt *all* the things.

Don't snitch on your visitors.

Avdelningar & mottagningar

SÖS akutmottagningar

SÖS avdelningar

▼ SÖS mottagningar

→ Venhälsan

→ **Hiv-mottagning**

Hivis - Jakten på ett vaccin mot hiv

Akut

Anestesi/IVA

BB SÖS - Graviditet och förlossning

Bild

Dagkirurgiskt centrum

Handkirurgi

Hudkliniken

Infektionsheten

Intermedicin

Kardiologi

Kvinnosjukvård/Förlossning

Kirurgi

Otopedi

Sachsska barn- och ungdomssjukhuset

Startsida / Avdelningar & mottagningar / SÖS mottagningar / Venhälsan / Hiv-mottagning

## Venhälsan

### Hiv-mottagning

På Venhälsans hiv-mottagning behandlas patienter med hiv. Vi tar emot personer med hiv som diagnostiserats på Venhälsans drop-in/STI-mottagning eller som remitteras från annan läkarmottagning eller annat sjukhus.

*Venhälsan är med i MINA VÄRDKONTAKTER. Gå in på [minavardkontakter.se](http://minavardkontakter.se) och läs mer.*

**Information om kvalitetsregistret InfCare HIV - Ett beslutsstöd och kvalitetsregister för att förbättra hiv-vården i Sverige (pdf) »**

På hiv-mottagningen arbetar läkare, sjuksköterskor, kuratorer, psykiatriker samt sekreterare. Vi tar emot vuxna personer, oavsett kön eller sexuell läggning, med hiv-infektion. Om du oroar dig för att du kanske bär på hiv-infektion är du välkommen att besöka [Venhälsans drop-in/STI-mottagning](#) för rådgivning och eventuell hiv-testning.

### Trygghet och kontinuitet

Vi har som mål att skapa kontinuitet och en säker vårdkvalitet för våra patienter. I denna strävan ingår att vi försöker se till att du får träffa samma läkare varje gång du kommer.

### Tystnadsplikt

För oss är det viktigt att du känner dig trygg hos oss och kan lita på att vi tillgodoser din rätt till integritet och sekretess. Vi gör allt för att denna rätt inte ska kränkas. När vi remitterar våra hiv-patienter till andra kliniker, på eller utanför Södersjukhuset, för undersökning och behandling är det ofrånkomligt att remisserna innehåller personliga uppgifter om dig. Men vi har försäkrat oss om att de vi remitterar till också tillgodoser din rätt till integritet och sekretess.



Q Sök här  
Utökad sökning

### Kontakt

#### Reception:

Tel. 08-616 25 00  
Fax 08-616 25 09

#### Rådgivningen:

Telefon: 08-616 39 97  
mån, ons: 07:30-12:00,  
13:00-14:30  
tis, tor, fre: 07:30-12

#### Provsvär:

Mina vårdkontakter:  
[www.minavardkontakter.se](http://www.minavardkontakter.se)

#### Hitta till oss:

Vi finns på Sjukhusbacken 14, plan -1 (huset tillhörer om huvudbyggnaden om du står med ansiktet mot huvudentrén). Hiss S om du kommer via kulverten.

[SL:s reseplanerare](#)

### Om vaccin mot hiv

**Hivis** är ett forskningsprojekt som syftar till att ta fram ett vaccin mot hiv. Här kan du läsa mer om [Hivis och jakten på ett vaccin mot hiv](#).

