Radboud Universiteit Nijmegen

Bachelorscriptie

DO NOT TRACK

- wat het is en wat het zou moeten zijn -

Auteur:
Patrick Schileffski
3017095
P.Schileffski@student.ru.nl

Begeleidster:
Prof. mr. dr. Mireille Hildebrandt
Institute for Computing and Information Sciences
Radboud Universiteit Nijmegen

5 juli 2012

Inhoudsopgave

1 Afkortingen

EFF: Electronic Frontier Foundation

EG: Europese Gemeenschap

EHRM: Europees Hof voor de rechten van de mens

EVRM: Europees verdrag voor de rechten van de Mens

EU: Europese Unie

FCC: Federal Communications Commission

GUID: Globally Unique Identifier

HGEU: Handvest van de grondrechten van de Europese Unie

ISP: Internet Service Provider

LSO: Local Shared Object

Tw: Telecommunicatiewet

URI: Uniform Resource Identifier

URL: Uniform Resource Locator

W3C: World Wide Web Consortium

Wbp: Wet bescherming persoonsgegevens

2 Inleiding

Het is financieel aantrekkelijk om gebruikers op het internet te volgen. Dit is al lang geen geheim meer en wordt door grote bedrijven als Google en Facebook maar ook door speciaal op tracking gerichte bedrijven gedaan. Het voornaamste doel van tracking is het aanleggen van profielen die vervolgens voor marketingdoeleinden kunnen worden gebruikt. Wat tracking precies is wordt in hoofdstuk 3 verder uitgelegd.

Trackers kunnen in verschillende type gegevens geïnteresseerd zijn: primair zijn ze in de interesses en het gedrag van de gebruikers geïnteresseerd maar ook de demografische en geografische gegevens worden onderzocht. Tracking kan op verschillende manieren worden doorgevoerd bijvoorbeeld door de analyse van het gedrag van de gebruiker op het internet maar ook door zijn mobiele randapparatuur met behulp van applicaties te onderzoeken. Binnen deze scriptie wordt alleen tracking op het internet onderzocht zodat ander vormen van tracking buiten de scoop vallen.

Om het gedrag van gebruiker te kunnen analyseren is het nodig om hem over meerdere tijdstippen en op meerdere locaties te observeren. De gebruiker laat op het internet digitale voetafdrukken achter die door trackers verzameld worden. Dit kan op verschillende manieren die in hoofdstuk 4 worden beschreven. Uit deze scriptie zal blijken dat door tracking privacyproblemen ontstaan. Daarom is het ook nodig om het wettelijke kader te onderzoeken. Dit gebeurt in hoofdstuk 3.6.

Er zijn verschillende technologische middelen om tracking tegen te gaan. Het World Wide Web Consortium (W3C) is actueel bezig met een standaard genoemd Do Not Track. Bovendien zijn er add-ons zoals Do Not Track Plus van het onlineprivacybedrijf Abine of Ghostery van Evidon die bepaalde vormen van tracking zullen voorkomen. Een aantal trackingblockers worden in hoofdstuk 4 beschreven. Omdat er veel vormen van tracking zijn en veel mogelijkheden zijn om tracking te blokkeren is de centrale vraag binnen deze scriptie

wat "do not track" eigenlijk zou moeten betekenen?

De volgende deelvragen zullen helpen om de onderzoeksvraag te beantwoorden:

- **Wat verstaat men op dit moment onder tracking?**
- **Hoe verhoud tracking zich tot het privacyrecht?**
- **Welke technische mogelijkheden zijn er op dit moment wat tracking betreft?**
- **Zijn Do Not Track Plus en de nieuwe technologie van W3C voldoende om tracking te vermijden?**

Verantwoording

Er zijn drie types actoren die van dit onderzoek kunnen profiteren. Allereerst de internetgebruikers die op het internet gevolgd en geanalyseerd worden. Ze kunnen worden

ingelicht over wat er op dit moment allemaal speelt en hoe ze kunnen voorkomen dat delen van hun privacy weggenomen wordt. Er zal blijken dat er maatschappelijke relevantie is om dit onderzoek door te voeren omdat duidelijk wordt in hoeverre gebruikers nog ongestoord kunnen internetten. Bovendien wordt onderzocht wat ze kunnen doen om rustiger te kunnen internetten.

Een tweede groep zijn de technici die op dit moment bezig zijn met het ontwerpen en implementeren van trackingblockers. Do Not Track Plus en de technologie van W3C zijn zeker een stap in de goede richting, maar is dat wat ze aanbieden al voldoende om tracking op een gebruiksvriendelijke manier te voorkomen?

Ten derde is er de wetgever die eventuele maatregelen moet nemen omdat de gebruikers verwachten dat ze worden beschermd terwijl hun recht op privacy eigenlijk in gevaar is. Er zijn wetten over privacy en zelfs speciale wetten voor e-privacy. Deze moeten eventueel worden aangepast als tracking na de wetgeving nog veranderde of de wetgeving met bepaalde aspecten van tracking geen rekening houdt.

Methode

Om de eerste deelvraag (Wat verstaat men op dit moment onder tracking?) te beantwoorden zal gekeken worden hoe het World Wide Web Consortium (W3C), Abine, Evidon en de Electronic Frontier Foundation (EFF) op dit moment tracking definiëren. Uiteindelijk wordt hieruit een eigen definitie voor tracking afgeleid.

De tweede deelvraag (Hoe verhoud tracking zich tot het privacyrecht?) wordt beantwoordt door de analyse van het Europees Verdrag voor de Rechten van de Mens, het handvest van de grondrechten van de Europese Unie, twee richtlijnen van de Europese Commissie en de Nederlandse wetgeving.

De derde deelvraag (Welke technische mogelijkheden zijn er op dit moment wat tracking betreft?) wordt beantwoord door te onderzoeken welke technieken er actueel voor tracking worden gebruikt. De klassieke vorm is tracking met behulp van cookies. Cookies zijn kleine bestanden met een unieke code die op de randapparatuur van gebruikers opgeslagen worden. Later kunnen deze unieke codes weer worden uitgelezen om terugkomende gebruikers te kunnen herkennen. Maar ook social media buttons, device fingerprinting, bepaalde browsers en IP-adressen kunnen tracking bevorderen.

De vierde deelvraag (Zijn bekende trackingblockers en de nieuwe technologie van het W3C voldoende om tracking te vermijden?) wordt beantwoord door te analyseren hoe trackingblockers werken. Bovendien wordt de werkwijze van de trackingblockers vergeleken met de trackingtechnieken die er zijn. Op die manier wordt duidelijk of trackingblockers voldoende mogelijkheden bieden om tracking te voorkomen en zo niet wat er ontbreekt.

Wat “do not track” eigenlijk zou moeten betekenen (onderzoeksvraag) laat zich gedeeltelijk uit de antwoorden op de vierde deelvraag afleiden. Trackingblockers zouden een passieve blok voor onwenselijke manieren van tracking moeten zijn. Een passieve blok is volgens Achterbergh en Vriens een vorm van regelen die geen actieve handeling van

de gebruiker vereist, maar na het installeren automatisch ervoor zorgt dat bepaalde verstoringen (hier tracking) niet kunnen inwerken op de essentiële variabelen (hier de privacy)[8]. Trackers zouden dus onder geen omstandigheden in staat mogen zijn om tracking toe te passen als iemand dat niet wenst. Hiervoor is niet per se een strengere wetgeving of ander regels nodig maar de mogelijkheid voor gebruikers en trackers om af te spreken welke vormen van tracking een gebruiker wenst en welke hij niet wenst. Bovendien moeten gebruikers worden ingelicht wat tracking precies is. Tracking is niet per definitie iets negatiefs maar kan ook door gebruikers worden gewenst die bijvoorbeeld met behulp van trackers op inhouden op het internet willen worden geattendeerd die ze interesseren.

3 Tracking

Dit hoofdstuk gaat over verschillende aspecten van tracking. Uit dit hoofdstuk zal blijken dat bij tracking gegevens worden verzameld en verwerkt. Daarom wordt allereerst beschreven wat gegevens zijn en hoe ze kunnen worden gecategoriseerd.

Vervolgens worden organisaties onderzocht die zich bezighouden met het voorkomen van tracking. Hierbij ligt de focus op het W3C, Abine, Evidon en de EFF. Het W3C houdt zich bezig met standaarden voor het internet, waaronder een standaard voor Do Not Track. Hoe dat precies werkt, wordt in hoofdstuk 5.7 beschreven. Abine en Evidon stellen allebei gratis add-ons voor browsers ter beschikking die bepaalde vormen van tracking zullen voorkomen. Deze add-ons worden in de hoofdstukken 5.3 en 5.4 beschreven. De EFF houdt zich bezig met device fingerprinting. Deze techniek kan voor tracking worden gebruikt. Meer informatie hierover staat in hoofdstuk 4.5.

Na deze analyse van meningen en definities van de organisaties wordt een definitie van tracking opgesteld.

In het volgende gedeelte wordt het fenomeen Filter Bubble beschreven. De Filter Bubble wordt onder andere veroorzaakt door tracking en zorgt ervoor dat mensen vooral met informatie worden voorzien die individueel op hun is toegepast. De hiermee verbonden filtering heeft invloed op het recht op informatie. Uit de definitie van tracking zal blijken dat tracking invloed heeft op privacy. Daarom wordt ook beschreven wat privacy is.

In het laatste grote gedeelte van dit hoofdstuk word het wettelijk kader met betrekking tot privacy en tracking onderzocht. De focus ligt op het Europees Verdrag voor de Rechten van de Mens, de handvest van de grondrechten van de Europese Unie, de EU richtlijn betreffende gegevensbescherming (95/46/EG), de EU richtlijn betreffende privacy en elektronische communicatie (2002/58/EG), en het nationale wet van Nederland.

3.1 Gegevens

Bij tracking worden gegevens van gebruikers verzameld die vervolgens meestal voor marketing en hier in het bijzonder voor behavioral advertising worden gebruikt. Gegevens op het internet kunnen we in drie categorieën indelen: gebruikers-, verbindings- en inhoudsgegevens.

De naam gebruikersgegevens suggereert al dat dit feiten en data zijn over de gebruiker. Hieronder vallen bijvoorbeeld NAW-gegevens, de geboortedatum en soortgelijke attributen van een gebruiker. Deze gegevens hoeven tijdens het gebruik van het internet niet worden uitgewisseld en zijn in eerste instantie alleen maar voor de provider bekend. Gebruikers worden op het internet niet aan de hand van hun gebruikersgegevens naar aan de hand van IP-adressen geïdentificeerd die aan de randapparatuur van de gebruiker worden toegewezen. Hoe dit precies werkt, wordt in hoofdstuk 4.2 uitgelegd. Gebruikersgegevens worden dus alleen uitgewisseld als de gebruiker ze ergens invoert voor bijvoorbeeld een registratie of bestelling.

Verbindingsgegevens gaan over de verbindingen die via het internet worden opgebouwd. Als een gebruiker website opvraagt, ontvangt hij bestanden die de browser van de gebruiker vervolgens als websites weergeeft. Om het verkeer tussen webservers en de browser van de gebruiker te regelen, moeten bepaalde verbindingsgegevens worden uitgewisseld. Standaard worden bij het opvragen van websites verbindingsinformaties over de afzender, de ontvanger, het tijdstip van de aanvraag en de naam van de dienst uitgewisseld. De gebruiker is zich niet per se bewust van de uitwisseling van dit soort informatie omdat hij meestal alleen adres in de browser invoert en vervolgens een website bekijkt zonder erover na te denken hoe de website in zijn browser terecht komt.

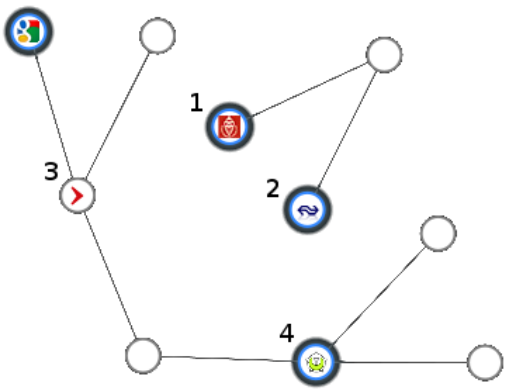
Uit de verbindingsgegevens laten zich onder bepaalde omstandigheden afleiden op welke locatie zich een gebruiker bevindt. Locatiegegevens laten zich vooral uit IP-adressen afleiden. Dit wordt in hoofdstuk 4.2.2 verder uitgelegd.

Inhoudsgegevens zijn de data die over het internet worden uitgewisseld. Met behulp van een opgebouwde verbinding tussen server en browser kunnen inhoudsgegevens worden uitgewisseld. Terwijl onder verbindingsgegevens alleen maar gegevens vallen wat wie van wie op welke tijdstip wil zien, bevatten inhoudsgegevens de echte inhoud. Als bijvoorbeeld een verbinding naar een website van een krant opgebouwd is en de gebruiker een artikel aanklikt, is de inhoud van dit artikel (teksten, foto's) inhoudsgegevens.

Tracking kan op ieder van deze types gegevens gericht zijn. Het gaat bij tracking altijd om het verzamelen van eigenschappen van een internetgebruiker. De meest directe informatie laat zich uit gebruikersgegevens afleiden. Deze moeten bewust door een gebruiker worden ingevoerd. Een manier om aan gebruikersgegevens te komen zijn squeezepages. Op dit soort websites worden gebruikers op een slimme manier ervan overtuigt gegevens op te geven om hierdoor van iets te kunnen profiteren. Maar wie veel meer profiteert, is de exploitant van de site die op die manier veel gebruikersgegevens verzamelt en deze voor eigen reclame kan gebruiken of aan derden door kan verkopen. Gebruikersgegevens kunnen ook worden verkregen door een illegale Man-in-the-middle-aanval bij registraties en bestellingen waar gebruikers hun gegevens op websites invoeren. Een ander manier is het illegale verkopen van klantenbestanden aan derden. Gebruikersgegeven kunnen dus alleen omslachtig op een slimme of illegale manier worden verzameld.

Technisch gemakkelijker is het om inhoudsgegevens te verkrijgen omdat ze het meest worden uitgewisseld. De meeste inhouden zijn geen directe persoonsgegevens, toch laten zich uit veel inhouden door interpretatie eigenschappen van de gebruiker afleiden. Kinderen bijvoorbeeld raadplegen vooral op hun gerichte websites. Websites over dure jachten, dure auto's en golfen worden meestal door rijke mensen geraadpleegd. Uit de inhoudsgegevens van de geraadpleegde websites kunnen dus eigenschappen als leeftijd of sociale status worden afgeleidt. Een ander voorbeeld waar een soortgelijke vertaalslag kan worden toegepast zijn kranten. Ze zijn vaak op een gepaalde doelgroep gericht. Zo wordt de Telegraaf waarschijnlijk vaker door laagopgeleiden gelezen en het NRC Handelsblad meer door hoogopgeleide mensen gelezen.

Uit alle websites die een gebruiker regelmatig oproept, laat zich een gebruikersprofiel afleiden. Welke rol tracking hierbij speelt wordt uit Figuur 1[1] duidelijk. De grafiek geeft weer hoe de websites van de Radboud Universiteit Nijmegen (1), de Nederlandse Spoorwegen(2), het NRC handelsblad(3) en Tweakers (4) aan elkaar worden gekoppeld. Op basis van de observaties kunnen websites en reclames worden aangepast om beter bij de gebruiker te passen. Dit was een eerste excursie die duidelijk maakt hoe tracking werkt. Hoe gegevens van gebruikers precies kunnen worden verzameld, wordt in hoofdstuk 4 verder uitgelegd.



Figuur 1: Collusion

3.2 Organisaties

Binnen deze paragraaf wordt onderzocht wat bepaalde organisaties van tracking vinden en hoe ze tracking beschrijven. Alle organisaties werken aan mogelijkheden om tracking te kunnen voorkomen.

3.2.1 World Wide Web Consortium

Brookman et al. [24] definiëren tracking voor het W3C als volgt: “Het letten op iemands surfgedrag om op basis van deze gegevens persoonlijke reclame aan te kunnen bieden.” Hiervoor noemt het W3C de volgende twee opties:

1. Het verzamelen of gebruiken van gebruikersgegevens door gebruik te maken van een unieke identificatie.
2. Het volgen of identificeren van een gebruiker, een user agent of een apparaat.

Bij de eerste optie maakt het W3C onderscheid tussen eerste en derde partijen. Bij de tweede optie worden meerdere bezoeken gevolgd die enerzijds op verschillende tijdstippen op dezelfde site anderzijds op meerdere sites kunnen plaatsvinden.

3.2.2 Abine

Tracking is volgens Abine (vgl. [11]) een verzamelbegrip voor verschillende methodes die websites, adverteerders, reclamenetwerken en anderen gebruiken om iets over het

[1] Deze grafiek werd door het browseradd-on Collusion aangemaakt

surfgedrag van gebruikers te leren. Volgens Abine wordt informatie verzameld over de sites die gebruikers bezoeken en hoe lang ze deze bezoeken, welke dingen een gebruiker leuk of niet leuk vindt, waarover de gebruiker zijn mening uit en informatie over zijn zoek- en koopgedrag. Tracker delen vervolgens de verzamelde informatie met anderen die bijvoorbeeld behavioral advertising toe kunnen passen.

