Bachelorscriptie
Informatica

Radboud Universiteit

Cookiewalls - Een probleem met een technische oplossing?

Auteur:
Koen van Ingen
s4058038

Inhoudelijk begeleider:
dr. Jaap-Henk Hoepman
jhh@cs.ru.nl

Tweede lezer:
mr. Merel Koning
m.koning@cs.ru.nl

Samenvatting

Nu er in Nederland een cookiewet van kracht is, waardoor iedere website verplicht is toestemming te vragen voor het plaatsen van cookies zou de privacy van gebruikers moeten verbeteren. Ze weten nu immers wat cookies zijn en hoe ze hiermee gevolgd kunnen worden. Helaas is het tegendeel waar: gebruiker irriteren zich massaal aan de cookiewalls en worden nog steeds gevolgd zonder dat ze het doorhebben. In deze scriptie gaan we een technische oplossing voor dit probleem zoeken. Na een analyse van hoe gebruikers gevolgd worden op het internet, wat hier tegen te doen is en hoe de wet nu precies in elkaar zit, zullen we een gebruikersvriendelijke technische oplossing proberen te vinden waar iedere gebruiker wat aan heeft.

Inhoudsopgave

Hoofdstuk 1

Inleiding

1.1 Probleemstelling

Als internetgebruiker kun je op het internet gemakkelijk gevolgd worden door verschillende bedrijven. Dit volgen gaat voornamelijk via cookies. Een cookie is een klein tekstbestandje dat een websitebeheerder op jouw computer kan plaatsen. Hierin kan hij informatie opslaan zodat hij, als je zijn website nogmaals bezoekt, jou kan identificeren. Deze cookies blijven vaak bewaard als je je internetbrowser zoals Internet Explorer of Google Chrome afsluit: zo hoef je als je op een ander moment dezelfde website bezoekt niet opnieuw in te loggen.

Dit klinkt tot nu toe allemaal vrij onschuldig, maar er zijn door de jaren heen heel wat bedrijven ontstaan die deze techniek misbruiken om gebruikers te volgen op het internet. Deze bedrijven worden ook wel profilers genoemd. Deze profilers 'huren' ruimte op verschillende websites waarin ze dan een klein plaatje of script plaatsen. Via zo'n script kunnen ze vervolgens ook cookies op jouw computer plaatsen. Omdat ze dit op verschillende websites doen en ze de geplaatste cookies op jouw computer vanaf die verschillende websites uit kunnen lezen, kunnen ze precies bijhouden welke websites je allemaal bezocht hebt en waar je op geklikt hebt. Zie voor een voorbeeld figuur 1.1. Hoe dit precies in zijn werk gaat komt in hoofdstuk 3 aan bod.

Als de profilers op deze manier voldoende informatie verzameld hebben verkopen ze deze door aan advertentiebedrijven. Advertentiebedrijven kunnen hiermee vervolgens speciaal op jou gerichte reclame maken: met de informatie van de profilers weten ze immers precies waar jouw interesses liggen. Door jou op deze manier gerichte reclame voor te schotelen verhogen ze de kans dat je daadwerkelijk op een advertentie klikt. En iedere klik levert hun weer extra geld op.

Omdat het op deze manier volgen van gebruikers nogal wat privacybezwaren met zich meebrengt heeft Europa de richtlijnen aangescherpt, vooral om gebruikers bewuster te maken van het feit dat ze gevolgd worden [6]. Hierdoor is er in Nederland de 'cookiewet' ingevoerd. Deze wet eist van websitebeheerders dat ze expliciet toestemming vragen voor het plaatsen van cookies. Hierdoor hebben veel Nederlandse websites nu een 'cookiewall': als je een website voor het eerst bezoekt zul je expliciet toestemming moeten geven

dat deze website cookies mag plaatsen op jouw computer. Ook moet de website jou informeren over het feit dat ze cookies gebruiken en waarvoor ze deze cookies gebruiken. We gaan de wet in hoofdstuk 5 bekijken.

Het probleem is nu echter dat veel gebruikers zich juist irriteren aan die cookiewalls en tegelijkertijd nog steeds totaal niet weten wat cookies zijn en wat voor gevolgen cookies kunnen hebben [9]. Momenteel zijn er voor de technischere mensen al wel manieren beschikbaar om dit te omzeilen, in de vorm van plugins voor je browser. Naast dat deze plugins de cookieschermen laten verdwijnen zijn ook de trackingcookies van profilers redelijk goed te blokkeren. Het probleem is echter dat er nog geen mooie universele en gebruikersvriendelijke plugin of andere oplossing bestaat waar iedere gebruiker wat aan heeft.

1.2 Huidige oplossingen

Er wordt momenteel al over oplossingen nagedacht. De Tweede Kamer denkt bijvoorbeeld na over het 'verlichten' en misschien zelfs afschaffen van de cookiewet [12]. Helaas is er een hoop van deze wet Europees geregeld, dus de cookiewet zal waarschijnlijk niet in zijn geheel verdwijnen. Ook wordt er momenteel niet opgetreden tegen het volgen van de internetgebruikers door de profilers en de inbreuk op de privacy die daarmee gemoeid is. Dit kan geconcludeerd worden uit feit dat hiervoor tot nu toe nog niemand is veroordeeld en dat er ook nog geen boetes uitgedeeld zijn. Verder houden buitenlandse bedrijven zich niet altijd aan de Nederlandse wet. Vanuit de overheid hoeven we dus voorlopig geen oplossing te verwachten.

Aan de technische kant zijn al wel een aantal deeloplossingen beschikbaar. Zo zijn er al al verschillende plugins die trackingcookies blokkeren zoals Ghostery en DoNotTrackMe. Ook kunnen internetbrowsers al zo ingesteld worden dat ze het één en ander blokkeren. Deze mogelijkheid en de functionaliteit van deze en enkele andere plugins bekijken we in hoofdstuk 4.

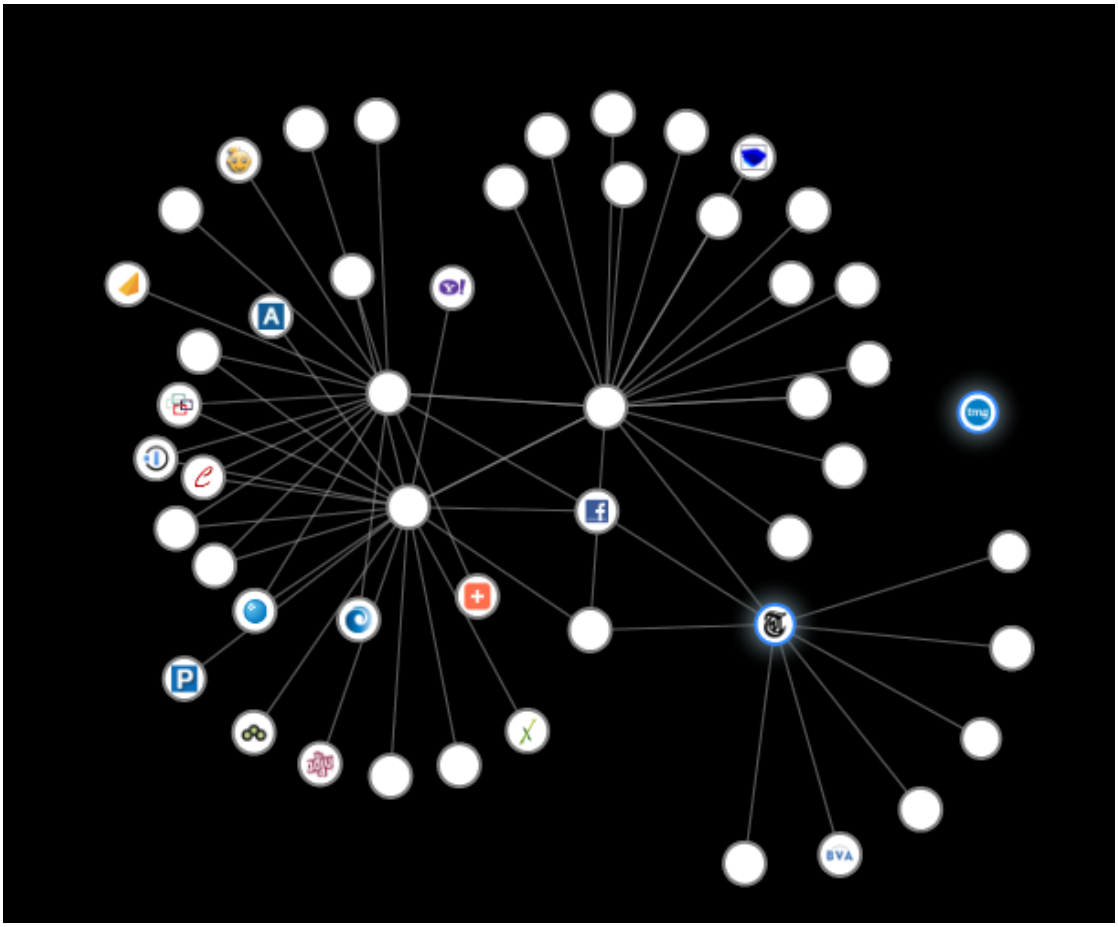
Ook voor de cookiewalls is er al een plugin genaamd CookiesOK [38]. Deze plugin belooft een oplossing te zijn voor de cookiewalls zoals vele websites deze momenteel hebben. Deze plugin probeert namelijk automatisch 'ja ik ga akkoord' te zeggen tegen iedere cookiemelding. Het nadeel is dan dat je automatisch alle cookies accepteert en dus nog steeds gevolgd wordt op het internet. We gaan de werking van deze plugin analyseren in hoofdstuk 6.

De beste oplossing ligt waarschijnlijk in de combinatie van een cookieblocker en een plugin zoals CookiesOK.

1.3 Onderzoeksvraag

De huidige problemen in combinatie met de mogelijke oplossing kunnen we nu samenvatten in de volgende onderzoeksvraag:
"Hoe kun je op een effectieve en gebruiksvriendelijke manier de cookiewall omzeilen en tegelijkertijd niet gevolgd worden door profilers?"

Met effectief bedoelen we hier dat zo goed als alle cookiewalls voor de gebruiker verdwijnen, terwijl er ondertussen geen trackingcookies worden geplaatst (en je als gebruiker dus niet gevolgd wordt). Als we die twee dingen op de juiste manier kunnen combineren hebben we een technische oplossing gevonden voor dit probleem.



Figuur 1.1: Een voorbeeld van het probleem: als we naar www.telegraaf.nl surfen werden er in dit geval 144 cookies geplaatst. Bovenstaande graph laat zien welke websites allemaal 'weten' dat we naar telegraaf.nl gegaan zijn, terwijl slechts twee partijen dit hoeven te weten (namelijk de Telegraaf zelf en de Telegraaf Media Group, beide gemarkeerd in de graph). Deze graph is gemaakt met de Firefoxplugin Collusion.

Hoofdstuk 2

Onderzoeksopzet

We gaan de volgende onderzoeksvraag beantwoorden:

"Hoe kun je op een effectieve en gebruiksvriendelijke manier de cookiewall omzeilen en tegelijkertijd niet gevolgd worden door profilers?"

Het antwoord op de vraag gaan we waarschijnlijk vinden in een plugin voor een browser die effectief (er zijn zo goed als nergens meer cookiewall zichtbaar op het internet) en gebruiksvriendelijk (iedereen kan het binnen enkele stappen installeren en gebruiken) de cookiewalls omzeilt en ondertussen alsnog trackingcookies blokkeert. Ondanks dat een plugin het meest voor de hand ligt gaan we ook nog kijken of er geen andere oplossingen mogelijk zijn.

2.1 Deelvragen

Het antwoord van de onderzoeksvraag gaan we vinden aan de hand van een aantal deelvragen. Deze worden hier kort toegelicht. Vervolgens beschrijven we de aanpak en de resultaten in de rest van de hoofdstukken.

Welke soorten cookies of andere manieren om gegevens op te slaan zijn er precies?

Met het antwoord op deze deelvraag weten we precies hoe er identificeerbare gegevens opgeslagen kunnen worden bij gebruikers, die profilers vervolgens gebruiken om gebruikers te volgen.

Hoe word je gevolgd op het internet?

Als we eenmaal weten hoe en op welke manier (dus met welke soorten cookies) deze gegevens worden opgeslagen kijken we verder naar hoe profilers dit gebruiken om gebruikers te volgen op het internet.

Wat kun je doen tegen het gevolgd worden op het internet?

Bij deze deelvraag gaan we kijken wat je er nu juist tegen kunt doen. Eén van de maatregelen is het installeren van een cookieblocker. Cookieblockers zijn gemaakt om het volgen van gebruikers juist tegen te gaan. We doen een korte inventarisatie en kijken welke cookieblockers er momenteel beschikbaar zijn. Omdat we in de vorige deelvraag al uitgezocht hebben hoe gebruikers worden gevolgd, gebruiken we dit hier om te kijken wat we daar tegen kunnen doen. Hoe dit precies in zijn werk gaat komt in de methode aan bod.

Hoe zit de wet precies in elkaar? Welke cookies mogen wel en welke niet volgens de wet?

Als we een technische oplossing zoeken voor een probleem dat door de wet geïntroduceerd is, moeten we de wet kennen om er een oplossing voor te vinden. Daarom gaan we binnen deze deelvraag de wet goed bestuderen.

Hoe werkt de cookiewall zoals deze op veel websites geïmplementeerd is?

Om de cookiewall te omzeilen moeten we weten hoe deze precies werkt. Dat gaan we in deze deelvraag uitzoeken.

Zijn er naast plugins nog andere mogelijkheden om dit probleem op te lossen?

Misschien zijn er naast een browserplugin wel betere oplossingen voor dit probleem. Hier zal met deze deelvraag naar gekeken worden.

Beantwoording hoofdvraag

Als we al deze deelvragen beantwoord hebben, kunnen we de hoofdvraag beantwoorden. Doordat we weten hoe cookies effectief te weren zijn (en dus effectief kunnen voorkomen dat gebruikers gevolgd worden) en hoe de cookiewall te omzeilen is kunnen we nu een oplossing maken voor dit probleem en de hoofdvraag beantwoorden.

2.2 Methode

Welke soorten cookies of andere manieren om gegevens op te slaan zijn er precies?

We beantwoorden deze vraag met een literatuurstudie. In de literatuur is voldoende te vinden over hoe cookies werken en wat voor soort cookies er zijn.

Hoe word je gevolgd op het internet?

Als we weten wat voor soort cookies er zijn en hoe gegevens opgeslagen worden op je computer onderzoeken we hoe het volgen dan precies in zijn werk gaat. Dit zullen we

voornamelijk onderzoeken aan de hand van een literatuurstudie. Verder zullen we een bevestiging doen door opgeslagen gegevens te monitoren en te kijken hoe deze veranderen.

Wat kun je doen tegen het gevolgd worden op het internet?

We zullen kijken wat voor maatregelen je kunt nemen tegen het gevolgd worden op het internet. Zo zijn er opt-out mogelijkheden en browserinstellingen. Daarnaast gaan we naar een aantal plugins kijken en deze vergelijken. In [19] zijn al een aantal plugins getest, maar voornamelijk op hun gebruikersvriendelijkheid. We zullen deze en een aantal andere populaire plugins gaan bekijken en hun functionaliteit vergelijken. Verder kijken we wat voor functionaliteit er al in de internetbrowsers aanwezig is. Ook doen we een korte eigen vergelijking waarbij we de cookieblockers testen op een aantal Nederlandse websites.

Hoe zit de wet precies in elkaar? Welke cookies mogen wel en welke niet volgens de wet?

Het huidige wetsartikel ([27]) gaan we analyseren. Verder is de wet momenteel nog in beweging: er is nog steeds discussie over, dus de wet kan in een korte tijd veranderen.

Daarnaast is veel van deze wet Europees geregeld en tot stand gekomen door een Europese richtlijn. We zullen voordat we de wet analyseren eerst naar deze richtlijn gaan kijken.

Hoe werkt de cookiewall zoals deze op veel websites geïmplementeerd is?

Er is momenteel een plugin genaamd 'CookiesOK' die de cookiewall op veel websites omzeilt. We gaan de broncode van deze plugin bekijken om te zien hoe deze precies werkt en hoe deze plugin de cookiewall omzeilt. Verder analyseren we ook een aantal websites waarbij we kijken in de code van de websites hoe de cookiewall daar precies opgebouwd is.

Zijn er naast plugins nog andere mogelijkheden om dit probleem op te lossen?

Misschien zijn er naast een browserplugin wel betere oplossingen voor dit probleem. Hiervoor gaan we op zoek naar inspiratie in zowel de literatuur als in de praktijk.

Hoofdstuk 3

Volgtechnieken op het internet

Zoals we in de inleiding kort hebben beschreven, gebruiken profilers verschillende technieken om internetgebruikers te volgen. Deze technieken hebben allemaal één ding gemeen: ze volgen de gebruiker als deze via zijn internetbrowser pagina's op het internet bezoekt. Als de gebruiker met zijn browser surft op het internet bezoekt hij verschillende pagina's op verschillende websites. Het bezoeken van deze pagina's gebeurt met het HTTP-protocol. Via dit protocol zendt de gebruiker, ook wel client genoemd, een HTTP-commando naar de website. De website, ook wel webserver genoemd, stuurt vervolgens een ~~HTTP-commando~~ terug samen met de gevraagde pagina.

Bij het opvragen van een pagina gebruikt de gebruiker een HTTP-GET-commando. De webserver antwoordt vervolgens met een HTTP-response-commando. Als een gebruiker later weer een nieuwe pagina wilt bezoeken, stuurt zijn browser weer een nieuw HTTP-GET-commando, waarbij de webserver weer opnieuw antwoordt met een HTTP-response-commando en hierbij een nieuwe pagina meestuurt.

3.1 Cookies en hun technische noodzaak

Doordat er bij het browsen op het internet enkel HTTP-commando's heen en weer gestuurd worden, kan een webserver geen onderscheid maken tussen verschillende gebruikers. Ieder HTTP-commando is niet gelinkt aan voorgaande commando's en zou dus ook van een andere gebruiker kunnen komen. Hierdoor is het voor een webserver niet mogelijk om met enkel HTTP-commando's extra informatie op te slaan zoals bijvoorbeeld of een gebruiker ingelogd is en eventuele instellingen voor een website. Eén van de oplossingen hiervoor is de cookie [5]. Een cookie is een klein tekstbestandje dat een webserver op de client kan plaatsen en later weer op kan vragen. Zo kan de webserver de client bijvoorbeeld een token geven of voorkeuren in een cookie opslaan. Deze cookies blijven dan opgeslagen op de computer van de gebruiker en kunnen opnieuw opgevraagd worden door de website als de gebruiker dezelfde site op een ander moment weer bezoekt.

We zullen in deze en de volgende sectie kort aan de hand van voorbeelden laten zien hoe deze cookies in de praktijk werken en hoe ze gebruikt worden door website-eigenaren en advertentiebedrijven. We gaan hiervoor precies kijken wat voor HTTP-commando's

er tussen de webserver en de client heen en weer gestuurd worden als de client een webpagina opvraagt. In de voorbeelden zijn steeds de niet relevante details weggehaald (er wordt namelijk nog meer informatie meegestuurd met HTTP).

