BROWSER PRIVACY: THE GOOD, THE BAD AND THE UGLY

Een analyse van de affordance van privacy in browsers

Abstract

Er is een verschil te vinden in hoe browsers gebruikers in staat stellen om veilig met hun data om te gaan. Van de drie onderzochte browsers presteerde er een heel slecht en de andere twee goed. Gebruikers kunnen middels goede toepassing van designelementen controle krijgen over eigen data. De drie manieren die ervoor zorgen dat dit gewaarborgd wordt zijn: proactieve meldingen, overzichtelijke instellingen in het voordeel van de gebruiker en voldoende voorlichting over veilig internetgebruik

- Vicentiu van der Wijk (4064453)
- Niels Kerssens & Pauline Romondt-Vis

- 20-02-2017
- CIW Eindwerkstuk (CI3V13002)

Universiteit Utrecht

Inhoud

1. Aanleiding 3

2. Theoretisch kader 5

2.1 Relevantie 5

2.2 Theorie 7

3. Methode 9

3.1 Corpusselectie 9

3.2 Meetinstrument 10

4.1 Analyse 13

4.1 Google Chrome 13

4.1.1 Meldingen 13

4.1.2 Instellingen 15

4.1.3 Voorlichting 17

4.1.4 Terugkoppeling theorie 19

4.2 Epic browser 20

4.2.1 Meldingen 20

4.2.2 Instellingen 21

4.2.3 Voorlichting 23

4.2.4 Terugkoppeling theorie 24

4.3 Internet Explorer 25

4.3.1 Meldingen 25

4.3.2 Instellingen 26

4.3.3 Voorlichting 27

4.3.4 Terugkoppeling theorie 28

5. Conclusie 29

5.2 Discussie 30

6. Bronnenlijst 31

1. Aanleiding

Anno 2016 is het gebruik van het internet niet meer weg te denken uit ons dagelijks leven. Bedrijven, consumenten en instanties maken sinds het ontstaan van het internet in een steeds hogere mate gebruik van het gemak en de verbondenheid van het web. Gebruikers verplaatsen meer van hun dagelijkse activiteiten naar online omgevingen (Van Dijck, 2013, p. 57). Voorbeelden van deze online omgevingen zijn sociale platformen zoals Facebook en Twitter en services van Google, zoals Gmail en YouTube. Uit cijfers blijkt dat dit soort platformen en services enorme populariteit kennen; gebruikers bezochten Google 241 miljoen keer en Facebook 206 miljoen keer van januari tot augustus 2016. Hiermee staan beide bedrijven in de top drie van de meest bezochte websites van 2016 (Statistica, 2016). Een andere bron ter illustratie van de impact van het internet is de publicatie van de CIA World Fact Book. Hierin staat dat er per juli 2015 3.2 miljard internetgebruikers waren, bijna de helft van de wereldpopulatie (2017, p. 334).

Gebruikers van het internet hebben volgens van Dijck (2013, p. 57) een nieuwe norm ontwikkeld om verschillende soorten persoonlijke informatie te delen via sociale platformen en applicaties; van hun trouwstatus tot ziektes en van eetgewoontes tot favoriete muziek (p. 58). De immersie van de gebruikers in deze ontwikkelingen kent ook een schaduwzijde. Veel gebruikers zijn slecht of niet op de hoogte van de mate waarin bedrijven op massale schaal hun persoonlijke gegevens verzamelen. Iedereen die gebruik maakt van Google, Facebook en soortgelijke platformen wordt onderworpen aan diens commerciële belangen (Stalder & Mayer, 2009). Door het gebruik van softwareontwikkelingen is het voor bedrijven eenvoudig om gegevens te verzamelen. Vrijwel op iedere website zijn er *trackers* te vinden; onzichtbare software die de gebruiker volgt gedurende zijn tijd online (2009). Er is volgens van Dijck (2009, p. 49) een wisselwerking te vinden in dit soort platformen: gebruikers krijgen de mogelijkheid om te participeren in ruil voor hun gegevens.

De plek waar deze gegevensuitwisseling tot stand komt, is tevens onmisbaar voor de toegang tot het internet: de browser. Voor gebruikers is het onmogelijk om controle te hebben over hun eigen data, nadat het de browser verlaten heeft (Stalder & Mayer, 2009). Gegevensverzameling gebeurt namelijk vaak zonder expliciete toestemming en zonder een mogelijkheid tot *opt-out*. Er zijn sinds het ontstaan van de eerste browser veel bedrijven geweest die hun eigen visie hebben ontwikkeld op het design van browsers. Firefox, Chrome en Internet Explorer zijn hierbij de bekendste (Tsalis, Mylonas en Gritzalis, 2016, p. 259). Er is bovendien ook een segmentatie te vinden binnen het browserlandschap. Naast deze drie populaire browsers zijn er ook een aantal niche categorieën ontstaan. Deze browsers leggen zich toe op bepaalde functies die niet of in mindere mate aanwezig

zijn bij de populair browsers (Dunn, 2016). Een voorbeeld hiervan is de Epic browser. Deze browser legt nadruk op de privacy van zijn gebruikers.

De grote schaal waarop gegevensverzameling voorkomt, is nadelig voor de gebruikers van internetplatformen. Het is relevant om onderzoek te doen, omdat deze gebruikers geen controle hebben over wat er met de data gebeurt en wie het verzamelt (Stalder & Mayer, 2009). In dit essay zal er onderzocht worden hoe gebruikers in staat worden gesteld om privacy te waarborgen in drie populaire browsers. De onderzoeksvraag in dit artikel zal zijn:

> *Op welke manieren waarborgen de designelementen in browsers de mogelijkheid voor gebruikers om de affordance user-agency over data te behalen?*

In het theoretisch kader van dit onderzoek zullen er eerst twee wetenschappelijke artikelen besproken worden om een beeld te vormen over gegevensverzameling. Daarbij zal er ook uitgelegd worden waarom deze artikelen interessant zijn voor het onderzoek. Vervolgens worden er theorieën geïntroduceerd waarmee de resultaten van de analyse worden geïnterpreteerd. In de methode wordt er verantwoord hoe het corpus tot stand is gekomen en wordt er tevens een meetinstrument gespecificeerd. De analyse bestaat uit het daadwerkelijke onderzoek naar de browsers. Als laatste volgt een conclusie op basis van de uitvoering, resultaten en eventuele aanbevelingen voor vervolgonderzoek.