Abine geeft dus alleen maar een brede definitie van tracking die inhoudt dat bij tracking op iemands surfgedrag gelet wordt om aan de hand van deze gegevens reclame op het internet voor diegene persoonlijk af te stemmen. Uit de definitie wordt duidelijk dat de gebruiker moet worden geïdentificeerd want anders zou de informatie niet aan de gebruiker kunnen worden gekoppeld. De identificatie van gebruikers zal later in het gedeelte over de wetten en richtlijnen bijzonder in het Nederlandse wet (hoofdstuk 3.6.5) nog een belangrijke rol spelen.

Verder heeft Abine een website op die ze uitleggen hoe tracking precies werkt. Dit wordt in hoofdstuk 4 verder uitgewerkt.

3.2.3 Evidon

Evidon geeft geen eigen definitie van tracking en verwijst op de blog van hun add-on Ghostery[13] alleen naar Wikipedia en andere artikelen wat het definiëren en beschrijven van trackingtechnieken betreft. Ze constateren op de blog dat er veel mogelijkheden bestaan om informatie over gebruikers te verzamelen en er steeds nieuwe technieken bij komen om iemands privacy op het web te onderscheppen.

Hieruit kan alleen worden geconcludeerd dat tracking volgens Evidon iets te maken heeft met het verzamelen van informatie over gebruikers en dat tracking invloed heeft op de privacy van internetgebruikers. Zoals bij de definitie van Abine kan ook uit de informatie van Evidon worden afgeleid dat gebruikers bij tracking identificeerbaar worden gemaakt.

3.2.4 Electronic Frontier Foundation

De EFF definieert tracking als volgt[17]:

> "Tracking is the retention of information that can be used to connect records of a person's actions or reading habits across space, cyberspace, or time."

Volgens de EFF wordt bij tracking dus informatie over personen opgeslagen. Deze informatie is een verbinding van acties en het leesgedrag van de gebruikers op meerdere momenten en locaties. Informatie over gebruikers op meerdere tijdstippen of meerder locaties kan alleen worden verzameld als de informatie aan een identiteit kan worden toegewezen. Anders zou geen koppeling van de losse informatie mogelijk kunnen zijn.

3.2.5 Samenvatting

Uit deze definities en beschrijvingen kunnen we concluderen dat tracking het verzamelen en verwerken van gegevens is. Deze gegevens bevatten informatie over de eigenschappen

en het gedrag van internetgebruikers. Abine zegt bovendien dat met behulp van deze informatie behavioral advertising kan worden toegepast. Volgens Evidon heeft tracking invloed op privacy, maar verder zijn er vanuit de organisaties geen meningen geuit over ethiek en legaliteit.

3.3 Definitie voor Tracking

Uit de hierboven genoemde meningen en definities kan de volgende definitie voor tracking worden afgeleidt:

Tracking is de verzameling en verwerking van gegevens over het gedrag van gebruikers. Hierbij wordt randapparatuur identificeerbaar gemaakt om de gebruiker bij zo veel mogelijk virtuele handelingen te kunnen observeren. Gebaseerd op deze gegevens wordt inhoud op het internet op individuele gebruikers of groepen van gebruikers aangepast.

Deze definitie beschrijft alleen tracking op het internet. Tracking is ook buiten het internet mogelijk, maar de focus van deze scriptie ligt op het internet. Daarom is deze definitie bewust zo specifiek gekozen.

3.4 Filter Bubble

Een van de negatieve gevolgen van tracking is de Filter Bubble. Ze is een bijeffect van tracking die Eli Pariser in een boek[20] beschrijft. Hij maakt de relevantie van dit onderwerp duidelijk door een citaat van Mark Zuckerberg te noemen: *"A squirrel dying in your front yard may be more relevant to your interests right now than people dying in Africa"*. Hiermee verklaarde Zuckerberg tegenover een journalist de relevantie van de news feed van Facebook.

De Filter Bubble creëert een situatie waarin gebruikers vooral de dingen ontvangen die binnen hun bereik gebeuren. Het is voor gebruikers moeilijker om belangrijke, nieuwe dingen waar te nemen. Veel uitgevers kiezen welke inhouden ze voor welke gebruiker op welk onderdeel van hun website getoond wordt. Hiervoor raadpleegt de uitgever een tracker die eigenschappen over de gebruiker ter beschikking stelt. Artikelen van die de uitgever denkt dat ze bijzonder goed bij het gebruikersprofiel passen, worden vervolgens opvallender op de startpagina geplaatst. Andersom moet de gebruiker langer naar artikelen zoeken die niet bij zijn profiel passen. Als hij niet oplet, bekijkt hij dus alleen nog informatie die voor hem van tevoren gefilterd werd.

Pariser schrijft dat hij in het begin van het internet nog het gevoel had dat het internet de mensen gaat verbinden en het internet goed voor de maatschappij en democratie zal zijn. Maar hij herkent met de Filter Bubble een onzichtbare verandering die volgens hem een groot probleem zou kunnen worden. De Filter Bubble werd hem duidelijk toen hij op Facebook niet meer alle posts van alle vrienden zag maar alleen nog de posts van vrienden die grotendeels dezelfde politieke voorkeur hebben dan hijzelf.

Facebook is niet de enige die zijn inhoud toepast of de profielen van gebruikers. Pariser noemt ook Google als voorbeeld. Op Google worden niet aan iedereen dezelfde zoekresultaten getoond. Volgens Pariser let Google op 57 verschillende signalen en maakt hiervan de lijst met zoekresultaten afhankelijk. Deze signalen zijn onder meer de locatie op die zich iemand bevindt, welke randapparatuur de zoekende gebruikt of met welke browser diegene op het internet gaat. Hoe deze signalen kunnen worden uitgelezen wordt gedeeltelijk in hoofdstuk 4.5 verder uitgelegd. Er is dus anders dan veel mensen nog denken, geen standaard Google meer. En het erge is volgens Pariser dat je niet meteen kunt zien wat het verschil met iemands anders zoekresultaten is. Hiervoor noemt hij een voorbeeld. Tijdens de revolutie in Egypte heeft Pariser twee vrienden gevraagd om voor hem op Google naar "Egypt" te zoeken. Aan de ene vriend werd informatie over de revolutie getoond, aan de ander vriend alleen maar op toeristen gerichte informatie en helemaal niets over de actuele stand van zaken wat de revolutie betreft. Pariser attendeert op het feit dat er nog veel meer sites zijn die hun inhoud aanpassen op zijn bezoekers. Hij noemt voorbeelden als de nieuwssites New York Times of Washington Post. Pariser citeert ook Eric Schmidt, voormalig CEO van Google en ondertussen CTO van Sun Microsystems: "It will be very hard for people to watch or consume something that is not tailored for them".

Alle filters die er om een mens worden geplaatst veroorzaken samen de Filter Bubble. Pariser beschrijft ze als je eigen, persoonlijke, unieke universum. De inhoud van de Filter Bubble is afhankelijk van wie je bent en wat je doet. Maar je beslist niet zelf wat in de Filter Bubble zit en nog belangrijker je kunt niet herkennen wat gefilterd wordt.

Pariser heeft het ook over het verschil van de rol van uitgever voor de tijd van het internet en nu. Hiervoor gebruikt hij de metafoor van een uitsmijter die bepaald wat er mag worden uitgezonden of gedrukt en wat niet. Deze rol nam vroeger de uitgever in. Het voordeel van het internet is volgens Pariser dat iedereen nu de mogelijkheid krijgt alles met iedereen te delen. Maar ondertussen zijn er nieuwe, algoritmische uitsmijters. En het nadeel is volens Pariser dat ze niets van ethiek weten. De Filter Bubble blokkeert alles wat voor een persoon onbelangrijk te zijn blijkt. Maar naast “belangrijke informatie” vindt Pariser dat ook onaangename en visie verbredende informatie en andere zienswijzen op een mens moeten kunnen afstromen.

Pariser herinnert dat de kranten in 1915 al hebben nagedacht over hun maatschappelijke verantwoording. Volgens hem kun je geen functionerende democratie hebben als de burgers geen goede informatiestroom kunnen ontvangen. Daarom waren de kranten dus al in die tijd kritisch bezig met hun werk. Pariser beweert dat het internet op dit moment ook in het jaar 1915 zit. Hij pleit voor meer transparantie die het mogelijk maakt dat iedereen kan snappen hoe de filters om zich heen werken. Bovendien vindt Pariser dat iedereen zelf moet kunnen beslissen wat voor hem gefilterd wordt en wat niet.

Uit de Filter Bubble wordt duidelijk dat tracking het recht van de vrijheid van informatie kan schenden. De vrijheid van informatie laat zich afleiden uit de vrijheid van meningsuiting die onder meer verankerd is in artikel 10 EVRM: “[een ieder heeft de] vrijheid om inlichtingen of denkbeelden te ontvangen”[27]. Websites die bepaalde informatie voor

een deel van de gebruikers verbergen, nemen de gebruiker de vrijheid om alle informatie te ontvangen. Daarom moet er een manier komen waarmee gebruikers kunnen zeggen dat ze niet willen worden gevolgd en informatie niet van tevoren zal worden gefilterd.

3.5 Privacy

Bij privacy kan worden onderscheiden tussen relationele en informationele privacy. Relationele privacy komt redelijk overeen met de bekende definitie van privacy die de juristen en rechters Warren en Brandeis 1890 formuleerden[1]:

> "[The] right to life has come to mean the right to enjoy life, – the right to be let alone"

Warren en Brandeis dat onder privacy het recht valt om alleen gelaten te worden. In hun eigen huis mogen burgers bijvoorbeeld niet zonder reden van de overheid worden geobserveerd omdat ze het recht hebben om alleen gelaten te worden. Dit recht geldt trouwens niet alleen binnen de eigen vier muren maar ook elders.

De tweede vorm, de informationele privacy betreft de automatische gegevensverwerking (AGV). Voorheen werden gegevens alleen maar op papier opgeslagen. Iemand die in de gegevens geïnteresseerd was, moest fysieke toegang tot de documenten hebben. Geheime gegevens konden dus gemakkelijk worden afgeschermd. Maar sinds het gebruik van AGV hoeft men voor veel gegevens niet meer toegang krijgen tot fysieke informatiedragers. De gegevens worden op servers opgeslagen en via netwerken gedeeld. Iedereen die toegang tot het netwerk en leesrechten heeft, kan dus de opgeslagen gegevens inzien. Bovendien is het mogelijk de communicatie binnen het netwerk af te luisteren en op die manier bij gegevens te komen. Het internet biedt vanwege zijn grootte bijzonder veel mogelijkheden voor het verkrijgen van data van anderen. Randapparatuur en servers binnen een bedrijfsnetwerk zijn meestal op het internet aangesloten. Hierdoor wordt het door bijvoorbeeld hacking mogelijk om in zwak beschermde lokale netwerken in te dringen en gegevens die binnen het netwerk gedeeld worden, te bekijken. Informationele privacy gaat dus vooral over goede gegevensbescherming. Dit geldt in het bijzonder voor gevoelige gegevens zoals financiële gegevens of iemands gegevens over zijn gezondheidstoestand.

Tracking heeft te maken met beide vormen van privacy. Mensen zijn zich meestal niet bewust dat ze op veel internetsites gevolgd en geobserveerd worden. Dat komt omdat tracking volledig automatisch en op de achtergrond kan gebeuren. Op het internet hoeft niemand observaties met verrekijkers door te voeren. Observeerders moeten alleen ervoor zorgen dat de internetgebruiker identificeerbaar wordt. Terwijl bij een fysieke observatie meestal de identiteit van de te observerende bekend is en iets over zijn gedrag zal worden vastgesteld is het bij tracking meestal andersom. Het gedrag kan gemakkelijk door middel van processen worden geobserveerd die op de achtergrond van websites en ander webdiensten draaien. Maar de resultaten van de observaties moeten vervolgens aan gebruikers worden gekoppeld om bijvoorbeeld gebruikersprofielen aan te kunnen leggen.

Het verzamelen van gegevens over het gedrag van mensen op het internet is een inmenging op hun privacy maar kan evenwel geoorloofd zijn zoals in de volgende paragraaf

uitgewerkt.

Omdat tracking al op heel veel websites wordt toegepast, zal het onwaarschijnlijk zijn dat dit nog een keer kan worden gestopt. Om wel de privacy van internetgebruikers te waarborgen, moeten deze een mogelijkheid krijgen om te kunnen zeggen "do not track". Met andere woorden "laat mij met rust en verwerk mijn gegevens niet". Zoals al in de inleiding uitgelegd, zal deze bachelorscriptie niet alleen onderzoeken wat do not track op dit moment betekent, maar ook wat het zou moeten betekenen.

3.6 Wetgeving

3.6.1 Europees Verdrag voor de Rechten van de Mens

In het Europees Verdrag voor de Rechten van de Mens (EVRM)[27] van de Raad van Europa omschrijft artikel 8 privacy:

> 1. Een ieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.

In artikel 8 lid 1 EVRM worden vier rechten samengevat, de rechten op

1. privéleven
2. familie- en gezinsleven
3. woning
4. correspondentie

Meyer-Ladewig[4] leidt van het recht op privéleven 22 rechten af die onder meer over gezondheid, medische handelingen, ondercuratelestelling of het afluisteren van telefoongesprekken gaan. Volgens Meyer-Ladewig valt ook het recht op privacybescherming onder artikel 8 lid 1 EVRM.

Meyer-Ladewig beschrijft dat er twee vormen van gegevens zijn die het EHRM onderscheidt: privégegevens en openbare gegevens. Voor openbare gegevens is artikel 8 EVRM niet van toepassing. De artikel is wel van toepassing als het om de bescherming van privégegevens en in het bijzonder van medische of sociale gegevens gaat[4].

Tracking heeft primair geen invloed op het recht op respect voor iemands familie- en gezinsleven en iemands woning. Daarom worden deze twee onderdelen niet verder geanalyseerd en doorgegaan met het recht op correspondentie.

Meyer-Ladewig noemt een aantal rechtspraken van het EHRM waaruit blijkt dat artikel 8 EVRM niet alleen voor briefwisseling van toepassing is maar ook bij telefoongesprekken en e-mails zelfs als ze vanuit het bureau worden verzonden. Deze activiteiten vallen volgens het EHRM onder het privéleven. Daarom moet iedereen die niet over bewaking geïnformeerd werd, vertrouwelijkheid kunnen verwachten[4]. Onafhankelijk van het medium valt de uitwisseling van informatie dus onder correspondentie en hiermee onder artikel 8 EVRM.

Verder is er veel jurisprudentie gewest wat het recht op de correspondentie van en met gevangenen betreft maar dat heeft niets te maken met privacy en wordt daarom niet verder behandeld.

Artikel 8 lid 2 EVRM beschrijft gevallen die een uitzondering voor de in Artikel 8 lid 1 genoemde rechten toestaan:

> 2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

Volgens Hollaender moet een inmenging bij de wet voorzien zijn, een erkend, legitiem doel beogen en in een democratische samenleving noodzakelijk zijn[2].

Bij de wet voorzien betekend volgens Meyer-Ladewig dat er voldoende rechtsgrond moet zijn in de nationale wet. Hiervoor moet het wet onder meer voor de burger toegankelijk en voorzienbaar zijn en mag het wet niet willekeurig zijn[4].

Met betrekking tot het legitimiteit van het doel beperkt zich het EHRM volgens Hollaender op de controle van de redelijkheid maar laat de staten hun speelruimte wat de precieze invulling betreft ("margin of appreciation")[2].

Wat de noodzakelijkheid voor de democratische samenleving betreft, bestaat volgens Hollaender aan de ene kant speelruimte binnen de beslissingsbevoegdheid voor de staten maar aan de ander kant wordt van de EHRM gevorderd dat een inmenging evenredig moet zijn en overeenstemt met een dwingend sociaal behoefde[2]. Hollaender constateert dat er na de terreuraanslagen van 11 september 2011 bepaalde mensenrechten waaronder het recht op privacy sterk beperkt werd om terroristen makkelijker te kunnen vinden. Veel van de ingezette methodes zijn volgens Hollaender niet conform artikel 8 EVRM.

Uit de analyse van artikel 8 EVRM en de betreffende jurisprudentie kan worden geconcludeerd dat de uitzonderingen die in artikel 8 lid 2 EVRM mogelijk worden gemaakt alleen maar in heel speciale gevallen gelden. Ook zonder jurisprudentie over tracking kan worden gezegd dat er geen recht bestaat om zich voor doeleinden als tracking in het recht op privéleven of correspondentie in te mengen. Tracking is daarom wettelijk gezien problematisch. Dit wordt ook in de volgende wetten en richtlijnen bevestigd.