Het eerste voorbeeld waar we naar kijken is een bezoek aan Google.nl. Als je als gebruiker naar google.nl gaat, stuurt de browser het volgende HTTP-GET-commando:

```
GET / HTTP/1.1
Host: www.google.nl
...
```

Google antwoordt vervolgens met een HTTP-response-commando, waarin ze de inhoud van een html-pagina meesturen. Zo'n response ziet er zo uit:

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Set-Cookie: PREF=ID=9cccfed350fbaffe:FF=0:TM=1365930398:LM=1365930398:S=
    RtdZ-IMEZjGpz2PG; expires=Tue, 15-Apr-2015 09:06:38 GMT; path=/;
    domain=.google.nl
Set-Cookie: NID=67=F5Q2Fobbs6yAml-2
    H9qVX0qK_nOx9CiKuBZWDzumCjLe3RyhbIFYKwuhHgRKdtM82-
    VnBWZe6aVrkQqAgQNOngr029HeBzUwwqlA0pBCYTVmOgYhW_rGY8jrNL16mePS;
    expires=Mon, 15-Oct-2013 09:06:38 GMT; path=/; domain=.google.nl;
    HttpOnly
...
```

Interessant zijn hier de twee keys 'Set-Cookie'. Hiermee worden lokaal twee cookie's opgeslagen, genaamd PREF en NID. Deze cookies bevatten beide een string tekst en verlopen pas in april 2015 en oktober 2013! Als we nu nogmaals naar google.nl gaan, zien we dat onze internetbrowser deze cookies inderdaad meestuurt in de HTTP-header van het GET-commando:

```
GET / HTTP/1.1
Host: www.google.nl
Cookie: PREF=ID=d2c5931773373ef7:U=0d7d956b6a8e73d4:FF=0:TM=1365930907:
    LM=1365930965:S=25QaqGgTFmoiZK6E; NID=67=
    LjKxvhp7rv1Xg2kWGKfaZMiKbCgUQCbPVifpRFDqJdB2HrL0kJrZMHL9yie1DgQl-
    dS7AvcIFUd0KCxZSmKCcgc4WzAU9-1Vj4A9ZkfC6pgyDU8AlTZXhl44QYYQG-Mx
...
```

Met deze cookies kan Google ons dus identificeren zonder dat we ook maar ergens ingelogd zijn. De cookies worden namelijk steeds meegestuurd totdat ze verlopen zijn, dus ook na een herstart van de computer of internetbrowser.

In deze sectie hebben we het alleen over Google gehad. Dit is slechts een voorbeeld, maar deze test is met praktisch iedere grote website te herhalen: ze gebruiken allemaal cookies. We hebben hiermee laten zien dat cookies dus een privacygevaar kunnen zijn. Desondanks zijn ze wel nodig om individuele gebruikers te kunnen identificeren: de gebruiker logt in met zijn gebruikersnaam en wachtwoord en krijgt vervolgens een token

van de server in de vorm van een cookie. Bij iedere HTTP-GET (oftewel: bij iedere klik op een link op die website) stuurt hij zijn cookie/token mee terug, waarmee de server dus weet dat deze gebruiker ingelogd is.

3.2 Verschil tussen first-party en third-party cookies

In de vorige sectie hebben we het enkel gehad voor first-party cookies: bij de Set-Cookie-flag in de HTTP-header stond altijd 'domain=.google.nl', wat dus betekent dat je internetbrowser deze cookie alleen meestuurt als je de website van Google bezoekt.

Google kan je dus mooi volgen rond al hun diensten, echter blijft dit dus beperkt tot hun eigen diensten. Maar helaas zijn er ook cookies die verder gaan dan dat, de zogenaamde third-party cookies. Deze cookies worden door een andere website dan degene die je bezoekt op je computer opgeslagen. Dit gebeurt doordat de websitebeheerder een script of afbeelding van een externe website op zijn eigen site heeft geplaatst. Als je vervolgens deze website bezoekt zal je webbrowser ook deze afbeelding of dit script laden met HTTP-GET-commando's. Deze HTTP-commando's gaan dan echter niet naar de oorspronkelijke website, maar naar het bedrijf dat dit script of deze afbeelding op de website heeft geplaatst. Het voordeel voor de websitebeheerder is dat hij met dit soort scripts van de externe partij zeer bruikbare statistieken over het gebruik van zijn website krijgt: de profiler houdt immers precies bij welke pagina's je allemaal bezoekt. Naast dat de profiler al deze clicks bijhoudt, plaatst hij meestal ook een cookie op jouw computer. Als je vervolgens op een andere website weer eenzelfde script of afbeelding van deze profiler tegenkomt, zal je internetbrowser de geplaatste cookie weer meesturen. Dit kan de profiler doen omdat hij naast de geplaatste cookie ook de url van de website die je op dat moment bezoekt meestuurt, de zogenaamde 'HTTP-referer'. Deze wordt bij een HTTP-GET-commando standaard meegestuurd. Deze referer vermeldt de webpagina waar de gebruiker 'vandaan komt', als hij via HTTP-GET een nieuwe pagina opvraagt. Doordat de profiler dan zowel de unieke cookie als de website die je bezocht hebt binnenkrijgt kan hij je over verschillende websites volgen en 'weet' hij dus wat voor websites je bezoekt.

Laten we weer een voorbeeld nemen. Als we naar youtube.com gaan, worden er heel wat HTTP-commando's heen en weer gestuurd. Youtube.com is namelijk een grote site, met veel plaatjes, filmpjes én advertenties die allemaal afzonderlijk met HTTP-commando's geladen moeten worden. Tussen deze HTTP-commando's zat ook een HTTP-request naar doubleclick.net, een groot bedrijf dat zich onder andere bezighoudt met profiling. Na een GET-commando naar doubleclick.net krijgen we de volgende HTTP-response:

```
HTTP/1.1 200 OK
Content-Type: image/gif
Set-Cookie: id=22dd811a95010037||t=1366012234|et=730|cs=002213
    fd481b706f5481e478de; expires=Wed, 15-Apr-2015 07:50:34 GMT; path=/;
    domain=.doubleclick.net
```

```
Set-Cookie: test_cookie=; domain=.doubleclick.net; path=/; Max-Age=0;
    expires=Mon, 21 Jul 2008 23:59:00 GMT
...
```

Aan *Content-Type: image/gif* is te zien dat onze webbrowser in dit geval een een plaatje opvroeg. Doubleclick.net stuurt ons vervolgens een cookie mee via de Set-Cookie flag in dit HTTP-response-commando. Deze cookie bevat het keyword 'id' en een waarschijnlijk unieke string. Let er ook op het domein: dat is nu doubleclick.net terwijl we gesurft hebben naar youtube.com! Ook verloopt deze cookie pas in 2015, waarmee Doubleclick ons in theorie dus twee jaar zou kunnen identificeren. Laten we nu eens naar nu.nl gaan. Nu.nl is een Nederlandse nieuwssite en heeft verder niets met Youtube te maken. Nu.nl maakt gebruik van advertenties van Doubleclick. Dit is duidelijk te zien aan een HTTP-GET-request naar doubleclick.net dat we krijgen als we de website nu.nl laden:

```
GET /adj/P4442.Nu.nl/home;sz=728x95;tile=4;kw=;tt=0945;gr=10;rg=0;nk=0;
    ord=8874230931700769? HTTP/1.1
Host: ad.nl.doubleclick.net
Referer: http://www.nu.nl/
Cookie: _drt_=NO_DATA; id=22dd811a95010037||t=1366012234|et=730|cs
    =002213fd481b706f5481e478de
```

Deze GET gaat naar doubleclick.net (zie het keyword Host). Er wordt ook een cookie meegestuurd, met id=22dd811a95010037. Deze id is exact hetzelfde als de id die we op youtube.com kregen van Doubleclick. Verder stuurt onze browser dus ook de HTTP-referer mee: dat is in dit geval http://www.nu.nl. Hiermee is duidelijk te zien dat Doubleclick 'weet' wie we zijn. Verder weet het bedrijf ook dat we nu.nl bezocht hebben, waarmee het bedrijf ons dus gemakkelijk kan volgen via third-party cookies.

Ook hier heb ik slechts een enkel voorbeeld laten zien, maar ook hier maakt dit voorbeeld wel duidelijk hoe third-party cookies werken en hoe advertentiebedrijven dit gebruiken om gebruikers over verschillende websites te kunnen volgen.

3.3 Tracking via first-party cookies

Tracking door HTTP-redirects

Gelukkig is het volgen via de third-party cookies eenvoudig tegen te gaan. Iedere moderne browser biedt namelijk de optie om deze third-party cookies te blokkeren en Mozilla was zelfs van plan dit in hun browser Firefox vanaf versie 22 zelfs standaard te doen [33]. Helaas is Mozilla op dit besluit teruggekomen en hebben ze deze verandering uitgesteld, omdat er toch nog functionaliteit kan breken op sommige websites [11]. Zelf surf ik echter al jaren op het internet met deze optie en ik ben nog geen problemen tegengekomen. De advertentie-industrie reageert in ieder geval niet blij op dit besluit [25]. Zij pleiten voor een opt-out systeem, zoals nu het geval is: als de gebruiker third-party cookies wil blokkeren moet hij dit zelf handmatig aanzetten.

Hoewel er in de praktijk nog weinig gebruikt gemaakt wordt van het volgen van gebruikers via first-party cookies [34], zal dit in de toekomst misschien veranderen. Google en Youtube werken nu namelijk al op die manier samen: wie zich op gmail.com aanmeldt, is ook meteen aangemeld op youtube.com, ook als third-party cookies geblokkeerd worden. Laten we eens gaan kijken hoe dit in zijn werk gaat.

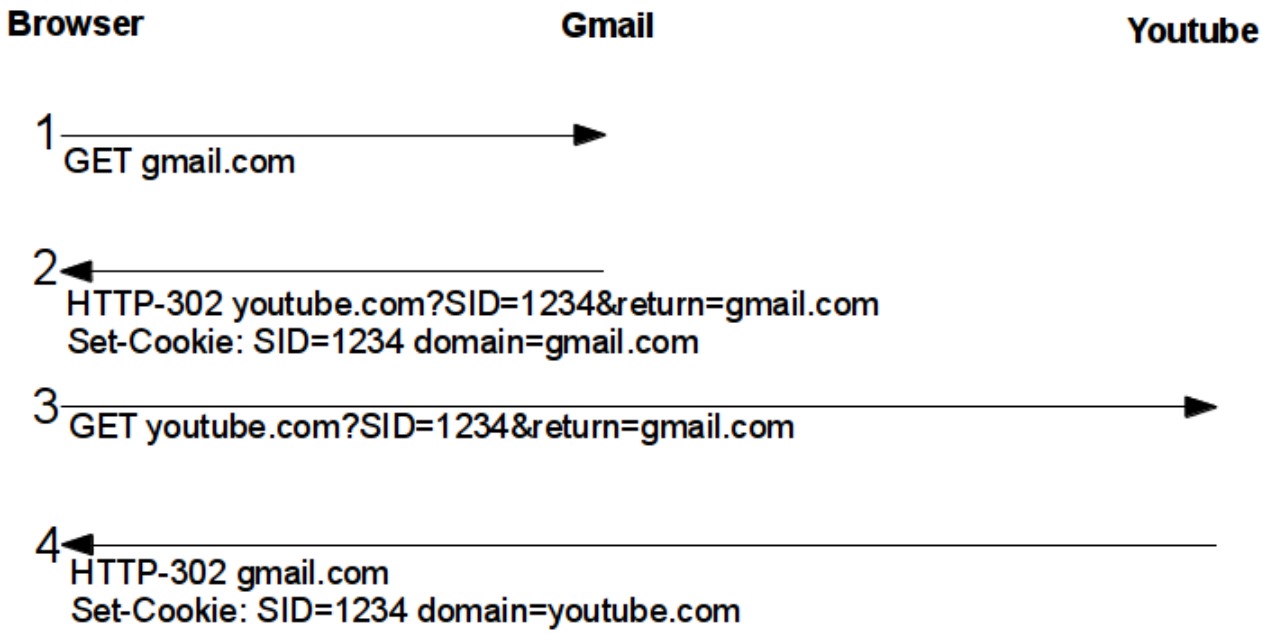
We starten weer met een schoon browserprofiel (we wissen dus alle cookies). Vervolgens surfen we naar gmail.com en melden ons daar aan met een Google-account. Zodra we aangemeld zijn zien we dat er zowel door google.com, accounts.google.com als youtube.com cookies zijn geplaatst op onze computer. Dit terwijl we niet op youtube.com zijn geweest en onze browser alle third-party cookies blokkeert. Als we een blik werpen op de verstuurde HTTP-headers zien we hoe dit mogelijk is. Er wordt namelijk gebruik gemaakt van HTTP-redirects, oftewel: de gebruiker wordt even kort doorgestuurd naar youtube.com en keert vervolgens weer terug bij google.com. Doordat hij op deze manier even kort op youtube.com is geweest, kan hij van dit domein ook cookies ontvangen.

We zullen dit illustreren aan de hand van de schematische tekening in figuur 3.1. De schematische weergave in de figuur is licht versimpeld: er wordt in deze figuur maar van een enkele fictieve cookie gebruikt gemaakt. Als we gmail.com bezoeken stuurt Google ons meteen door naar accounts.google.com. Vervolgens loggen we in met onze gegevens, die onze webbrowser daarna via een HTTP-POST naar google.com toestuurt (stap 1 in de figuur). De webserver van Google doet nu echter iets vreemds: in plaats van dat ze via een HTTP-response een html-pagina terugsturen, sturen ze ons een HTTP-302-melding. Dit is geen html-pagina, maar een redirect, oftewel een doorverwijzing. Met deze doorverwijzing worden we naar youtube.com gestuurd. Met deze doorverwijzing plaatst Google meteen een aantal cookies (SID=1234 in de figuur stap 2). Door deze doorverwijzing vragen we via een GET de website van Youtube op, waarbij we meteen de door Gmail geplaatste cookies meesturen (stap 3 in de figuur). Youtube stuurt ons vervolgens weer terug naar Gmail. Ze sturen echter een aantal cookies mee, die gelijk zijn aan de cookies die we van Gmail hebben ontvangen (stap 4 in de figuur). Deze redirect ziet er zo uit:

```
HTTP/1.1 302 Moved Temporarily
Content-Type: text/html; charset=UTF-8
Set-Cookie: GoogleAccountsLocale_session=nl; Secure
Set-Cookie: APISID=X1wGGnxGetU2HnEY/A1OoX6m0kFAwztNJb;Domain=.youtube.
    com;Path=/;Expires=Thu, 13-Apr-2023 17:53:21 GMT
Set-Cookie: SAPISID=dDUwSE2Sg-3x6772/AbvTveL2GBHlPWfOO;Domain=.youtube.
    com;Path=/;Expires=Thu, 13-Apr-2023 17:53:21 GMT;Secure
```

Let op het domein hier, dat is youtube.com. Door de HTTP-redirect zitten we nu namelijk op youtube.com en is dat voor onze browser het first-party domein. Onze browser blokkeert de verkregen cookies dus niet. Op deze manier zijn er dus third-party cookies geplaatst terwijl onze browser deze juist blokkeert!

Nu is Youtube eigendom van Google, dus is het logisch dat deze twee partijen nauw samenwerken. Echter laat dit voorbeeld wel zien wat er in de praktijk mogelijk is. Zo zou iedere website die momenteel gebruik maakt van Doubleclick ons kunnen redirecten



Figuur 3.1: Schematische weergave hoe Gmail en Youtube samenwerken en first-party cookies uitwisselen.

naar doubleclick.net voordat de eigenlijke site geladen wordt. Dan heeft het blokkeren van third-party cookies geen effect meer. Dit wordt momenteel in de praktijk nog niet gedaan, zoals we in het begin van deze sectie al meldden, maar dat het mogelijk is, is met dit voorbeeld wel aangetoond.

Tracking via javascript en URL's

Als een gebruiker third-party cookies blokkeert worden third-party javascripts echter gewoon toegelaten. Deze scripts hebben toegang tot de first-party cookies van de website die de gebruiker op dat moment bezoekt. De informatie in deze cookies kunnen ze vervolgens doorspelen naar een derde partij, die hiermee de gebruiker alsnog kan volgen terwijl hij third-party cookies blokkeert.

Een bekend voorbeeld van een partij die hier veel gebruik van maakt is Google Analytics [14]. Websitebeheerders kunnen de scripts van Google Analytics op hun website toevoegen om zo statistische informatie over het gebruik van hun website te verzamelen. Vervolgens plaatst dit script een aantal first-party cookies. Eén van deze cookies is __utma. Deze cookie kan gebruikers onderscheiden en wordt ondertussen natuurlijk ook weer terug naar Google gestuurd.

Laten we ook hier een voorbeeld van nemen. We wissen weer al onze cookies en stellen de browser zo in dat deze third-party cookies blokkeert. We bezoeken nu www.geenstijl.nl. Als we enkel deze site laden en verder nergens op klikken, hebben we de volgende cookies ontvangen van het domein geenstijl.nl:

```
__utma = 43608755.1804972556.1366120981.1366120981.1366120981.1
__utmb = 43608755.1.10.1366120981
__utmc = 43608755
__utmz = 43608755.1366120981.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd
    =(none)
rsi_segs = G07609_10697|G07609_0
```

__utma verloopt pas in 2015. Als we nu naar de HTTP-headers kijken, zien we dat deze cookie ook naar Google gestuurd wordt, als waarde in een URL, waarmee er een plaatje wordt opgevraagd via een HTTP-GET:

```
GET /__utm.gif?utmwv=5.4.1&utms=1&utmn=829609424&utmhn=www.geenstijl.nl&
    utmcs=ISO-8859-1&utmsr=1680x1050&utmvp=1664x885&utmsc=24-bit&utmul=nl
    &utmje=0&utmfl=11.2%20r202&utmdt=GeenStijl%20%3A%20Tendentieus%2C%20
    ongefundeerd%20en%20nodeloos%20kwetsend&utmhid=1096134074&utmr=-&utmp
    =%2F&utmht=1366120981098&utmac=UA-1914562-4&utmcc=__utma%3D43608755
    .1804972556.1366120981.1366120981.1366120981.1%3B%2B__utmz%3D43608755
    .1366120981.1.1.utmcsr%3D(direct)%7Cutmccn%3D(direct)%7Cutmcmd%3D(
    none)%3B&utmu=q~ HTTP/1.1
Host: www.google-analytics.com
```

Als we het desbetreffende plaatje op `http://google-analytics.com/__utm.gif` openen, zien we dat dit een gif-afbeelding van 1x1 pixel is. Google gebruikt dit plaatje dus enkel om cookies te ontvangen, want zo'n plaatje heeft verder geen enkel nut voor de gebruiker. Deze HTTP-GET wordt met behulp van javascript gegenereerd zodra de gebruiker de webpagina opent.

Als we een aantal andere websites proberen die gebruik maken van Google Analytics blijken die op dezelfde manier deze cookies naar Google te sturen. Deze cookies zijn echter voor iedere website uniek, iedere website heeft zijn eigen Google Analytics-cookies. Doordat dit first-party cookies zijn, zijn deze ook niet aan elkaar te 'linken': als je naar nu.nl gaat stuur je de unieke Google Analytics-cookie van die site naar Google. Google kan deze echter onmogelijk koppelen aan een Google Analytics-cookie van een andere site, omdat Google die cookie enkel op kan vragen als je de desbetreffende site bezoekt. Daarom gebruikt Google deze techniek waarschijnlijk enkel om een gebruiker binnen een website te volgen, in plaats van tussen websites.

3.4 Flashcookies

De flashplayer

Naast dat de webbrowser cookies en dus identificerende data kan opslaan, kunnen eventuele browserplugins dit ook. De bekendste is hier de Adobe Flash Player. Deze plugin zorgt ervoor dat de gebruiker flashobjecten van een webpagina af kan spelen. Veel webpagina's maken hier gebruik van. Onder andere youtube.com voor de filmpjes en bekende websites met online spelletjes. Ook advertenties zijn vaak met flash gemaakt.

Veel webpagina's werken alleen optimaal als de gebruiker de flashplayer geïnstalleerd heeft. Als een gebruiker zonder flashplayer op één van deze websites komt wordt hij er in veel gevallen op gewezen om deze plugin te installeren. Hierdoor heeft meer dan 95 procent van de internetgebruikers deze plugin geïnstalleerd staan [20]. Chrome, de webbrowser van Google levert deze plugin zelfs standaard mee [1].

Cookies

De flashplayer wordt vaak gebruikt voor grote flashobjecten als filmpjes of spelletjes. Hierdoor heeft Adobe de mogelijkheid ingebouwd om lokaal data op te slaan als cache, genaamd 'Local Shared Objects'. Deze data wordt net als cookies onder een bepaald domein opgeslagen. Het verschil met de 'gewone' browsercookies is echter dat deze data standaard geen verloopdatum heeft en veel meer informatie kan bevatten dan de 4KB die een cookie maximaal mag zijn. Omdat ook hier veel identificerende informatie in opgeslagen kan worden en de flashplayer deze LSO's vaak gebruikt als een soort state-mechanisme noemen we deze vaak ook wel 'flashcookies'.

De flashcookies worden door de flashplugin opgeslagen in een lokale map op je computer. Deze opslag werkt 'buiten de browser om', waardoor het wissen van cookies in de webbrowser deze cookies gewoon intact laat. Ook werken deze flashcookies in iedere browser waarin de flashplugin geladen is, waardoor profilers je dus kunnen volgen tussen meerdere webbrowsers. Voorheen konden gebruikers zelfs gevolgd worden als ze met hun webbrowser in privénavigatiemodus surften. De bedoeling van deze modus is dat er in zo'n browsersessie geen geschiedenis en cookies opgeslagen worden. Echter werden er dan wel flashcookies geregistreerd. Gelukkig is dit inmiddels gefixt [39]: de flashplayer detecteert nu of je webbrowser in privénavigatiemodus draait. Als dit het geval is bewaart hij geen flashcookies.

Net als de webbrowser onderscheid maakt tussen first- en third-party cookies, doet de flashplayer dit ook. Standaard worden third-party flashcookies geaccepteerd. Dit gedrag is te wijzigen via het control panel van Adobe [2]. Op dit control panel zijn de flashcookies ook te wissen, en zelfs in zijn geheel te blokkeren. Adobe waarschuwt wel dat de functionaliteit van websites hierdoor in het geding kan komen.

Volgtechnieken

Advertentiebedrijven maken ook gebruik van flashcookies om gebruikers te volgen. Dit is onderzocht in [37]. Ze hebben daar de 100 populairste websites in 2009 bekeken en onderzocht of deze flashcookies gebruiken. In 2009 bleken 54 van de 100 websites flashcookies te gebruiken. Dit aantal is in 2012 afgenomen tot 37 van de 100 [4]. Van de 100 websites gebruikten in 2009 98 gewone http-cookies, terwijl dat in 2012 100 van de 100 zijn. De meest gebruikte namen waren 'volume', 'id' en 'userid'. Volume zal waarschijnlijk over een geluidsinstelling gaan, omdat flash vaak voor media wordt gebruikt. Id en userid zijn wat zorgwekkender: hiermee krijgen gebruikers een uniek id mee dat wordt opgeslagen in een flashcookie. Van de 100 websites bleken 31 website een overlappend id te gebruiken tussen de gewone browsercookie en de flashcookie. Ook

kwamen de onderzoekers er achter dat in sommige gevallen de gewone browsercookie, als deze gewist werd, 'hersteld' werd door de flashcookie. In deze gevallen heeft het wissen van een browsercookie dus totaal geen effect, want deze wordt dan gewoon teruggeplaatst omdat de website je nog steeds kan identificeren via de flashcookie.

3.5 HTML5-storage

Een recente ontwikkeling op het web is de nieuwe webstandaard HTML5. Deze standaard is nog in ontwikkeling en dus niet compleet. Eén van de nieuwe features in deze standaard is de ondersteuning voor local storage. Hierdoor kan er lokaal data opgeslagen worden in de vorm van key-value paren. Het grote voordeel tegenover flash is dat er geen plugin voor nodig is, terwijl het voordeel tegenover gewone http-cookies is dat HTML5-storage geen verloopdatum heeft en veel groter is. http-cookies mogen maximaal 4KB groot zijn, flashcookies zijn standaard 100KB terwijl HTML5-storage 5MB is. Deze grootte zorgt ervoor dat er veel lokaal opgeslagen kan worden, zoals bijvoorbeeld ingevulde webformulieren of zelfs documenten en bestanden. Omdat er voor HTML5-storage geen plugin nodig is, kan deze storage gemakkelijk vanuit de browser gewist worden. In Firefox is bijvoorbeeld een druk op 'Extra -> Recente geschiedenis wissen' voldoende om naast de http-cookies ook de HTML5-storage te wissen. Verder wordt HTML5-storage niet zoals flashcookies gedeeld tussen verschillende browsers.

Omdat HTML5 een vrij recente ontwikkeling is en er tegenwoordig vanuit privacy-bewegingen en zelfs de overheid steeds meer verzet komt tegen het volgen van gebruikers wordt hier bij de HTML5-storage wat beter over nagedacht aldus de onderzoekers uit [46]. Ze haalden daarbij ook meteen een voorbeeld aan over hoe het key-value-systeem van HTML5 hieraan kan bijdragen: als een gebruiker op de website example.com als voorkeursthema zwart-wit wenst, wordt er met behulp van javascript lokaal een key-value-paar 'theme=BW' aangemaakt. Dit is dan mogelijk voor iedere voorkeur op die website. Dit soort instellingen worden dan volledig lokaal aangemaakt en opgeslagen: er is geen verbinding meer nodig met de server. Ondanks dat dit een vooruitgang is (alles gebeurt lokaal) blijft het plaatsen van 'gewone cookies' met id's in de HTML5-storage ook nog steeds mogelijk. Hoe dit in de praktijk zal uitpakken is dus nog onbekend. Misschien dat een browser in de toekomst een instelling kan bevatten om HTML5-storage enkel lokaal te houden. Op die manier kunnen er wel voorkeuren in de HTML5-storage opgeslagen worden maar worden deze nooit naar de server verzonden.

HTML5-storage is vrij nieuw en wordt daarom in de praktijk nog niet veel gebruikt. Er zijn al enkele websites die deze opslag gebruiken om gebruikers te identificeren, aldus [4]. Momenteel is nog niet bekend of third-party storage standaard toegestaan gaat worden in HTML5 [46].

3.6 Browser fingerprinting

Een nieuwe techniek om individuele gebruikers te identificeren is door middel van browser fingerprinting. Hiermee wordt er lokaal op de computer van de gebruiker geen data

opgeslagen, maar worden de instellingen van de gebruiker zoals browser, schermresolutie en geïnstalleerde plugins gebruikt om een gebruiker te identificeren. De EFF heeft hier een onderzoek naar gedaan [10].

Browser fingerprints bestaan uit een aantal uniek identificeerbare elementen. De eerste is de User Agent. Deze string wordt met ieder HTTP-commando naar de server meegestuurd en vertelt welke browser, welk besturingssysteem en welke versie de client draait. In ons geval was dat steeds:

```
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:17.0) Gecko/20100101
    Firefox/17.0
```

Hierin staat dus het besturingssysteem (Linux), de webbrowser (Firefox) en de versie (17.0). Een ander identificeerbaar item is de lijst met plugins. Een server kan een check doen of een client een plugin heeft of niet. Met deze check kan hij dus ook de plugins en zelfs de versienummers hiervan achterhalen. Verder is via de flashplayer op te vragen welke lettertypes een client geïnstalleerd heeft staan. Dit is vaak ook een redelijk unieke lijst. Daarnaast zijn er nog een aantal kleinere identificeerbare items zoals cookies en javascript (die kunnen aan en uit staan), en de schermresolutie van de client. Deze informatie verandert natuurlijk ook weer als een gebruiker een instelling verandert, een update installeert of een nieuwe plugin installeert. In het onderzoek hebben ze echter met slimme algoritmes kunnen bepalen of een fingerprint nieuw is of veranderd. Met fingerprinting is het dus mogelijk om een gebruiker te identificeren. Zo kan een gewiste cookie weer hersteld worden, net als met de flashcookies gedaan werd.

In het onderzoek komt ook naar voren dat er helaas vrij weinig tegen te doen is: cookies of wat dan ook wissen heeft geen effect, want deze worden simpelweg niet gebruikt hiervoor. Mozilla heeft als reactie op dit onderzoek al de User Agent-string van hun webbrowser aangepast (zie `https://bugzilla.mozilla.org/show_bug.cgi?id=728831`), zodat nu enkel de major-versie (dus 17) getoond wordt in plaats van de minor-versie (17.0.5). Andere maatregelen, zoals de User Agent-string verbergen of plugins blokkeren hebben weinig effect zolang maar weinig mensen dit doen: je wordt er alleen maar meer uniek mee omdat je één van de weinige mensen bent die dit doet.

Via de website `http://panopticlick.eff.org/` kun je je webbrowser laten testen op 'uniekheid'. Het gebruikersprofiel van de webbrowser die we in deze sectie gebruikt hebben om het cookiegedrag van websites te analyseren blijkt na een test op die website ook uniek te zijn en minstens 21 bits identificerende informatie te bevatten.

Hoofdstuk 4

Maatregelen om volgen te voorkomen

Zoals we in hoofdstuk 3 hebben gezien gebruiken profilers vooral cookies om gebruikers op het internet te volgen. Het blokkeren van alle cookies is dus een effectieve maatregel om de meeste profilers tegen te houden. We hebben echter ook gezien dat cookies op veel websites noodzakelijk zijn. Zonder cookies werken dingen als loginsessies bijvoorbeeld niet goed, waardoor veel websites niet te gebruiken zijn. Alle cookies blokkeren is dus een te sterke maatregel. We zullen daarom in dit hoofdstuk gaan kijken naar wat minder strenge maatregelen en de effectiviteit hiervan. We zullen eerst kijken naar wat voor maatregelen er al ingebouwd zijn in de meestgebruikte browsers. Daarna gaan we kijken naar plugins voor deze browsers. Met een plugin is de functionaliteit van een browser namelijk eenvoudig uit te breiden.

4.1 Standaardmaatregelen

Third-party cookies blokkeren

Op dit moment bieden de meestgebruikte browsers allen de mogelijkheid om alle cookies te blokkeren. Helaas is deze maatregel 'te streng' omdat dit functionaliteit breekt met veel websites. We hebben in hoofdstuk 3 echter ook het verschil uitgelegd tussen first- en third-party cookies. We konden hierbij duidelijk zien dat veel profilers juist gebruik maken van third-party cookies om gebruikers te volgen. Iedere moderne browser biedt de mogelijkheid om third-party cookies standaard te blokkeren. Dit is echter niet in alle browsers even gemakkelijk in te stellen, met name in Internet Explorer zit deze optie diep verborgen, blijkt uit onderzoek [19]. Door deze optie aan te zetten worden alle toekomstige third-party cookies geblokkeerd: je zult als gebruiker dus geen nieuwe third-party cookies meer binnenkrijgen. Echter blijven de third-party cookies die momenteel al opgeslagen zijn op je computer nog gewoon benaderbaar in iedere browser behalve Firefox [34]. Je zult dus expliciet alle cookies moeten wissen om deze instelling effect te laten hebben.

In de praktijk blijkt deze instelling momenteel best veel effectiviteit te bieden: de profilers volgen gebruikers voornamelijk via third-party cookies en dat wordt op deze manier volledig geblokkeerd. Verder zijn er geen nadelige gevolgen bekend van het blokkeren van third-party cookies: alle websites blijven gewoon werken. De vraag is echter wel hoe lang dit nog effectief is. Zeker omdat Firefox in toekomstige versies third-party cookies waarschijnlijk standaard gaat blokkeren [33]. Als andere browsers dit voorbeeld gaan volgen zullen in de toekomst het merendeel van de gebruikers third-party cookies standaard blokkeren. Profilers zullen dan op andere volgtechnieken over moeten gaan om gebruikers te kunnen volgen. Zoals we hebben gezien zijn er nog voldoende alternatieven zoals tracking via first-party, flashcookies, HTML5-storage en browserfingerprinting.

Statistiekencookies worden echter niet op deze manier tegengehouden. Zoals we hebben gezien gebruikt Google Analytics enkel first-party cookies om gebruikers te volgen. Hiervoor zijn er dus andere maatregelen nodig, waarop we later terugkomen.

Cookies wissen aan het einde van de browsersessie

Naast het blokkeren van third-party cookies kun je de browser ook zo instellen dat hij na iedere browsersessie (dus zodra je de browser afsluit) alle cookies wist. Ook HTML5-storage is op deze manier automatisch te wissen. Het voordeel hiervan is dat je via cookies en HTML5-storage enkel te volgen bent binnen één browsersessie. Ook ben je hierdoor iedere keer als je met een nieuwe browsersessie begint voor de meeste websites een unieke bezoeker: je hebt immers nog geen cookie ontvangen van de website, waardoor veel websites je als een nieuwe bezoeker zien. Het nadeel hiervan is dus dat je sinds de cookiewet ook bij ieder bezoek weer de cookiewall voorgeschoteld krijgt.

Naast het plaatsen van vaste cookies, maken de meeste websites ook gebruik van sessiecookies: als je op een website inlogt, krijg je een 'token' van die website in de vorm van een sessiecookie. Aan deze cookie kan de website zien dat jij ingelogd bent. Deze sessiecookie wordt altijd gewist zodra je je browser afsluit, of zodra je te lang inactief bent (hij verloopt namelijk na een korte tijd).

De website plaatst deze sessiecookie zodra je inlogt. De inloggegevens kunnen echter al wel ingevuld zijn: veel websites bieden namelijk de optie om deze gegevens te onthouden. Als je deze optie aanvinkt maakt de website een vaste cookie aan die dus blijft bestaan als je je browser afsluit: met deze cookie kan de website je bij een volgend bezoek identificeren en automatisch inloggen: je krijgt dan aan de hand van de vaste cookie automatisch een sessiecookie toegewezen.

Als je echter alle cookies wist aan het einde van browsersessie kan deze vaste cookie niet bewaard blijven, waardoor je dus steeds opnieuw moet inloggen op iedere website. Dit is minder gebruiksvriendelijk. Verder kun je op deze manier nog steeds deels gevolgd worden, echter alleen binnen een enkele browsersessie.

Doordat deze methode eigenlijk meer nadelen dan voordelen heeft zullen we gaan kijken naar effectievere maatregelen die minder nadelen hebben en ook binnen een browsersessie de juiste cookies blokkeren.

4.2 Opt-out mogelijkheden

youronlinechoices.eu

Op aandringen van de EU is er een online website gelanceerd die consumenten de mogelijkheid moet bieden om te 'opt-outen' voor het online gevolgd worden. De website biedt op deze manier een mogelijkheid voor consumenten om meer controle te krijgen over hun online privacy. Via `http://www.youronlinechoices.eu/nl/` kun je voor de aangesloten advertentienetwerken een opt-out instellen. Door op deze manier een opt-out in te stellen zul je niet meer gevolgd worden door deze bedrijven. Ondanks dat dit de belofte is, maken niet alle aangesloten bedrijven deze waar [16].

Het nadeel van deze opt-out mogelijkheid is dat deze enkel werkt bij de aangesloten bedrijven. Ieder bedrijf dat er niet bijzit zal jou dus nog steeds volgen. Ook is het voorlopig nog niet wettelijk verplicht voor een bedrijf om deze opt-out mogelijkheid te bieden en worden er dus ook nog steeds geen sancties gegeven aan bedrijven die niet meedoen. Het is op deze manier dus eigenlijk maar een deels werkende oplossing.

Een ander probleem van deze website is dat de opt-out mogelijkheid die je hier selecteert ergens opgeslagen moet worden op een manier dat ieder aangesloten bedrijf kan zien dat jij opt-out en dus niet gevolgd wil worden. Deze opt-out wordt in een cookie opgeslagen. Youronlinechoices.eu laat ieder aangesloten bedrijf een script draaien, waarmee dit bedrijf een third-party cookie met de opt-out op jouw computer kan plaatsen. Je browser moet third-party cookies dus accepteren om deze instelling te laten werken. Helaas zorgen third-party cookies zoals we in hoofdstuk 3 gezien hebben er ook weer voor dat je veel gemakkelijker te volgen bent op websites die niet meedoen hieraan.

Op `http://www.youronlinechoices.eu/nl/uw-advertentie-voorkeuren` kun je je computer laten scannen en zo zien van welke bedrijven je allemaal cookies hebt ontvangen. Na een scan kun je ieder aangesloten bedrijf individueel 'uitzetten' of alles in één keer uitzetten. Bij het opt-outen wordt er vervolgens lokaal een cookie op je computer gezet bij ieder bedrijf dat je geselecteerd hebt. Hier ontstaat ook meteen een probleem: dit werkt alleen voor de momenteel aangesloten bedrijven. Mocht er in de toekomst een nieuw bedrijf aan de lijst toegevoegd worden zul je opnieuw je computer laten scannen om ook hiervoor een opt-out in te stellen. Eenmalig naar deze website gaan is dus niet voldoende.

Een ander probleem met youronlinechoices.eu is dat deze website tijdens de scan ieder aangesloten bedrijf bezoekt, waarmee ook weer cookies meekomen. Met andere woorden: als je met een schoon browserprofiel deze scan uitvoert zul je na een scan zien dat er honderden cookies geplaatst zijn door de aangesloten bedrijven. Het is dus niet slim om een scan te doen en daarna de opt-out mogelijkheid niet te gebruiken: dit zal voor veel extra onnodige third-party cookies zorgen.

Do-not-track-header

In de nieuwe HTML5-standaard is een extra header toegevoegd die de browser mee kan sturen met een HTTP-GET-commando, namelijk de DNT-header. DNT staat voor Do

Not Track en geeft dus aan dat de gebruiker niet gevolgd wil worden. Via een instelling in de browser kan een gebruiker aangeven dat hij niet gevolgd wil worden, waardoor de browser standaard een DNT-header meestuurt met ieder HTTP-verzoek.

De Do-not-track-header beschrijft enkel een verzoek aan profilers: het maakt het namelijk technisch niet onmogelijk voor profilers om je te volgen. Bedrijven kunnen dus zelf kiezen of ze dit verzoek accepteren of niet. Er wordt momenteel ook niet opgetreden tegen bedrijven die niet meedoen aan dit verzoek.

De bedoeling van Do-not-track was dat het een opt-out systeem is: standaard moet deze instelling dus uitstaan en de gebruiker moet deze handmatig aanzetten. Dit is gedaan omdat profilers anders waarschijnlijk het verzoek zullen negeren als praktisch iedere gebruiker deze header meezendt. Er zullen namelijk weinig gebruikers zijn die expliciet aangeven dat ze wél gevolgd willen worden.

Helaas is dit bij het opt-out systeem fout gegaan: Microsoft zendt in Internet Explorer 10 namelijk standaard een Do-not-track-header mee [3]. Hiermee is het dus geen opt-out systeem meer en door deze instelling zijn profilers weer minder geneigd om een Do-not-track-verzoek te honoreren. Hiermee is ook dit een maatregel die helaas niet voldoende is om het volggedrag van profilers te voorkomen.

4.3 Beschikbare plugins

Naast de standaardfunctionaliteit zijn webbrowsers uit te breiden met een grote hoeveelheid plugins. Er zijn ook een groot aantal plugins die iets proberen te doen tegen profiling. Dit kan gaan van het compleet blokkeren van advertenties tot blacklisting of enkel het wissen van cookies. We zullen een aantal van de meest populaire plugins in deze sectie kort toelichten. Doordat in zowel de Chrome webstore als de Firefox add-on-pagina te zien is hoe vaak een plugin is gedownload kunnen we gemakkelijk de populariteit vergelijken. We zullen in deze sectie de meest populaire plugins bekijken en kijken hoe ze bijdragen aan het voorkomen van profiling op het internet.

Adblock Plus

Adblock Plus is met 15 miljoen downloads verreweg de populairste add-on voor Firefox. Adblock Plus is een add-on die standaard alle advertenties probeert te blokkeren op het internet. Adblock Plus werkt met een blacklist waarop reclamewebsites staan. Als een element van een website op die blacklist staat, blokkeert Adblock Plus dit element bij het laden van de webpagina, waardoor reclame dus ook niet zichtbaar is voor de gebruiker. De negatieve kant van Adblock Plus is dat website-eigenaren inkomsten mislopen doordat Adblock Plus al hun advertenties blokkeert.

In de standaardinstelling richt Adblock Plus zich voornamelijk op het blokkeren van advertenties. Ondanks dat ook dit wel heel wat trackingcookies blokkeert werkt dit niet zo effectief als plugins die hier specifiek voor bedoeld zijn. Zo plaatst scorecardresearch.com (een profiler) een cookie zodra we naar *telegraaf.nl* gaan. Echter worden de cookies van andere profilers (zoals Doubleclick) op deze website wel geblokkeerd.

Adblock Plus biedt echter ook een extra filter om tracking te blokkeren [30]. Dit is helaas geen standaardinstelling, waardoor de meeste gebruikers dit extra filter niet zullen installeren. Adblock Plus is te downloaden op `http://adblockplus.org`.

Betterprivacy

Betterprivacy is een add-on die specifiek bedoeld is om flashcookies te wissen. Betterprivacy breidt de browser uit met extra opties om flashcookies te wissen, zodat deze voortaan ook gewist worden als de gebruiker zijn 'normale cookies' wilt wissen. Verder kan de add-on zo ingesteld worden dat deze automatisch alle flashcookies wist bij het afsluiten van de browser. Betterprivacy is te downloaden op `https://addons.mozilla.org/en-US/firefox/addon/betterprivacy/`

Ghostery

Ghostery is een add-on die specifiek is gericht op het blokkeren van trackingscripts en trackingcookies. Ghostery kan dus zowel scripts als profilers blokkeren. Het blokkeren hiervan gaat door middel van een blacklist die automatisch dagelijks bijgewerkt wordt. Ghostery categoriseert profilers in verschillende groepen, van statistieken tot advertentie en privacy. Doordat Ghostery ook bepaalde scripts blokkeert, kan hij ook effectief optreden tegen flashcookies en HTML5-storage, want deze cookies worden ook door scripts op je computer opgeslagen. Verder voorkomt Ghostery ook het volgen via first-party cookies in veel gevallen. Alle cookies van Google Analytics worden bijvoorbeeld geblokkeerd. Tenslotte ondersteunt Ghostery de mogelijkheid om bij het afsluiten van de browser automatisch de flashcookies te wissen, al zijn de instelmogelijkheden hiervan niet zo uitgebreid als die van Betterprivacy. Ghostery is te vinden op `http://www.ghostery.com`.

DoNotTrackMe

DoNotTrackMe is een add-on die net als Ghostery ook trackingcookies en scripts blokkeert. Ook DoNotTrackMe werkt met een blacklist. DoNotTrackMe is verder helaas niet in te stellen en de blacklist is ook niet aan te passen zoals bij Ghostery wel het geval is. DoNotTrackMe vergelijkt zichzelf in hun faq ook met Ghostery. Volgens hun is het verschil dat ze minder functionaliteit breken en dat ze sneller zijn. De add-on is te downloaden op `https://www.abine.com/dntdetail.php`

Disconnect.me

Disconnect.me blokkeert net als de vorige besproken add-ons trackingcookies van profilers. Ook Disconnect.me werkt hierbij met een blacklist. Losse websites en profilers zijn te whitelisten in de plugin, voor het geval er functionaliteit breekt. Verder blokkeert de plugin naast trackingcookies ook advertenties. Het is dus een mooie combinatie van Ghostery en Adblock Plus. Disconnect.me is te downloaden op `disconnect.me`.

4.4 Vergelijking van plugins

Als we kijken naar de plugins die we zojuist opgesomd hebben kunnen we grofweg een onderscheid maken tussen twee verschillende soorten. Aan de ene kan heb je plugins die specifiek trackingcookies blokkeren met een blacklist, zoals Ghostery en DoNotTrackMe. Aan de andere kant heb je de plugins die zich juist richten op één taak, zoals Adblock Plus op het blokkeren van advertenties en Betterprivacy op het wissen en instellen van flashcookies. We zullen de plugins die specifiek cookies blokkeren hier kort met elkaar vergelijken.

Het eerste wat opvalt is dat ze allen tekort schieten in gebruikersvriendelijkheid: zonder veel kennis van zaken zijn ze minder effectief en de standaardinstelling is lang niet altijd de optimale, blijkt uit onderzoek [8]. Het nadeel van dit soort plugins is namelijk dat ze teveel kunnen blokkeren waardoor sommige websites niet meer goed werken. Vooral onervaren gebruikers komen er dan niet snel achter dat dit soort plugins de oorzaak kunnen zijn van een niet functionerende website.

Digitaltrends.com heeft Ghostery met DoNotTrackMe vergeleken [7]. Hun conclusie was dat ze beide wel redelijk werkten. Ghostery blokkeerde meer, maar daarbij was de kans dat er functionaliteit breekt op websites ook groter. LifeHacker heeft de plugins ook met elkaar vergeleken. Zij vonden Disconnect.me zowel qua gebruikersvriendelijkheid als qua aantal features de meest geschikte plugin [15].

De reden dat er functionaliteit kan breken is vrij simpel: alle plugins werken met een blacklist waarin een aantal reguliere expressies gebruikt worden om 'trackingcontent' te blokkeren. Als we bijvoorbeeld naar de anti-trackinglijst van Adblock Plus kijken (zie `https://easylist-downloads.adblockplus.org/easyprivacy.txt`), staan daar de volgende dingen in:

```
com/a.gif?
.webmetrics.js
/csi?v=*&action=
```

Als een website dus een noodzakelijk stukje javascript in webmetrics.js plaatst, of als de afbeelding a.gif wel een belangrijke afbeelding is (meestal is dit namelijk een 1x1-gif om gebruikers te tracken en cookies te sturen), dan zal de website niet meer optimaal werken.

Verder heeft Jonathan Mayer van de Stanford University ook een aantal plugins met elkaar vergeleken [21]. Volgens dit onderzoek uit 2011 zijn de filters van Adblock Plus de meest effectieve. Het nadeel van die laatste is wel dat de extra filters handmatig toegevoegd moeten worden. Verder heeft deze moeite met sommige scripts zoals bijvoorbeeld die van Google Analytics. Ghostery scoort in dat opzicht weer beter: deze vervangt de Google Analytics-scripts namelijk met een soort dummy-bestanden (want het volledig blokkeren van Goole Analytics-scripts kan ervoor zorgen dat een website niet meer werkt).

Het is ook mogelijk meerdere plugins tegelijk te draaien. Ze conflicteren namelijk niet snel met elkaar [18]. Beide filters worden zo gecombineerd. Echter wordt de kans dat

er functionaliteit breekt nu wel groter: als één van de plugins iets blokkeert dat eigenlijk niet geblokkeerd had moeten worden zal de website al niet meer volledig werken. Ook is het zo lastiger te achterhalen waar het fout gaat: je weet immers niet welke plugin nu iets verkeerds blokkeert.

Eigen vergelijking

Omdat er op het internet weinig vergelijkingsmateriaal te vinden is, gaan we hier in een kort onderzoekje de plugins met elkaar vergelijken op een aantal Nederlandse websites. We bezoeken eerst de website zonder plugins en kijken wat ze aan cookies plaatsen. Hier maken we onderscheid tussen first-party, third-party en flashcookies. Omdat third-party cookies ook met een browserinstelling te blokkeren zijn, is het resultaat bij de first-party en flashcookies hier het meest belangrijk. In het geval van first-party cookies bekijken we alleen de cookies die gebruikt worden om gebruikers te volgen, zoals Google Analytics. De plugins gebruiken we in de standaard instellingen, waarbij we alleen aan Adblock Plus het extra anti-trackingfilter hebben toegevoegd. In onderstaande tabel staan de websites, het totaal aantal first-party, third-party en flashcookies dat ze plaatsten en daarnaast het aantal cookies dat er nog geplaatst worden als de betreffende plugin geactiveerd is:

Site	Soort	Totaal	Adblock+	Ghostery	DNTme	Disconnect.me
nu.nl	1st-party	7	4	0	1	3
	3rd-party	21	0	0	18	0
	flash	1	1	1	1	1
geenstijl.nl	1st-party	7	4	1	1	1
	3rd-party	63	9	6	8	6
	flash	3	3	3	3	3
telegraaf.nl	1st-party	12	8	0	0	2
	3rd-party	144	0	1	17	2
	flash	1	1	1	1	1

In dit specifieke voorbeeld scoort Ghostery duidelijk het best. De andere drie add-ons scoren redelijk gelijk. Wat echter wel een belangrijke vermelding is, is dat de first-party cookies die Adblock Plus doorlaat allemaal van Google Analytics komen, terwijl de first-party cookies die de andere plugins doorlaten juist *niet* van Google Analytics komen. Als we aan Adblock Plus de volgende entry toevoegen: `||google-analytics.com^` krijgen we geen enkele first-party trackingcookie meer binnen. Volgens [21] kunnen sommige sites echter niet goed functioneren zonder deze cookies en scripts, waardoor hier Ghostery beter gebruikt kan worden (deze vervangt Google Analytics door een dummy-script). Ook de auteurs van het filter van Adblock Plus hebben deze entry bewust weggelaten om deze reden [44].

Een ander opvallend punt is dat geen enkele plugin ook maar iets doet met flashcookies: ze laten ze allemaal door. Enkel Ghostery biedt de mogelijkheid om flas-

hcookies aan het einde van de browsersessie te verwijderen.

Het is belangrijk om te beseffen dat dit slechts een voorbeeld is met drie websites. Dit onderzoekje is dus niet representatief om de algemene kwaliteit van de plugins te vergelijken. Wel geeft het aan dat er zeker verschillen zijn tussen de plugins.

Zelf zou ik gaan voor Adblock Plus, omdat je hier sowieso het meeste overzicht hebt over wat er allemaal geblokkeerd wordt en je hiermee zelf gemakkelijk filters toe kan voegen. Voor de gemiddelde gebruiker lijkt mij bijvoorbeeld DoNotTrackMe meer geschikt: deze heeft veel minder instellingen en werkt met één klik.

4.5 Overzicht effectieve oplossingen

In dit hoofdstuk hebben we heel wat oplossingen besproken. Om tot een goede eindoplossing te komen (zo min mogelijk gevolgd worden, maar de gebruikerservaring zo min mogelijk negatief beïnvloeden) zullen we een aantal oplossingen moeten combineren en een aantal oplossingen juist niet gebruiken.

Van de standaardmaatregelen blijkt het blokkeren van third-party cookies effectief te zijn en geen nadelen met zich mee te brengen. Dit is dus een goede optie. Daarnaast bieden browsers de mogelijkheid om cookies aan het einde van de sessie te wissen. Zoals we gezien hebben zorgt dit voor een mindere gebruikerservaring, omdat gebruikers zo geen instellingen op het web kunnen onthouden.

Van de opt-out-mogelijkheden bleek er geen één erg effectief te zijn. youronlinechoices.eu werkt namelijk alleen als we geen third-party cookies blokkeren en als de profilers mee willen werken. Doordat we liever third-party cookies blokkeren dan dat we youronlinechoices.eu gebruiken is dit geen effectieve maatregel. De Do-not-track-header is enkel een verzoek: bedrijven kunnen dit negeren. Maar deze optie aanzetten brengt geen nadelen met zich mee, waardoor dit mogelijk een goede extra maatregel is.

Daarnaast hebben we verschillende plugins vergeleken. Uit verschillende onderzoeken en ons eigen onderzoek blijkt dat het gebruiken van zo'n extra plugin zeker een effectieve maatregel is om ook first-party cookies te blokkeren. Daarom is ook het installeren van minimaal één plugin een goede maatregel.

Hoofdstuk 5

Juridisch kader

Het nieuwe cookiebeleid is begonnen bij een Europose richtlijn uit 2009. De Nederlandse cookiewet is vervolgens een implementatie van deze richtlijn. We zullen in dit hoofdstuk zowel de Europese richtlijn als de Nederlandse implementatie van die richtlijn bekijken. Ook bekijken we hoe de huidige implementatie van deze wet door websites (de cookiewall) past in deze richtlijn en of deze voldoet. Daarnaast zullen we enkele begrippen die hier verband mee houden uitleggen, zoals 'implied consent'.

5.1 De Europese richtlijn

Al in 2009 heeft de Europese Unie een richtlijn goed gekeurd waarmee het cookiebeleid strenger moet worden. Deze richtlijn wordt de e-privacy directive genoemd, de 2009/136/EG [40]. Deze richtlijn vernieuwt en herziet hiermee de oude e-privacyrichtlijn, de 2002/58/EG [41]. De richtlijn uit 2002 is een uitbreiding op de originele privacy directive uit 1995, de 95/46/EG [42]. Momenteel bestaan dus de richtlijn uit 1995 en die uit 2009 naast elkaar, waar de richtlijn uit 2009 die uit 2002 heeft vervangen en zich voornamelijk toespitst op elektronische communicatie terwijl de 95/46/EG vooral definities en rechten met betrekking tot privacy en gegevensbescherming bevat en zich toespitst op de situaties uit de tijd dat het internet nog niet zo'n groot privacygevaar kende als tegenwoordig. Deze twee richtlijnen zijn de basis voor de cookiewet, zoals hij momenteel bestaat in Nederland. Voordat we naar de Nederlandse wet kijken, zullen we in deze sectie eerst deze richtlijn analyseren.

De nieuwe richtlijn bevat een aantal punten die van belang zijn voor de wetgeving zoals we die nu in Nederland kennen. Eén van de voorstellen in de 2009/136/EG is overweging 66, hiermee moeten gebruikers nu expliciet op de hoogte gesteld worden als derden informatie op hun apparatuur willen plaatsen. De tekst luidt als volgt:

> "Het is mogelijk dat derden informatie op de apparatuur van een gebruiker willen installeren of toegang tot reeds opgeslagen informatie willen krijgen, dit om tal van redenen, gaande van wettige handelingen (b.v. bepaalde types cookies) tot ongeoorloofde indringing in de privésfeer (b.v. spyware of virussen). Daarom is het van kapitaal belang dat gebruikers duidelijke en omvattende informatie krijgen wanneer zij een handeling stellen die kan resulteren in een dergelijke opslag of toegang. De wijze

> waarop informatie wordt gegeven en een recht van weigering wordt aangeboden moet zo gebruikersvriendelijk mogelijk zijn."

Naast dat gebruikers een duidelijke melding moeten krijgen, moet ook een 'recht van weigering' worden aangeboden. Volgens diezelfde overweging 66 mag er een uitzondering gemaakt worden als dit technisch noodzakelijk is:

> "Uitzonderingen op de verplichting om informatie te geven en een recht van weigering aan te bieden moeten worden beperkt tot situaties waarbij de technische opslag of toegang strikt noodzakelijk is voor het wettige doel of om het gebruik mogelijk te maken van een specifieke dienst waarom de abonnee of gebruiker heeft verzocht."

Verder wordt in overweging 66 al een melding gemaakt dat, wanneer dit technisch mogelijk is, toestemming van de gebruiker moet worden gevraagd:

> "Wanneer dit technisch mogelijk en doeltreffend is, kan, overeenkomstig de desbetreffende bepalingen van richtlijn 95/46/EG, de toestemming van de gebruiker met verwerking worden uitgedrukt door gebruik te maken van de desbetreffende instellingen van een browser of een andere toepassing. Deze bepalingen moeten doeltreffender worden afgedwongen via uitgebreide bevoegdheden die aan de desbetreffende nationale instanties worden verleend."

Dat dit technisch mogelijk is weten we inmiddels: een cookiewall is een technische implementatie om gebruikers toestemming te vragen. Deze bepaling moet worden afgedwongen door nationale instanties, oftewel: iedere lidstaat moet zorgen dat een instelling deze bepalingen af gaat dwingen. Voor toestemming wordt de volgende definitie uit artikel 2 sub h, 95/46/EG gehanteerd:

> "toestemming van de betrokkene", elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem/haar betreffende persoonsgegevens worden verwerkt.

Uit deze definitie blijkt dus dat de toestemming ook specifiek moet zijn. Hierdoor moet de gebruiker op iedere website die cookies gebruikt expliciet aangeven dat hij akkoord gaat met het plaatsen van cookies. Als je als gebruiker enkel een mededeling onder of bovenin het scherm krijgt die aangeeft dat de website cookies gebruikt (zoals `www.nu.nl` hanteert), voldoet de website niet aan de richtlijn. Er worden dan namelijk al cookies geplaatst voordat je toestemming hebt gegeven. Ook een algemene browserinstelling waarmee je in het algemeen toestemming geeft is in strijd met de richtlijn, omdat je dan niet specifiek voor iedere website toestemming geeft.

Een enkele mededeling onder of bovenin het scherm wordt ook wel een 'implied consent-melding' genoemd. Implied consent betekent vrij vertaald 'toestemming geven uit stilzwijgen'. In de richtlijn staat echter dat toestemming een *specifieke* wilsuiting moet zijn, waarmee implied consent dus in strijd is met de richtlijn.

Overweging 66 ondersteunt een wijziging van artikel 5 lid 3 2002/58/EG. Deze luidt met de nieuwe richtlijn nu als volgt:

> "3. De lidstaten dragen ervoor zorg dat de opslag van informatie of het verkrijgen van toegang tot informatie die reeds is opgeslagen in de eindapparatuur van een abonnee of gebruiker, alleen is toegestaan op voorwaarde dat de betrokken abonnee of gebruiker toestemming heeft verleend, na te zijn voorzien van duidelijke en volledige informatie overeenkomstig Richtlijn 95/46/EG, onder meer over de doeleinden van de verwerking.

> Zulks vormt geen beletsel voor enige vorm van technische opslag of toegang met als uitsluitend doel de uitvoering van de verzending van een communicatie over een elektronisch communicatienetwerk, of, indien strikt noodzakelijk, om ervoor te zorgen dat de aanbieder van een uitdrukkelijk door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij deze dienst levert."

Dit artikel zorgt dat gebruikers toestemming moeten geven als er informatie op hun computer opgeslagen en later weer opgevraagd wordt. De toestemming moet vrij en specifiek zijn, zoals we eerder hebben gezien. Ook de uitzondering voor technisch noodzakelijke doeleinden is gemaakt. Dit artikel is te vertalen naar cookies: gebruikers moeten toestemming geven voor het plaatsen van cookies op hun computer, omdat er enkel voor technisch noodzakelijke cookies een uitzondering is gemaakt. Hierbij maakt het soort cookie niet uit: ook bij flashcookies en browser fingerprinting wordt er toegang verkregen tot informatie die reeds is opgeslagen in de eindapparatuur van de gebruiker, waarbij ook hier toestemming noodzakelijk is.

Naast toestemming spreekt dit artikel ook over 'duidelijke en volledige informatie overeenkomstig richtlijn 95/46/EG'. In artikel 10 95/46/EG wordt deze informatieverstrekking uitgelegd:

> "De Lid-Staten bepalen dat de voor de verwerking verantwoordelijke of diens vertegenwoordiger aan de betrokkene, bij wie de betrokkene zelf betreffende gegevens worden verkregen, ten minste de hierna volgende informatie moet verstrekken, behalve indien de betrokkene daarvan reeds op de hoogte is:
>
> a) de identiteit van de voor de verwerking verantwoordelijke en, in voorkomend geval, van diens vertegenwoordiger,
> b) de doeleinden van de verwerking waarvoor de gegevens zijn bestemd
> c) verdere informatie zoals
>
> - de ontvangers of de categorieën ontvangers van de gegevens;
> - antwoord op de vraag of men al dan niet verplicht is om te antwoorden en de eventuele gevolgen van niet-beantwoording,
> - het bestaan van een recht op toegang tot zijn eigen persoonsgegevens en op rectificatie van deze gegevens, voor zover die, met inachtneming van de specifieke omstandigheden waaronder de verdere informatie verkregen wordt, nodig is om tegenover de betrokkene een eerlijke verwerking te waarborgen."

Hierbij moeten dus onder andere 'de ontvangers of de categorieën ontvangers van de gegevens' verstrekt worden. In het geval van cookies zijn dit de derde partijen die gebruikers via cookies volgen: zij plaatsen namelijk de cookies en verkrijgen hiermee informatie over de gebruikers. Als een websitebeheerder aan deze informatieverstrekkingsplicht wil voldoen zal hij dus duidelijk moeten melden welke partijen allemaal cookies plaatsen en gebruikers volgen. Daarnaast moeten 'de doeleinden van de verwerking waarvoor de gegevens zijn bestemd' verstrekt worden. Trackinginformatie wordt door de profilers vaak doorverkocht aan onder andere adverteerders. Dit moet dus ook duidelijk aan de gebruiker gemeld worden.

Verder gaat het derde punt van sub c over het recht om je eigen gegevens te rectificeren. Dit is in het geval van cookies mogelijk door je cookies te wissen. Een websitebeheerder moet zijn gebruikers dan ook duidelijk wijzen op deze mogelijkheid en hoe de

gebruiker dit kan doen. Dit kunnen ze doen door duidelijk uit te leggen hoe de gebruiker zijn cookies kan wissen. Met het wissen van cookies kan de website het surfgedrag van het verleden van de gebruiker niet meer bijhouden en ziet hem als een nieuwe gebruiker.

De implementatie op de websites moet, zoals in overweging 66 2009/136/EG is aangegeven, verder zo gebruikersvriendelijk mogelijk zijn. Zowel het verstrekken van informatie als het vragen om toestemming moet zo gebruikersvriendelijk mogelijk zijn. Dit roept bij de huidige implementaties nog wel eens vragen op. Gebruikers ergeren zich namelijk mateloos aan de huidige implementatie [9], doordat cookiewalls er zo irritant mogelijk uitzien. Ook moet een gebruiker na het wissen van zijn cookies opnieuw toestemming geven en websites zijn vaak niet te bezoeken als een gebruiker niet akkoord gaat. Gebruikersvriendelijk is de huidige implementatie in ieder geval niet.

Cookies bevatten vaak een uniek nummer, waarmee ze herleidbaar kunnen zijn naar één persoon. Hierdoor kunnen het persoonsgegevens zijn. De definitie van een persoonsgegeven is te vinden in de 95/46/EG en luidt als volgt:

> "persoonsgegevens", iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon, hierna "betrokkene"te noemen; als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit.

Cookies kunnen een identificatienummer bevatten. Als dit het geval is, zijn cookies persoonsgegevens. Volgens artikel 4 punt 1 95/46/EG past ieder lidstaat zijn eigen bepalingen op deze persoonsgegevens toe:

> "Elke Lid-Staat past zijn nationale, ter uitvoering van deze richtlijn vastgestelde bepalingen toe op de verwerking van persoonsgegevens indien:
>
> a) die wordt verricht in het kader van de activiteiten van een vestiging op het grondgebied van de Lid-Staat van de voor de verwerking verantwoordelijke; wanneer dezelfde verantwoordelijke een vestiging heeft op het grondgebied van verscheidene Lid-Staten, dient hij de nodige maatregelen te treffen om ervoor te zorgen dat elk van die vestigingen voldoet aan de verplichtingen die worden opgelegd door de toepasselijke nationale wetgeving;
> b) de voor de verwerking verantwoordelijke niet gevestigd is op het grondgebied van de Lid-Staat, maar in een plaats waar de nationale wet uit hoofde van het internationale publiekrecht van toepassing is;
> c) de voor de verwerking verantwoordelijke persoon niet gevestigd is op het grondgebied van de Gemeenschap en voor de verwerking van persoonsgegevens gebruik maakt van al dan niet geautomatiseerde middelen die zich op het grondgebied van genoemde Lid-Staat bevinden, behalve indien deze middelen op het grondgebied van de Europese Gemeenschap slechts voor doorvoer worden gebruikt."

Sub a zorgt ervoor dat een bedrijf zich in ieder EU-land aan de daar geldende verplichtingen met betrekking tot de verwerking van persoonsgegevens moet houden. Sub b breidt dit uit naar de plaatsen waar dezelfde wet van toepassing is als in het EU-land, zoals kolonies. Sub c gaat vervolgens over de bedrijven die geen vestiging in het EU-land hebben, maar hier wel actief zijn. Door sub c moeten dus ook buitenlandse bedrijven die

geen vestiging in een EU-land hebben, maar wel binnen de EU-markt actief zijn zich ook aan de verplichtingen met betrekking tot de verwerking van persoonsgegevens houden zoals die binnen de EU-landen waar ze actief zijn gelden.

In Nederland bestaat hiervoor de Wet bescherming persoonsgegevens [28] waar we later op terugkomen. Hier moet namelijk extra nauwkeurig naar gekeken worden en dan met name hoe er met deze persoonsgegevens omgegaan wordt. Het doel van profilers is vooral om zoveel mogelijk nuttige informatie over jouw internetgebruik te verzamelen en deze vervolgens door te verkopen. Hiermee verkopen ze dus persoonsgegevens door aan derden. Artikel 6 uit de 95/46/EG gaat verder in op deze verwerking van persoonsgegevens:

> "De Lid-Staten bepalen dat de persoonsgegevens:
>
> a) eerlijk en rechtmatig moeten worden verwerkt;
> b) voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden moeten worden verkregen en vervolgens niet worden verwerkt op een wijze de onverenigbaar is met die doeleinden. Verdere verwerking van de gegevens voor historische, statistische of wetenschappelijke doeleinden wordt niet als onverenigbaar beschouwd, mits de Lid-Staten passende garanties bieden;
> c) toereikend, ter zake dienend en niet bovenmatig moeten zijn, uitgaande van de doeleinden waarvoor zij worden verzameld of waarvoor zij vervolgens worden verwerkt;
> d) nauwkeurig dienen te zijn en, zo nodig, dienen te worden bijgewerkt; alle redelijke maatregelen dienen te worden getroffen om de gegevens die, uitgaande van de doeleinden waarvoor zij worden verzameld of waarvoor zij vervolgens worden verwerkt, onnauwkeurig of onvolledig zijn, uit te wissen of te corrigeren;
> e) in een vorm die het mogelijk maakt de betrokkenen te identificeren, niet langer mogen worden bewaard dan voor de verwezenlijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, noodzakelijk is. De Lid-Staten voorzien in passende waarborgen voor persoonsgegevens die langer dan hierboven bepaald voor historische, statistische of wetenschappelijke doeleinden worden bewaard."

Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is voor de verwezenlijking van de doeleinden. Cookies worden echter zoals we in hoofdstuk 3 gezien hebben soms meer dan een jaar bewaard, terwijl het bezoek van de gebruiker aan een website nooit langer dan een dag in beslag zal nemen. Ook de voorkeuren van een gebruiker hoeven geen jaren bewaard te worden.

Samenvattend komt het er op neer dat er voor het gebruik van alle niet-functionele cookies nu expliciet toestemming vereist is van de gebruikers. Hierbij is 'implied consent' dus niet voldoende. Dit is echter een richtlijn, EU lidstaten hebben daarom nog iets 'speling' bij de implementatie van deze richtlijn. Lidstaten mogen namelijk zelf bepalen hoe ze een richtlijn uitwerken, enkel het beoogde resultaat staat vast [43].

5.2 Nederlandse implementatie

De implementatie van de geanalyseerde gegevens uit de Europese richtlijn is terechtgekomen in artikel 11.7a van de Telecommunicatiewet [27]. We zullen deze implementatie hier kort bespreken. Het eerste punt uit deze wet luidt als volgt:

> "Onverminderd de Wet bescherming persoonsgegevens dient een ieder die door middel van elektronische communicatienetwerken toegang wenst te verkrijgen tot gegevens die zijn opgeslagen in de randapparatuur van een gebruiker dan wel gegevens wenst op te slaan in de randapparatuur van de gebruiker:
>
> a. de gebruiker duidelijke en volledige informatie te verstrekken overeenkomstig de Wet bescherming persoonsgegevens, en in ieder geval omtrent de doeleinden waarvoor men toegang wenst te verkrijgen tot de desbetreffende gegevens dan wel waarvoor men gegevens wenst op te slaan, en
> b. van de gebruiker toestemming te hebben verkregen voor de desbetreffende handeling."

Als een website dan cookies wil plaatsen moet hij volgens punt b uit deze wet van de gebruiker toestemming hebben verkregen. Toestemming is in de Wet bescherming persoonsgegevens (WBP) op dezelfde manier gedefinieerd als in de 95/46/EG [29]. Zoals we gezien hebben moet toestemming een vrije wilsuiting zijn en is implied consent niet voldoende.

Websites zullen dus een cookiewall moeten plaatsen als ze cookies plaatsen. Ze kunnen er ook voor kiezen om helemaal geen cookies te plaatsen. Ze moeten dan een cookievrije website maken maar dit is niet altijd technisch mogelijk. Een voorbeeld is een internetforum waar gebruikers plaatjes of video's kunnen embedden: als een gebruiker hier een forumpost plaatst met een youtubefilmpje kan iedereen die deze pagina bezoekt een trackingcookie binnenkrijgen doordat het filmpje dan geladen wordt, waarmee de gebruiker een niet-functionele cookie van Youtube kan ontvangen. Een voorbeeld hiervan is zelfs op de website van de Radboud Universiteit te vinden, namelijk op `http://www.ru.nl/@869289/nijmeegse-tweedaagse/` Op deze link is namelijk een youtubefilmpje te vinden. Ondanks dat dit filmpje niet meteen begint te spelen, wordt het al wel geladen waardoor Youtube cookies kan plaatsen. Dit is te testen door eerst alle cookies te wissen en vervolgens naar deze site te gaan. Youtube zal doordat het filmpje geladen wordt dan cookies plaatsen. Een screenshot van deze test is in de bijlage onder figuur A.1 te vinden.

Naast de toestemming van de gebruiker is volgens punt a ook een duidelijke informatieverstrekking conform de WBP verplicht. Deze informatieverstrekking is als volgt gedefinieerd in artikel 33 WBP:

> 1. "Indien persoonsgegevens worden verkregen bij de betrokkene, deelt de verantwoordelijke vóór het moment van de verkrijging de betrokkene de informatie mede, bedoeld in het tweede en derde lid, tenzij de betrokkene daarvan reeds op de hoogte is.
> 2. De verantwoordelijke deelt de betrokkene zijn identiteit en de doeleinden van de verwerking waarvoor de gegevens zijn bestemd, mede.

3. De verantwoordelijke verstrekt nadere informatie voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen."

De verantwoordelijke is in dit geval de websitebeheerder. Hij moet dus melden waarvoor de gegevens gebruikt zullen worden. Dit wordt dan meestal geplaatst in de cookiewall of implied consent-pop-up: deze bevat een link naar het cookie- of privacybeleid van de website. De informatieverstrekking moet volgens punt 1 plaatsvinden vóór het moment dat de persoonsgegevens van de gebruiker verkregen zijn. Dit is in het geval van een implied consent-melding niet mogelijk: doordat je hier de website al bezoekt worden er al cookies geplaatst en opgevraagd, waarmee je dus niet op tijd geïnformeerd bent. Dit is naast toestemming nog een reden waarom enkel een implied consent-melding wettelijk niet toegestaan is. Verder plaatsen sommige websites al trackingcookies voordat je akkoord bent gegaan met het plaatsen van cookies. Dit is natuurlijk ook tegen deze informatieverstrekking. Een voorbeeld van zo'n website is de sociale netwerksite `www.hyves.nl` en dit voorbeeld is in figuur A.2 te vinden.

Punt 2 van de informatieverstrekking eist dat de betrokkene zijn identiteit en de doeleinden van de verwerking waarvoor de gegevens zijn bestemd mededeelt. Dit gaat in veel gevallen goed: in de cookiewalls van websites wordt zo goed als altijd uitgelegd waar cookies voor gebruikt worden.

Punt 3 is wat lastiger: hier moet de verantwoordelijke nadere informatie verstrekken om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen. De verzamelde gegevens worden veelal doorgespeeld aan derde partijen en profilers. De vraag is dan of zij zorgen voor een zorgvuldige verwerking. Dit maken websites veelal niet bekend.

Naast deze drie punten moeten gebruikers ook nog hun persoonsgegevens 'in kunnen trekken' of terug kunnen vorderen. Dit is mogelijk door cookies te wissen. Een website moet zijn gebruikers dus ook uitleggen hoe ze dit moeten doen.

Als we kijken naar de implementatie van de wetgeving op de 25 populairste Nederlandse websites, dan is dit dramatisch: van de 25 websites voldoet slechts één website aan de wet, namelijk nos.nl. De website van de NOS geeft namelijk de vereiste informatie en vraagt toestemming voordat ze cookies plaatsen. Ze geven de gebruiker echter geen keuze: je kunt de website niet bezoeken als je geen cookies accepteert of als je alle cookies met een browserinstelling blokkeert. Waar dit bij de meeste commerciële websites geen probleem is (je kunt natuurlijk altijd kiezen om de website niet te bezoeken), is dit bij een website van de publieke omroep, die gefinancierd wordt met overheidsgeld, discutabel. Deze discussie valt echter buiten de scope van deze scriptie. Het onderzoek is in sectie B te vinden.

Ook de Nederlandse wet maakt net als de richtlijn een uitzondering voor technisch noodzakelijke cookies:

> "Het bepaalde in het eerste en tweede lid is niet van toepassing, voor zover het de technische opslag of toegang tot gegevens betreft met als uitsluitend doel:

a. de communicatie over een elektronisch communicatienetwerk uit te voeren, of
b. de door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij te leveren en de opslag of toegang tot gegevens daarvoor strikt noodzakelijk is."

Technisch noodzakelijke cookies mogen dus wel, maar third-party trackingcookies niet. Statistiekencookies zitten hier eigenlijk 'tussenin'. Door middel van statistiekencookies worden gebruikers namelijk slechts binnen één website gevolgd. Echter wordt er bij statistiekencookies ook gebruik gemaakt van een uniek nummer, waarmee individuele gebruikers dus identificeerbaar zijn. Daarnaast zijn statistiekencookies niet technisch noodzakelijk, waardoor ook hier toestemming voor gevraagd moet worden.

Handhaving cookiewet

Op het gebied van handhaving van de cookiewet zijn er twee partijen die bij overtreding op kunnen treden. Omdat de cookiewet zelf in de telecommunicatiewet is geïmplementeerd, zal hier de Autoriteit Consument en Markt (ACM) bij overtreding op moeten treden, zoals in artikel 15.1 van de Telecommunicatiewet gedefinieerd is:

"Met het toezicht op de naleving van het bepaalde bij of krachtens andere bepalingen van deze wet dan bedoeld in het eerste en tweede lid en met het toezicht op de naleving van de bepalingen van de roamingverordening zijn belast de bij besluit van de Autoriteit Consument en Markt aangewezen ambtenaren."

Echter zijn cookies zelf persoonsgegevens, waar netjes mee omgegaan moet worden. Als dit dus niet gebeurt zoals in de Wet bescherming persoonsgegevens is vermeld zal hier het College bescherming persoonsgegevens (CBP) tegen op moeten treden zoals dit in artikel 51 lid 1 WBP gedefinieerd is:

"Er is een College bescherming persoonsgegevens dat tot taak heeft toe te zien op de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de wet bepaalde. Tevens houdt het College toezicht op de verwerking van persoonsgegevens in Nederland, wanneer de verwerking plaatsvindt overeenkomstig het recht van een ander land van de Europese Unie."

Als je dit onderscheid formeel moet maken, dan zou het CBP moeten optreden als gebruikers zonder hun toestemming toch gevolgd worden door profilers: hier wordt namelijk de Wet bescherming persoonsgegevens overtreden. Als het echter gaat om een cookiewall die niet volgens de wet functioneert, als een website bijvoorbeeld enkel een implied consent-melding plaatst zal de ACM hier tegen op kunnen treden. Tussen deze twee gebieden zit dan ook nog een overlappend gebied waarop beide partijen in actie kunnen komen. Hoe deze handhaving precies in zijn werk gaat en de eventuele sancties vallen buiten het bereik van deze analyse.

Momenteel zijn er echter nog geen gevallen bekend waarbij één van de partijen heeft opgetreden tegen overtreding van de cookiewet.

5.3 Toekomstige ontwikkelingen in deze wetgeving

Een meerderheid van de Tweede Kamer heeft inmiddels twijfels bij deze wet en daarom willen ze de pop-ups afschaffen [12]. Om dit mogelijk te maken willen ze de cookiewet

afzwakken, waardoor 'implied consent' voldoende is: de website hoeft enkel een duidelijke mededeling te plaatsen waarmee de gebruikers op de hoogte zijn van het cookiebeleid. Dit is dan in strijd met de richtlijn, die expliciete toestemming vereist zoals we hebben gezien. Ook de informatieverstrekking komt dan in het geding: die moet namelijk gebeuren vóór dat de gebruiker cookies ontvangt. Veel websites lopen al vooruit op deze wetsaanpassing en hebben nu al enkel een implied consent cookiewall, zoals bijvoorbeeld `www.nu.nl`.

Een ander probleem is dat een aantal websites momenteel niet te bezoeken zijn door gebruikers die alle cookies volledig blokkeren. Dit komt doordat de website ergens moet opslaan dat een gebruiker akkoord gaat met het plaatsen van cookies, waarbij deze instelling in een cookie bewaard wordt. Dit is volgens de wet geen probleem (want dit kan gezien worden als een functionele cookie), maar als een gebruiker alle cookies blokkeert kan hij deze cookie niet opslaan, en dus niet akkoord gaan met de cookiewall. In de richtlijn wordt hier verder niet op ingegaan: daar wordt enkel gesproken over de privacy van internetgebruikers.

Enkele websites lopen al vooruit op de wetswijziging en gaan over naar enkel een implied consent-melding: onder andere de publieke omroep gaat hun cookiewall neerhalen [36]. Echter wordt het eigenlijke probleem hiermee niet opgelost: gebruikers worden nog steeds gevolgd op het internet door profilers en ze zijn hier verder nog steeds niet erg bewust van. Ook hebben gebruikers op het internet nog steeds geen keuze: ze kunnen niet zomaar opt-outen, waardoor deze nieuwe wetgeving eigenlijk niets verandert aan de huidige situatie.

Verder ligt er inmiddels een wetsvoorstel waarmee ook voor statistiekencookies, zoals die van Google Analytics, een uitzondering gemaakt wordt [17]. Zoals we gezien hebben in hoofdstuk 3 zijn dit voornamelijk first-party cookies, maar lijken ze niet rechtstreeks gebruikt te worden om gebruikers te volgen (al is dit met een kleine technische aanpassing wel mogelijk). Dit voorstel is waarschijnlijk in strijd met de Europese richtlijn, daarin wordt namelijk alleen een uitzondering gemaakt voor technisch noodzakelijke cookies. Statistiekencookies zijn niet technisch noodzakelijk en mogen volgens de richtlijn dus niet zonder toestemming geplaatst worden.

5.4 Kritiek

Al in 2010, dus nog voordat Nederland dit in de wet had staan, had de Bits of Freedom al kritiek op de nieuwe Europese richtlijn [45]. Ze waren toen al bang dat de gebruikersvriendelijkheid van het web verminderd zou worden. Ook zal de privacy van gebruikers niet veel verbeteren: gebruikers zullen overhaast met alle cookiewalls akkoord gaan, waarmee dit dus averechts werkt. Nu de wet er eenmaal is ergeren de gebruikers zich inderdaad massaal aan de cookiewalls [9].

De Bits of Freedom kwam in 2010 al met andere oplossingen. Zo zouden browsers een whitelist bij kunnen houden van cookies waarvoor geen toestemming nodig is. Verder had Europa ook een opt-out mogelijkheid als youronlinechoices.eu verplicht kunnen stellen voor ieder bedrijf dat binnen de EU opereert. Mocht opt-out niet voldoende zijn, is opt-in ook nog mogelijk maar dat zal veel kritiek vanuit de advertentieindrustrie krijgen.

Tenslotte zijn initiatieven als het bel-me-niet-register ook opt-out. Belangrijk is dat de toestemming zowel bij opt-out als bij opt-in niet meer specifiek is: de gebruiker geeft dan eenmaal zijn keuze in het algemeen aan. Hierdoor zal naast zo'n regeling als youronlinechoices.eu ook het begrip toestemming opnieuw gedefinieerd moeten worden of er zou een uitzondering gemaakt moeten worden waarmee gebruikers wel 'globale toestemming' in hun browser moeten kunnen geven. Er was in ieder geval nog heel wat meer mogelijk dan de huidige richtlijn, want zoals we al eerder gezien hebben is de huidige implementatie op websites verre van gebruikersvriendelijk terwijl dit wel één van de eisen was uit overweging 66 2009/136/EG.

Hoofdstuk 6

De cookiewall

6.1 Werking cookiewall op websites

Hoewel het aantal websites met een cookiewall aan het dalen is (steeds meer websites kiezen voor de ook erg irritante implied consent, oftewel enkel een mededeling) zijn er nog een aantal grote websites met een cookiewall. Hieronder vallen onder andere nos.nl, telegraaf.nl en ns.nl. We zullen deze drie cookiewalls hier kort bekijken en hun manier van werken beschrijven, zowel aan de functionele kant (de kant van de gebruiker), als aan de technische kant (wat er allemaal wordt opgeslagen en heen en weer gestuurd).

Nos.nl

De cookiewall van de NOS is dezelfde als die op alle andere sites van de publieke omroep. Er wordt een korte beschrijving gegeven over waarom ze toestemming voor het plaatsen van cookies moeten vragen. Onderaan het venster staan nog een aantal links waarmee je meer te weten kunt komen over cookies (de NOS legt namelijk in de pop-up niet uit wat cookies zijn). Zodra je op 'Ja ik accepteer cookies' klikt is de website te bezoeken.

Zodra je akkoord gaat met het plaatsen van cookies worden er ook meteen heel wat cookies geplaatst, van onder andere doubleclick. De NOS slaat verder onder het domein *cookies.publiekeomroep.nl* een cookie op met als key 'npo_cookie_consent' en als waarde een lange string die vertelt dat je akkoord gegaan bent met het plaatsen van cookies. In het geval van *uitzendinggemist.nl* is deze string:

```
a%3A1%3A%7Bs%3A5%3A%22sites%22%3Ba%3A1%3A%7Bi%3A0
%3Bs%3A23%3A%22www.uitzendinggemist.nl%22%3B%7D%7D
```

Deze string lijkt weinig identificerende elementen te bevatten. Ook is deze string tussen meerdere browsersessies gelijk: als we alle cookies wissen en nogmaals naar deze site gaan krijgen we dezelfde cookie.

Ook zonder akkoord te gaan bij de cookiewall (en dus enkel de website van de NOS te bezoeken) worden er al enkele cookies geplaatst, maar dit is enkel een sessionid waarmee de NOS jou kan identificeren binnen hun website en wat lege cookies (cookies met enkel

een naam en value 0). Dit wordt gezien als een functionele cookie en is dus toegestaan binnen de wet.

Als je je browser alle cookies laat blokkeren is de website van de NOS niet te bezoeken: de NOS kan dan namelijk niet zien of onthouden dat jij expliciet aangegeven hebt dat je cookies accepteert. Zoals we eerder gezien hebben zijn verschillende HTTP-requests niet van elkaar te onderscheiden. Dus voor de mensen die alle cookies blokkeren (waarmee veel profilers dus geen effect meer hebben op ze) kunnen door de cookiewall ineens veel websites niet meer bezoeken. Gelukkig is de publieke omroep één van de weinige partijen die ook een cookievrije website aanbiedt, voor de NOS is dat op `http://cookievrij.nos.nl`. Dit is een uitgeklede variant van de normale website, maar deze website maakt geen gebruik van cookies en bevat dus ook geen cookiewall. Echter wordt er op de cookievrije website nog wel gebruik gemaakt van functionele cookies, maar deze website blijft tenminste werken voor gebruikers die alle cookies weigeren.

Een voordeel van de publieke omroep is dat ze gebruik maken van een gezamenlijke cookiewall: als je op één van de websites akkoord bent gegaan met het plaatsen van cookies kun je vervolgens alle andere websites van de publieke omroep bezoeken [26]. Dit werkt ook als je third-party cookies blokkeert. De NPO maakt namelijk net als Google en Youtube gebruik van een HTTP-redirect: bij een bezoek van één van de websites van de NPO stuurt deze site je namelijk door naar *cookies.publiekeomroep.nl* die vervolgens controleert of je al akoord gegaan bent met het plaatsen van cookies (want alleen zij kunnen de cookies onder hun domein uitlezen). Als je nog niet akkoord gegaan bent krijg je hier een cookiewall voorgeschoteld. Als je al akkoord gegaan bent wordt je weer terug naar de website waar je vandaan kwam gestuurd. Deze website werd namelijk via een HTTP-GET naar cookies.publiekeomroep.nl meegestuurd dus ze kunnen je daar naartoe terugsturen. Bij dit terugsturen vraag je via een HTTP-GET weer de originele pagina op, maar nu met één extra parameter, namelijk *?cookie_consent=1*. Aan deze parameter kan de originele website dan zien dat je cookies accepteert. Vervolgens plaatst die website een cookie onder zijn eigen domein met de naam *site_cookie_consent* en als waarde 'yes'. Door deze cookie hoef je bij een volgend bezoek aan die site niet meer doorgestuurd te worden naar cookies.publiekeomroep.nl, omdat deze site aan die cookie al kan zien dat je akkoord gegaan bent met het plaatsen van cookies. Door deze parameter zelf 'handmatig' mee te sturen is de cookiewall van de publieke omroep dus te omzeilen: als we al onze cookies wissen en vervolgens naar `http://www.nos.nl/?cookie_consent=1` surfen krijgen we inderdaad geen cookiewall te zien, terwijl onze browser nergens een cookie heeft opgeslagen waarin staat dat we akkoord gaan met het plaatsen van cookies.

Telegraaf.nl

Ook de Telegraaf Media Group maakt gebruik van een cookiewall. Alle dochters die hieronder vallen hebben een cookiewall. Net als bij de publieke omroep maakt de Telegraaf Media Group gebruik van HTTP-redirects: als je bijvoorbeeld naar telegraaf.nl gaat, word je doorgestuurd naar tmgonlinemedia.nl waar je een cookiewall voorgeschoteld krijgt. Als je hier akkoord gaat stuurt tmgonlinemedia.nl je weer terug naar telegraaf.nl. Net als bij de publieke omroep stuurt hij een parameter mee die aangeeft dat

je cookies accepteert.

Een groot verschil met de publieke omroep is echter dat de Telegraaf Media Group je wel een keuze biedt: als je de cookiewall voorgeschoteld krijgt kun je op de knop 'geavanceerde instellingen' klikken waar je kunt kiezen wat voor soort cookies er geplaatst mogen worden. Hier is te kiezen tussen 'Functioneel', 'Beperkt' en 'Standaard'. De Telegraaf geeft hierbij een vergelijkingstabel. Uit deze tabel is op te maken dat het verschil tussen beperkt en standaard vooral is dat bij beperkt er niets met social media gedaan wordt. Bij Functioneel zal de Telegraaf daarnaast ook geen 'Advertenties tonen op basis van surfgedrag'. Dat er geen gepersonaliseerde advertenties getoond worden geeft echter geen garantie dat gebruikers ook daadwerkelijk niet gevolgd worden. We zullen daarom kort een vergelijking doen tussen deze drie instellingen en kijken wat het verschil in cookies is hier.

Het verschil tussen 'Beperkt' en 'Functioneel' lijkt niet zo groot te zijn. In beide gevallen zijn er twee bedrijven die identificerende third-party cookies plaatsen, namelijk scorecardresearch.com en ads.p161.net. Het enige verschil is dat bij de instelling 'Beperkt' ook scanscout.com een cookie plaatst. Dit blijkt een profiler te zijn [35].

Het verschil tussen 'Beperkt' en 'Standaard' is echter enorm. Bij standaard worden er namelijk third-party cookies geplaatst van meer dan tien verschillende bedrijven, waaronder ook het grote doubleclick. De cookieinstelling bij de Telegraaf op beperkt zetten heeft dus wel degelijk effect.

Een ander groot voordeel tegenover de publieke omroep is dat de website van de Telegraaf ook te bezoeken is voor iemand die alle cookies blokkeert: de cookiewall wordt dan namelijk niet getoond en daarnaast worden er ook geen cookies geplaatst (want dit is natuurlijk onmogelijk). Je wordt in dit geval nog wel geredirect naar tmgonlinemedia.nl, maar als daar geen cookies geplaatst kunnen worden kom je weer terug op telegraaf.nl waar je dan zonder cookiewall opkomt.

NS.nl

De NS heeft ook een cookiewall. Deze is naast ns.nl ook te vinden op een aantal andere sites, zoals ov-fiets.nl en spoordeelwinkel.nl. Als je bij ns.nl akkoord gaat met het plaatsen van cookies ga je dat bij de andere sites ook. De NS plaatst namelijk een cookie met naam 'ns-cookie-toestemming' waarin je toestemming wordt opgeslagen. NS.nl werkt echter met third-party cookies: als je third-party cookies blokkeert kun je de website van de NS nog wel bezoeken, maar dan zul je als je later naar een gerelateerde website als ov-fiets.nl gaat op iedere gerelateerde website apart aan moeten geven dat je akkoord gaat met het plaatsen van cookies.

De NS biedt in de cookiewall ook twee instellingen voor het plaatsen van cookies. Naast een standaardinstelling is er ook een minimale instelling. Bij de minimale instelling worden er geen 'Cookies voor het verbeteren van deze site' geplaatst, maar nog wel 'Cookies voor het vlot laten verlopen van uw sitebezoek'. In de praktijk komt dit verschil neer op dat er bij de minimale instelling geen statistiekencookies van 'sitestat.com' geplaatst worden terwijl dit bij de standaardinstelling wel het geval is. Ook plaatst de NS dan geen cookies van Google Analytics. Verder maakt de NS verder geen gebruik van

advertenties en profilers. Er ligt inmiddels een wetsvoorstel om statistiekencookies net als functionele cookies ook uit te zonderen van de toestemmingseis [17]. Als dit voorstel erdoor komt, is de cookiewall op de website van de NS niet meer nodig.

Ook de website van de NS is te bezoeken als we alle cookies blokkeren. De NS test dit door eerst een cookie 'ns_cookietest' te plaatsen. Als deze cookie bij een volgende HTTP-GET weer gevonden wordt, 'weet' de NS dat we cookies kunnen accepteren en zullen ze de cookiewall voorschotelen.

6.2 Werking plugin 'CookiesOK'

Zoals we in de inleiding al vermeldden bestaat er al een plugin genaamd 'CookiesOK' die probeert de cookieschermen weg te halen door automatisch akkoord te gaan met het opslaan van cookies. Het nadeel is dus wel dat hiermee allerlei cookies meekomen. Ook kiest de plugin op bijvoorbeeld telegraaf.nl voor de meest ruime oplossing: alle cookies worden hier geaccepteerd en er wordt geen gebruik gemaakt van bijvoorbeeld de beperkte instelling van de Telegraaf. Er is namelijk verder niets in te stellen aan de plugin. Dit is aan de ene kant een voordeel, want dit maakt de plugin gemakkelijk voor gebruiker, maar in dit geval kan het dus ook een nadeel zijn.

Naast het autmatisch akkoord gaan met de cookiewall stuurt de plugin ook een extra HTTP-header mee met ieder HTTP-verzoek. Deze header heeft de waarde *X-CookiesOK: I explicitly accept all cookies.* Een websitebeheerder zou dit verzoek kunnen honoreren en dus geen cookiewall voorschotelen aan de gebruiker. Helaas is deze header geen standaard (zoals de DoNotTrack-header wel moet gaan worden) en wordt hij dus door bijna alle websites genegeerd. Ik heb in ieder geval een tijdje gesurft met deze header aan, maar zonder CookiesOK, maar ik ben geen enkele site tegengekomen die door deze header geen cookiewall voorschotelt.

In de praktijk blijkt de plugin aardig goed te werken: de grote en bekende websites zijn nu zonder cookiewall te bezoeken. Er 'flitst' de eerste keer dat je zo'n website bezoekt nog wel even snel een cookiewall langs, maar dit is niet hinderlijk. Op ns.nl flitst deze wall echter bij iedere klik op een link langs. Hier is dus nog wat verbetering mogelijk. Verder probeert de plugin ook zoveel mogelijk de 'implied consent'-meldingen weg te halen, want ook die zijn hinderlijk.

Technische analyse 'CookiesOK'

Voor deze analyse bekijken we de Firefox-versie van CookiesOK. We bekijken revisie 57, te downloaden op `https://addons.mozilla.org/firefox/downloads/file/193198/cookiesok-Release_candidate.rev57-fx.xpi`. Deze plugin is gemaakt in javascript met de addon-SDK van Mozilla, te vinden op `https://addons.mozilla.org/en-US/developers/docs/sdk/latest/dev-guide/tutorials/index.html`. Deze SDK geeft al heel wat kant-en-klare functies waarmee het gedrag van de browser is aan te passen.

Als we het xpi-bestand downloaden en uitpakken (ondanks de extensie .xpi is het gewoon een zip-bestand), krijgen we heel wat bestanden te zien. Het bestand *main.js*

bevat code en voert vervolgens de andere bestanden uit. Als we deze plugin willen combineren met andere plugins dan is dit mogelijk door het bestand main.js aan te passen. Dit bestand 'knoopt' namelijk alles aan elkaar van deze plugin. De rest van de bestanden laten we ongewijzigd.

Het bestand waar het eigenlijke werk gebeurt is *cookiesok.js*. Onderaan in dit bestand is de functie *init()* te vinden, die bij iedere website aangeroepen wordt. Eerst wordt er gekeken of de website een css-klasse 'CookiesOK' heeft toegevoegd aan de cookiewall. Op deze manier kunnen websites ervoor zorgen dat hun cookiewall automatisch verdwijnt bij het gebruik van deze plugin. Mocht dit het geval zijn, dan wordt automatisch op dit object geklikt (en verdwijnt de cookiewall voor de gebruiker). Helaas ben ik nog geen enkele website tegengekomen die deze css-klasse heeft toegevoegd. Als dit niet het geval is zal CookieOK in zijn eigen offline database die we in de volgende sectie gaan bekijken of daar de website staat. Als dit het geval is voert hij de actie uit de database uit op het html-object dat bij deze actie staat vermeld. Mocht de website ook hier niet in voorkomen, dan gaat de plugin online kijken op de website van de maker of daar relevante gegevens staan. Deze stap gebeurt natuurlijk enkel als de gebruiker in het optiescherm toestemming heeft gegeven aan de plugin om online te gaan kijken. Mocht dit niet mogelijk zijn dan wordt de functie *tryDefaultPlugins()* aangeroepen. Deze functie probeert een aantal 'standaard cookiewalls' te omzeilen met generieke namen. Als ook dit niet werkt kan de cookiewall of cookie-toolbar niet omzeild worden met deze plugin. We zullen in de volgende subsecties zowel de offline als de online database in detail bespreken.

Offline database

De offline database is te vinden in het bestand *database.js*. Dit is een enorm javascript-bestand en bevat slechts één string (een json-object) genaamd *var cookiesOKDatabase*. In deze variabele staan allemaal key-value-paren waarop vanuit een javascript-functie gematcht kan worden. Dit zijn een aantal voorbeelden van deze key-value-paren:

```
"cookies.eredivisielive.nl":{"action":"click","target":"#
    edl_cookie_popup .css-button-green"}
"ov-chipkaart.nl":{"action":"click","target":".button.big.roze.cookie.
    optin"}
"telegraaf.nl":{"action":"csshide","target":"#cookiepolicy"}
```

De key is in dit geval de domeinnaam oftewel de website waarop je op dat moment bent. Als value worden er steeds twee dingen meegegeven: een *action* en een *target*. Action kan hier een klik zijn (er moet op een accepteren-knop geklikt worden, vaak het geval bij cookiewalls) of een hide of remove (er moet bijvoorbeeld een implied-consent-melding verborgen worden). Het target is vervolgens het html-object (het deel van de website, bijvoorbeeld de toolbar of de accepteren-knop) waarop de actie uitgevoerd moet worden.

Online database

De online database werkt op dezelfde manier als de offline database, behalve dat de key-value-paren nu van de server van CookiesOK opgehaald worden. De online database wordt enkel geraadpleegd als deze optie is aangezet bij de instellingen van de plugin en als de offline database geen resultaat oplevert.

Bij de online database wordt er een HTTP-GET naar de volgende url gedaan: `ht tp://cookiesok.com/dcheck.php?domain=`. Achter het '='-teken komt vervolgens de gevraagde website te staan. In het geval van de website ns.nl zie de url er zo uit: `http://cookiesok.com/dcheck.php?domain=ns.nl`. Vervolgens krijgen we het volgende key-value-paar terug:

```
{"action":"remove","target":"#dialog-cookie"}
```

Dit is eenzelfde paar als bij de offline database, waarmee de online methode weinig verschilt van de offline methode, behalve dat de online database vele malen groter is.

Enkele voorbeelden

NOS.nl

Zoals we gezien hebben linkt nos.nl bij de cookiewall door naar cookies.publiekeomroep.nl. Daar bestaat het belangrijkste gedeelte van de cookiewall uit het volgende stukje broncode:

```
<div id="lightbox2">
<div class="holder">
 <h1 class="logo">Cookies op NOS</h1>
 <div class="frame">
  <div class="text"><p>Bericht over cookiegebruik (ingekort)</p></div>
  <div class="links-box">
  <a href="/accept/" class="accept-link">
  <span>Ja, ik accepteer de cookies</span></a>
```

In de CookiesOK-database vinden we de volgende entry:

```
{"action":"click","target":"#lightbox2 .accept-link"}
```

Het gezochte target is hier dan dus `<div id="lightbox2">`. Omdat onze action 'click' is, klikken we vervolgens op de /accept/-link, die bij de `<a>`-link staat.

NS.nl

De cookiewall van de NS wordt gegenereerd door het volgende stukje broncode van ns.nl:

```
<!-- overlay dialog -->
<div id="dialog-cookie" style="display: none;">
 <div class="box default">
 <h2>Cookies</h2>
```

```
<div class="dialog-body">
 <p>Bericht over cookiegebruik (ingekort)</p>
</div>
<p class="actions">
 <a ns:sitestat="$.link.cookies.accept" href="" class="button allow" ><
     span>Cookies toestaan</span></a>
 <a ns:sitestat="$.link.cookies.settings" href="#extensive" data-
     cookietab="extensive" class="forward next-content"><span>Uw cookie-
     instellingen</span></a></p>
</div>
```

Het eerste stukje commentaar verklapt al dat dit enkel een overlay is en dus geen 'echte' cookiewall. Als deze layer weggehaald wordt, is de website gewoon te gebruiken. CookiesOK haalt met een remove-actie dit stukje code dan ook weg van de website. Dit gebeurt met het volgende key-value-paar.

```
{"action":"remove","target":"#dialog-cookie"}
```

Door de actie "remove" wordt er enkel een element van de webpagina weggehaald. De klasse die hier weggehaald wordt is "dialog-cookie", wat overheen komt met `<div id="dialog-cookie">`. Doordat dit enkel een remove-actie is, zou dit ook met een Adblock Plus-regel kunnen. Adblock haalt namelijk ook enkel elementen weg van een webpagina. Door de volgende twee regels aan het Adblock-filter toe te voegen verdwijnt de cookiewall inderdaad van ns.nl:

```
ns.nl##.box.default
ns.nl##.trans-layer
```

Veiligheidsrisico's

Met de click-actie kan CookiesOK op willekeurige elementen op een webpagina klikken. In de database staat netjes gedefinieerd waar de cookie-elementen staan, waardoor de plugin daar op klikt. Als iemand echter toegang kan krijgen tot deze database, dan zou hij ook op andere elementen van een webpagina kunnen klikken. We zullen hier een klein voorbeeld geven van deze actie. We kijken hiervoor naar de website van Eneco, www.eneco.nl. Deze website heeft enkel een implied-consent-melding die met een enkele klik op accepteren weggehaald kan worden. De broncode ziet er zo uit:

```
<div class="cookiePopup">
 <a href="#" class="Close"></a>
 <h2>Eneco cookies</h2>
 <p>Bericht over cookiegebruik (ingekort)</p>
 <a id="ctl20_AllowButton" class="MainButton" href="javascript:
     __doPostBack(&#39;ctl20$AllowButton&#39;,&#39;&#39;)"><strong>
     Toestemming voor cookies</strong></a><br />
</div>
```

Vanuit de database wordt deze balk weggehaald met de volgende actie:

```
{"thuis.eneco.nl":{"action":"click","target":".cookiePopup #
    ctl20_AllowButton"}}
```

Deze website bevat echter ook een andere knop waarop geklikt kan worden:

```
<div class="Inside">
 <knip>
 <a id="plhcontent_0_linkButtonUsp" class="Button" href="javascript:
     __doPostBack(&#39;plhcontent_0$linkButtonUsp&#39;,&#39;&#39;)">
 <strong>Bekijk Toon nu</strong></a>
</div>
```

Als we de entry in de database aanpassen naar het volgende, wordt er inderdaad automatisch op deze knop geklikt:

```
{"thuis.eneco.nl":{"action":"click","target":".Inside #
    plhcontent_0_linkButtonUsp"}}
```

Dit voorbeeld is nog een vrij onschuldige actie, maar hier hoeft het niet bij te blijven. De vraag is echter hoe groot de kans is dat iemand jouw offline database.js kan modificeren. Als hij hier ongevraagd bij kan komen, kan hij waarschijnlijk ook wel ongevraagd een andere kwaadaardige plugin installeren. De offline database wordt meegeleverd bij de installatie van de plugin. Deze plugin wordt enkel via de Mozilla add-on-pagina aangeboden. Als iemand hier de plugin kan modificeren kan hij dat ook met andere plugins en zijn er veel gevaarlijkere dingen mogelijk. De offline database vormt daardoor geen verhoogd veiligheidsrisico tegenover het überhaupt installeren van een plugin.

De online database is misschien een ander verhaal. Hierbij wordt er een request naar de CookiesOK-server gestuurd. Als iemand toegang krijgt tot deze server zal hij dus alle CookiesOK-gebruikers die de online-optie hebben ingeschakeld op willekeurige elementen op een webpagina kunnen laten klikken. De veiligheid van de online optie ligt hiermee dus in handen van de veiligheid van de server.

Een aanvaller kan echter ook als man-in-the-middel tussen de gebruiker en de website in gaan zitten. In dit geval kan hij al het verkeer dat tussen de gebruiker en de website plaatsvindt modificeren. Hierbij zal hij dus ook de database-entries kunnen veranderen. Echter valt ook dit risico mee: een aanvaller kan dan namelijk ook de gehele website veranderen, iets dat een veel groter risico is. Website die van een beveiligde SSL-verbinding gebruik maken zijn ook niet kwetsbaar voor deze aanval: bij deze websites is een man-in-the-middle niet mogelijk, want in dit geval maakt CookiesOK ook gebruik van een beveiligde verbinding naar de CookiesOK-server. Een voorbeeld van deze beveiligde verbinding is te vinden in figuur A.3.

Omdat er ook bij de online database enkel risico's zijn op een moment dat een aanvaller al andere gevaarlijkere dingen kan doen, valt het extra veiligheidsrisico van deze plugin wel mee.

Hoofdstuk 7

Op weg naar een oplossing

7.1 Een browserplugin

Als één van de onderzoeksvragen hadden we de volgende vraag gedefinieerd:
Zijn er naast plugins nog andere mogelijkheden om dit probleem op te lossen?

'Dit probleem' verwijst hier naar het probleem uit de hoofdvraag:
Hoe kun je op een effectieve en gebruiksvriendelijke manier de cookiewall omzeilen en tegelijkertijd niet gevolgd worden door advertentiebedrijven?

Voor het omzeilen van de cookiewall is slechts één oplossing beschikbaar, namelijk de plugin CookiesOK, zoals we gezien hebben. Voor het andere probleem, het gevolgd worden door advertentiebedrijven en profilers, zijn meerdere maatregelen beschikbaar die allemaal deels werken. Sommige maatregelen hadden duidelijke nadelen op de gebruikerservaring van het web en andere maatregelen waren niet effectief. Als we de effectieve maatregelen uit hoofdstuk 4 opsommen komen we op de volgende eisen uit:

- De oplossing moet third-party cookies blokkeren.
- De oplossing moet trackingcookies en scripts blokkeren (daar zijn verschillende plugins voor beschikbaar).

Omdat deze maatregelen of met een browserinstelling of via een plugin gebeuren, lijkt het de handigste oplossing om een browserplugin te schrijven die deze oplossingen combineert en daarnaast CookiesOK integreert.

We gaan in deze scriptie een browserplugin ontwikkelen als oplossing voor deze onderzoeksvraag. We beperken ons tot de browser Mozilla Firefox. In deze browser zijn browserinstellingen ook via een plugin te regelen [22].

7.2 Adblock Plus

We hebben in hoofdstuk 4 gezien dat Ghostery in de meeste testen als beste plugin uit de bus kwam. Adblock Plus was een goede tweede. Voor de individuele gebruiker zal

Ghostery momenteel de beste oplossing zijn als hij maatregelen wil nemen tegen het volgen door profilers. Als we echter standaard third-party cookies gaan blokkeren, telt de effectiviteit van een plugin vooral op het gebied van first-party cookies. Ook hier scoort Ghostery zeer goed. Ghostery heeft echter voor de ontwikkelaar als nadeel dat het een commercieel product is [13]. Daardoor is er zeer weinig documentatie te vinden over de precieze werking van Ghostery. Ook het eventueel aanpassen van de blacklist of het zelfs raadplegen van de blacklist is hierdoor lastig. Aan de gebruikerskant zijn er natuurlijk extra elementen en uitzonderingen toe te voegen, maar de blacklist zelf is niet volledig vrij te raadplegen.

Adblock Plus is daarentegen ontwikkeld onder de GPL 3.0 licentie en bevat uitgebreide documentatie over hoe de broncode in elkaar zit [31]. Daarnaast is het toevoegen van filters aan Adblock Plus zeer eenvoudig. Ook zijn de filters zelf vrij te raadplegen en aan te passen. We zullen daarom de plugin Adblock Plus gaan aanpassen en hier onze extra maatregelen en eisen in gaan verwerken. Daarnaast zullen we CookiesOK gaan combineren met Adblock Plus zodat we de cookiewalls kunnen omzeilen.

7.3 Gebruikersvriendelijkheid

We willen de cookiewall op een gebruikersvriendelijke manier omzeilen en niet gevolgd worden. Onze plugin moet dus zo gebruikersvriendelijk mogelijk zijn. Adblock Plus is dat in zijn huidige vorm in ieder geval niet: na de installatie moet de gebruiker eerst nog zelf een filter toevoegen voordat de plugin pas goed zijn werk doet. Verder bevat het instellingenmenu instellingen waarvan de gemiddelde gebruiker geen weet heeft wat ze doen.

Omdat de gevorderde gebruiker deze instellingen juist wél wil kunnen raadplegen kunnen we ze ook niet weglaten. Daarom gaan we het huidige instellingenmenu van Adblock Plus onder een aparte knop 'Geavanceerde instellingen' plaatsen. Daar kunnen gebruikers dan eventueel ook handmatig extra filters toevoegen mochten ze er behoefde aan hebben.

Het standaard instellingenscherm (waar je terecht komt zodra je in Firefox bij de plugin op voorkeuren klikt) laten we enkel de volgende instellingen bevatten:

Zorg dat bedrijven mij niet kunnen volgen
: Deze instelling zet het trackingfilter aan en blokkeert third-party cookies, staat standaard aan.

Omzeil de cookiewall
: Deze instelling activeert CookiesOK, staat standaard aan.

Gebruik online database voor cookiewall
: Deze instelling staat CookiesOK toe om online te gaan zoeken, staat standaard uit. Hier moeten we ook duidelijk het privacygevaar van online gaan vermelden.

Blokkeer advertenties
: Deze instelling blokkeert advertenties, staat standaard aan.

7.4 Implementatie

Doordat Adblock Plus en CookiesOK beide bootstrapaddons zijn, waren ze vrij eenvoudig met elkaar te integreren. Een bootstrapaddon is een plugin die zonder dat de browser opnieuw opgestart hoeft te worden is te installeren en te activeren. Hij wordt in de browsercode 'gebootstrapt' [23]. Dit bootstrappen gebeurt in het bestand *bootstrap.js*, een bestand dat beide plugins hebben. Door dit deze twee bestanden samen te voegen (en de ontstane conflicten op te lossen), worden beide addons gecombineerd tot een enkele, werkende addon. De code van beide addons bevinden zich dan in aparte mappen, waardoor ze verder geen last hebben van elkaar: ze werken conflictloos langs elkaar heen.

Omdat Adblock Plus een uitgebreidere en grotere plugin is dan CookiesOK, kiezen we ervoor om de code van CookiesOK op deze manier in Adblock Plus te integreren. De meeste instellingen die we aan onze addon aan willen passen, zitten ook aan de Adblock Plus-kant. CookiesOK heeft namelijk slechts twee instellingen nodig: of hij wel of niet de online database mag gebruiken en of hij wel of niet de cookiewalls moet omzeilen. Deze twee instellingen gaan we opslaan in de *about:config*-database van Firefox. Dit kan met de Mozilla Preferences Service [24]. Op deze manier kunnen we deze instellingen vanuit het Adblock Plus-deel van de plugin instellen, waarna de instellingen na een paar kleine aanpassingen ook in het CookiesOK-deel effect hebben.

Nadat deze stappen voltooid waren, werkt de basisfunctionaliteit van de plugin al. Adblock Plus kan door filters toe te voegen de juiste tracking blokkeren en CookiesOK is te activeren via *about:config*. De enige belangrijke taak is nu nog dit geheel zo gebruikersvriendelijk mogelijk te maken. Om dit voor elkaar te krijgen maken we gebruik van een nieuwe first-run pagina die in de laatste ontwikkelversie van Adblock Plus te vinden is [32]. Deze nieuwe first-run pagina zorgt er al voor dat nieuwe gebruikers eenvoudig de extra anti-tracking filters toe kunnen voegen aan Adblock Plus. Doordat er slechts enkele grote aan- en uitzetknoppen op deze pagina staan is hij erg simpel in gebruik.

De first-run pagina bestaat uit een html-pagina met een javascriptdeel erachter die met de plugin communiceert. Door zowel de html-pagina als dit javascriptdeel aan te passen kunnen we op deze first-run pagina een extra knop toevoegen om CookiesOK aan en uit te zetten. Op dezelfde manier kunnen we CookiesOK wel of niet toestaan om online te gaan voor de meest recente database. Verder passen we het anti-tracking filter aan: voortaan worden ook standaard third-party cookies geblokkeerd als de gebruiker dit filter activeert.

Naast CookiesOK voegen we een knop toe om het standaard advertentiefilter van Adblock Plus aan en uit te zetten, dit was namelijk niet mogelijk met de originele first-run pagina. Door ook deze instelling aan de first-run pagina toe te voegen hoeft de gemiddelde gebruiker nooit meer het officiële en uitgebreide instellingenscherm van Adblock Plus te raadplegen. Hierdoor kunnen we van de first-run pagina het officiële optiescherm maken: door in Firefox bij deze plugin op 'voorkeuren' te drukken kom je voortaan op deze first-run pagina. Het uitgebreide instellingenscherm van Adblock Plus maken we nog steeds benaderbaar met een knop 'geavanceerde filterinstellingen' in het

Firefox optiescherm.

Bij de originele first-run pagina waren alle filters nog uitgeschakeld. We veranderen dit en maken voor de gebruiker al vast een nieuwe standaardkeuze: standaard zetten we het advertentiefilter, malwarefilter, anti-trackingfilter al aan. Ook activeren we standaard CookiesOK. Een screenshot van de uiteindelijke plugin is te vinden in de appendix, in figuur A.5.

7.5 Evaluatie plugin en suggesties voor verbetering

Als we kijken hoe onze plugin in de praktijk werkt, is het eerste dat opvalt dat hij vrij simpel in gebruik is: je installeert de plugin en na de installatie krijg je een scherm voorgeschoteld waarin alle belangrijke filters en instellingen al meteen goed staan. Door grote pictogrammen is het voor de gebruiker eenvoudig te begrijpen wat ieder filter doet, waarmee hij filters desgewenst in en uit kan schakelen.

Als we kijken naar de prestatie van de plugin met betrekking tot het filteren van tracking is deze gelijk aan die van Adblock Plus: we gebruiken immers die filters. Daarnaast blokkeert de plugin standaard alle third-party cookies, waarmee enkel de prestaties van het blokkeren van first-party cookies van belang zijn. De enige cookies die hij op dit gebied toelaat zijn de cookies van Google Analytics. Hoewel die eenvoudig met een extra filter te blokkeren zijn, zit die instelling niet in onze gebouwde plugin, simpelweg omdat veel websites met Google Analytics dan niet meer werken. Hier is dan wel omheen te komen met dummy-scripts, zoals Ghostery en scriptblocker NoScript doen, maar dit implementeren is niet triviaal waardoor ik dit heb laten zitten.

Het omzeilen van de cookiewall gaat met CookiesOK. CookiesOK presteert hierin vrij goed, maar laat enkele cookiewalls toch verschijnen. Door de optie 'online database' aan te zetten presteert hij nog beter. Maar dit heeft weer privacygevolgen waardoor deze optie standaard uit staat.

Er zijn echter nog wel enkele verbeteringen mogelijk: Google Analytics blokkeren is hier een voorbeeld van. Ook het blokkeren of automatisch wissen van flashcookies wordt nu niet gedaan. Ondanks dat flashcookies steeds minder gebruikt worden zou het blokkeren of automatisch wissen een zinvolle verbetering zijn. Daarnaast zou een extra knop in de browser een mooie toevoeging zijn om de plugin snel te raadplegen.

7.6 Toetsing plugin juridisch kader

Vanuit de Europese richtlijn die we in hoofdstuk 5 beschreven hebben weten we dat websitebeheerders *specifieke* toestemming moeten vragen voor het plaatsen van niet-functionele cookies. Door het gebruiken van onze plugin geven we echter nog geen toestemming: we geven met deze plugin enkel aan dat we geen cookiewalls meer willen zien, we gaan er niet akkoord mee. Hoewel websitebeheerders hier zelf natuurlijk niets tegen kunnen doen, zijn wij door het 'omzeilen' van de cookiewall in strijd met de richtlijn bezig: we laten ons namelijk niet informeren en geven geen toestemming.

Aan de andere kant is er nog iets merkwaardigs aan de hand: zodra we het anti-tracking filter aanzetten (dit staat standaard aan bij de installatie), worden er, als we er vanuit gaan dat het filter 'perfect werkt', enkel nog functionele cookies geplaatst. Met andere woorden: alle cookies waarvoor we eigenlijk specifieke toestemming moeten geven worden door het gebruik van het filter nu niet eens geplaatst. Doordat er dus enkel functionele cookies geplaatst worden hoeven we hier ook geen toestemming voor te geven. Onze plugin is dus, mits het anti-tracking filter perfect werkt (dat is niet te garanderen omdat een blacklist in de praktijk onmogelijk compleet kan zijn), niet in strijd met de richtlijn.

De situatie wordt echter anders als de gebruiker wat aan de standaardinstellingen van de plugin gaat veranderen: als hij bijvoorbeeld alle filters uitschakelt, waarmee de functionaliteit van de plugin gelijk is aan die van CookiesOK zal hij wel gevolgd worden. Echter geeft hij nu geen specifieke toestemming waarmee hij dus in strijd met de richtlijn bezig is. Andersom gaat het wel goed: als de gebruiker niet de cookiewalls automatisch wil omzeilen, maar wel alle anti-tracking filters aanzet geeft hij wel specifieke toestemming voor iedere website. Hij zal echter doordat de filters wel aan staan niet gevolgd worden.

Hoofdstuk 8

Conclusies

8.1 Volgtechnieken

Er zijn verschillende technieken mogelijk om gegevens op de computer van de internetgebruiker op te slaan, waarvan de cookie de bekendste is. Naast cookies kunnen websites ook gegevens opslaan in flashcookies en HTML5-storage. Flashcookies worden aangemaakt door de flashplayer van Adobe en kunnen daardoor in meerdere browsers geraadpleegd worden, de meeste computers hebben namelijk maar een enkele flashplayer geïnstalleerd die in alle browsers actief is. HTML5-storage is vrij recent. In deze opslag kunnen websites ook gegevens opslaan, maar in veel browser moet hier toestemming voor gegeven worden. Ook is de HTML5-specificatie nog niet af waardoor dit allemaal nog kan wijzigen. Momenteel wordt dit door profilers nog maar weinig gebruikt.

We hebben gezien dat cookies de voornaamste techniek zijn om gebruikers mee te volgen. Ook weten we dat cookies noodzakelijk zijn voor een goede werking van het web. Met name third-party cookies maken het voor profilers gemakkelijk om gebruikers over verschillende websites te volgen, doordat deze third-party cookies tijdens het surfen naar een pagina naar de profiler worden verzonden. Via de HTTP-referer weet deze dan naar welke website de gebruiker heeft gesurft, waardoor hij de gebruiker over verschillende websites kan volgen. Naast third-party cookies kunnen gebruikers ook via first-party cookies gevolgd worden: dit gaat dan via HTTP-redirects of javascript.

Momenteel worden in de praktijk third-party cookies het meest gebruikt om gebruikers te volgen. Gezien het feit dat browsermakers erover nadenken om deze cookies als standaardinstelling te blokkeren zullen profilers naar andere volgtechnieken uit gaan wijken. We hebben met een voorbeeld aangetoond dat gebruikers ook gemakkelijk via first-party cookies gevolgd kunnen worden door middel van HTTP-redirects.

Een andere volgtechniek is browser fingerprinting. Deze techniek is gebaseerd op het feit dat iedere webbrowser uniek is en dus een unieke 'vingerafdruk' heeft: iedereen heeft wel een andere versie, andere plugins of andere lettertypen. Als profilers deze informatie zouden gebruiken kunnen ze gebruikers volgen op het internet zonder dat ze lokaal bij de gebruiker informatie op hoeven te slaan. Dit wordt momenteel gelukkig in de praktijk nog niet gedaan.

8.2 Maatregelen