2. Theoretisch kader

Het theoretisch kader is opgedeeld in twee paragrafen. In de eerste paragraaf worden er twee artikelen behandelt die bijdragen aan de beeldvorming van de verzameling van gebruikersgegevens. Daarna zal er uitgelegd worden waarom deze artikelen relevant zijn voor dit onderzoek. In de tweede paragraaf worden er twee benaderingen uiteengezet die bijdragen aan de interpretatie van de resultaten van de analyse. De theorieën dienen als een conceptueel kader waaraan designelementen van browsers getoetst worden. Hiermee wordt gepoogd de hoofdvraag te beantwoorden.

2.1 Relevantie

Het eerste artikel betreft een onderzoek verricht door Shah & Kesan (2009, pp. 315-336). Het beschrijft de geschiedenis van dataverzameling op het internet. De auteurs beargumenteren in hun stuk welke invloeden hebben geleid tot het ontstaan van *cookies*. *Cookies* zijn een vorm van *trackers*; onzichtbare software die gebruikersgegevens verzamelt (p. 318). *Cookies* zorgen ervoor dat de handelingen die de gebruiker uitvoert op websites geregistreerd worden. De software is zo ontworpen dat informatie uit *cookies* gedeeld kan worden met andere vormen van *trackers* (p. 319). Door het volgen van de handelingen die gebruikers uitvoeren en het delen van deze informatie ontstaat er een profiel van de gebruiker (p. 319).

Cookies zijn ontstaan tijdens het designproces van de eerste browser. De ontwerpers implementeerden een functie die de browser in staat stelde om informatie te vergaren over zijn gebruikers. Vanwege de mogelijke consequenties die de functie had voor privacy werd er in het eindproduct besloten om dit niet te realiseren (Shah & Kesan, 2009, p. 317). Deze beslissing werd al snel tenietgedaan met de komst van de eerste commerciële browser: Netscape. *Cookies* waren voor het bedrijf achter Netscape interessant vanwege de potentiele verkoop van gepersonaliseerde informatie (p. 318). Shah & Kesan stellen dat de commerciële belangen op dat moment belangrijker waren dan het waarborgen van privacy (p. 320). In eerste instantie was het de bedoeling van de ontwerpers van Netscape om cookies beperkt beschikbaar te maken: alleen de website waarop de *cookie* geplaatst was, zou bij de data moeten kunnen. Door een ontwerpfout bleek echter dat *cookies* vrij toegankelijk waren en dat andere *cookies* of software gebruik konden maken van de opgeslagen data (p. 321). Wat begon als een ontwerpfout is tegenwoordig nog steeds geïmplementeerd in het design van *cookies*.

Cookies worden in het kader van dit onderzoek besproken vanwege de huidige toepassing van de software. Sinds Netscape maakt iedere browser gebruik van *cookies*. Daarnaast schetsen Shah &

Kesan (2009, p. 321) een beeld waarbij commerciële belangen bij het ontwerp van browsers voorrang hebben op privacy. Ondanks een cruciale ontwerpfout en gevaar voor privacy werden *cookies* toch geïmplementeerd. Hun publicatie omschrijft *cookies* als een designelement in browsers (p. 321). Hiermee wordt er geïmpliceerd dat *cookies* en daarbij dataverzameling een bewuste implementatie is. Het is relevant voor dit onderzoek, omdat browsers en dataverzameling blijkbaar niet los van elkaar kunnen worden gezien.

Het tweede artikel dat voortbouwt op het fenomeen dataverzameling en *trackers* is een artikel van Stalder & Mayer (2009). De auteurs beschrijven een landschap waarin grote zoekbedrijven zoals Google op massale schaal gegevens verzamelen om gebruikersprofielen te creëren. Deze profielen worden vervolgens doorverkocht aan adverteerders. Bedrijven zoals Google hebben volgens de auteurs twee doelstellingen: het indexeren van het web om zoekopdrachten te kunnen faciliteren en het indexeren van personen (2009). Stalder & Mayer benadrukken dat het één niet zonder het ander kan bestaan; gebruikers ruilen hun data in voor het gebruik van de diensten van zoekbedrijven (2009). De tweede doelstelling is volgens de auteurs een gevaar voor privacy, omdat het voor gebruikers niet overzichtelijk is wat er verzameld wordt en wat er gebeurt met deze data. Het is voor gebruikers ook niet mogelijk om zich af te melden voor deze handelingen (2009).

Google verzamelt data door een groot aantal producten aan te bieden aan consumenten en bedrijven. Diensten zoals Gmail, Google Maps en Google Health registreren alle handelingen die gebruikers uitvoeren om deze vervolgens te verzenden naar de servers van Google (Stalder & Mayer, 2009). Daarnaast bezit Google nog een aantal andere diensten die minder bekend zijn bij de massa: AdSense, AdWords, DoubleClick en Google Analytics. Deze tools worden gebruikt door websites en bedrijven voor marktonderzoek. Voor Google hebben deze diensten een andere invulling: het zijn *trackers* die gebruikers volgen met als doel een profiel te creëren (2009). Deze diensten maken het voor Google mogelijk om alle technische informatie van een gebruiker te vergaren, zonder dat deze hiervoor expliciet toestemming heeft verleend. Gebruikers worden zelfs gevolgd op websites die geen eigendom van Google zijn (2009). Als voorbeeld van de schaal waarop dit gebeurt, noemen de auteurs een onderzoek dat uitwijst dat op 80% van de Duitse websites één of meerdere tools aanwezig zijn (2009). Daarnaast blijkt uit verschillende enquêtes dat een overgroot deel van de ondervraagden geen idee heeft van de profilering die Google toepast. Google is voor velen nog steeds alleen een zoekmachine (2009).