3.6.2 Handvest van de grondrechten van de Europese Unie

Naast het EVRM bestaat het Handvest van de grondrechten van de Europese Unie (HGEU) [28]. Hiervan gaan twee artikelen over privacy. De opsplitsing in twee artikelen komt overeen met de twee vormen van privacy die in hoofdstuk 3.5 beschreven werden.

[2]Uitspraak van het EHRM op 25 maart 1983 in de rechtszaak Zilver.

Artikel 7 HGEU beschrijft het recht op relationele privacy en artikel 8 HGEU het recht op informationele privacy:

> *Artikel 7*
>
> **Eerbiediging van het privé-leven en het familie- en gezinsleven**
>
> Eenieder heeft recht op eerbiediging van zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn communicatie.
>
> *Artikel 8*
>
> **Bescherming van persoonsgegevens**
>
> 1. Eenieder heeft recht op bescherming van de hem betreffende persoonsgegevens.
>
> 2. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Eenieder heeft recht op toegang tot de over hem verzamelde gegevens en op rectificatie daarvan.
>
> 3. Een onafhankelijke autoriteit ziet toe op de naleving van deze regels.

Artikel 7 HGEU komt ongeveer overeen met artikel 8 EVRM. Het enige verschil is dat artikel 7 HGEU de term "communicatie" in plaats van "correspondentie" (Artikel 8 EVRM) gebruikt. Zoals al eerder genoemd, concludeert Meyer-Ladewig uit een aantal rechtspraken dat met correspondentie niet alleen briefverkeer bedoelt is maar ook telefoongesprekken en e-mails[4]. De term "communicatie" is daarom een betere keuze dan "correspondentie" omdat telefonie en e-mails hier duidelijker mee worden gedekt.

Artikel 8 HGEU specificeert de bescherming van persoonsgegevens. Uit artikel 8 HGEU blijkt dat iemand van die persoonsgegevens verwerkt worden hiervoor toestemming moet geven. Verder laat HGEU nog steeds veel speelruimte voor de invulling van de bescherming van persoonsgegevens. Het HGEU en het EVRM zijn de basis voor de onderaan staande richtlijnen, over gegevensbescherming en privacy.

3.6.3 EU richtlijn betreffende gegevensbescherming

In richtlijn 95/46/EG van het Europees Parlement en de Raad[26] is de informationele privacy voor gegevensverwerking vormgegeven. In artikel 2 worden *persoonsgegevens* als volgt gedefinieerd:

> "iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon[...]; 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"

Bij tracking worden per gebruiker gegevens verzameld en aan een profiel gekoppeld. Daarom zijn de verzamelde gegevens volgens artikel 2 van de richtlijn "persoonsgegevens".

Artikel 8 lid 2 van de handvest van de grondrechten van de EU gaat over de verwerking van persoonsgegevens. Ook voor *verwerking* geeft richtlijn 95/46/EG een definitie:

> "elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procédés, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op enigerlei andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens"

Bij tracking worden een aantal van deze acties ondernomen. Dit zijn onder meer het verzamelen, bewaren, bijwerken, gebruiken en verspreiden van gegevens. Daarom is bij tracking dus sprake van "verwerking van persoonsgegevens".

Verder staat in artikel 8 lid 2 van het handvest, dat de gebruiker toestemming moet gegeven voor de verwerking van zijn persoonsgegevens. Ook *toestemming* wordt in richtlijn 95/46/EG gedefinieerd:

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

Er zijn dus drie voorwaarden aan die een toestemming volgens richtlijn 95/46/EG moet voldoen:

1. De toestemming moet vrij zijn.
2. De toestemming moet specifiek zijn.
3. De toestemming moet een op informatie berustende wilsuiting zijn.

Een toestemming is vrij als de toestemming uit eigen wil geeft en niet gedwongen wordt. Omdat de toestemming specifiek moet zijn, kan er niet van worden uitgegaan dat de keuze van een gebruiker wat een specifieke cookie betreft ook voor alle andere cookies geldt. De term o"p informatie berustende wilsuiting" kan heel breed en situatieafhankelijk worden geïnterpreteerd. Een wilsuiting kan een schriftelijk contract een mondelinge afspraak of zelfs een gebaar zijn die beide partijen gelijk opvatten.

Als we deze voorwaarden bekijken en ervan uitgaan dat tracking een verwerking van persoonsgegevens is, wordt een probleem duidelijk. Veel websites laten voor commerciële doeleinden tracking op hun website toe. Maar internetgebruikers geven voordat ze deze websites openen geen toestemming dat ze willen worden gevolgd. Sterker nog, de meeste internetgebruikers weten niet eens dat ze worden gevolgd . Als we later een antwoord op de onderzoeksvraag geven, moet met dit aspect rekening gehouden worden.

Verder wordt in artikel 8 lid 1 het verwerken van persoonsgegevens uit bijzondere categorieën verboden:

> De Lid-Staten verbieden de verwerking van persoonlijke gegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, of het lidmaatschap van een vakvereniging blijkt, alsook de verwerking van gegevens die de gezondheid of het seksuele leven betreffen.

Met behulp van tracking word informatie verzameld ongeacht bij welke categorie ze behoort. Op de website van de onlineapotheek DocMorris (www.docmorris.com) herkent Ghostery (zie 5.4) bijvoorbeeld twee trackers (WebTrends en Zanox). Deze kunnen de bezoeker op de website observeren en aan de hand van de medicijnen die hij bekijkt en koopt, achterhalen welke ziektes en klachten hij misschien heeft.

Een ander voorbeeld waar trackers informatie kunnen verzamelen uit één van de bijzondere categorieën zijn pornosites. Op www.sex.com herkent Ghostery bijvoorbeeld twee trackers (AddThis en Google Analytics) en één Twitter-Button die zoals in hoofdstuk 4.6 verder uitgelegd wordt ook voor tracking kan worden gebruikt. Tijdens het bezoeken van een pornosite laten dus websiteaanbieders toe dat de bezoekers worden geobserveerd. Uit deze observaties zou bijvoorbeeld informatie kunnen worden afgeleidt over iemands seksuele voorkeur. Maar gegevens die de gezondheid of het seksuele leven betreffen mogen volgens artikel 8 lid 1 niet worden verwerkt als ze niet aan de eigenschappen voldoen die volgens artikel 8 leden 2 en 3 een uitzondering toestaan.

Artikel 8, lid 2 sub b tot en met sub e en artikel 8 lid 3 zijn in het geval van tracking niet van toepassing. Hiervoor zal tracking nodig moeten zijn voor bijvoorbeeld het verdedigen van iemands vitale belangen, preventieve geneeskunde of medische diagnose. Alleen aan artikel 8 lid 2 sub a zouden trackers kunnen voldoen:

> Lid 1 is niet van toepassing wanneer:
>
> a) de betrokkene uitdrukkelijk heeft toegestemd in een dergelijke verwerking, tenzij in de wetgeving van de Lid-Staat is bepaald dat het in lid 1 bedoelde verbod niet door toestemming van de betrokkene ongedaan kan worden gemaakt;

Tracking van iemands eigenschappen uit een van de bijzondere categorieën is dus volgens de richtlijn betreffende gegevensbescherming alleen toegestaan als de gebruiker daar uitdrukkelijk toestemming voor heeft gegeven.

Naar aanleiding van artikel 29 van de richtlijn werd een groep opgericht voor de bescherming van personen in verband met de verwerking van persoonsgegevens:

> 1. Er wordt een Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens ingesteld, hierna „de Groep" te noemen. De Groep is onafhankelijk en is van raadgevende aard.

Anders dan in de wet beschreven zal de "Groep" hierna "Artikel 29 werkgroep" worden genoemd. In de verblijvende leden van artikel 29 en artikel 30 worden organisatorische dingen en de taakbeschrijving voor de Artikel 29 werkgroep beschreven. Omdat deze voor het onderzoek over Do Not Track niet van belang zijn, worden ze niet verder behandeld.

3.6.4 EU richtlijn betreffende privacy en elektronische communicatie

EU richtlijn 2002/58/EG[25] betreffende privacy en elektronische communicatie vult de eerder genoemde wetten aan. Artikel 3 geeft het toepassingsgebied van de richtlijn aan:

> Deze richtlijn is van toepassing op de verwerking van persoonsgegevens in verband met de levering van openbare elektronische communicatiediensten over openbare communicatienetwerken in de Gemeenschap, met inbegrip van openbare communicatienetwerken die systemen voor gegevensverzameling en identificatie ondersteunen.

De richtlijn geldt dus voor het verwerken van persoonsgegevens en om misverstanden te voorkomen wordt nadrukkelijk gezegd dat de richtlijn ook geldt als er sprake is van gegevensverzameling en identificatie. De richtlijn geldt daarom in het geval van tracking waar gebruikers worden geïdentificeerd en vervolgens profielen worden aangelegd waarin gegevens over het gedrag van de gebruikers wordt verzameld.

De focus van richtlijn 2002/58/EG ligt op communicatie via de telefoon, maar in de preambule gaan de punten 24 en 25 over trackingtechnieken als cookies. Punt 24 luidt als volgt:

> Eindapparatuur van gebruikers van netwerken voor elektronische communicatie en in die apparatuur bewaarde informatie maken deel uit van de persoonlijke levenssfeer van de gebruikers die op grond van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden bescherming vereist. Zogeheten spionagesoftware, webtaps, verborgen identificatoren en andere soortgelijke programmatuur kunnen de terminal van de gebruiker zonder diens medeweten binnenkomen teneinde toegang tot informatie te krijgen, verborgen informatie op te slaan of de activiteiten van de gebruiker te traceren en kunnen ernstig inbreuk maken op de persoonlijke levenssfeer van die gebruikers. Het gebruik van die programmatuur dient alleen te worden toegestaan voor legitieme doeleinden met medeweten van de betrokken gebruikers.

Hieruit wordt duidelijk dat cookies (vgl. punt 25) invloed kunnen hebben op de privacy van de gebruiker. Het wordt nog een keer bevestigd dat tracking inbreuk kan maken op de persoonlijke levenssfeer van gebruikers. Bovendien wordt in de laatste zin van punt 24 expliciet vermeldt dat het gebruik van technieken als cookies alleen is toegestaan als de gebruiker hiervan in kennis wordt gezet.

Het tweede punt dat zich bezighoudt met cookies is punt 25:

> Dergelijke programmatuur, bijvoorbeeld zogeheten cookies, kan evenwel een legitiem en nuttig hulpmiddel zijn om bijvoorbeeld de doeltreffendheid van het ontwerp van websites en van reclame te onderzoeken, en om de identiteit te bepalen van gebruikers die onlinetransacties verrichten. Wanneer dergelijke programmatuur, bijvoorbeeld cookies, voor een legitiem doel bestemd

> is, zoals het vergemakkelijken van de levering van diensten van de informatiemaatschappij, dient hun gebruik te worden toegestaan op voorwaarde dat gebruikers worden voorzien van duidelijke en nauwkeurige informatie, overeenkomstig Richtlijn 95/46/EG, over de doeleinden van cookies of soortgelijke programmatuur, welke verzekert dat de gebruiker zich ervan bewust is dat er informatie op de door hem gebruikte eindapparatuur wordt geplaatst. De gebruikers dienen de gelegenheid te hebben te weigeren dat een cookie of soortgelijke voorziening op hun eindapparatuur wordt opgeslagen. Dat is met name belangrijk in situaties waarin ook andere gebruikers toegang hebben tot de eindapparatuur en zo tot op die apparatuur opgeslagen gegevens die privacygevoelige informatie bevatten. De informatie en het recht van weigering kan voor het gebruik van de verschillende programmatuur bestemd om op de eindapparatuur van gebruikers te worden geïnstalleerd, éénmaal gedurende eenzelfde verbinding worden aangeboden en geldt dan ook voor het eventuele verdere gebruik van die programmatuur gedurende volgende verbindingen. De wijze waarop informatie wordt gegeven, een recht van weigering wordt aangeboden of toestemming wordt gevraagd dient zo gebruikersvriendelijk mogelijk te zijn. Aan toegang tot specifieke inhoud van een website kan nog altijd de voorwaarde worden verbonden dat een cookie of soortgelijke voorziening, indien gebruikt voor een legitiem doel, bewust wordt aanvaard.

Punt 25 maakt duidelijk dat de wetgever niet alle type cookies generaliseert maar cookies die een legitiem en nuttig hulpmiddel zijn en ander cookies onderscheid. Cookies als hulpmiddel met een legitiem doel mogen volgens de richtlijn worden ingezet mits de gebruiker hierover geïnformeerd wordt en de mogelijkheid krijgt om het gebruik van cookies te weigeren. Hoe dit precies in elkaar zit wordt in artikel 5 verder gespecificeerd:

> 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.

Samengevat moet de gebruiker voor het gebruik van trackingcookies en dergelijke a) de toestemming geven en b) van tevoren met informatie worden voorzien over onder meer de doeleinden van de cookies.

De Artikel 29 werkgroep noemt in zijn advies 16/2011 drie voorbeelden onder die geen toestemming van de gebruiker nodig is[10]:

1. sessiecookies bij beveiligde login. Dit type cookie is bedoeld om de gebruiker te

identificeren nadat deze is ingelogd op een dienst van de informatiemaatschappij, en is nodig om de gebruiker te herkennen en de integriteit van de verbinding met de server over het communicatienetwerk in stand te houden; –

2. cookies voor winkelwagentjes. Door webwinkels wordt gewoonlijk dit type cookie gebruikt om vast te leggen welke artikelen de gebruiker heeft gekozen door op een knop te klikken met een tekst als "in winkelwagentje". Dit cookie is dus nodig voor het leveren van een uitdrukkelijk door de gebruiker gevraagde dienst van de informatiemaatschappij; –
3. beveiligingscookies. Deze cookies zijn nodig om te voldoen aan de beveiligingsvereisten van Richtlijn 95/46/EG of andere wetgeving bij het leveren van een uitdrukkelijk door de gebruiker gevraagde dienst van de informatiemaatschappij. Met zo'n cookie kan bijvoorbeeld een unieke identificator worden vastgelegd waarmee de dienst van de informatiemaatschappij een terugkerende gebruiker met grotere zekerheid kan herkennen. Wanneer geprobeerd wordt in te loggen met een onbekend apparaat, kunnen dan aan de gebruiker extra beveiligingsvragen worden voorgelegd.

In de richtlijn betreffende privacy en elektronische communicatie wordt dus onderscheid gemaakt tussen verschillende doeleinden van cookies. Aan de ene kant trackingcookies die een inmenging op de privacy kunnen zijn en aan de ander kant functionele cookies waarvoor minder strenge regels gelden.

3.6.5 Nederland

De voorschriften uit de bovenstaande richtlijnen zijn in Nederland in twee wetten van geïmplementeerd. Ten eerste in de Wet bescherming persoonsgegevens (Wbp) en ten tweede in de Telecommunicatiewet (Tw). Artikel 8 Wbp. regelt de verwerking van persoonsgegevens en dus tracking:

> Persoonsgegevens mogen slechts worden verwerkt indien:
>
> a. de betrokkene voor de volgen verwerking zijn ondubbelzinnige toestemming heeft verleend;
>
> b. de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst;
>
> c. de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is;
>
> d. de gegevensverwerking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene;
>
> e. de gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt, of

> f. de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.

Persoonsgegevens worden in artikel 1 lid 1 Wbp. als volgt gedefinieerd:

> a. persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;

Bij tracking worden volgens de Wbp. persoonsgegevens verwerkt, want een van de doelen van tracking is het identificeren van gebruikers. De enige situatie die tracking in Nederland toestaat is de onder artikel 8 Wbp. genoemde ondubbelzinnige toestemming. Alle ander leden die het verwerken van persoonsgegevens toelaten, zijn in het geval van tracking niet van toepassing. Het is uit het oog van adverteerders omstreden of lid f van toepassing zou zijn. De industrie vindt dat cookies nodig zijn voor hun belang, maar onder meer jurist Bert van der Sloot vindt dat ze geen gerechtvaardigde belang hebben om persoonsgegevens zonder ondubbelzinnige toestemming te mogen verwerken (vgl. [7]).

Behalve voor marketing wordt tracking bijvoorbeeld ook van analysetools ingezet om voor de websitebeheerder informatie over de bezoeken te verzamelen. Een bekend tool is Google Analytics. Omdat Google Analytics de gebruikers over meerdere bezoeken en over meerdere websites volgt, valt het tool duidelijk onder de categorie trackers. Andere tools zoals bijvoorbeeld statcounter verzamelen alleen gegevens over één bezoek op één website en op één tijdstip. In dat geval wordt dus voor ieder bezoek, ook van dezelfde gebruiker, op ieder website op die de analysetool actief is een nieuwe cookie geplaatst. Het primaire doel is dus nog steeds de analyse van bezoeken op een website maar niet meer met als achterliggend doel om de gebruiker verder te tracken. In dat geval zal het plaatsen van cookies geen verwerken van persoonsgegevens zijn en niet onder de Wbp. vallen.

Artikel 11.7a Tw. is gebaseerd op de eerder beschreven richtlijnen 95/46/EG en 2002/58/EG en wordt in het volgende gedeelte geanalyseerd.