# HTTP

No.	Time	Source	Destination	Protocol	Length	Info
159	6.386222000	130.241.215.126	217.114.84.41	HTTP	464	GET /Avdelninga
-Hypertext Transfer Protocol						
> GET /Avdelningar--mottagningar/Mottagningar/Venhalsan/Venhalsan-hivmottagning/						
Host: www.sodersjukhuset.se\r\n						
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:42.0) Gecko/20100101 Firefox/42						
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n						
0000	74 26 ac e9 c1 40 34 02	86 f7 ad 46 08 00 45 00	t&...@4. ...F..E.			
0010	01 c2 d9 df 40 00 40 06	d7 4a 82 f1 d7 7e d9 72	....@.@. .J...~.r			
0020	54 29 e0 e2 00 50 3d c7	8c e1 29 94 40 04 80 18	T)...P=. ..).@...			
0030	00 e5 bd 8f 00 00 01 01	08 0a 06 5b 55 40 09 00	..... vdelning			
0040	41 8e 47 45 54 20 2f 41	76 64 65 6c 6e 69 6e 67	A.GET /A vdelning			
0050	61 72 2d 2d 6d 6f 74 74	61 67 6e 69 6e 67 61 72	ar--mott agningar			
0060	2f 4d 6f 74 74 61 67 6e	69 6e 67 61 72 2f 56 65	/Mottagn ingar/Ve			
0070	6e 68 61 6c 73 61 6e 2f	56 65 6e 68 61 6c 73 61	nhalsan/ Venhalsa			
0080	6e 2d 68 69 76 6d 6f 74	74 61 67 6e 69 6e 67 2f	n-hivmot tagnig/			
0090	20 48 54 54 50 2f 31 2e	31 0d 0a 48 6f 73 74 3a	HTTP/1. 1..Host:			
00a0	20 77 77 77 2e 73 6f 64	65 72 73 6a 75 6b 68 75	www.sod ersjukhu			

# HTTPS

No.	Time	Source	Destination	Protocol	Length	Info
14	4.274869000	130.241.215.126	217.114.84.41	TLSv1	261	Client Hello
↳Server Name Indication extension						
Server Name list length: 24						
Server Name Type: host_name (0)						
Server Name length: 21						
Server Name: www.sodersjukhuset.se						
0000	74 26 ac e9 c1 40 34 02	86 f7 ad 46 08 00 45 00	t&...@4. ...F..E.			
0010	00 f7 c8 9c 40 00 40 06	e9 58 82 f1 d7 7e d9 72	....@.@. .X...~.r			
0020	54 29 97 ae 01 bb 23 04	0f 4e 5a af 99 8d 80 18	T)....#. .NZ.....			
0030	00 e5 4a de 00 00 01 01	08 0a 06 59 c7 da 08 ff	..J..... .Y....			
0040	bd 17 16 03 01 00 be 01	00 00 ba 03 03 b5 ed e3	.....			
0050	bc 74 70 05 2d 31 16 74	81 eb 92 e2 e3 ac 50 c7	.tp.-1.t .....P.			
0060	10 d5 f6 21 e1 8d 40 fb	ae 33 1f 52 d9 00 00 16	...!...@. .3.R....			
0070	c0 2b c0 2f c0 0a c0 09	c0 13 c0 14 00 33 00 39	.+./.... .....3.9			
0080	00 2f 00 35 00 0a 01 00	00 7b 00 00 00 1a 00 18	./5.... .{.....			
0090	00 00 15 77 77 77 2e 73	6f 64 65 72 73 6a 75 6b	...www.s odersjuk			
00a0	68 75 73 65 74 2e 73 65	ff 01 00 01 00 00 0a 00	huset.se .....			



*“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

www.openbsd.org

norwegian

0h 42m Flight Tracker

-1°C at Oslo


Hardware Platforms  
Security [Crypto](#)  
Events [Papers](#) [Innovations](#)

Getting OpenBSD  
[Buy CDs/Shirts/Posters](#)  
[Download](#)

Getting Source  
[AnonCVS](#)  
[CVSsync](#)  
[CVS on Web](#)  
[Daily Changelog](#)

OpenBSD Resources

Free, functional, and secure



# OpenBSD 5.6

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 system. Our efforts emphasize portability, standardization, correctness, [proactive security](#) and [integrated cryptography](#). As an example of the effect OpenBSD has, the popular [OpenSSH](#) software comes fr

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

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

# 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)

- SSL/TLS certificates are now *free*, thanks to...
- ...**Let's Encrypt** ([letsencrypt.org](https://letsencrypt.org)) – free and automated. Just out of beta. No excuses anymore!
- Use HTTP Strict Transport Security (HSTS)

For bonus points: Public Key Pinning

# Sahlgrenska Universitetssjukhuset



Avdelningar och  
mottagningar



Undersökningar, diagnoser  
och behandlingar



Om ditt besök  
hos oss



## HIV-mottagning

På [Sahlgrenska sjukhuset](#)

031 - 3423442

### TELEFONTIDER

Må - 08:00 - 15:00 1 mån av tid  
Fr

Gröna stråket 16

Plan K  
Sahlgrenska sjukhuset  
413 45 Göteborg

[Visa adress på karta](#)

[Karta över sjukhusområdet \(pdf\)](#)

### VÄGBESKRIVNING

Hållplats: Sahlgrenska huvudentré.  
P-plats: P-hus Dubbdäcket.