De twee besproken artikelen illustreren een aantal punten waarom het maatschappelijk relevant is om onderzoek te doen naar dataverzameling. Het artikel van Stalder & Mayer laat zien dat het verzamelen van persoonlijke gegevens op grote schaal voorkomt en dat gebruikers slecht op de hoogte zijn van deze praktijken. Tevens raken gebruikers het eigendom kwijt over hun data; er is geen mogelijkheid tot het inzien of afmelden van dataverzameling (2009). De specifieke relevantie voor

browsers is te vinden in het feit dat volgens Shah & Kesan browsers al sinds de begindagen commerciële belangen behartigen door de implementatie van *cookies* (2009, p. 322). Daarnaast is binnen het vakgebied van mediastudies zeer weinig onderzoek gedaan naar de rol van browsers in het tegengaan van dataverzameling. De meeste publicaties spitsen zich toe op wat er met de data gebeurt na het verzamelen. Het is daarom wetenschappelijk relevant om te onderzoek wat de mogelijkheden voor de gebruikers zijn om secuur met data om te gaan.

2.2 Theorie

Zoals beschreven in het artikel van Stalder & Mayer (2009) raken gebruikers de macht kwijt over hun data op het moment dat er gebruik wordt gemaakt van het internet. Een bron die het verlies van controle over data uitvoerig bespreekt is een publicatie van Jose van Dijck (2009, pp. 41-58). Van Dijck stelt de vraag in haar paper welke rol mediaplatformen hebben in het sturen van *user-agency*. Met *user-agency* wordt binnen het artikel van van Dijck gedoeld op de controle die gebruikers hebben over eigen content en gegevens op het internet (p. 44). De auteur beschrijft de opkomst van het web 2.0, met daarbij de belofte van een participatiecultuur. Met deze term wordt beschreven hoe gebruikers in de tijd van het web 2.0 makkelijk eigen content kunnen creëren en delen. Een voorbeeld hiervan is YouTube (p. 44). Van Dijck stelt dat het binnen de participatiecultuur belangrijk is dat gebruikers het eigendom hebben van hun content; van sociale media berichten tot persoonlijke gegevens (p. 48).

De participatiecultuur heeft volgens van Dijck (2009, p. 46) een minder rooskleurige wending aangenomen; web 2.0 bedrijven geven gebruikers de mogelijkheid om content te creëren en te delen, maar verzamelen wel gegevens voor commerciële doeleinden (p. 47). Gebruikers zijn bereid om deze gegevens af te staan, omdat ze toegang en participatie ervoor terugkrijgen. Van Dijck benoemt dat gebruikers van web 2.0 platformen geen *content-providers* maar *data-providers* zijn; data over gebruikers is veel interessanter voor bedrijven dan *content* (p. 52). Gebruikers zijn als het ware *content-creators* voor bedrijven. De content wordt gecreëerd doordat gebruikers hun persoonlijke data afstaan (p. 53). Bij dit proces beargumenteert van Dijck dat gebruikers hun *agency* volledig kwijtraken. Het is namelijk onduidelijk wat er precies met de gegevens gedaan wordt en gebruikers hebben geen controle over de data (p. 55) Van Dijck stelt dat het kwalijk is dat gebruikers de macht kwijtraken over iets wat oorspronkelijk van hun is: persoonlijke informatie (p. 55).

In een ideale wereld zouden gebruikers grip moeten hebben op de content en gegevens die ze produceren op het internet; gebruikers horen *agency* te hebben over data. Uit de besproken artikelen blijkt dat dit niet het geval is: dataverzameling komt veelvuldig voor en gebruikers zijn er niet van op de hoogte. Daarnaast raken gebruikers de controle kwijt op het moment dat de gegevens de browser

verlaten. Dit onderzoek zal zich daarom ook toespitsen op wat gebruikers binnen de browser kunnen doen om secuur met data om te gaan. Hiervoor zal er gekeken worden naar hoe de designelementen van browsers bijdragen aan *user-agency* over data.

Een laatste concept dat dieper ingaat op designelementen en het uiteindelijke doel van deze elementen is de *affordance* theorie. De term kent zijn ontstaan in de psychologie en ecologie en beschrijft de wisselwerking van hoe dieren omgaan met hun omgeving in termen van mogelijke acties (Gibson, 2015, p. 119). In 1988 brak een andere onderzoeker met de traditionele notie van *affordances* (Norman, 2003, pp. 80-134). Norman benadrukte de perceptie van de genoemde *affordances* door deze te bespreken als een designelement dat gebruikers helpt of tegenwerkt om een bepaalde actie uit te voeren (p. 86). Norman kwam zelf terug op zijn theorie in 2009 (p. 59) door te stellen dat designelementen en *affordances* niet hetzelfde zijn. Een *affordance* moet gezien worden als een hoger doel dat bereikt kan worden door designelementen (2009, p. 61). Een voorbeeld dat wordt aangehaald is een trap. De *affordance* van een trap is dat de gebruiker op een hogere verdieping terecht komt en de treden zijn het designelement dat daarbij helpt (2009, p. 61). Een recenter voorbeeld wordt besproken in een tekst geschreven door Curinga (2014). Curinga stelt dat de *affordance* van *blogging* niet het typen is van een kort berichtje, maar het verspreiden van ideeën op het internet. *Blogging* is hierbij alleen maar de manier waarop gebruikers in staat worden gesteld om dit doel te bereiken (2014). Volgens Curinga draagt het nadenken over affordances bij aan de constructie van een conceptueel model tussen wat gebruikers kunnen bereiken met software en hoe designelementen dit ondersteunen of tegenwerken (2014). Daarbij benadrukt Curinga dat *affordances* relationeel zijn; niet alle gebruikers kunnen hetzelfde bereiken. Een IT-specialist heeft meer kennis dan de gemiddelde internetgebruiker (2014).