> 1. 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.

Artikel 11.7a lid 1 Tw. gaat over gegevens die op randapparatuur zijn opgeslagen of zullen worden opgeslagen. Zoals we later in hoofdstuk 4.3 zullen zien, is dat onder meer bij cookies het geval.

Artikel 11.7a lid 1 sub a Tw. beschrijft dat de gebruiker over de doeleinden moet worden ingelicht als een websiteaanbieder cookies op randapparatuur wil plaatsen of uitlezen. Volgens artikel 11.7a lid 1 sub b Tw. moet diegene die gebruik maakt van cookies hiervoor bovendien toestemming krijgen van de gebruiker. In Artikel 11.1g wordt vastgelegd dat toestemming bedoeld is als in artikel 1 lid 1 Wbp die als volgt luid:

> elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt;

Deze vorm van wilsuiting is overgenomen uit de richtlijn betreffende gegevensverwerking (95/46/EG, hoofdstuk 3.6.3) en wordt daarom hier niet nog een keer uitgelegd.

Artikel 11.7a lid 2 Tw. zorgt dat iedereen die cookies op randapparatuur op welke manier dan ook wil plaatsen of uitlezen zich in ieder geval aan de vereisten moet houden die in artikel 11.7a lid 1, sub a en b genoemd worden:

> 2. De in het eerste lid, onder a en b, genoemde vereisten zijn ook van toepassing in het geval op een andere wijze dan door middel van een elektronisch communicatienetwerk wordt bewerkstelligd dat via een elektronisch communicatienetwerk gegevens worden opgeslagen of toegang wordt verleend tot op het randapparaat opgeslagen gegevens.

Artikel 11.7a lid 2 Tw. is bijvoorbeeld van toepassing als de gebruiker randapparatuur koopt die al een vorm van tracking ondersteund zonder dat de tracker na der hand nog iets via het elektronische communicatienetwerk op het apparaat zou moeten plaatsen of uitlezen. Als trackers bijvoorbeeld met behulp van van tevoren geïnstalleerde software op de randapparatuur automatisch gegevens kunnen ontvangen zal deze vorm van tracking niet onder artikel 11.7a lid 1 vallen. Als de gegevens dermate geanonimiseerd zijn dat identificatie onmogelijk is, zal het ook niet door de Wbp. worden gedekt. Lid 2 zorgt daarvoor dat de gebruiker van de beschreven randapparatuur toch toestemming moet geven.

Onder artikel 11.7a lid 3 Tw. worden uitzonderingen genoemd waar de vereisten van de vorige leden niet geldig zijn. Uitzonderingen zijn mogelijk als de cookie bedoeld is voor de communicatie over het netwerk. Als twee gebruikers dus bijvoorbeeld in een chat met elkaar communiceren en de chat alleen voor het behouden van de verbinding tussen de gebruikers gebruik maakt van cookies, zijn artikel 11.7a lid 1 en lid 2 Tw. niet van toepassing. Ze zijn ook niet van toepassing als cookies alleen maar ingezet worden met als doel een gevraagde dienst te kunnen leveren. Een bank die internetbankieren aanbiedt, zou dus niet verplicht zijn om toestemming voor het gebruik van cookies te vragen of de gebruiker over het doel van de cookies te informeren mits de ingezette cookies alleen voor functionele redenen worden gebruikt:

> 3. 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.

Artikel 11.7a lid 4 biedt de mogelijk tot algemene maatregel van bestuur voor de onder artikel 11.7a lid 1 genoemde voorwaarden. Hierdoor is het mogelijk om het wet naderhand zonder dat zich de Eerste en Tweede Kamer hiermee bezig moeten houden nog een keer te wijzigen. Specifiek wordt het College bescherming persoonsgegevens hier om advies gevraagd:

> 4. Bij algemene maatregel van bestuur kunnen in overeenstemming met Onze Minister van Veiligheid en Justitie nadere regels worden gegeven met betrekking tot de in het eerste lid, onder a en b, genoemde vereisten. Het College bescherming persoonsgegevens wordt om advies gevraagd over een ontwerp van bedoelde algemene maatregel van bestuur.

De Nederlandse wet maakt dus zoals de richtlijn betreffende privacy en elektronische communicatie onderscheid tussen twee vormen van tracking. Het is volgens de wet nodig dat de gebruiker het plaatsen van cookies kan weigeren die bepaalde, primair van gebruikers gewenste functionaliteit mogelijk maken. Dit geldt ook voor cookies die door derde partijen woorden geplaatst die alleen in dienst zijn voor de eerste partij en de gebruiker niet identificeerbaar maken. In de Wbp. wordt een strengere regeling gehandhaafd wat tracking betreft. Hieruit blijkt dat voor tracking een uitdrukkelijke toestemming van de gebruiker moet worden gegeven.

Het geven van een uitdrukkelijke toestemming is veel bediscussieerd omdat hierbij meestal aan pop-ups gedacht wordt. De Artikel 29 werkgroep stelt in advies 16/2011 andere, gebruiksvriendelijke manieren voor onder die toestemming van de gebruiker zou kunnen worden verkregen[10]:

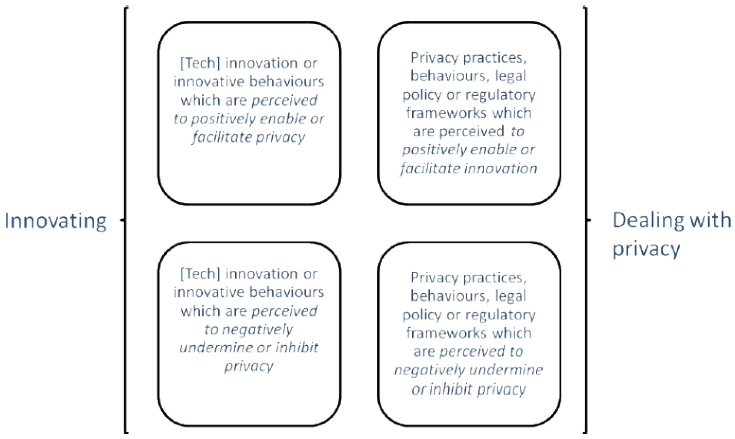
1. een statische informatiebanner bovenaan een webpagina, waarmee de gebruiker wordt gevraagd om toestemming voor het plaatsen van cookies, met een hyperlink naar een nadere toelichting over de voor de verwerking verantwoordelijken en het doel van de verwerking. [...]
2. een splashscreen bij het laden van de website, [die bijvoorbeeld] op websites van brouwerijen [gebruikt wordt] om te jonge bezoekers tegen te houden; –
3. een standaardinstelling die doorgifte van gegevens naar derden niet toelaat, zodat de gebruiker moet klikken om toestemming te geven om te worden gevolgd. [In een mogelijke oplossing van het Duitse webmagazine Heise zijn knopen van social media standaard] lichtgrijs. Pas als de gebruiker erop klikt, wordt de knop actief en kunnen gebruikersgegevens worden vastgelegd of ontvangen; –

4. een standaardinstelling voor webbrowsers waarmee het verzamelen van gedragsgegevens wordt verhinderd. [...]

3.6.6 Ontwikkelingen

Op dit moment blijkt dat Europa graag een regulering voor tracking wil hebben (vlg. [10]) waar de gebruiker ondubbelzinnige toestemming voor tracking moet geven. In Nederland gelden al de hierboven beschreven wetten die een ondubbelzinnige toestemming voor tracking voorschrijven. De marketinglobby zet zich op dit moment ervoor in dat er meer mogelijk wordt met opt-out-oplossingen. Dit komt onder meer omdat anders alleen maar nog een klein aantal mensen zou kunnen worden bereiken wat volgens de marketinglobby fatale gevolgen voor de adverteerders zou hebben. Volgens Arnoud Engelfried[14] zal 80% geen keuze maken en van de overgebleven 20% nog eens de helft cookies weigeren. Bij een opt-in regulering zal daarom nog maar 10% van de mensen kunnen worden bereikt.

Gezien de actualiteit van het onderwerp heeft de EU studie[9] laten doorvoeren over het samenspel tussen internetinnovaties en privacy. Binnen de studie wordt duidelijk dat persoonsgegevens in toenemende mate in een sterk gefragmenteerd en decentraal vlechtwerk uit verschillenden systemen en instellingen worden opgenomen. Later in de studie wordt het samenhang van internetinnovaties en privacy in een twee bij twee matrix gevisualiseerd:



Figuur 2: Tweezijdige verhouding tussen privacy en internetinnovatie

Het kwadrant boven links geeft innovaties weer die privacy bevorderen. Als voorbeelden noemt de studie de sociale netwerksites Diaspora en de zoekmachine IxQuick. Beide zijn innovatief maar letten tegelijkertijd op de privacy van de gebruiker.

Het kwadrant boven rechts staat voor toepassingen die voor privacy bedoelt zijn maar tegelijkertijd innovatief zijn. Als voorbeelden worden hier het kinderenspel PrivacyVille van Zynga of Surfwel Island van Disney genoemd.

Onderaan links staan innovaties die privacy ondergraven of afzien van privacy. Als voorbeelden worden hier Google Street View, nieuwe cookie-technieken als flash-cookies en Deep Packet Inspection genoemd. Het laatste is een herkenningssysteem voor onder meer

spamberichten met als gevolg dat je voor je provider de inhoud van alle mails toegankelijk moet maken.

Het kwadrant onderaan rechts staat voor het invloed dat privacy op internetinnovaties kan hebben. Hier zou bijvoorbeeld in Duitsland Google Street View onder vallen. Omdat Google Street View zo een grote invloed op privacy heeft kwam in Duitsland veel protest op toen Google Street View introduceerde[19] met als gevolg dat Street View in Duitsland alleen in de grote steden beschikbaar is.

3.7 Conclusie

De wetten onderscheiden twee vormen wat de identificatie op het internet. Voor het legitieme en op het primaire doel van een website gerichte gebruik van cookies en vergelijkbare technieken schrift de wetgever voor dat de gebruiker geïnformeerd wordt en de mogelijkheid heeft om cookies en dergelijke te weigeren. Tracking daarentegen is volgens de wet alleen toegestaan onder de voorwaarde dat de gebruiker informatie over de vorm en het doel van de tracking kan krijgen en de gebruiker bovendien ondubbelzinnige toestemming gegeven heeft. De wetten noemen vooral cookies als trackingtechniek maar zoals in het volgende hoofdstuk wordt uitgelegd zijn er nog meer technieken om gebruikers op het internet te identificeren. De Artikel 29 werkgroep stelt voor dat de ondubbelzinnige toestemming door pop-ups, statische informatiebanners, splashscreens of instellingsmogelijkheden in der browser kan worden verkregen. Hiernaast stelt de Artikel 29 werkgroep websitebeheerders voor om gebruik te maken van standaardinstellingen die doorgifte van gegevens pas naar uitdrukkelijke toestemming mogelijk maken (vgl [10]).

Wat privacy betreft zou het kwadrant boven links uit de bovenstaande grafiek het doel moeten zijn. Innovatie is altijd nodig. Toch moet bij ieder innovatie ook weer aan privacy worden gedacht. Zoveel nieuwe, handige mogelijkheden, nieuwe toestellen en browserplug-ins met zich mee brengen, zoveel nieuwe mogelijkheden ontstaan er ook voor tracking. Om het duidelijk te maken: Een oud mobieltje, een gewoon navigatiesysteem of een rekenmachine hebben minder functionaliteit dan een nieuw smartphone, maar gebruikers van deze apparaten kunnen ook nauwelijks worden getrackt. Smartphones zijn zeker geen slechte uitvinding, maar wat er op dit moment nog ontbreekt, zijn de mogelijkheden om privacy te beschermen en te kunnen zeggen in hoeverre de gebruiker gevolgd worden wilt. Welke technieken er precies bestaan om iemand te tracken en wat op dit moment al mogelijk is om tracking te voorkomen, zal in de volgende hoofdstukken worden beschreven.

4 Trackingtechnieken

Binnen dit hoofdstuk worden mogelijkheden zijn om internetgebruikers te kunnen tracken. Bijna alle technieken waren in eerste instantie voor de technische werking van het internet. Met de opkomst van webwinkels werd het bijvoorbeeld nodig om een klant een virtueel winkelmandje ter beschikking te kunnen stellen. Om een winkelmandje aan een gebruiker te kunnen koppelen werd het met behulp van een cookie aan de browser van de gebruiker gekoppeld.

Later herkende de reclame-industrie dat het met behulp van cookies niet alleen mogelijk is om boodschappen aan een gebruiker te koppelen, maar bijna zijn volledig gedrag op het internet. Door internetgebruiker te pas en te onpas op het internet te tracken kan een profiel van de gebruiker worden aangemaakt. Deze profielen kunnen bijvoorbeeld van reclameaanbieder worden gebruikt die op basis van deze informatie de meest geschikte reclame voor een gebruiker kan kiezen.

Tracking heeft vanwege het inzet voor marketingdoeleinden bij gebruikers een negatieve connotatie maar is aan de ander kant voor sommige gebruikers wenselijk. Door het tracken van een gebruiker kunnen inhouden op het internet aan de hand van zijn vastgesteld profiel worden aanbevolen. Het is belangrijk dat de gebruiker voor ieder vorm van tracking en bij ieder tracker een keuze heeft.

Zoals eerder beschreven is er een nieuw "cookiewet" (artikel 11.7a Tw) in Nederland dat het voor trackers moeilijker maakt om gebruikers via cookies te volgen. Maar cookies zijn bij lange niet de enige mogelijkheid om internetgebruikers te kunnen identificeren. Binnen dit hoofdstuk zullen we meerdere technieken bekijken die een identificatie op het internet mogelijk maken. Aan het eind van het hoofdstuk kunnen we concluderen dat artikel 11.7a Tw. waarschijnlijk onvoldoende is om tracking te voorkomen. Toch is de nieuwe wet een stap in de goede richting. De wetgever signaleert dat het niet toegestaan is om internetgebruikers zonder hun weten te tracken en dat het nodig is dat gebruikers meer mogelijkheden krijgen om hun privacy op het internet zelf te beschermen.

4.1 Algemeen

Een trackingtechniek is binnen dit kader een techniek die het mogelijk maakt om internetgebruikers te kunnen identificeren of op een andere manier informatie over internetgebruikers te kunnen verzamelen. Er zijn veel trackingtechnieken en het is onmogelijk om ze allemaal de beschrijven omdat niet eens bekend is op welke manier tracking allemaal wordt toegepast. De meeste trackers zullen niet zeggen hoe ze de gebruikers precies volgen. Daarom zijn binnen dit hoofdstuk alleen bekende technieken beschreven wat dus niet betekent dat de lijst met de onderstaande technieken volledig is.

Zoals al bij de eigen definitie van tracking (hoofdstuk 3.3) aangeduid, kan tracking ook buiten het internet plaatsvinden. Een klantenkaart van een winkel werkt op dezelfde manier als een cookie. De klant krijgt een uniek nummer en zijn boodschappen worden

aan zijn profiel gekoppeld. Het maakt niet uit of de klantenkaart anoniem is of niet, in beide gevallen krijgt de winkel een beeld welke producten klanten samen met ander producten kopen. Op die manier kan een winkel zo ingericht worden dat de klant naast de aanbiedingen makkelijk producten vindt en koopt die hij ook interessant vindt en waarvoor hij anders niet gekozen had. Als de klantenkaart niet anoniem is, heeft de winkel bovendien de mogelijkheid om klanten met specifieke aanbiedingen te winkel in te lokken. Maar zoals eerder aangegeven, focust deze scriptie niet op trackingtechnieken buiten het internet.

4.2 Tracking met IP adressen

Omdat ieder randapparatuur een IP-adres toegewezen krijgt, biedt het zich aan deze voor tracking te gebruiken. Deze paragraaf maakt duidelijk dat tracking met behulp van IP-adressen mogelijk is. Bovendien bevatten IP-adressen in sommige gevallen additionele informatie voor gebruikersprofielen zoals de locatie op die zich de gebruiker bevindt. Omdat de effectiviteit van tracking met behulp van de IP-adres van veel factoren afhankelijk is, zullen IP-adressen vooral in combinatie met ander trackingtechnieken veel potentieel hebben.

Aangezien het gebruik van IPv6 nog niet veel verbreid is, worden binnen deze paragraaf alleen IPv4-adressen behandeld. Maar zoveel is duidelijk: omdat bij IPv6 adressen van 128 bit worden gebruikt, kunnen hiermee veel meer dingen worden geïdentificeerd dan met IPv4 (32 bit). Het potentieel van tracking met IPv6-adressen is daarom nog groter dan van IPv4-adressen.