De voornaamste maatregel tegen het volgen van gebruikers is het blokkeren van de juiste cookies. Het blokkeren van alle third-party cookies lost momenteel de meeste problemen op: de meeste profilers maken nog steeds enkel gebruik van third-party cookies om gebruikers te volgen. First-party cookies zijn vooral statistiekencookies. Om ook de juiste resterende first-party cookies te blokkeren zijn verschillende plugins of ook wel cookieblockers genoemd beschikbaar, waarbij Ghostery als meest effectieve plugin uit de bus kwam. Adblock Plus kwam als een goede tweede plugin uit onze korte test. Adblock Plus is door het open source karakter en gemakkelijk uit te breiden filters daarom een goede keuze om onze oplossing op te gaan bouwen.

Naast het installeren van extra plugins zijn er nog twee opt-out mogelijkheden. Youronlinechoices.eu is een opt-out website waar je kunt aangeven dat je niet gevolgd wil worden. Deze website zal vervolgens de aangesloten profilers allen een script laten draaien waarmee ze een opt-out cookie kunnen zetten op jouw computer. Helaas werkt dit alleen als je third-party cookies inschakelt terwijl dat ook weer nadelen heeft. Ook werkt dit alleen maar bij de aangesloten bedrijven. Naast youronlinechoices.eu kun je je browser ook een extra Do-not-track-header laten meesturen. Hiermee geef je aan dat je niet gevolgd wil worden. Omdat dit enkel een verzoek is hoeven profilers dit niet te honoreren. Ook sturen sommige browsers als standaardinstelling deze header mee, waardoor het geen opt-out maar een opt-in systeem is geworden. Hierdoor zijn profilers minder geneigd zich aan zo'n verzoek te houden.

8.3 Juridisch Kader

We hebben gezien dat de Nederlandse wet van een Europese richtlijn uit 2009 afstamt. Uit deze richtlijn is op te maken dat voor het plaatsen van niet-functionele cookies specifieke toestemming vereist is. Naast dat websitebeheerders toestemming moeten vragen moeten ze hun gebruikers ook informeren over wat er met de cookies gedaan wordt: hoe ze verwerkt worden. Ook moeten ze gebruikes wijzen op hoe ze hun cookies kunnen wissen. Deze informatieverstrekking moet gebeuren vóór dat gebruikers toestemming hebben gegeven. Op dit moment mogen websitebeheerders dan ook geen niet-functionele cookies plaatsen. Hiermee is 'implied consent' verboden: deze term betekent vrij vertaald 'toestemming geven uit stilzwijgen', oftewel dat websitebeheerders er vanuit gaan dat je toestemming geeft als je hun website gebruikt. Ze plaatsen dan enkel een melding of balk bovenin het scherm van de gebruiker. Doordat de gebruiker hier vóór dat hij toestemming heeft gegeven en geïnformeerd is over het cookiegebruik al niet-functionele cookies heeft ontvangen is implied consent tegen de richtlijn.

De regels met betrekking tot informatieverstrekking komen voort uit het feit dat cookies persoonsgegevens kunnen zijn: als ze een uniek identificatienummer bevatten zijn ze herleidbaar tot een persoon, waarmee ze dus als persoonsgegevens behandeld moeten worden. Hierdoor moet er dus informatie verstrekt worden met betrekking tot de verwerking van deze gegevens.

De Nederlandse implementatie van de Europese richtlijn is terechtgekomen in artikel 11.7a van de Telecommunicatiewet. Deze implementatie zorgt ervoor dat websites in Nederland nu ook specifieke toestemming moeten vragen voor het plaatsen van niet-functionele cookies en implied consent verboden is. Doordat cookies persoonsgegevens zijn vallen deze onder de Wet bescherming persoonsgegevens, waarmee ook de eerder beschreven informatieverstrekking in Nederland vereist is. Het College bescherming persoonsgegevens (CPB) ziet toe op de handhaving van deze verwerking. De Autoriteit Consument en Markt (ACM) ziet toe op de handhaving van de Telecommunicatiewet en dus ook de cookiewet. Hier zit nog overlappend gebied: als artikel 11.7a wordt overtreden moet de ACM optreden, maar als het om persoonsgegevens gaat juist het CBP. In sommige gevallen kunnen beide partijen optreden omdat in het geval van cookies deze twee zaken nauw verwant zijn.

8.4 Cookiewall

We hebben verschillende cookiewalls bekeken. Allemaal hebben ze een vangpagina waar de gebruiker akkoord moet gaan met het plaatsen van cookies. Daarnaast hebben sommige cookiewalls nog een extra instelling, waarmee er minder of zelfs geen cookies geplaatst kunnen worden. Sommige websites zijn door de cookiewall niet meer te bezoeken als de gebruiker alle cookies blokkeert.

Een oplossing voor de cookiewall is de plugin CookiesOK. Deze plugin probeert automatisch akkoord te gaan met iedere cookiewall. Hij doet dat op basis van een lokale database met voor iedere website specifieke instructies. Naast de lokale database kan de plugin online de meest recente instructies opvragen, maar dit zorgt er wel voor dat de maker van de plugin kan zien naar welke websites je allemaal surft, omdat bij iedere webpagina contact met de website van de maker van CookiesOK wordt gezocht.

8.5 Oplossing plugin

In de inleiding hadden we de volgende onderzoeksvraag geformuleerd:

"Hoe kun je op een effectieve en gebruikersvriendelijke manier de cookiewall omzeilen en tegelijkertijd niet gevolgd worden door profilers?"

Als oplossing voor deze onderzoeksvraag hebben we een browserplugin gebouwd die de aspecten uit de vraag oplost. We hebben de plugin gemaakt op basis van de bestaande plugins Adblock Plus en CookiesOK. CookiesOK zorgt er bij onze combinatie voor dat de cookiewalls omzeild worden, terwijl het Adblock Plus-deel ervoor zorgt dat we niet gevolgd worden door profilers. Dit is gedaan door aan Adblock Plus extra filters toe te voegen die tracking blokkeren. Ook blokkeren we met onze plugin standaard third-party cookies.

De 'gebruikersvriendelijke manier' hebben we geïmplementeerd door het optiescherm van onze plugin zo simpel mogelijk te maken en de standaardinstelling al optimaal te la-

ten zijn: zo worden standaard alle tracking cookies geblokkeerd en de cookiewall omzeild. De gebruiker kan met een enkele klik deze instellingen aanpassen.

Uiteindelijk hebben we dus een oplossing voor het probleem gevonden waarmee de gebruiker én zo goed als geen cookiewalls meer ziet én zo goed als niet gevolgd wordt op het internet.

Hoofdstuk 9

Bibliografie

[1] Adobe. Flash player in Google Chrome
http://helpx.adobe.com/flash-player/kb/flash-player-google-chrome.html.

[2] Adobe. Flash control panel
http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager03.html.

[3] Julia Angwin. Microsoft zet Do Not Track standaard aan
http://blogs.wsj.com/digits/2012/05/31/microsofts-do-not-track-move-angers-advertising-industry/.

[4] Mika Ayenson, Dietrich James Wambach, Ashkan Soltani, Nathan Good, and Chris Jay Hoofnagle. Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning (July 29, 2011). Available at SSRN: http://ssrn.com/abstract=1898390 or http://dx.doi.org/10.2139/ssrn.1898390.

[5] A. Barth. Http state management mechanism. Technical Report 2070-1721, U.C. Berkeley, 2011. http://tools.ietf.org/html/rfc6265#section-3.

[6] Cookierecht. Achtergrond cookiewet
https://cookierecht.nl/diensten/juridisch-advies/achtergrond-cookiewet/.

[7] Andrew Couts. Privacy plug-in showdown: Do Not Track Plus vs. Ghostery
http://www.digitaltrends.com/web/do-not-track-plus-vs-ghostery/ Geraadpleegd op 10 mei 2013.

[8] L.F. Cranor. Can users control online behavioral advertising effectively? volume 10, pages 93–96, 2012.

[9] Louise Dancet. Kort onderzoekje over de irritatie van de cookiewet,
https://cookierecht.nl/juridisch-weblog/steeds-bredere-irritatie-over-de-cookiewet.

[10] Peter Eckersley. How unique is your web browser? In MikhailJ. Atallah and NicholasJ. Hopper, editors, *Privacy Enhancing Technologies*, volume 6205 of *Lecture Notes in Computer Science*, pages 1–18. Springer Berlin Heidelberg, 2010.

[11] Brendan Eich. C is for Cookie, nadelen van het blokkeren van third-party cookies `https://brendaneich.com/2013/05/c-is-for-cookie/` Geraadpleegd op 21 mei 2013.

[12] Wout Funnekotter. De tweede kamer wil een einde aan de cookiepopups, `http://tweakers.net/nieuws/87250/meerderheid-tweede-kamer-wil-einde-aan-cookie-popups.html`.

[13] Ghostery. EULA `https://addons.mozilla.org/en-US/firefox/addon/ghostery/license/`.

[14] Google. Analytics en het gebruik van cookies `https://developers.google.com/analytics/devguides/collection/gajs/cookie-usage`.

[15] Alan Henry. The Best Browser Extensions that Protect Your Privacy `http://lifehacker.com/the-best-browser-extensions-that-protect-your-privacy-479408034` Geraadpleegd op 12 mei 2013.

[16] Thomas Hogeling. Het volg-me-niet-register maakt belofte niet waar `https://www.bof.nl/2011/09/09/het-volg-me-niet-register-maakt-belofte-niet-waar/` Geraadpleegd op 10 mei 2013.

[17] Internetconsultatie. Aanpassing artikel 11.7a Telecommunicatiewet (Cookiebepaling) `http://www.internetconsultatie.nl/cookiebepaling`.

[18] Jplus. Forumpost over het draaien van meerdere plugins tegelijk `http://forums.xkcd.com/viewtopic.php?f=20&t=88040` Geraadpleegd op 10 mei 2013.

[19] Pedro Leon, Blase Ur, Richard Shay, Yang Wang, Rebecca Balebako, and Lorrie Cranor. Why johnny can't opt out: a usability evaluation of tools to limit online behavioral advertising. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '12, pages 589–598, New York, NY, USA, 2012. ACM.

[20] Flash Marketshare. `http://www.statowl.com/flash.php`.

[21] Jonathan Mayer. Tracking the Trackers: Self-Help Tools `http://cyberlaw.stanford.edu/node/6730` Geraadpleegd op 20 mei 2013.

[22] Mozilla. Firefox SDK preferences service `https://addons.mozilla.org/en-US/developers/docs/sdk/1.11/packages/api-utils/preferences-service.html` Geraadpleegd op 1 juni 2013.

[23] Mozilla. Bootstrapped extensions https://developer.mozilla.org/en-US/docs/Extensions/Bootstrapped_extensions.

[24] Mozilla. Preferences in Firefoxextenties https://developer.mozilla.org/en-US/docs/Code_snippets/Preferences.

[25] Assosiation of national advertisers. Let the Consumer Choose http://www.ana.net/blogs/show/id/25279 Geraadpleegd op 21 mei 2013.

[26] Nederlandse Publieke Omroep. Aangesloten website bij de NPO http://cookies.publiekeomroep.nl/data/sites/nos.nl/reconsider/ Geraadpleegd op 11 mei 2013.

[27] De Nederlandse overheid. Huidige wetgeving over cookies, http://wetten.overheid.nl/BWBR0009950/volledig/geldigheidsdatum_28-05-2013#Hoofdstuk11_111_Artikel117a.

[28] De Nederlandse overheid. Wet bescherming persoonsgegevens, http://wetten.overheid.nl/BWBR0011468/geldigheidsdatum_28-05-2013.

[29] Wet Bescherming Persoonsgegevens. Definitie van toestemming in artikel 1 sub i http://wetten.overheid.nl/BWBR0011468/geldigheidsdatum_25-06-2013.

[30] Adblock Plus. Tracking filter http://adblockplus.org/nl/features#tracking Geraadpleegd op 20 mei 2013.

[31] Adblock Plus. Documentatie broncode http://adblockplus.org/jsdoc/adblockplus/.

[32] Adblock Plus. New first-run page https://adblockplus.org/development-builds/new-first-run-page.

[33] Dimitri Reijerman. Tweakers.net: Firefox 22 blokkeert standaard third party-cookies http://tweakers.net/nieuws/87475/firefox-22-blokkeert-standaard-third-party-cookies.html.

[34] Franziska Roesner and Tadayoshi Kohnoand David Wetherall. Slides Detecting and Defending Against Third-Party Tracking on the Web https://www.usenix.org/sites/default/files/conference/protected-files/nsdi-webtracking.pdf.

[35] Profiler Scanscout. http://www.tremorvideo.com/about-us/privacy/ Geraadpleegd op 11 mei 2013.

[36] Joost Schellevis. Publieke omroep haalt cookiemuur neer http://tweakers.net/nieuws/88332/publieke-omroep-haalt-cookiemuur-neer.html.

[37] Ashkan Soltani, Shannon, Quentin Mayo Canty, Lauren Thomas, and Chris Jary Hoofnagle. Flash cookies and privacy, 2009. http://www.aaai.org/ocs/index.php/SSS/SSS10/paper/download/1070/1505.

[38] Nick Sulkers. Huidige plugin om cookieschermen weg te halen http://www.cookiesok.nl/.

[39] Berin Szoka. Adobe Flash ondersteunt nu Private Browsing http://techliberation.com/2010/02/17/privacy-innovation-adobe-flash-supports-private-browsing-deletes-flash-cookies/.

[40] Europese Unie. E-privacy directive 2009/136/EG http://www.ivir.nl/wetten/telecom/eu/2009_136_EG_universele_dienst_privacy.pdf.

[41] Europese Unie. E-privacy directive 2002/58/EG http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:NL:HTML.

[42] Europese Unie. Privacy directive 95/456/EG http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:nl:HTML.

[43] Europese Unie. Definitie van een richtlijn http://www.europa-nu.nl/id/vh7bhovywnh7/richtlijn Geraadpleegd op 26 mei 2013.

[44] EasyList van Adblock Plus. De problemen van Google Analytics http://adblockplus.org/blog/the-wrong-way-to-deal-with-privacy-concerns Geraadpleegd op 2 juni 2013.

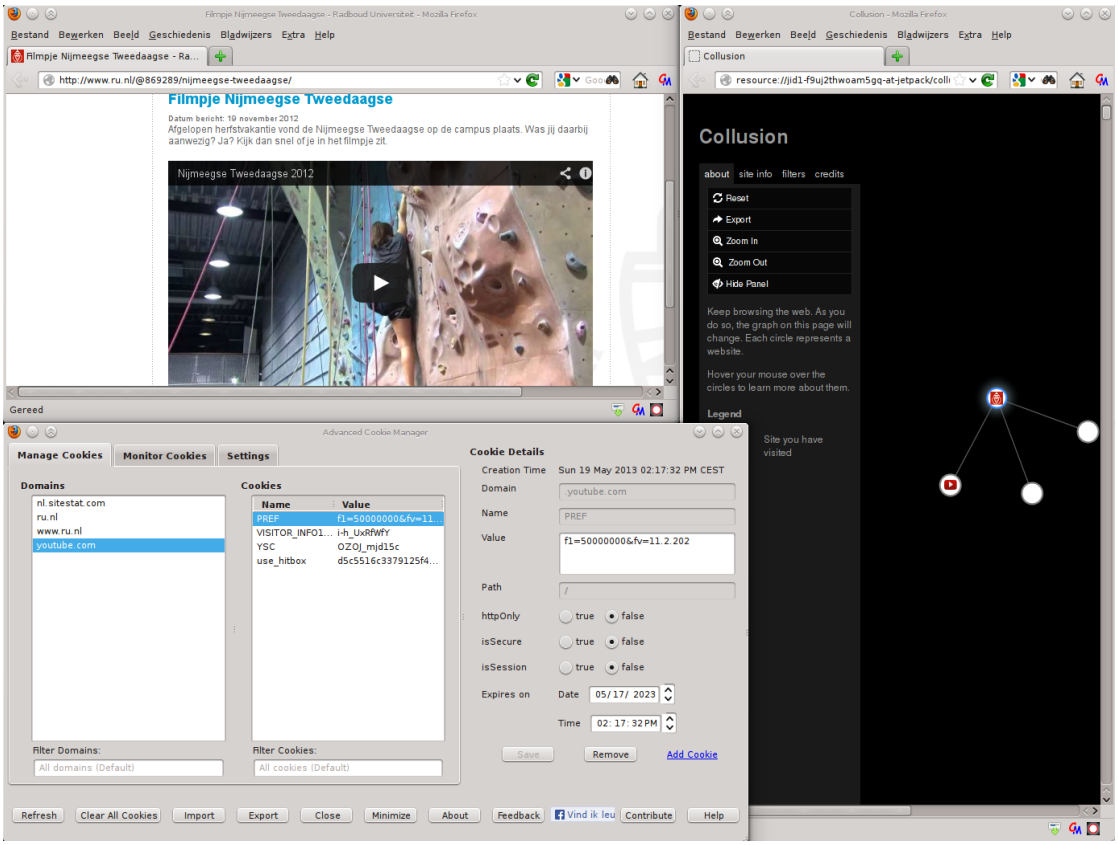
[45] Ot van Daalen. Bits Of Freedom over nieuwe cookierichtlijn https://www.bof.nl/2010/06/07/nieuwe-regels-voor-cookies-wenselijk-of-niet/.

[46] William West and S. Monisha Pulimood. Analysis of privacy and security in html5 web storage. *J. Comput. Sci. Coll.*, 27(3):80–87, January 2012.

Bijlage A

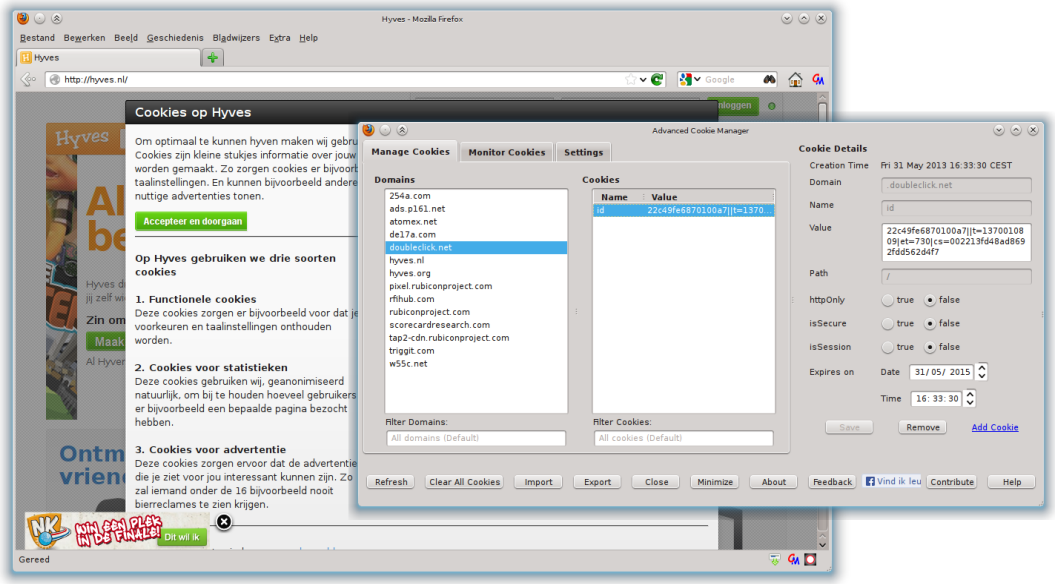
Screenshots

A.1 Screenshot cookies bij een youtubefilmpje



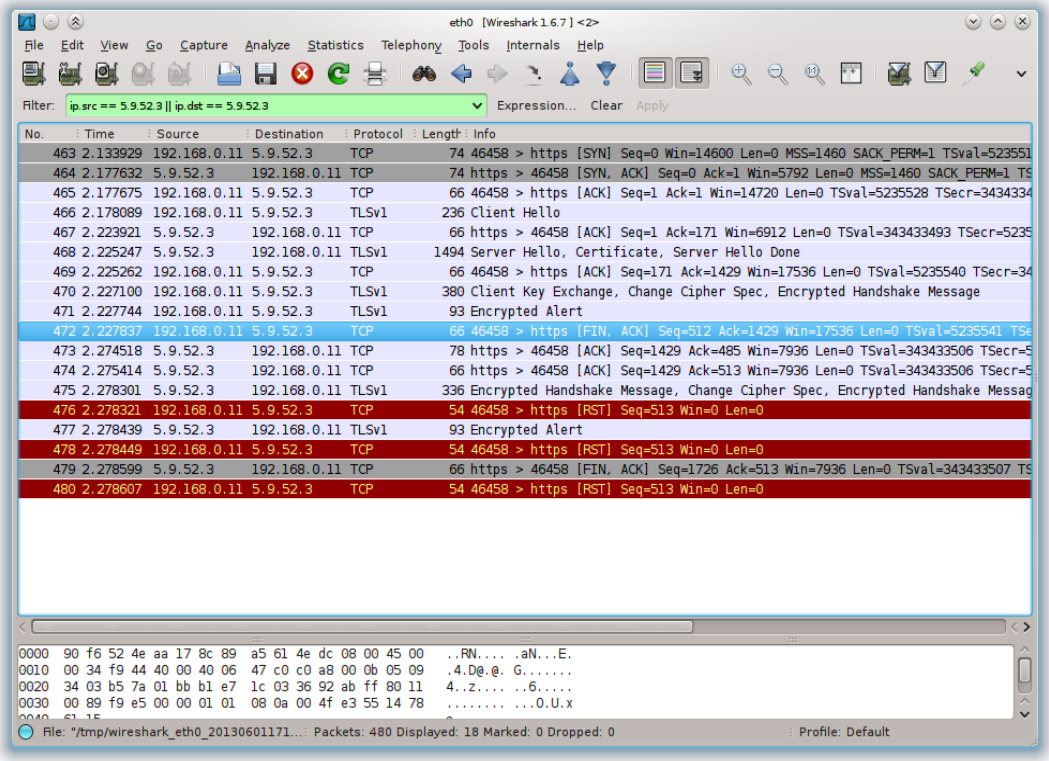
Figuur A.1: Als we onderstaande website van de RU bezoeken wordt er al een youtube-filmpje geladen. Ondanks dat het filmpje nog niet afgespeeld is hebben we al wel cookies ontvangen van Youtube zoals linksonder in de afbeelding te zien is.

A.2 Screenshot cookiewall van Hyves

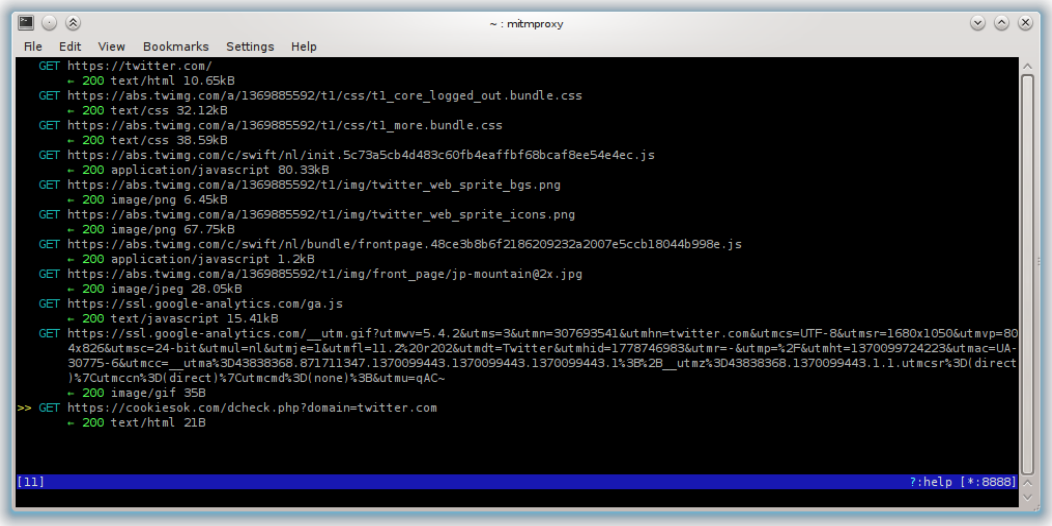


Figuur A.2: Bij een enkel bezoek aan Hyves worden er al heel veel cookies geplaatst. We zijn echter nooit akkoord gegaan met het plaatsen van cookies.

A.3 Screenshot beveiligde verbinding CookiesOK

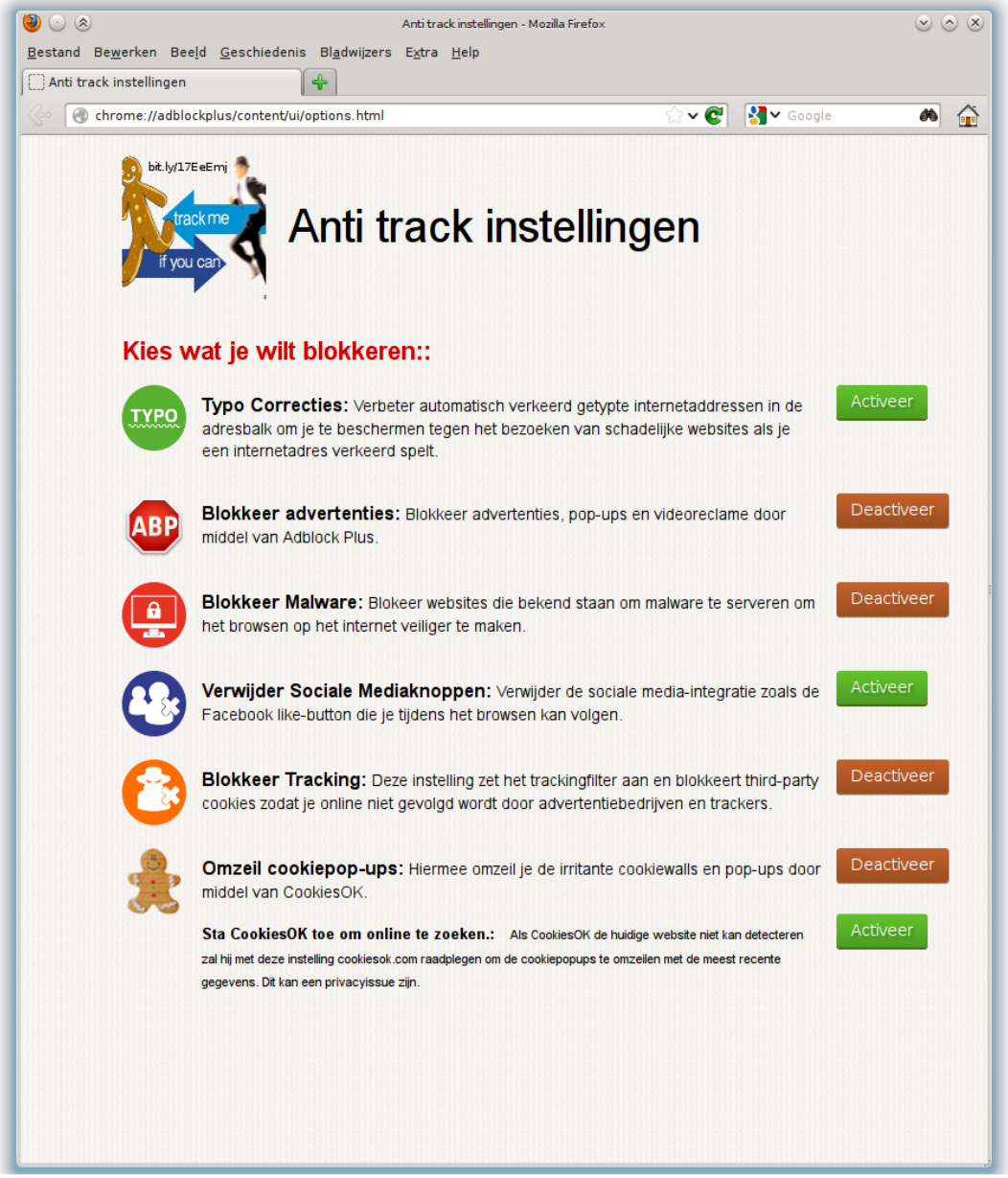


Figuur A.3: In dit geval werd twitter.com bezocht. Alle requests naar de server van CookiesOK (het ip-adres 5.9.52.3) zijn hier beveiligd met SSL



Figuur A.4: Als we met een zelf ondertekend certificaat als man-in-the-middle gaan kijken wat er precies naar CookiesOK verzonden wordt zien we dat dit inderdaad een zelfde request naar de online database is als bij 'normale' http-websites.

A.4 Screenshot gebouwde plugin



Figuur A.5: Een screenshot van het instellingenscherm van de uiteindelijk gebouwde plugin.

Bijlage B

Onderzoek informatieverstrekking websites

In dit onderzoek gaan we kijken naar de 25 populairste websites in Nederland. Deze top komt van `http://www.alexa.com/topsites/countries/NL` op 6 juni 2013. We gaan kijken of ze voldoen aan de punten van informatieverstrekking bij het gebruik van persoonsgegevens zoals dit in hoofdstuk 5 uitgelegd is. We gaan naar de volgende punten kijken:

1. Of de website tracking- of statistiekencookies plaatst. Als dit niet het geval is hoeven we natuurlijk niet verder te kijken.
2. Of de website een cookiewall heeft. Als een website deze namelijk niet heeft is deze sowieso al in overtreding en hoeven we niet verder te kijken.
3. Of de website met cookiewall géén tracking of statistiekencookies plaatsen voordat deze daarvoor toestemming heeft (punt 1 artikel 33 WBP).
4. Of de website de doeleinden van de verwerking van persoonsgegevens vermeldt (punt 2 artikel 33 WBP). Hierbij moeten de website duidelijk vermelden waar de cookies naartoe gaan en wat ze er mee doen, enkel een melding 'advertenties personaliseren' is niet voldoende.
5. Of de website precies vermeldt welke cookies er allemaal geplaatst worden (deels punt 3 artikel 33 WBP, maar niet helemaal omdat een zorgvuldige verwerking moeilijk te waarborgen is).
6. Of de website uitlegt hoe een gebruiker zijn persoonsgegevens kan vernietigen, waarmee de website dus uit moet leggen hoe een gebruiker zijn cookies kan wissen.

Nr	Website	Plaatst cookies?	Cookie-wall?	Plaatst cookies voor toestem-ming	Vermeldt doeleinden	Vermeldt exact cookies	Legt cookie-wissen uit
1	google.nl	Ja	Nee				
2	google.com	Ja	Nee				
3	facebook.com	Ja	Nee				
4	youtube.com	Ja	Nee				
5	wikipedia.org	Nee					
6	live.com	Ja	Nee				
7	marktplaats.nl	Ja	Nee				
8	linkedin	Ja	Nee				
9	nu.nl	Ja	Nee				
10	amazon.com	Ja	Nee				
11	ing.nl	Nee					
12	telegraaf.nl	Ja	Ja	Ja	Nee	Nee	Ja
13	twitter.com	Ja	Nee				
14	yahoo.com	Ja	Nee				
15	blogspot.nl	Ja	Nee				
16	rabobank.nl	Nee					
17	bol.com	Ja	Nee				
18	ad.nl	Ja	Nee				
19	abnamro.nl	Nee					
20	imdb.com	Ja	Nee				
21	xhamster.com	Ja	Nee				
22	wordpress.com	Ja	Nee				
23	buienradar.nl	Ja	Nee				
24	msn.com	Ja	Nee				
25	nos.nl	Ja	Ja	Nee	Ja	Ja	Ja