In het kader van dit onderzoek wordt het concept *affordance* besproken aan de hand van *user-agency*. Zoals gesteld door van Dijck (2009, pp. 41-58) en Stalder & Mayer (2009) zouden gebruikers van het internet controle moeten hebben over hun gegevens. Gebruikers zouden als het ware *agency* moeten hebben over data. Het behalen van *user-agency* is alleen mogelijk binnen de browser; uitwisseling van gegevens gebeurt in de browser en er is geen controle meer nadat het de browser verlaten heeft. Designelementen van browsers zouden gebruikers dus in staat moeten stellen om *user-agency* over data te behalen. De *affordance* die centraal staat in dit onderzoek is daarom ook *user-agency*, oftewel handelsmogelijkheid over data. Deze handelsmogelijkheid kan behaald worden door het juiste gebruik van designelementen. In deze paper zal er getoetst worden hoe designelementen gebruikers helpen of tegenwerken om de *affordance user-agency* over data te behalen. Ook zal er onderzocht worden of er rekening is gehouden met de complexiteit van designelementen. De onderzoeksvraag van dit essay zal zijn: *op welke manieren waarborgen de designelementen in browsers de mogelijkheid voor gebruikers om de affordance user-agency over data te behalen?*

3. Methode

De methodesectie is opgesplitst in twee paragrafen: de eerste paragraaf bespreekt de selectie van het corpus en de tweede paragraaf zal een theorie introduceren die zal dienen als meetinstrument voor het uitvoeren van de analyse. De theorie beschrijft een aantal pijnpunten als het aankomt op het design van software. Vanuit deze benadering worden er een aantal categorieën gevormd die zich specificeren op designelementen. Er zal getoetst worden hoe de categorieën zich verhouden met de designelementen van browsers en daarmee de bijdrage aan het behalen van de *affordance* user-agency over data.

3.1 Corpusselectie

De keuze voor het corpus is ontstaan uit een aantal artikelen waarin browsers worden besproken. De selectie van Internet Explorer en de Epic browser komt voort uit publicaties geschreven op de websites Computerworld, Maketecheasier, Techworld en Lifehacker. Deze websites houden zich bezig met technologie en software. De beslissing om Chrome te onderzoeken is gebaseerd op de paper van Stalder & Mayer (2009); de auteurs beschrijven het gevaar voor privacy aan de hand van Chrome.

Chrome is relevant om te onderzoeken vanwege een aantal punten die worden besproken door Stalder & Mayer (2009). De auteurs benoemen het monopolie die Google heeft op het internet met de verschillende verbonden diensten en producten. Volgens de auteurs verzamelt Google op massale schaal gegevens en behartigt daarmee zijn commerciële belangen (2009). Stalder & Mayer illustreren door het bespreken van *omnibox* en *chrome history* search. Beide functies zijn volgens de auteurs ontworpen om zeer gedetailleerd informatie te verzamelen over zijn gebruikers (2009). De eerste functie zorgt ervoor dat alles wat in de URL-balk wordt getypt, verzameld wordt door Google. Hieronder vallen links naar websites en zoekopdrachten. Ook als de gebruiker de invoer verwijdert, wordt er nog steeds data verzonden. De tweede functie indexeert alle data van alle apparaten waarop men met een Googleaccount is ingelogd. Deze data wordt vervolgens verstuurd naar de servers van Google (2009).

De Epic browser wordt door verschillende bronnen benoemd tot de meest veilige browser voor het beschermen van gebruikersdata (Henry, 2014; Bilbao, 2016; Dunn, 2016). De artikelen benadrukken dat de designfilosofie van de ontwerpers zich toe zou spitsen op privacy. Daarnaast wordt er op de website van de Epic browser gesteld dat alle vormen van *trackers* standaard geblokkeerd worden (Henry, 2014; Bilbao, 2016; Dunn, 2016).

Internet Explorer is gekozen vanwege het wijdverspreide gebruik en het gevaar dat gebruikers lopen door de browser te gebruiken. Aan de hand van statistieken gepubliceerd door Microsoft beschrijft de website Computerworld dat er nog 55% van de *users* op het internet gebruik maken van Internet Explorer (Keizer, 2015). Zowel Computerworld als Maketecheasier (Gomez, 2016) benadrukken daarbij dat de browser achterloopt qua technisch ontwerp op concurrenten. De onderliggende code van de browser zou nog een aantal functies bevatten die niet meer veilig zijn. Daarnaast is Microsoft per juli 2015 gestopt met het ondersteunen van Internet Explorer (Gomez, 2016; Keizer, 2015).

Om ervoor te zorgen dat het onderzoek naar browsers niet wordt beïnvloed door opties en de geschiedenis van de onderzoeker zullen er een aantal maatregelen moeten worden genomen. Allereerst zal er gebruik worden gemaakt van een laptop met daarop een schone installatie van Windows 10. Daarnaast worden de meest recente versies van de drie browsers geïnstalleerd: Chrome (56.0.2924.76, januari 2017), Epic browser (55.0.2661.75, november 2016) en Internet Explorer (11.0.11, augustus 2014). Ook is het belangrijk om te benoemen dat er niks veranderd wordt aan de instellingen van de browsers.

3.2 Meetinstrument

Het ontwerp van browsers en specifiek designelementen zal geanalyseerd worden aan de hand van theorie over het design van software. Omdat er binnen *media studies* weinig onderzoek gedaan is die expliciet toepasbaar is op deze casus, zal er gebruik gemaakt worden van theorie uit een ander vakgebied. Binnen het landschap van de *computer sciences* zijn er een aantal publicaties te vinden met als onderwerp designelementen in software. In het bijzonder is het concept van *value-sensitive design* van waarde als meetinstrument. *Value-sensitive design* wordt omschreven door Friedman & Kahn als een theoretisch geraamte voor software ontwerp waarbij de menselijke waarden centraal staan (2002, pp. 1177-1201). De theorie is opgedeeld in elf verschillende categorieën. Vanwege de omvang van dit onderzoek is het niet mogelijk om alle categorieën te bespreken. Daarnaast wordt de theorie toegepast als meetinstrument op een specifieke casus en zijn daarom niet alle categorieën bruikbaar. Binnen dit onderzoek er alleen gekeken naar designelementen. Drie van de elf categorieën beschrijven designelementen en specifiek de interactie tussen gebruiker en software. De categorieën die gebruikt worden voor de analyse zijn: (1) *privacy*, (2) *autonomy* en (3) *informed consent*.