Hudkliniken, Gröna stråket 16. Den  
gula byggnaden vid Gröna stråkets  
västra ända, ungefär halften vid



### Hbt-diplomerad mottagning



UNDERSÖKNINGAR, DIAGNOSER OCH  
BEHANDLINGAR

- [HIV](#) >



VÄSTRA  
GÖTALANDSREGIONEN

Sahlgrenska Universitetssjukhuset

031-342 10 00

Besök oss i sociala medier:



## Request Headers

**:host:** www.facebook.com

**:method:** GET

**:path:** /sahlgrenska

**:scheme:** https

**:version:** HTTP/1.1

**accept:** text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8

**accept-encoding:** gzip, deflate, sdch

**accept-language:** en-US,en;q=0.8

**referer:** https://www.sahlgrenska.se/omraden/omrade-5/hud--och-konssjukvard/enheter/hiv-mottagning/

# *Referrer Policy*, W<sub>3</sub>C draft

Firefox, Chrome, Safari, Microsoft Edge:

```
<meta name="referrer" content="never">
```

(no-referrer actually preferred keyword, but doesn't  
work with Edge)

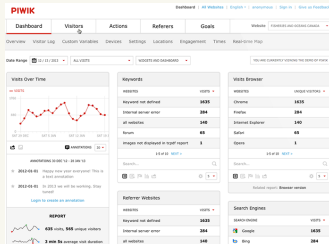


*No More Shall We  
Third-Party*

# Piwik

*a.k.a.: You can have useful data without sacrificing the privacy of your users on the altar of Google.*

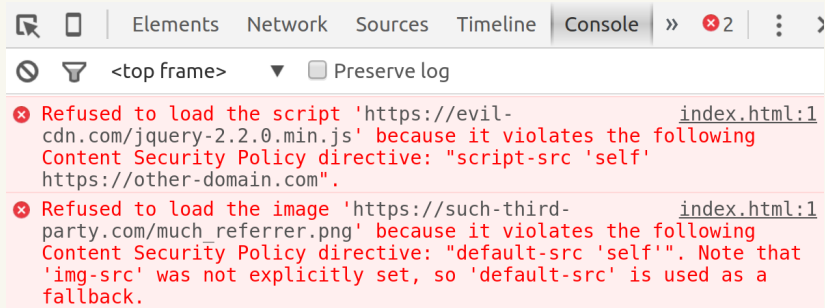
- Open source, PHP + MYSQL
- *You* own the data
- Various privacy options
- Can be used without cookies



Totally *radical* alternative: don't track.

# *Content Security Policy*

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



Check yourself: <https://securityheaders.io/>

# *We're making it easier!*

Soon(ish): online tool to check your website  
(or someone else's)

```
er.ex • untitled • site_controller.ex site_view.ex web.ex
third_party_cookies = Enum.reduce json["cookies"], [], fn(x), acc ->
  case String.ends_with?(x["domain"], registerable_domain) do
    true -> acc
    false -> acc ++ [x]
  end
end

meta_referrer = json["content"]
  |> Floki.find("meta[name='referrer']")
  |> Floki.attribute("content")
  |> List.to_string
```



Funding: Internetfonden / The Internet Foundation IIS

# *Once More, With Feeling*

Use HTTPS – for *everything, always*.

Don't leak referrers.


No third-party resources without consent. *Self-host*.

Embrace Content Security Policy.

# *In conclusion...*

Individuals matter.

*It's possible to protect privacy.*

Join us! 

*Thank you!*

Amelia Andersdotter

@teirdes

amelia@andersdotter.cc

ameliaandersdotter.eu

Anders Jensen-Urstad

@ndrsju

anders@unix.se

anders.unix.se

**dataskydd.net**