4.2.1 Algemeen

Ieder randapparaat binnen een netwerk heeft volgens het TCP/IP-protocol zijn eigen IP-adres. Hierdoor kan randapparatuur binnen het netwerk worden geïdentificeerd en het dataverkeer worden gecoördineerd. Dit is vergelijkbaar met een combinatie uit postcode en huisnummer die de postbode helpt de post en pakketjes bij de goede ontvanger af te leveren. De meeste huishoudens krijgen maar één IP-adres waarmee het hele huishouden het internet op gaat. Als binnen een huishouden meerdere computers op het internet aangesloten zijn, gebeurt dit via een thuisnetwerk waarbinnen lokale IP-adressen worden verdeeld. Het externe IP-adres onthult dus alleen welke huishouden en welke servers data uitwisselen, maar niet welke specifieke computer binnen het huishouden met een server communiceert. Bij behavioral advertising dat alleen gebaseerd is op tracking met IP-adressen, zou dus iedereen met dezelfde aansluiting dezelfde reclame krijgen. Als de moeder bijvoorbeeld in laarzen is geïnteresseerd zou ook de zoon reclame voor laarzen ontvangen.

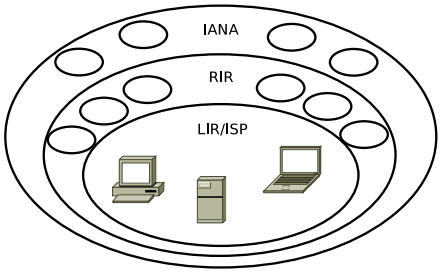
Huishoudens krijgen afhankelijk van de provider dagelijks een nieuwe IP-adres toegewezen. Om deze redenen was het lang twijfelachtig of een IP-adres een persoonsgegeven is. Maar

binnen het proces Scarlet/Sabam heeft het Hof van Justitie van de Europese Unie op 24 november 2011 vastgelegd dat IP-adressen persoonsgegevens zijn:

> "Aangezien [...] IP-adressen de precieze identificatie van die gebruikers mogelijk maken, vormen zij beschermde persoonsgegevens." (par. 51)

Scarlet is een internet service provider (ISP) is die over de NAW-gegevens van haar klanten beschikt. Hiermee is een snelle en directe identificatie van huishouden mogelijk. Aan de ander kant weten ze niet precies welk gezinslid welke handeling uitvoert. Dat geldt ook voor tracker die bovendien niet over de NAW-gegevens beschikken. Toch zijn bewoners van eenpersoonshuishoudens en vaak ook alle gebruikers van meerpersoonshuishoudens door combinatie met andere trackingtechnieken te identificeren.

Naast de identificatie van internetaansluitingen bieden IP-adressen ook nog een andere informatie. Uit IP-adressen laten zich, anders dan bij postadressen, niet meteen locatiegegevens afleiden. Echter worden blokken van IP-adressen centraal van de Internet Assigned Numbers Authority (IANA) verdeeld. De IANA verdeelt de blokken aan vijf Regional Internet Registrys (RIR). Voor Europa en grote delen van Asia is het Réseaux IP Européens Network Coordination Centre verantwoordelijk. Een RIR verdeelt vervolgens weer delen van de aan hem toegewezen blokken aan Local Internet Registrys. De uiteindelijke toewijzing van een IP-adres aan een internetaansluiting wordt dan door de ISP doorgevoerd.



Figuur 3: Veredeling van IP-adressen

4.2.2 Lokalisering

IP-adressen geven in eerste instantie de lagen van het netwerk weer. Maar omdat IP's onderverdeeld worden, kan vaak met een afwijking van enkele kilometers worden vastgelegd waar iemand zich bevindt die een vaste internetverbinding gebruikt. Tijdens het schrijven van dit gedeelte van de scriptie zit ik op de Radboud Universiteit in Nijmegen. Er zijn websites die informatie laten zien die zij uit een IP-adres en hieraan gekoppelde derde informatie kunnen afleiden. Een van de websites is http://whatismyipaddress.com. Hier krijg ik de volgende informatie over de aan mij toegewezen IP-adres:

IP Information: 131.174.132.35

ISP: UCI - Radboud University Nijmegen

Organization: UCI - Radboud University Nijmegen

Connection: Broadband

Services: None Detected

City: Nijmegen

Region: Gelderland

Country: Netherlands

Zo te zien is het mogelijk een IP-adres van de Radboud Universiteit meteen te identificeren, omdat de Radboud Universiteit een eigen ISP heeft. Het kan daarom ook worden afgeleid waar zich iemand bevindt die een IP-adres van de Radboud Universiteit heeft. Dit is natuurlijk alleen het geval als diegene op het lokale netwerk zit en zich niet van buiten via VPN, SSH of dergelijke op het netwerk ingelogd heeft.

Voor zover bekend is de lokalisering van mobile randapparatuur moeilijker omdat ze hun IP onafhankelijk van de locatie random uit een pool van beschikbare IP-adressen krijgt.

Als IP-adressen informatie over de verblijfplaats van een persoon bevatten, kan dit voor tracking worden gebruikt. Voor behavioral advertising wordt het op die manier bijvoorbeeld mogelijk om regionale of zelfs lokale reclame aan te bieden. Een klein bedrijf zou zo ervoor kunnen kiezen om alleen binnen het afzetgebied reclame te maken. Maar ook globaal gezien kan de locatie van een internetaansluiting interessant zijn. Nederlanders hebben bijvoorbeeld andere interesses en over het algemeen meer geld dan mensen in ontwikkelingslanden. Het bovenstaande IP-adres laat bovendien zien dat de gebruiker student of medewerker van de Radboud Universiteit moet zijn. Hieruit kan met grote waarschijnlijkheid worden afgeleidt dat de gebruiker wetenschapper is. Deze aanname geldt niet voor niet-wetenschappelijke medewerkers van de universiteit die een kleiner deel uitmaken dan studenten en wetenschappelijke medewerkers. Veel grote bedrijven hebben een eigen ISP. De IP-adressen van deze bedrijven kunnen daarom soortgelijke informatie prijsgeven.

Zoals al eerder uitgelegd, worden voor internetaansluitingen van particulieren meestal geen vaste IP-adressen verdeeld maar wisselende IP-adressen. Hierdoor kan minder informatie uit de IP-adres worden afgeleid. Ik heb de bovenstaande test nog een keer in Duitsland op een particuliere internetaansluiting uitgevoerd met het volgende resultaat:

IP Information: 77.182.0.186

ISP: Telefonica Germany

Organization: Telefonica Germany

Connection: Broadband

Services: None Detected

City: Attendorn

Region: Nordrhein-Westfalen

Country: Germany

Uit de ISP laat zich in dat geval duidelijk minder informatie afleiden, namelijk alleen dat de aansluiting één van rond 24 miljoen aansluitingen van de provider O_2 (een dochteronderneming van Telefonica Germany) is. Bovendien klopt de aangegeven locatie (Attendorn) niet. Ze wijkt in deze steekproef rond 30 kilometer af van de eigenlijke locatie (Siegen).

4.2.3 Conclusie

Gebruikers kunnen met IP-adressen worden gelokaliseerd en geïdentificeerd. Dit geldt in het bijzonder voor eenpersoonshuishoudens. Bovendien zijn gebruikers van de meeste mobiele randapparatuur binnen een sessie identificeerbaar omdat mobiele randapparatuur meestal maar door één gebruiker benut wordt en een externe IP-adres toegewezen krijgt. In dat geval wordt dus zoals bij een eenpersoonshuishouden één IP-adres aan één unieke gebruiker toegewezen. Binnen een sessie waar het IP-adres normaal gesproken niet veranderd, kan van deze personen een profiel worden aangelegd. Later zal duidelijk worden dat IP-adressen in combinatie met ander trackingtechnieken veel kunnen bijdragen aan de identificatie van een gebruiker. Bijvoorbeeld In combinatie met device fingerprinting (hoofdstuk 4.5) kunnen ook profielen van gebruikers met gedeelte IP-adressen worden aangelegd.

4.3 Tracking met cookies

Er zijn meerdere type cookies om het gedrag van internetgebruikers te analyseren. Meestal worden er drie types cookies onderscheiden: gewone (first party) cookies, third party cookies en local shared objects (LSOs).

4.3.1 First party cookies

First-party cookies worden van oudsher functioneel ingezet om het gebruiksgemak te bevorderen. Ze ondersteunen de communicatie tussen de gebruiker en de server van de website. First-party cookies worden bijvoorbeeld gebruikt bij webwinkels waar de gebruiker een virtueel winkelmandje krijgt. De cookie is nodig omdat de winkel een onaangemelde gebruiker niet kan identificeren. Via de cookie wordt het winkelmandje aan de browser van de gebruiker gekoppeld. Een tweede toepassing van first-party cookies zijn websites waar een gebruiker zich moet aanmelden. Vaak is een koppeling aan een cookie vereist om te voorkomen dat de gebruiker zich bij ieder handeling waarvoor hij aangemeld is, opnieuw moet identificeren. Het studentenvolgsysteem OSIRIS van de Radboud Universiteit Nijmegen is een voorbeeld van een website met aanmelding. Een deel van de cookie kan als volgt eruit zien:

Basisdomein: ru.nl

Naam: OSI_STU_LOGIN

Inhoud: username:3017095&

Host: sis.ru.nl

Pad: /student/

Verloopt: 1368038891 *(unix timestamp voor 8 mei 2013, 20:48:11)*

In de cookie staat dus informatie over de domein en de pad waarop hij geldig is, de unieke identificatiecode (onder “inhoud”), wie de websitehost is en wanneer de cookie verloopt.

4.3.2 Third party cookies

De tweede groep bestaat uit third-party cookies. Deze worden door een ander partij, dan de website of dienst die de gebruiker opvraagt, geplaatst. De derde partij krijgt vervolgens de mogelijkheid om het gedrag van de bezoekers van die website te analyseren. Op deze manier kunnen bijvoorbeeld nieuwssites de mogelijkheid tot het analyseren van het gedrag van hun gebruikers aan trackers verkopen. Vervolgens kan de nieuwssite met behulp van de analyse van de tracker weer zijn aanbod verbeteren en zijn reclameruimte geoptimaliseerd inzetten. Deze vorm van reclame wordt bijvoorbeeld van Wehkamp of Zalando toegepast. Ze tonen reclame voor eerder bekeken producten op websites van derden. De aanpassing van een websites is niet op reclame beperkt en kan ook bij ander onderdelen plaatsvinden. Yahoo claimt bijvoorbeeld dagelijks 13 miljoen verschillende homepagina's met nieuws te laten zien[21] die aangepast zijn op het profiel van ieder afzonderlijke bezoeker.

Omdat third-party cookies meestal geen directe meerwaarde voor de gebruiker bieden en invloed op zijn privacy hebben, blokkeren sommige browsers third-party cookies standaard. De meeste andere browsers bieden ook de mogelijkheid om third-party cookies zelf uit te schakelen. Maar Dilger beschrijft hoe Google van third-party cookies gebruik kon maken hoewel Safari, met zijn standaardinstellingen geen third-party cookies toelaat. Door een zo genoemde webbaken werd het voor Google mogelijk op sites van derde partijen het gedrag van internetgebruikers te observeren (vgl. [15]). Hiervoor werd gebruik gemaakt van een kleine, 1x1 pixel grote, transparante afbeeldingen (webbakens). Een website die tracking via webbaken mogelijk wil maken, laadt hiervoor tijdens het opnenen een afbeelding van de tracker. Hierdoor wordt het volgens Köhntopp mogelijk meerdere gegevens waaronder cookies door te sluizen (vgl. [3]). Deze manier van tracking werkt vanzelfsprekend niet alleen met kleine, onzichtbare afbeeldingen maar ook met grote reclamebanners die van trackers als DoubleClick ter beschikking worden gesteld.

Webbakens kunnen niet alleen op websites worden ingezet maar ook in HTML-Mails. Hiervoor wordt een kleine afbeelding in bijvoorbeeld een reclamemail ingevoegd. Vervolgens kan de afzender of een derde partij die de afbeelding ter beschikking stelt, zien wanneer de afbeelding afgeroepen wordt en dus of en wanneer de gebruiker de mail geopend heeft.

4.3.3 Local shared objects

Nog een andere vorm van cookies, zogenaamde evercookies, bieden nog meer mogelijkheden dan gewone HTTP-cookies. Het principe is hetzelfde maar ze zijn resistenter tegen het verwijderen door de gebruiker. Door gebruik te maken van flash kunnen andere opslaglocaties worden gebruikt dan voor gewone cookies. Als gebruikers met gewone middelen cookies verwijderen, worden alleen de cookies op de gebruikelijke locaties verwijderd, maar niet de evercookies die op een atypische plek zijn opgeslagen. Na het verwijderen van de gewone cookies kunnen deze met informatie uit evercookies weer worden hersteld.

Deze eigenschappen worden vooral voor tracking gebruikt. Voor een website zal het niet nodig om zijn gebruikers per se te kunnen herkennen maar voor trackers heeft dit een enorme toegevoegde waarde. Met evercookies kunnen handelingen op het internet gemakkelijker bij gebruikers worden geplaatst dan met gewone cookies die sommige gebruikers regelmatig verwijderen.

4.3.4 Conclusie

Met behulp van cookies kan bepaalde functionaliteit van websites worden gerealiseerd. Naast de toepassingen (winkelmandjes en identificatie van gebruikers binnen een besloten bereik) zijn er nog talloze andere functionaliteiten te bedenken die met behulp van cookies kunnen worden geïmplementeerd. Veel gebruikers zijn in eerste instantie sceptisch als ze ervaren dat cookies worden ingezet. Deze scepsis is voor functioneel ingezette cookies ongegrond. Maar cookies kunnen ook voor tracking worden ingezet en gebruikers identificeren. Cookies zijn de meestgebruikte en meest bekende trackingtechniek. Daarom worden ze ook zo expliciet in de eerder behandelde wetten en richtlijnen genoemd.

4.4 Sessie IDs

Een andere manier om gebruikers te kunnen identificeren, bieden sessie IDs. Deze werken op een vergelijkbare manier dan cookies maar er worden geen bestanden op de randapparatuur opgeslagen of uitgelezen. Sessie IDs zorgen ervoor dat een gebruiker tijdens een sessie identificeerbaar is.

Ieder van de bovengenoemde vormen van cookies is afhankelijk van een klein gedeelte dat op de randapparatuur van de gebruiker opgeslagen wordt. Als de opslag van cookies om welke reden dan ook onmogelijk is, zou een internetgebruiker dus niet via cookies identificeerbaar zijn. In dat geval kunnen sessie IDs worden gebruikt. Sessie IDs hoeven geen gebruik te maken van cookies en kunnen de voor de identificatie nodige informatie in de URI meegeven. Als een gebruiker dus een website bezoekt, wordt een sessie ID aangemaakt die de gebruiker de hele tijd met zich mee neemt terwijl hij op de site onderweg is. De URI van een website kan dan bijvoorbeeld als volgt eruit zien:

http://www.website.nl/index.php?id=d691a5

In dit voorbeeld is *d691a5* de ID die de gebruiker voor de sessie toegewezen wordt. Als een gebruiker naar een ander pagina op de server gaat, wordt altijd de ID meegegeven zodat het nieuwe onderdeel van de website de gebruiker kan identificeren. Op die manier zou een webwinkel een winkelwagen kunnen implementeren zonder af te dwingen dat de gebruikers zich óf eerst registreren en aanmelden óf een cookie moet worden gebruikt.

Sessie IDs kunnen parallel met ander technieken als cookies worden gebruikt. Het gebruik van het ene sluit het ander niet uit. Als een sessie ID geen parallelle cookie heeft, is ze niet persistent. Ze wordt niet door de browser onthouden en zal daarom na het verlaten van de website vergeten worden. Om te voorkomen dat de sessie door een derde gebruiker kan

worden voortgezet, beëindigen de meeste servers sessies die voor een bepaalde tijd niet gebruikt worden. Een ander mogelijkheid om het overnemen van sessies te voorkomen is het koppelen van de sessie ID aan ander gegevens zoals de IP-adres van de gebruiker.

4.4.1 Conclusie

Sessie IDs bieden veel voordelen. Ze maken een gebruiker zoals cookies identificeerbaar, maar dan alleen voor een bepaalde sessie. Een webwinkel of een andere site waar een gebruiker zich moet aanmelden, zal meestal niet geïnteresseerd zijn in het herkennen van een gebruiker bij een volgende sessie, maar wil de gebruiker alleen tijdens één bezoek kunnen identificeren. Sessie IDs maken deze en andere functionaliteit mogelijk en tasten tegelijkertijd niet verregaand de privacy van de gebruiker aan.

4.5 Tracking met device fingerprints

Bepaalde eigenschappen over de randapparatuur en de browser kan met behulp van JavaScript worden opgevraagd. Omdat veel gebruikers niet alleen de standaardfonts en standaardapplicaties gebruiken, maar de randapparatuur bewust of onbewust aanpassen, wordt randapparatuur identificeerbaar. Onbewuste aanpassingen gebeuren bijvoorbeeld met het installeren van programma's die eigen fonts gebruiken en daarom nieuwe systeemfonts installeren zoals tekstverwerkers. Het is verbazingwekkend hoe snel een computer uniek eigenschappen heeft. De EFF heeft heeft Panopticlick[3] ontwikkelt waarmee gebruikers kunnen zien hoe uniek hun randapparatuur is.