De categorie (1) *privacy* wordt omschreven door middel van twee richtlijnen die ontstaan zijn in het vakgebied van de *human-computer interaction* (HCI). De eerste richtlijn stelt dat gebruikers geïnformeerd moeten worden waar en wanneer er data opgeslagen wordt en door wie deze data

wordt verzameld (Friedman en Kahn, 2002, p. 1181). De tweede richtlijn stelt dat gebruikers op de hoogte moeten worden gesteld van welke informatie zij delen en wie er toegang tot heeft (p. 1181). De volgende categorie (2) *autonomy* benadrukt dat gebruikers een zo groot mogelijke controle moeten hebben over de software. Daarbij stellen Friedman & Kahn dat er wel een grens is; de gemiddelde gebruiker hoeft niet over programmeerkennis te beschikken om een optie in of uit te schakelen (2002, p. 1189). De categorie *autonomy* wordt gewaarborgd op het moment dat gebruikers controle krijgen over de juiste opties wanneer nodig. Hierbij is het belangrijk dat de keuzes niet onnodig ingewikkeld zijn (2002, p. 1189). De laatste categorie (3) *informed consent* draagt bij tot succesvol implementeren van *autonomy* en *privacy. Informed constent* houdt in dat gebruikers goed geïnformeerd moeten worden over de keuzes tussen mogelijke opties. Hierbij is het belangrijk dat er accurate informatie gegeven wordt over de voor- en nadelen van een keuze. Daarnaast moet de gebruiker deze keuze ook kunnen begrijpen en er akkoord mee gaan (Friedman & Kahn, 2002, p, 1190). Friedman & Kahn stellen dat de gebruikers keuzes moeten krijgen, waarbij wordt gesproken in termen van potentiële effecten in plaats van technische mechanismen (p. 1191). Ook wordt het belangrijk geacht dat de *default settings* het verlies van *informed consent* tegengaan. Dit houdt in dat gebruikers niet de mogelijkheid moeten kwijtraken om überhaupt keuzes te kunnen maken (p. 1191).

Er wordt in dit onderzoek gekeken hoe de designprincipes zoals omschreven in *value sensitive design* zich verhouden tot de daadwerkelijke features. Daarnaast wordt er gekeken hoe en of deze features bijdragen aan de *affordance user-agency* over gebruikersdata. Om de categorieën toepasbaar te maken op deze specifieke casus worden ze gemodificeerd. Vanuit het eerste concept *privacy* kan de nieuwe categorie (1) *meldingen* worden geëxtraheerd. Het tweede concept, *autonomy* kan gebruikt worden om de categorie (2) *instellingen* te vormen. Het laatste concept, *informed consent*, kan geconverteerd worden tot de categorie (3) *voorlichting*.

De drie classificaties zullen gebruikt worden om de analyse uit te voeren. Binnen de categorie (1) *meldingen* zal er gekeken worden of de browser de gebruiker op de hoogte stelt als er data uitwisseling plaatsvindt. Hierbij is het belangrijk om te kijken of gebruikers de mogelijkheid hebben om te zien wie de data verzamelt en welke data er verzameld wordt. Om dit te kunnen testen zullen er middels de drie browsers verschillende websites worden bezocht. De keuze van de websites komt voor uit een online publicatie van de Wall Street Journal (2016). De Wall Street Journal heeft een index gemaakt van websites die het hoogste aantal *trackers* bevatten. Op de eerste plaats komt *dictionary.com* met 234 *trackers*, op de tweede plaats staat *msn.com* met 207 *trackers* en op de derde plaats *photobucket.com* met 127 *trackers*.

De tweede categorie (2) *instellingen* is opgesplitst in twee punten. Ten eerste zal er onderzocht worden wat voor mogelijkheden gebruikers hebben als het aankomt op de bescherming van privacy. Een belangrijk punt hierbij is het overzicht van deze opties en de begrijpelijkheid ervan. De gebruikers

moeten niet onnodig technische taal voorgeschoteld krijgen, maar wel een zo groot mogelijke controle over de browser. Vervolgens zullen de standaardinstellingen bekeken worden. Hierbij is het van belang dat deze instellingen al standaard in het voordeel van de gebruiker staan.

De laatste categorie (3) *voorlichting* zal gebruikt worden om te analyseren of gebruikers actief worden betrokken bij keuzes die nadelig kunnen zijn voor hun privacy. Hierbij wordt er wederom gekeken naar de standaardinstellingen en of deze de gebruikers in heldere taal voorlichten en in termen van potentiele effecten. Daarbij is het belangrijk dat gebruikers een goed overwogen keuze kunnen maken tussen de verschillende opties wat betreft de bescherming van gegevens. Er zal ook onderzocht worden of de browsers de gebruikers voorlichten over hoe er veilig op het internet kan worden gesurft.

4.1 Analyse

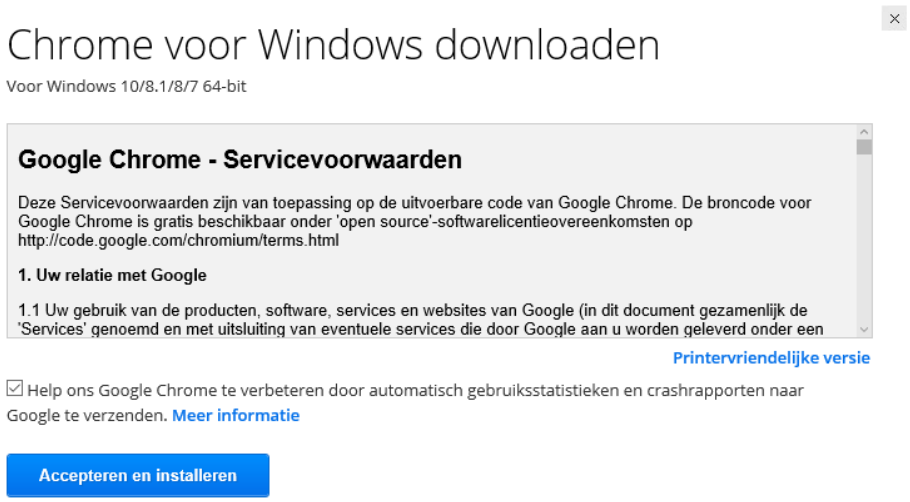
In de analysesectie wordt er getoetst hoe de categorieën (1) *meldingen*, (2) *instellingen* en (3) *voorlichting* zich verhouden met de designelementen in de drie browsers. Daarbij wordt er onderzocht hoe de designelementen bijdragen aan de handelingsmogelijkheid van gebruikers om secuur met data om te gaan. De analyse is opgedeeld per browser.

4.1 Google Chrome

4.1.1 Meldingen

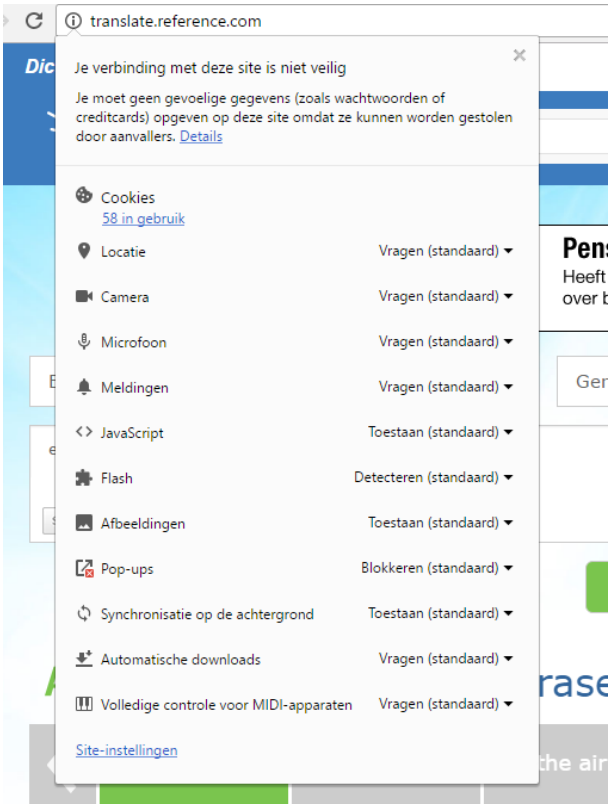
In de categorie (1) *meldingen* is er aandacht besteed aan een aantal punten. Allereerst is er gekeken of er meldingen getoond worden op het moment dat er data uitwisseling plaatsvindt. Daarnaast is er getoetst of de browser de gebruiker informeert waar de data heengaat en wie dit verzamelt. Ook meldingen over welke data er uitgezonden wordt door de gebruiker is meegenomen.

Op het moment dat Google Chrome gedownload wordt door de gebruiker, volgt er een pop-up met een overeenkomst (zie afbeelding 1). In dit document wordt gesproken met termen die gelden als vakjargon, wat zorgt voor een onoverzichtelijk geheel voor de gebruiker. In de sub-paragraaf (3) *voorlichting* wordt er dieper ingegaan op de overeenkomst. Onder het document is er iets opmerkelijks te vinden: gebruikers hebben een optie om automatisch gebruikersstatistieken en crashrapport naar Google te verzenden. Deze optie is standaard aangevinkt. Dit feit zal besproken worden in de sub paragraaf over (2) *instellingen.*



(Afbeelding 1)

Na de installatie van Chrome, zijn de websites *dictionary.com*, *msn.com* en *photobucker.com* bezocht. Tijdens het browsen werd er binnen (1) *meldingen* gelet op pop-ups of andere informatie over privacy en dataverzameling. Specifiek zijn de meldingen over *trackers* en *cookies* van belang, omdat er middels deze tools data wordt verzameld. De website *dictionary.com* werd als eerste bezocht. Tijdens het navigeren op de website verschenen er geen pop-ups of meldingen. Dit is bijzonder vanwege het artikel op de website van de Wall Street Journal (2016): de meeste *trackers* zouden op *dictionary.com* te vinden zijn. Na het bestuderen van de interface, viel er een icoontje op (afbeelding 2). In de linkerbovenhoek van de URL-balk is een informatie-icoon te vinden. Op het moment dat de gebruiker op het icoontje drukt, verschijnt er informatie over de website (afbeelding 2). De weergave van het icoontje is interessant; gebruikers krijgen informatie over instellingen en cookies, maar moeten zelf achter de mogelijkheid komen. Op het moment dat de gebruiker op details klik, opent de browser een website met uitleg over potentiele gevaren. Hier zal verder op ingegaan worden in de categorie (3) *voorlichting*. Als de gebruiker op *cookies* in gebruik of site-instellingen klikt (afbeelding 2) volgt er een scherm met instellingen over cookies op de website. Dit zal verder besproken worden in de categorie (2) *instellingen*. Na het bezoeken van de verschillende websites waren er volgens Chrome 58 *trackers* op *dictionary.com*, 68 *trackers* op *msn.com* en 323 *trackers* op *photobucket.com*. Bij ieder van de drie websites gaf het drop-down menu bij het icoontje aan, dat de website niet veilig was. Chrome stelt de gebruikers in staat om informatie op te doen over *trackers*, maar geeft hier geen uitleg bij.