Panopticlick vraagt met JavaScript de volgende informatie af:

- User Agent
- HTTP_ACCEPT headers
- Browser plug-in details
- Tijdzone
- Resolutie en Kleurendiepte van de beeldscherm
- Systeemfonts
- Of cookies door de browser worden toegestaan

Van de gebruikers die tot nu toe met Panopticlick de uniekheid van hun instellingen hebben laten onderzoeken, gebruikten ongeveer 85%[4] unieke instellingen. Hun randapparatuur was dus eenduidig identificeerbaar zonder gebruik te maken van ander trackingtechnieken.

[3] https://panopticlick.eff.org

[4] Het aandeel zal nog verder omlaag gaan als meer gebruikers deze test doorvoeren en hiermee hun gegevens aan de projectdatabase toevoegen. (Bron: https://panopticlick.eff.org/faq.php, stand: 5 juli 2012)

4.5.1 Combinatie

Gecombineerd met andere gegevens, zoals een IP-adres is het met een device fingerprint vaak mogelijk om een gebruiker eenduidig te identificeren. IP-adressen en device fingerprints vullen elkaar ideaal aan. De IP-adres helpt om de huishouden van de gebruiker te identificeren en de device fingerprint om de eindapparatuur binnen de huishouden te identificeren. Ervan uitgaande dat niet iedereen in de huishouden dezelfde eindapparatuur met dezelfde instellingen gebruikt, worden gebruikers door een combinatie van device fingerprints en het toegewezen IP-adres eenduidig identificeerbaar.

4.5.2 Entropie

Uniekheid is met behulp van entropie meetbaar. Entropie geeft de mate van informatiedichtheid aan. Als eenheid voor informatiedichtheid wordt meestal 'bits' gekozen. Om alle mensen op de wereld te kunnen identificeren hebben en ongeveer 33 bits informatie van iemand nodig. Dit komt omdat er ongeveer 6,79 miljard mensen op de wereld leven en 33 bits 8 miljard verschillende toestanden mogelijk maken.

Om iemand te kunnen identificeren moeten we eigenschappen van diegene weten. Hierdoor wordt entropie verkleint. Eckersley[16] definieert de verkleining van entropie als volgt:

$$\Delta S = -\log_2 \mathbb{P}(X = x) \text{ (baserend op de Shannon entropie[6])}$$

$\mathbb{P}(X = x)$ is in dat geval de kans om iemand met deze eigenschappen eenduidig te identificeren.

Het rekenen met entropie wordt aan de hand van een klein voorbeeld duidelijker: als we een Nederlandse vrouw zoeken die in januari 2012 naar Nijmegen verhuisde en haar geboortedag weten zou ze theoretisch bijna eenduidig identificeerbaar zijn:

Nederland had 2011 een bevolking van 16.655.799 mensen[5]. Om iedereen te kunnen identificeren zouden we rond 24 bits ($2^{24} = 16.777.216$) informatie nodig hebben.

Vervolgens berekenen we de verkleining van de entropie veroorzaakt door de eigenschappen die we over de persoon weten:

- Er leven 8.412.317 vrouwen in Nederland[6]:
  - $\Delta S = -\log_2 \mathbb{P}(\frac{8.412.317}{16.655.799}) \approx 0,99$ bits
- Nijmegen heeft 165.253 inwoners[7]:
  - $\Delta S = -\log_2 \mathbb{P}(\frac{165.253}{16.655.799}) \approx 6,66$ bits

[5] Bron: Centraal Bureau voor Statistiek
[6] Bron: Centraal Bureau voor Statistiek
[7] Bron: Buurtmonitor (ABF Research)

- In jan 2012 zijn in Nijmegen 79.628 mensen verhuisd[8]:
  - $\Delta S = -\log_2 \mathbb{P}(\frac{79.628}{16.655.799}) \approx 7,71$ bits
- Ieder jaar heeft 365 mogelijke geboortedatums, en ieder vierde jaar is een schrikkeljaar met één dag meer[9]:
  - $\Delta S = -\log_2 \mathbb{P}(\frac{1}{365,25}) \approx 8,51$ bits
- **Totaal:** $\Delta S \approx 23,87$ *bits*

Dit voorbeeld maakt duidelijk hoe iemand aan de hand van een aantal eigenschappen kan worden geïdentificeerd. In het voorbeeld is weliswaar de naam van de persoon niet bekend maar we weten dat een persoon met deze eigenschappen theoretisch uniek is. Hetzelfde geldt bij device fingerprinting. Vaak zijn de naam of ander gegevens van de gebruiker onbekend, maar voor doeleinden als behavioral advertising zal dat niet uitmaken. Het is belangrijk dat de gebruiker naar aanleiding van zo efficiënt mogelijke reclame iets koopt. Reclame wordt efficiënt als ze toegepast is op interesses die uit geobserveerde eigenschappen kunnen worden afgeleid.

4.5.3 Conclusie

De effectiviteit van device fingerprinting is in zekere mate afhankelijk van de gebruiker en de randapparatuur. Vooral op mobiele randapparatuur zal device fingerprinting ineffectief zijn omdat deze minder instellingsmogelijkheden heeft dan een computer. Het besturingssysteem, de standaardbrowser, de fonts en de resolutie worden meestal niet door de gebruiker aangepast. Daarom is mobiele randapparatuur zelden uniek. Computers en laptops daarentegen zijn goed met device fingerprinting en nog beter in combinatie met de IP-adres identificeerbaar.

4.6 Tracking met buttons van social media

Een andere manier voor tracking zijn de Like buttons van Facebook of vergelijkbare buttons. Ze worden vrijwillig door veel sitebeheerders op hun sites gezet. Volgens Roosendaal[5] is het voor Facebook mogelijk om te kijken welke sites zijn aangemelde gebruikers en zelfs zijn toekomstige gebruikers bezoeken.

Als een Facebook-gebruiker van Like buttons gebruik maakt, wordt dit aan zijn vrienden meegedeeld. Omdat de knop altijd aan Facebook moet vragen of de gebruiker aangemeld is en al aangegeven heeft of die iets leuk vindt, kan de knop vanuit de site waarop die staat met Facebook communiceren. Facebook kan dus bijhouden welke websites door gebruikers worden bekeken. Roosendaal heeft bovendien vastgesteld dat niet alleen surfprofielen

[8] Bron: Centraal Bureau voor Statistiek

[9] Dit is een schatting ervan uitgaande dat op ieder dag van het jaar ongeveer evenveel Nederlanders jarig zijn.

van actieve gebruikers maar ook van toekomstige gebruikers worden aangemaakt. Via een cookie wordt eerst het gedrag bijgehouden en als de gebruiker later een account bij Facebook aanmaakt kan Facebook de met de cookie verzamelde informatie en aan de nieuwe gebruikersaccount koppelen. Deze vorm van tracking kan natuurlijk niet alleen van Facebook worden toegepast maar ook van ander social media.

4.6.1 Conclusie

Tracking door social media heeft een groot potentieel en er is minder bekend dan het gewone tracking met bijvoorbeeld cookies. Uit de gebruikersaantallen wordt duidelijk welk potentieel tracking door social media heeft. In maart 2012 waren er 901 miljoen gebruikers per maand actief op Facebook [10]. 170 miljoen gebruikers hadden in april 2012 een Google+ account[11].

Tracking via social media buttons haakt in op de trend van social media-gebruik. Veel websitebeheerders installeren ze om hun website bekender te maken en om met de trend mee te gaan zonder zich ervan bewust te zijn dat op die manier hun gebruikers worden geobserveerd.

4.7 Tracking door browseraanbieders

Voor aanbieders van browsers is er nog een andere mogelijkheid om gebruikers te kunnen volgen. Ze kunnen het hele dataverkeer via een centrale server bundelen en door deze bundeling per browser opslaan welke sites bezocht worden wat de gebruiker op de websites doet.

Het bundelen van het hele dataverkeer is bij typische browser niet gebruikelijk en zal waarschijnlijk ook niet door de gebruiker worden geaccepteerd. Een browser van die bekend is dat hij wel van deze techniek gebruik maakt is de mobile browser van Opera.

4.7.1 Conclusie

Tracking door browseraanbieders kan meestal alleen worden voorkomen als de gebruiker een alternatieve browser gaat gebruiken. Later zal duidelijk worden dat er geen add-ons bestaan die deze vorm van tracking kunnen blokkeren omdat de browser ongeacht ieder script of add-on de hele dataverkeer moet kunnen inzien om een website weer te kunnen geven. De gebruiker bevestigt voor het gebruiken van een browser de gebruikersvoorwaarden, maar dat betekent meestal niet dat hij de gebruikersvoorwaarden ook gelezen heeft. Daarom zullen er veel gebruikers zijn, die zich niet bewust zijn dat ze de hele tijd door hun browser gevolgd worden. Daarom zou het fijn zijn als gebruikers van browsers die tracking toepassen expliciet hierop worden gewezen.

[10] https://newsroom.fb.com/content/default.aspx?NewsAreaId=22
[11] http://googleblog.blogspot.de/2012/04/toward-simpler-more-beautiful-google.html

4.8 Conclusie

Er zijn veel meer trackingtechnieken dan de veel bediscusseerde cookies. Cookies, IP-adressen en JavaScript hadden initieel alleen een technische functie. In de loop van de tijd heeft er *function creep* plaatsgevonden. Adverteerders herkenden het potentieel van deze technieken en weten hoe ze deze voor tracking kunnen inzetten. Om terug te komen op het schema van de EU-studie uit hoofdstuk 3.6.6, vindt er een shift plaats van de kwadrant links boven naar de kwadrant links onder. Er vindt veel innovatie op het internet plaats, maar deze onderschept vaak de privacy van de gebruiker. Terwijl men van cookies theoretisch nog afstand zou kunnen doen en ze voor de functionaliteit door sessie IDs kunnen worden vervangen, zijn er ander technieken waarvan moeilijk afstand kan worden gedaan. Een voorbeeld zijn IP-adressen die volgens het TCP/IP-protocol nodig zijn voor dataverkeer via het internet.

Dit hoofdstuk zal duidelijk maken dat er veel mogelijkheden zijn om tracking toe te passen en dat het daarom nodig is dat de gebruiker een mogelijkheid moet krijgen om ongewenste vormen van tracking te weigeren. De in hoofdstuk 3.6.5 beschreven artikel 11.7a Tw. is al een stap in de goede richting, maar geeft de gebruiker nog geen garantie.

Uit dit hoofdstuk mag niet worden geconcludeerd dat bepaalde technologie moet worden verboden of door andere technologie moet worden vervangen die privacyvriendelijker is. Als bepaalde technologie wordt verboden zal in de toekomst weer nieuwe technologie voor tracking worden misbruikt. Veel belangrijker is het om de *function creep* te stoppen die optreedt omdat met tracking veel geld kan worden verdiend.

5 Trackingblockers

5.1 Algemeen

Binnen deze scriptie worden technieken die het voorkomen van tracking ondersteunen onder het begrip trackingblocker samengevat. Dit hoofdstuk focust zich op technieken die de in hoofdstuk 4 beschreven trackingtechnieken blokkeren en door de gebruiker zelf kunnen worden ingezet. Een voorbeeld voor een niet onderzochte trackingblocker is de jQuery plug-in socialshareprivacy[12] die door de Artikel 29 werkgroep aanbevolen wordt (zie hoofdstuk 3.6.5). Deze plug-in kan alleen door websitebeheerder worden gebruikt maar niet door gebruikers.

Voor de analyse van de trackingblockers wordt op resistente trackingtechnieken geattendeerd. Bovendien wordt het nut voor softwareaanbieders vastgesteld om gratis trackingblockers zoals Do Not Track Plus of Ghostery ter beschikking te stellen.

5.1.1 Resistente trackingtechnieken

Zoals in hoofdstuk 5.8 samengevat, is er geen trackingblocker die ieder vorm van tracking kan voorkomen. Er zijn zelfs trackingtechnieken die erg resistent zijn tegen trackingblockers zoals de browsers die het hele dataverkeer via een server bundelen (vgl. hoofdstuk 4.7). In dat geval is het inzetten van browserplug-ins nutteloos omdat de server onafhankelijk van eventueel geïnstalleerde trackingblockers ieder browser kan identificeren en dus tracken.

Een niet verder uitgewerkte maar toch potentiële en grotendeels resistente vorm van tracking bieden GUIDs. Als de mogelijkheid bestaat om via het internet een GUID van een onderdeel van de randapparatuur uit te lezen, kan de gebruiker hiermee worden geïdentificeerd. Het is meestal niet mogelijk om een GUID naderhand te wijzigen. Ze is zoals een burgerservicenummer een identificatienummer die de hardware voor zijn hele "leven" krijgt. Hierdoor wordt het mogelijk om een terugkomende computer te herkennen. Omdat het voor de gewone gebruiker niet mogelijk is om een applicatie op onderdelen van de hardware te installeren, die de GUID alleen maar aan bepaalde, zelf gekozen partijen weergeeft, is tracking met behulp van een GUID resistent tegen ieder binnen deze scriptie onderzochte trackingblocker.

5.1.2 Het nut voor aanbieders

Er zijn aanbieders die trackingblockers gratis ter beschikking stellen. De vraag die hierbij opkomt, is wat het nut voor deze aanbieders is als ze noch geld voor het downloaden noch voor het gebruik vragen. Om dit op te helderden, heb ik contact opgenomen met Abine de producent van Do Not Track Plus, dat in hoofdstuk 5.3 verder beschreven wordt.

[12] http://www.heise.de/extras/socialshareprivacy/

Mijn eerste vermoeden was dat deze programma's ieder vorm van tracking blokkeert, behalve tracking door het programma zelf. Deze exclusieve trackingmogelijkheid zou de producent van de software door kunnen verkopen om op die manier geld te verdienen. Volgens Abine (vgl. Appendix A) is dat bij Do Not Track Plus niet het geval. De enige gegevens die volgens hun worden opgeslagen zijn de instellingen van de gebruiker en deze worden lokaal op de computer van de gebruiker en niet bij Abine of derden opgeslagen en zijn alleen voor de gebruiker zichtbaar.

Dit wordt in hun privacybeleid bevestigt: *"Abine will not track, store or transmit to any server or third party, information regarding users' behavioral data (to include web browsing activity), nor will we "deliver or help others deliver any targeted advertising to users"*[13]. Kort gezegd volgt Abine zijn gebruikers niet en laat zijn gebruikers ook niet door derden volgen.

Nu zijn de bewering van Abine dat door hun programma geen tracking plaatsvindt en het privacybeleid nog geen bewijs. Maar het is mogelijk om het dataverkeer tussen de eigen computer en Abine te observeren. Volgens Abine is het enige verkeer tussen hun en de eindapparatuur een dagelijkse update van de blockeringsregels. Verder wordt er geen informatie met Abine uitgewisseld.

Nu we weten dat Abine niet zelf tracking toepast, blijft nog steeds de vraag wat het nut is om gratis software ter beschikking te stellen. Hierover zegt Abine dat het hun missie is om gebruikers de controle over hun eigen privacy terug te geven. Financieel gezien is er nog een ander aspect die Abine's kosteloze service verklaart. Abine wil met Do Not Track Plus meer naamsbekendheid krijgen en tevreden gebruikers binden in de hoop dat deze betere, betaalde producten kopen.

Het nut voor aanbieders van gratis trackingblockers is dus hetzelfde als voor de meeste andere aanbieders van gratis software: naamsbekendheid. De naamsbekendheid biedt mogelijkheden om andere producten te verkopen.

5.2 No Script

No Script is een add-on voor Mozilla Firefox en slechts één van de vele add-ons die het mogelijk maken om bepaalde scripts door de browser te laten blokkeren. Voor Safari bestaat bijvoorbeeld de add-on JavaScript Blocker. Voor Google Chrome bestaat bijvoorbeeld de add-on NotScripts. Met No Script kan tracking door middel van webbakens en buttons van social media worden voorkomen. Bovendien is het mogelijk om device fingerprinting praktisch te voorkomen.

5.2.1 Werkwijze

No Script maakt het mogelijk om JavaScript, Java, Flash, Silverlight en andere plug-ins te deactiveren. De add-on biedt veel instellingsmogelijkheden. De belangrijkste instelling

[13] http://www.abine.com/about.php

is welke type scripts de gebruiker daadwerkelijk wil deactiveren. Bovendien heeft de gebruiker de keuze alle boven genoemde type scripts consequent te deactiveren, tijdelijke toestemmingen voor bepaalde domeinen te geven of plug-ins van bepaalde domeinen altijd te activeren.

Omdat webbakens en social media buttons meestal met behulp van JavaScript worden geladen, is het mogelijk om ze met behulp van No Script te blokkeren. Omdat No Script onderscheid kan maken tussen de domein van een website en derde domeinen, hoeft de gebruiker niet eens afstand te doen van bepaalde met JavaScript geïmplementeerde functionaliteit op de website.