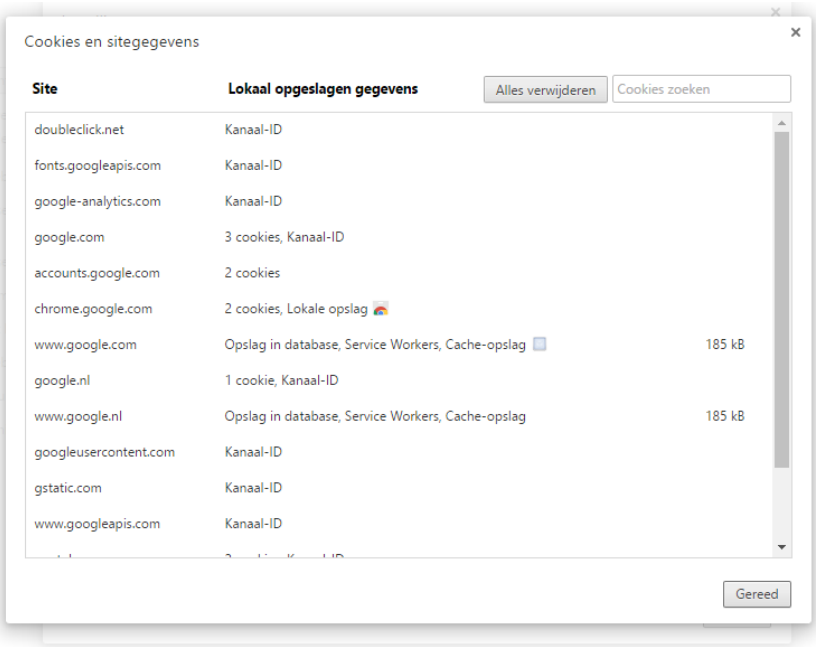


(Afbeelding 2)

4.1.2 Instellingen

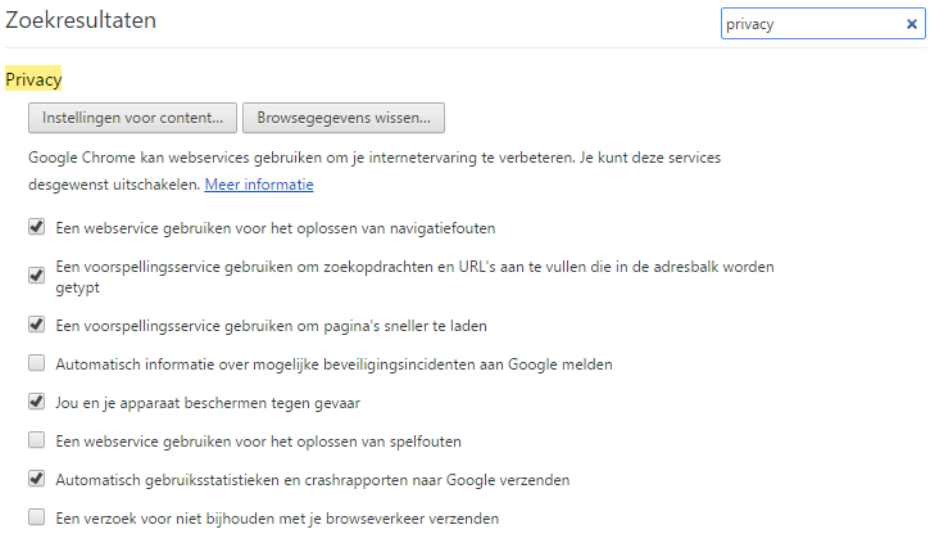
In de tweede categorie (2) *instellingen* is er onderzoek gedaan naar de opties die leiden tot de bescherming van gevoelige data. Het is hierbij belangrijk dat de opties al standaard in het voordeel van de gebruiker staan en dat de keuzes niet te ingewikkeld zijn. Het is in deze categorie essentieel dat gebruikers controle hebben over de browser zonder de nood over technische kennis (Friedman & Kahn, 2012, p. 1189).

Allereerst is de melding die gebruikers krijgen bij het installeren van Chrome opmerkelijk. Voordat de browser überhaupt is geïnstalleerd, worden gebruikers blootgesteld aan een optie die nadelig is: het verzamelen van crashrapporten en gebruikersstatistieken (afbeelding 1). De optie is standaard ingeschakeld en het is niet onwaarschijnlijk dat de meeste gebruikers weinig aandacht besteden aan deze pop-up. Op het moment dat de gebruiker klikt op de link naar meer informatie volgt een pagina met uitleg over crashrapporten. Op deze pagina ontbreekt toelichting over gebruikersstatistieken. Dit zal worden besproken in (3) *voorlichting*. Binnen de browsers is er ook onderzocht of er gebruik is gemaakt van *short-cut*s om belangrijke instellingen te tonen. Chrome doet dit aan de hand van het icoontje uit afbeelding 2. Het is mogelijk om direct een aantal instellingen aan te passen. Twee opties vallen direct op: gebruikers kunnen aanpassen of *javascript* en *flash* ingeschakeld zijn. Beide zijn plug-ins voor browsers, die gebruikt worden om content te visualiseren op websites. *Javascript* en *flash* staan bekend als gevaarlijk vanwege ontwerpfouten. Voor *trackers* is het mogelijk om via deze plug-ins gebruikersgegevens te bemachtigen. Zoals te zien in afbeelding 2 zijn beide opties ingeschakeld. De enige instelling die niet aanpasbaar is, betreft *cookies* (afbeelding 2). Pas op het moment dat de gebruiker op site-instellingen of op de hyperlink onder *cookies* klikt, volgt het scherm over *cookies*. Hierbij wordt er een overzicht getoond van alle *cookies*. In dit overzicht is er geen optie om *cookies* in - of uit te schakelen, maar is het wel mogelijk om *cookies* te verwijderen (afbeelding 3).