Voor het afroepen van de meeste attributen die voor device fingerprinting worden gebruikt is JavaScript nodig. Zonder JavaScript kunnen alleen de user agent en HTTP_ ACCEPT headers worden opgevraagd maar niet details over browserplug-ins, tijdzone, resolutie en kleurendiepte van de beeldscherm en systeemfonts. Hierdoor wordt de uniekheid van de randapparatuur zo klein dat device fingerprinting praktisch onmogelijk wordt.

5.2.2 Evaluatie

De standaardinstellingen van No Script zijn heel streng wat het toelaten van plug-ins betreft. Het instellen van het gewenste niveau van blokkering vraagt tijd en moeite. Hierdoor kunnen gebruikers snel gefrustreerd raken, met als gevolg dat ze de add-on deactiveren.

No Script kan afhankelijk van de instellingen een aantal trackingtechnieken voorkomen, maar er zijn ook technieken waartegen No Script niet bestendig is. Hierbij horen onder meer tracking met IP-adressen en cookies en tracking door middel van browseraanbieders.

We kunnen concluderen dat No Script op het gebied van tracking maar een deeloplossing biedt. No Script heeft aan de ander kant een positief bijeffect. Door scripts en plug-ins te blokkeren, wordt de beveiliging van de computer beter omdat geen schadelijke scripts kunnen worden gedraaid.

5.3 Do Not Track Plus

Do Not Track Plus is een add-on die gratis wordt aangeboden door Abine. De add-on is compatibel met de browsers Chrome, Firefox, Safari, en Internet Explorer. Met Do Not Track Plus wordt communicatie met bekende trackers en bekende adverteerders die op een zwarte lijst staan, geblokkeerd.

5.3.1 Werkwijze

De werkwijze van Do Not Track Plus komt gedeeltelijk overeen met de werkwijze van No Script. Do Not Track Plus blokkeert actief de communicatie met trackers die op een zwarte lijst staan. Anders dan bij No Script wordt doelgerichter geblokkeerd. Het

voordeel hiervan is dat Do Not Track Plus geen negatieve invloed op de functionaliteit van een website heeft. Do Not Track Plus zorgt niet alleen voor het blokkeren van tracking, maar ook voor het blokkeren van gepersonaliseerde reclame. Met Do Not Track Plus kan dus tracking met third party cookies, social media buttons en behavioral advertising worden voorkomen.

5.3.2 Evaluatie

Do Not Track Plus wantrouwt zoals de meeste trackingblockers webservers. Door de actieve blokkering van inhouden van bepaalde derde partijen biedt Do Not Track Plus zijn gebruikers de mogelijkheid om zelf iets tegen tracking te kunnen doen.

De werkwijze van Do Not Track Plus voorkomt zowel tracking als ook behavioral advertising mits de tracker of adverteerder bekend is. Maar iedereen die niet op de zwarte lijst van Abine staat, wordt ook niet geblokkeerd. Dit is dus een van de zwakke punten van Do Not Track Plus. Verder focust Do Not Track Plus zich vooral op tracking met cookies en social media buttons. Anders dan bij No Script zal tracking met behulp van device fingerprinting wel mogelijk zijn.

Doordat Do Not Track Plus over het algemeen minder blokkeert dan No Script en bovendien doelgericht blokkeert zal het door veel gebruikers als gebruiksvriendelijker worden ervaren. Met de standaardinstellingen zal zich het zichtbare gedrag van de browser en de weergave van website nauwelijks veranderen. Do Not Track Plus blokkeert tracking op het achtergrond en laat via een icon in de browserwerkbalk zien hoeveel er actueel geblokkeerd wordt.

5.4 Ghostery

Ghostery wordt zoals Do Not Track Plus gratis aangeboden en is als add-on voor Chrome, Firefox, Safari, en Internet Explorer beschikbaar. Bovendien is Ghostery compatibel met Opera en iOS. Ghostery wordt aangeboden door Evidon. De add-on is in principe een grote broer van Do Not Track Plus omdat ze bijna hetzelfde doet maar iets meer keuzemogelijkheden biedt.

5.4.1 Werkwijze

Opvallend is dat bij Ghostery in eerste instantie alle filters gedeactiveerd zijn. De gebruiker wordt na de installatie gevraagd welke inhoud van derde partijen en welke cookies geblokkeerd moeten worden. Hiervoor start Ghostery na de installatie een instellingsassistent op.

Anders dan Do Not Track Plus onderscheidt Ghostery de trackers en de cookies in meerdere categorieën. Derde partijen worden ingedeeld in *reclame*, *analyse*, *privacy*, *trackers* en *widgets*. Cookies worden ingedeeld in *reclame*, *analyse*, *trackers* en *widgets*.

De gebruiker kan dus met minder moeite bepalen of alleen bepaalde cookies of inhoud van derde partijen zullen worden.

Ghostery geeft de mogelijkheid om geanonimiseerd gegevens ter beschikking te stellen. Deze gegevens worden voor GhostRank gebruikt. Met behulp van deze gegevens zal de add-on verder worden verbeteren. Volgens het privacybeleid[18] van Ghostery worden met behulp van GhostRank nieuwe trackers op het internet gezocht, de prestatie van de add-on geanalyseerd en statistische berekeningen doorgevoerd. Het gebruik van GhostRank is vrijwillig wordt alleen door opt-in geactiveerd. Volgens het privacybeleid worden de gegevens van GhostRank nooit voor reclamedoeleinden gebruikt.

Na de installatie en activering van de blokkering valt bij Ghostery op dat de add-on in tegenstelling tot Do Not Track Plus pop-ups in de voorgrond laat zien. Anders dan Do Not Track Plus toont Ghostery standaard naast de icon in de browserwerkbalk voor 15 seconden een pop-up aan de rechter bovenkant met de namen van de trackers en cookies zien die er actueel wel of niet door Ghostery worden geblokkeerd. Deze pop-up meldingen zijn voor veel gebruikers oninteressant en laten zich gemakkelijk in de instellingen deactiveren.

5.4.2 Evaluatie

Uit de beschrijving van de werkwijze wordt duidelijk dat Ghostery een soortgelijk product is als Do Not Track Plus. Ghostery blokkeert dezelfde vormen van tracking als Do Not Track Plus en biedt meer instellingsmogelijkheden en functionaliteit. Aan de ander kant moet Ghostery na de installatie eerst worden ingericht en blokkeert in eerste instantie helemaal niets. Daarom is Ghostery minder gebruiksvriendelijk dan Do Not Track Plus. Bovendien trekt Ghostery met zijn pop-ups iets meer aandacht dan sommige gebruikers wensen.

Een voordeel van Ghostery ten opzichte van Do Not Track Plus is de mobiele browser voor iOS. Hiermee is Evidon naast het W3C de organisatie binnen deze scriptie die zich ook op mobiele randapparatuur richt. Een nadeel aan de Ghostery-browser is dat hij standaard net zoals de browseradd-on niets blokkeert en alle ongewenste trackers in het begin een keer moeten worden ingesteld. Een ander nadeel is dat de Ghostery-browser op dit moment alleen met iOS compatibel is.

5.4.3 Vergelijking met Do Not Track Plus

Omdat nu meerdere keren duidelijk gemaakt werd dat Do Not Track Plus en Ghostery vergelijkbaar zijn, kunnen we concluderen dat het zinvol is maar één van de twee add-ons te gebruiken. Het indelen van trackers en cookies in categorieën is voor de meeste gebruikers overbodig gespeel. Tijdens het testen[14] van beide add-ons viel op dat het aantal

[14] De tests zijn niet wetenschappelijk gefundeerd en gewoon steekproefgewijze observaties uit het alledaagse leven.

geblokkeerde trackers van beide add-ons meestal ongeveer even groot was maar Ghostery in de meeste gevallen aangaf iets meer te blokkeren. Hieruit kan worden geconcludeerd dat Ghostery waarschijnlijk iets effectiever is dan Do Not Track Plus. Aan de ander kant is Ghostery minder gebruiksvriendelijk.

Voor gebruikers die de meeste vormen van tracking willen voorkomen maar daar weinig moeite in wil steken zal Do Not Track Plus de betere keuze zijn. Gevorderden gebruikers en gebruikers die zich meer met tracking uit elkaar hebben gezet, kunnen beter Ghostery gebruiken omdat ze deze add-on beter op hun behoefden kunnen aanpassen. Gebruikers van mobiele randapparatuur hebben nog geen keuze en kunnen alleen maar Ghostery gebruiken en dat ook alleen maar met iOS.

5.5 AVG

AVG is een grote aanbieder van internetveiligheidssoftware. Ze zijn de eerste bekende aanbieder die eind maart 2012 bekend maakte dat ze in hun actuele en nieuwe producten een trackingblocker ter beschikking stellen[12]. In de toekomst zal andere veiligheidssoftware waarschijnlijk deze stap volgen.

5.5.1 Werkwijze

Volgens het persbericht is het mogelijk met de software van AVG tracking volledig te blokkeren of naar eigen wensen gedeeltelijk toe te laten. Zoals in hoofdstuk 4 uitgelegd, bestaan er veel mogelijkheden om iemand op het internet te volgen. AVG legt in zijn persbericht uit dat hun software reclamenetwerken, social media buttons en tracking door webanalyse herkennen, identificeren en blokkeren kan. De gebruiker kan dus informatie krijgen over de trackers die op een website actief zijn. Aan de hand van deze informatie kan de gebruiker afwegen welke trackers hij wil laten blokkeren en welke niet. Bovendien biedt AVG zijn gebruikers de mogelijkheid om aan websites mee te delen dat ze niet willen worden gevolgd. AVG noemt op haar website verder geen details over de werkwijze van de Do Not Track oplossing.

5.5.2 Evaluatie

AVG zorgt met het nieuwe tool voor de volledigheid van haar internetveiligheidspakket. Gebruikers hoeven niet meer verschillende add-ons te installeren om tracking efficiënt te kunnen voorkomen, maar krijgen hiervoor standaard tools aangeleverd. Do Not Track van AVG voorkomt reclamenetwerken, social media buttons en tracking door webanalyse dus samengevat dezelfde trackingtechnieken als Do Not Track Plus en Ghostery maar is gebruiksvriendelijker omdat de trackingblocker samen met het standaardpakket geïnstalleerd en geactiveerd wordt.

5.6 Proxyservers

Meestal worden proxyservers binnen een bedrijfsnetwerk ingezet. Hierdoor kunnen datastromen worden gekoppeld en veelgevraagde informatie in een cachegeheugen worden opgeslagen. Dit bevordert de efficiëntie van het dataverkeer voor aangesloten randapparatuur. Maar tegen tracking is een ander aspect van proxyservers interessanter.

Zoals randapparatuur binnen een thuisnetwerk niet via hun lokale IP-adres op het internet identificeerbaar is, kan ook worden gezorgd dat een internetaansluiting niet meer via de externe IP-adres identificeerbaar is. Hiervoor moet een verbinding met een ander netwerk worden opgebouwd. Typisch gebeurt dit via proxyservers. Voor de buitenwereld gebruikt de randapparatuur na het verbinden met een proxyserver het ip-adres van de proxyserver. Het ip-adres van de verbonden randapparatuur wordt dus voor de buitenwereld verborgen. De proxyserver zorgt vervolgens dat de bestanden intern correct worden afgeleverd bij de verbonden randapparatuur.

Er zijn veel proxyservers over de hele wereld die gratis kunnen worden gebruikt om onder andere het internet anoniemer te kunnen gebruiken[15]. Omdat alle datastromen via de proxyserver gaan, ontstaat een bottleneck. Veel gratis proxyservers zijn overbelast en vertragen het dataverkeer. Daarom zijn er ook aanbieders als Proxy Solutions die proxyservers tegen betaling ter beschikking stellen en hiervoor een bepaalde bandbreedte garanderen.

Het gebruik van een proxyserver en de hiermee verbonden bundeling van de datastromen heeft als nadeel dat de proxyserver alles mee kan lezen. Bovendien heeft de gebruiker altijd dezelfde ip-adres namelijk die van de proxyserver. Een manier om nog meer anonimiteit te creëren waarbij de kans dat iemand meeleest niet groter wordt, biedt *The Onion Routing* (TOR). Hierbij gaat de verbinding via drie verschillende servers en wordt de dataverkeer per server versleuteld. Alleen de server helemaal aan het eind moet alles weer decoderen om het dataverkeer met het "gewone" internet mogelijk te maken. De laatste server kan dus zoals gewone proxyservers meelezen. Omdat het dataverkeer altijd via wisselende routes binnen het TOR-netwerk plaatsvindt, wordt de anonimiteit van de gebruiker vergroot ten opzichte van een proxyserver. Om te voorkomen dat de laatste server meeleest kunnen versleutelde verbindingen worden gebruikt.

5.7 World Wide Web Consortium

Het W3C is actueel met de standaardisering van Do Not Track bezig en Roy Fielding heeft hiervoor op 14 november 2011 een eerste ontwerp voorgesteld. Tot 13 maart 2012 werd in samenwerking met David Singer een tweede versie van de *Tracking Preferences Expressions* [22] geschreven. In het voorstel worden in hoofdstuk 5 twee opties voor Do Not Track voorgesteld. In de versie van 13 maart 2012 is nog niet besloten welke van de twee opties of dat zelfs beide opties worden gekozen. Daarom zullen hier beide opties worden besproken.

[15] Websites als www.proxy4free.com bieden een overzicht van beschikbare, kosteloze proxyservers.

5.7.1 Bekende URI waar een useragent de trackingstatus kan opvragen

De eerste optie wordt geïmplementeerd door het aanleggen van sites met een bekende URI waar de randapparatuur van de gebruiker de trackingstatus van een website kan opvragen. Hiervoor stelt het W3C het volgende URI-template voor:

/.well-known/dnt{+pathinfo}

Concreet zal dus voor een website

http://example.com/over/here?q=hello#top

als bron voor de trackingstatus een site met de volgende URI kunnen worden aangelegd:

http://example.com/.well-known/dnt/over/here

De site met informatie over de trackingstatus van een website mag uiteraard niet zelf gebruikers volgen. Op de site zal machinaal leesbare informatie worden aangeboden die door de randapparatuur zal kunnen worden geïnterpreteerd. Een voorbeeld voor de machinaal leesbare code is volgens het W3C:

```
{
      "path": "/",
      "tracking": true,
      "received": "1",
      "response": "t1",
      "same-site": [
      "example.com",
      "example_vids.net",
      "example_stats.com"
],
  "partners": [
      "api.example-third-party.com"
],
      "policy": "/tracking.html",
      "edit": "http://example-third-party.com/your/data",
      "options": "http://example-third-party.com/your/consent"
}
```

Interpretatie van de Informatie

De informatie kan door de browser op een voor de gebruiker duidelijke duidelijke manier worden weergegeven. Hiervoor moet de code als volgt worgen geïnterpreteerd:

path: geeft het bereik, dus de adresstam van de pagina's op de server aan voor die de informatie geldig is.

tracking: geeft met true/false informatie of tracking volgens definitie volgens hoofdstuk 3.2.1 wordt toegepast.

received: geeft aan welke keuze de server van de browser heeft ontvangen: 1: DNT actief, 0: DNT inactief, null: geen keuze.

response: geeft de mogelijkheid om aan te geven voor welke redenen tracking op de server gebruikt wordt. Deze begint met t als de gebruiker tracking toestaat of met een n als gebruiker tracking niet toestaat, gevolgd door tekens die de reden aangeven. De redenen worden volgens deze tabel afgekort:

Reden	Betekenis
1	Ontworpen voor gebruik alleen als eerste partij
3	Ontworpen voor gebruik als derde partij
a	Beperkt tot reclameaudits
c	Voorafgaande toestemming ontvangen van deze useragent
f	Beperkt tot fraudedetectie
g	Voor de nakoming van regionale/ geografische beperkingen
q	Beperkt tot (het bepalen van) reclamehoeveelheden
r	Beperkt tot verwijzingsgegevens

same site (optioneel): hier kunnen ander domeinen van dezelfde aanbieder staan die (onderdelen van) de site bevatten.

partners (optioneel): hier kunnen partners dus derde partijen staan die het door de siteaanbieder is toegestaan om gebruikers te volgen.

policy (optioneel): bevat URI-verwijzing naar document met voor gebruiker leesbare informatie over het trackingbeleid van de website. (Vertaling van machineleesbar informatie naar natuurlijke taal)

edit (optioneel): URI-referentie naar mogelijkheid om gegevens te bekijken en verwijderen die over hem op de site verzameld werden.

options (optioneel): URI-referentie om de useragent de mogelijkheid te geven om voor tracking op deze site te kunnen in- of uitschrijven.

Door dit voorstel wordt het mogelijk om de gebruiker over tracking te informeren en de gebruiker de mogelijkheid gegeven om de website niet te bezoeken als hij niet op de aangegeven manier wil worden gevolgd. Als onder de boven beschreven URI-template geen informatie kan worden gevonden, weet de gebruiker bovendien van tevoren dat de aanbieder van de website Do Not Track nog niet geïmplementeerd heeft.

Het voordeel van dit voorstel is dat de gebruiker in tegenstelling tot bijvoorbeeld pop-ups zeker kan zijn dat hij niet tijdens het eerste bezoek gevolgd wordt. Hij hoeft namelijk geen websites met actieve trackers te openen om zich over tracking op dezelfde websites te informeren.

5.7.2 HTTP header voor het communiceren van de trackingstatus

De tweede optie die het W3C voorstelt is een HTTP response header met de volgende doelen: De user-agent zal de mogelijkheid krijgen om te kunnen bevestigen dat de server met die gecommuniceerd wordt het DNT-verzoek van de gebruiker ontvangen heeft. Bovendien zal het mogelijk zijn om de kunnen bepalen op welke manier de gebruiker zal worden gevolgd. Als de server denkt eerder of op een ander manier al toestemming te hebben gekregen om een gebruiker te mogen volgen, zal de user-agent met deze HTTP-header de mogelijkheid krijgen om dit te zien en zo nodig aan te passen. Bovendien zal de header ervoor kunnen zorgen dat de server een duidelijke belofte maakt over het gebruik van de gegevens die hij via de aanvraag binnenkrijgt. De server zal bovendien op een bekende locatie meer informatie over tracking en privacy op de betroffen websites ter beschikking stellen. Tot slot zal de HTTP-header ook nog de mogelijkheid geven om de gebruiker individuele informatie te leveren.

Zoals bij de eerste optie wordt ook hier een voorbeeld door het W3C aangeleverd met machinaal leesbare code die van de server via de HTTP header naar de browser gestuurd wordt. De code kan volgens de onderaan staande semantiek worden geïnterpreteerd om op een gebruiksvriendelijke manier over het gebruik trackingtechnieken te informeren:

Tk-Response	= "Tk:" [CFWS] Tk-Status [CFWS] [opt-in-flag] [CFWS] [reason-code]
Tk-Status	= no-dnt / not-tracking / first-party / service-provider
no-dnt	= “0”
not-tracking	=”1”
first-party	= %x66 ; lowercase f
service-provider	= %x73 ; lowercase s
opt-in-flag	= “1”
reason-code	= ALPHA

Semantiek

Het W3C levert voor de bovenstaande header de volgende semantiek:

Tk: 0 (no-dnt) geeft aan dat de partij niet de trackingregels nakomt

Tk: 1 (not-tracking) geeft aan dat

- de partij de trackingregels nakomt en
- de partij de aanvraag wil verwerken volgens de specificatie voor derde partijen.

Tk: f (first party) geeft aan dat

- deze partij de trackingregels nakomt,

- de bron als eerste partij bedoelt is en
- deze partij de aanvraag wil verwerken volgens de specificatie voor eerste partijen.

Tk: s (service-provider) geeft aan dat

- deze partij de trackingregels nakomt,
- de bron bedoelt is als derde partij die acteert als een uitbesteed serviceaanbieder voor een eerste partij en
- deze partij de aanvraag wil verwerken volgens de vrijstelling voor een derde partij die acteert als een uitbesteedserviceaanbieder van een eerste partij zoals in de tracking-complicance beschreven.

De **opt-in-flag** geeft aan dat de server ervan uitgaat dat de gebruiker zijn goedkeuring gegeven heeft dat deze partij aanvullende rechten heeft om hem te volgen. Zonder de opt-in-flag behandelt de server aanvragen alsof de gebruiker zijn toestemming niet gegeven heeft voor aanvullende rechten om hem te volgen.

De **reason-code** kan worden gebruikt om naar meer informatie te verwijzen.

5.7.3 Evaluatie

Het grootste nadeel aan de implementaties van het W3C is dat de gebruiker afhankelijk is van de server die hij bezoekt. Beide implementaties maken het mogelijk dat eindapparatuur tegen trackers zegt in hoeverre de gebruiker wil worden gevolgd. Maar in beide gevallen zou de server het verzoek theoretisch kunnen negeren en de gebruiker blijven volgen. De gebruiker heeft dus geen garantie dat hij niet gevolgd wordt.

Ondertussen zijn de meeste browsers voorzien van een Do Not Track functie. Deze komt niet overeen met de definities van het W3C. Mozilla Firefox stuurt bijvoorbeeld actueel alleen maar een extra regel binnen de HTTP-request die aangeeft of de gebruiker de Do Not Track optie geactiveerd heeft. Deze keuze wordt dus aan de webserver meegedeeld en kan ook naar derden worden doorgestuurd. Trackers en adverteerders laten dan idealiter afhankelijk van de keuze van de gebruiker hetzij gepersonaliseerde hetzij algemene reclame zien en tracken de gebruiker niet als hij de Do Not Track-optie geactiveerd heeft.

Een standaard voor Do Not Track biedt de mogelijkheid om uiteindelijk iedereen mee te kunnen delen welke vormen van tracking de gebruiker niet wenst. Het voordeel is dat deze standaarden niet alleen voor een bepaalde trackingtechniek van toepassing zou zijn en breed kunnen worden opgevat. Het grote nadeel is dat de gebruiker tracking niet actief kan voorkomen maar de servers die hij bezoekt, moet vertrouwen. Als een webserver bijvoorbeeld niet naar Do Not Track verzoeken luistert en liever continu tracking inzet om hiermee geld te verdienen, kan de standaard niet afdwingen dat de server wel van tracking afziet. Andersom zou onder de voorwaarde dat zich ieder webserver aan Do Not Track houdt, tracking op geen effectiever manier kunnen worden geregeld.

5.8 Samenvatting

De volgende tabel geeft weer welke van de hierboven beschreven trackingblockers welke van de in hoofdstuk 4 beschreven trackingtechnieken voorkomt. Hiervoor staan de trackingblockers in de rijen en de trackingtechnieken in de kolommen. Bij de trackingtechnieken staan geen sessie IDs omdat ze vanwege de lage effectiviteit nauwelijks voor tracking worden ingezet.

Trackingblocker / **Trackingtechniek**	IP-adres (4.2)	Cookies van trackers (4.3)	Device Fingerprints (4.5)	Social Media (4.6)	Browseraanbieders (4.7)
No Script (5.2)	✘	✘	✔	✔	✘
Do Not Track Plus (5.3)	✘	✔	✘	✔	✘
Ghostery (5.4)	✘	✔	✘	✔	✘
AVG (5.5)	✘	✔	✘	✔	✘
Proxyservers (5.6)	✔	✘	✘	✘	✘
Do Not Track (W3C) (5.7)	O	O	O	O	O

Legenda:

✔ Trackingtechniek kan met behulp van trackingblocker actief worden voorkomen.

O Trackingblocker kan verzoeken dat trackingtechniek niet wordt toegepast.

✘ Trackingtechniek kan met behulp van trackingblocker **niet** worden voorkomen.

Dit tabel is geen uitputtend overzicht en bevat alleen de door mij onderzochte trackingtechnieken en -blocker.

6 Conclusie

Uit de bovenstaande samenvatting wordt duidelijk dat er geen trackingblocker is die alle vormen van de in hoofdstuk 4 geïnventariseerde trackingtechnieken kan voorkomen. In dat geval zouden in een rij alleen maar groene kruisjes staan. Positief is dat vier van de vijf beschreven trackingtechnieken actief kunnen worden voorkomen. Opvallend is dat alleen het W3C een oplossing ontworpen heeft waar de webserver vrijwillig op wens van de gebruiker afstand zou moeten doen van tracking. De ander trackingblockers helpen om tracking actief te voorkomen en geven de gebruiker de mogelijkheid zelf te kiezen welke tracker hij wil toelaten en welke niet. Aan de ander kant zouden alleen de opties van het W3C ieder willekeurige vorm van tracking kunnen voorkomen omdat de voorstellen niet op specifieke technieken focussen, maar algemeen de communicatie over tracking tussen gebruiker en webserver bevorderen.

Do Not Track van het W3C is op dit moment nog in het ontwikkelstadium en wordt nog niet toegepast. De actuele versies van de bekende internetbrowser gebruiken op dit moment een afgeslankte versie van Do Not Track. Hierbij wordt een extra regel aan de HTTP-header toegevoegd die informatie aan de server meegeeft of de gebruiker de Do Not Track functie van zijn browser ingeschakeld heeft.

De Federal Communications Commission (FCC) heeft vijf criteria voor Do Not Track geformuleerd[23]:

1. Door iedereen geïmplementeerd
2. Gemakkelijk te gebruiken, vinden en begrijpen
3. Persistentie
4. Niet alleen voor gebruik, maar ook voor verzameling
5. Effectief en afdwingbaar

Deze vijf criteria zullen bij het vinden van de ideale oplossing van do not track helpen. Het eerste, derde en vijfde criterium hebben allemaal te maken met effectiviteit. Do not track heeft alleen nut als het door iedereen geïmplementeerd is. Bovendien moet het afdwingbaar zijn en mag niet kunnen worden omgaan. Ook speelt gebruiksgemak voor de FCC een belangrijke rol. Vaak zijn privacy en gebruiksgemak tegenstrijdig. Toch is de FCC van mening dat do not track gebruiksvriendelijk moet zijn.

We kunnen dus concluderen dat do not track een korte, krachtige en gebruiksvriendelijke afspraak moet zijn die iedereen kent en snapt en die door ieder webserver geaccepteerd en geïmplementeerd wordt.

De ideeën van het W3C zijn een stap in de goede richting, maar er ontbreekt nog een besluit over de precieze realisering van Do Not Track. Vervolgens moet het ontwerp nog worden geïmplementeerd. Dat geldt aan de ene kant voor het W3C dat de uiteindelijke standaard moeten definiëren en aan de ander kant voor webservers die de standaard moeten overnemen en zich aan de hiermee verbonden regels moeten houden.

Samengevat zou do not track een gebruiksvriendelijke implementatie moeten zijn, die tracking effectief kan voorkomen. Do not track moet het bovendien mogelijk maken om zich over tracking te kunnen informeren en op basis van de verkregen informatie bewust tracking toe te laten of te weigeren. De standaard moet zo specifiek mogelijk zijn, maar wel de hele bandbreedte van tracking afdekken. Bovendien moet do not track zo tijdloos mogelijk zijn om te voorkomen dat het binnenkort achterhaald is. Do not track moet niet alleen een verplichting zijn, maar een afspraak aan die zich alle partijen ook om morele redenen houden.

7 Appendix A: Communicatie met Abine

Vraag:

Can I be sure that Abine self does not apply tracking with the tool DNT+?

Antwoord:

Thanks for your question; it's a good one. DNT+ does not track any of your web activity. It has no ability to collect data about what sites you visit or any other web behavior. The tool can save your personal settings and preferences, but those are stored locally on your computer and are not visible to us.

Our software is built entirely around the principle of privacy. We have no ability to track our users. **You can verify this fact yourself by using an app that monitors the requests made for your computer's information throughout the day. 2 examples of apps like these are Live HTTP Headers or WireChart,** neither of which we make. Our software makes 1 request per day to your computer for updated tracker blocking rules. You will be able to see that request and what it entails; there is no further communication or transfer of information.

You can also see in part A of our Privacy policy that "Abine will not track, store or transmit to any server or third party, information regarding users' behavioral data (to include web browsing activity), nor will we "deliver or help others deliver any targeted advertising to users" (part C).

The natural next question some customers ask is how Abine makes money. In case you were curious, I thought I'd share the answer with you. Our mission is to give consumers control back over their private information online. Building tools for consumers that improve privacy is all we do. DNT+ is our free product. **Our focus is to make DNT+ a great product that people love and by doing that we believe that some people will enjoy it enough to want to upgrade to paid products** that offer additional privacy protection, such as our subscription service, DeleteMe.

8 Glossarium

Artikel 29 werkgroep: Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens ingesteld naar aanleiding van EU richtlijn 95/46/EG betreffende gegevensbescherming.

Behavioral advertising: Het gepersonaliseerd maken van reclame op basis van eigenschappen die trackers over een gebruiker hebben verzamelt.

Cookie: Een klein bestand met een unieke code dat via de browser op randapparatuur kan worden opgeslagen en uitgelezen.

Eindapparatuur: → Randapparatuur

Evercookie: Cookie die met behulp van Flash op een andere locatie opgeslagen wordt dan gewone cookies.

Gebruiker: Iemand die met behulp van randapparatuur gebruik maakt van het internet.

IP-adres: Een adres die volgens het TCP/IP-protocol binnen een netwerk aan randapparatuur wordt toegewezen. Omdat er nog weinig gebruik wordt gemaakt van IPv6-adressen worden binnen deze scriptie alleen IPv4-adressen bedoelt.

Local Shared Objects: Gegevens die met behulp van Adobe Flash of op randapparatuur geplaatst wordt.

MAC-adres: De unieke GUID van een netwerkadapter waarmee hij binnen een netwerk kan worden geidentificeerd.

Opt-in: Een optie waar je ergens in moet schrijven om iets te ontvangen.

Opt-out: Een optie waar je ergens uit kunt schrijven om iets niet te ontvangen.

Profiel: Informatie over de eigenschappen of het gedrag van een gebruiker of gebruikersgroep.

Randapparatuur: Computers, laptops, tabletcomputers, mobieltjes of ander apparatuur waarmee een gebruiker het internet kan gebruiken.

Social media: Sociale netwerksites als Facebook, Twitter, Google+, LinkedIn, etc.

Tracken: Gebruik maken van een techniek die het mogelijk maakt om internetgebruikers te kunnen identificeren of op een ander manier mogelijk maakt om informatie over internetgebruikers te verzamelen.

Tracker: Een organisatie die tracking toepast.

Tracking: De verzameling en verwerking van persoonsgegevens over het gedrag van gebruikers. Hierbij wordt randapparatuur identificeerbaar gemaakt om de gebruiker bij zo veel mogelijk virtuele handelingen te kunnen observeren. Gebaseerd op deze gegevens wordt inhoud op het internet op individuele gebruikers of groepen van gebruikers aangepast (vgl. hoofdstuk 3.3).

Trackingtechniek: Een techniek die het mogelijk maakt om gebruikers te kunnen observeren.

Trackingblocker: Een techniek die tracking of delen hiervan voorkomt.

Volgen: → Tracken.

9 Referenties

Wetenschappelijk

[1] Samuel D. Warren & Louis Brandeis. The right to privacy. *Harvard Law Review*, IV(5):p. 193–220, dec 1890.

[2] Adrian E. Hollaender. *Kompendium der Menschenrechte*. Leykam, 2007.

[3] Marit Köhntopp & Kristian Köhntopp. Datenspuren im internet. *Computer und Recht (CR)*, 4:248–257, feb 2000.

[4] Jens Meyer-Ladewig. *EMRK*. Nomos Verlagsgesellschaft, 2011.

[5] Arnold Roosendaal. Facebook tracks and traces everyone: Like this! *Social Science Research Network Electronic Paper Collection*, 2011.

[6] Claude E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27 (3):379–423, 1948.

[7] Bart van der Sloot. Het plaatsen van cookies ten behoeve van behavioural targeting vanuit privacyperspectief. *Privacy & Informatie*, 2:62–70, apr 2011.

[8] Jan Achterbergh & Dirk Vriens. *Organizations: social systems conducting experiments*. 2e druk. Springer (Heidelberg), 2010.

Niet wetenschappelijk

[9] Does it help or hinder? promotion of innovation on the internet and citizens right to privacy. Study.

[10] Groep Gegevensbescherming Artikel 29. Advies 16/2011 over de best practice recommendation on online behavioural advertising van easa/iab.

[11] Abine. How to turn on do not track in your browser, sep 2011.

[12] Susanne Mildner AVG. Avg führt “do not track” feature ein. persbericht, mrt 2012.

[13] The Purple Box. List of elements and techniques used to track, aug 2011.

[14] Hans de Jongh. 'cookiewet' bedreigt de toekomst van online marketingbureaus. *Het Financieele Dagblad*, 2012.

[15] Daniel Eran Dilgner. Google reportedly ignoring safari users' privacy settings to better track its ads, feb 2012.

[16] Peter Eckersley. A primer on information theory and privacy, jan 2010.

[17] Peter Eckersley. What does the "trackïn "do not track"mean?, feb 2011.

[18] Ghostery. Privacy policy, mrt 2010.

[19] Jennifer Koch. Bürgerproteste gegen google. *Rheinische Post*, aug 2010.

[20] Eli Pariser. *The Filter Bubble: What The Internet Is Hiding From You.* Viking, 2011.

[21] Julianne Pepitone. Yahoo's levinsohn: Honestly, we're fine, okt 2011.

[22] Roy T. Fielding & David Singer. Tracking preference expression (dnt), mrt 2012.

[23] Hannes Tschofenig & Rob van Eijk. Do not track. apr 2011.

[24] Justin Brookman & Sean Harvey & Erica Newland & Heather West. Tracking compilance and scope, mrt 2012.

Wetteksten

[25] Eu richtlijn 2002/58/ec betreffende privacy en elektronische communicatie, 2e geconsolideerde versie van 2009.

[26] Eu richtlijn 95/46/ec betreffende gegevensbescherming, 1e geconsolideerde versie van 2003.

[27] Europees verdrag voor de rechten van de mens.

[28] Handvest van de grondrechten van de europese unie, dec 2000.