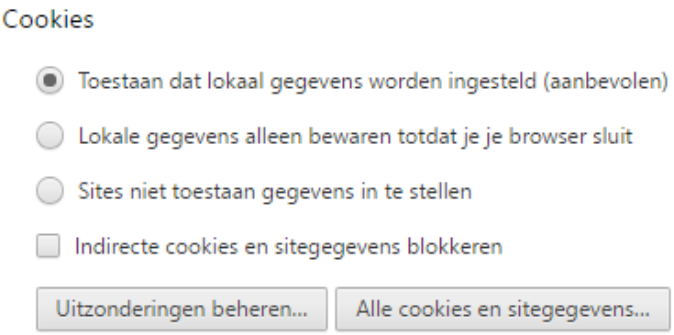
(Afbeelding 3)

Om bij het instellingenmenu te komen, moeten gebruikers via het drop-down menu rechts op instellingen klikken. Op het hoofscherm van de instellingen is niks over privacy of databescherming te vinden. Er kan beargumenteerd worden dat het handig is om dit soort instellingen zo toegankelijk mogelijk te maken voor gebruikers. Op het moment dat zulke opties verstopt zijn, is de kans groot dat gebruikers hier niet mee in aanraking komen. Om bij het privacy-menu te komen, moeten gebruikers het woord “privacy” intypen in de zoekbalk rechtsboven (afbeelding 4). De instellingen staan standaard niet in het voordeel van de gebruiker. Er worden namelijk gebruikersstatistieken verstuurd en er wordt geen verzoek verstuurd tot het niet bijhouden van browserverkeer.



(Afbeelding 4)

Daarnaast moeten gebruikers op instellingen voor content (afbeelding 4) drukken voordat de opties voor *cookies* zichtbaar worden (afbeelding 5). Ook hier staan de standaardinstellingen niet in het voordeel van de gebruiker: *cookies* worden toegestaan.



(Afbeelding 5)

Samenvattend kan er gesteld worden dat de standaardinstellingen van Chrome nadelig voor de gebruiker zijn. Alle opties die die dataverzameling mogelijk maken, staan ingeschakeld. Gebruikers hebben wel de mogelijkheid deze instellingen te controleren. Er wordt op een overzichtelijke manier getoond welke opties er zijn. Wel moeten gebruikers, vanwege het ontbreken van een *short-cut,* meer moeite doen om bij de privacy-instellingen te komen. Daarnaast is het binnen Chrome niet mogelijk om *cookies* van derde partijen te blokkeren.

Volgens het concept van *value-sensitive design* (Friedman & Kahn, 2002, p. 1189) moeten gebruikers controle krijgen over de opties wanneer nodig. Daarbij moeten gebruikers zo veel mogelijk kunnen veranderen zonder dat het te ingewikkeld wordt. Deze twee punten worden gewaarborgd door Chrome: gebruikers krijgen de mogelijkheid om alle opties te veranderen zonder het gebruik van ingewikkelde taal.

4.1.3 Voorlichting

Binnen de categorie (3) *voorlichting* is er getoetst of de taal en uitleg binnen de browsers duidelijk is. Gebruikers moeten geïnformeerd worden over keuzes die nadelig kunnen zijn. Deze categorie draagt bij aan (1) *meldingen* en (2) *instellingen,* omdat gebruikers door het toepassen van (3) *voorlichting* een betere keuze kunnen maken tussen het belang van bepaalde meldingen en het goed instellen van opties. Er moet gesproken worden in termen van potentiële effecten in plaats van technische mechanismen (Friedman & Kahn, 2002, p. 1191).

Tijdens het downloaden van Chrome verschijnt er een melding zoals beschreven in 4.1.1 (afbeelding 1). Om te toetsen of deze melding voldoet aan de voorwaarden van de categorie (3)

meldingen is het document onderzocht. De overeenkomst bevat veel verwijzingen naar andere documenten op het moment dat privacy besproken wordt. Gebruikers krijgen niet te zien waarmee ze akkoord gaan zonder het lezen van die andere documenten. Hierbij wordt er ook letterlijk gesteld dat als gebruikers akkoord gaan met de voorwaarden van de browser, hun gegevens gebruikt worden voor de diensten van Google. Er wordt verder niet in detail besproken wat deze keuze inhoudt en het document bestaat volledig uit vakjargon.

Aan de hand van afbeelding 2 wordt er besproken dat Chrome, na het klikken op het informatie-icoontje, de gebruiker inlicht over de veiligheid van een website. Ondanks dat de gebruiker zelf achter de mogelijkheid tot het inzien van deze melding moet komen, vind er voorlichting plaats. Als de gebruiker op details klikt dan volgt er een webpagina waar uitleg gegeven wordt over de gevaren van onveilige pagina's (afbeelding 6). Deze uitleg is helder en informeert gebruikers direct waarop ze moeten letten. Het is belangrijk om te noemen dat gebruikers zelf achter deze informatie moeten komen. Chrome begeleidt of informeert gebruikers niet proactief

Controleren of de verbinding van een site beveiligd is

Als u wilt controleren of het veilig is om een bepaalde website te bezoeken, kunt u de beveiligingsgegevens voor de site controleren. U krijgt een waarschuwing in Chrome als u de site niet veilig of via een privéverbinding kunt bezoeken.

1. Open een pagina in Chrome op uw computer.
2. Kijk naar de beveiligingsstatus links van het webadres om de veiligheid van de site te controleren:
   - Veilig
   - Informatie of Niet veilig
   - Niet veilig of Gevaarlijk
3. Klik op het pictogram om de details en rechten van de site te zien. Boven aan het venster ziet u een samenvatting van hoe privé de verbinding wordt beschouwd door Chrome.

(Afbeelding 6)

Bij het tonen van de keuze of gebruikers crashrapporten en gebruikersstatistieken willen verzenden naar Google ontbreekt er uitleg. De pagina die geladen wordt toont geen informatie over het verzamelen van gebruikersstatistieken, alleen over de verzameling van crashrapporten.

Google stelt de gebruikers van Chrome in staat om genoeg informatie op te doen over het veilig gebruik van de browser en de privacy-instellingen die daarbij horen. Het enige wat nadelig is voor de gebruikers is het feit dat er zelf actie ondernomen moet worden voor het opdoen van kennis. Chrome toont ook alleen maar passief informatie in plaats van dat het gebruikers actief voorlicht. Daarnaast is het document dat uitleg geeft over de voorwaarden onoverzichtelijk en moeilijk te begrijpen. Het is ook vreemd dat de informatie over gebruikersstatistieken niet te vinden is op de

pagina over gebruikersstatistieken. Over het algemeen is te stellen dat Chrome helder uitleg geeft over veilig browsen, op het moment dat gebruikers deze informatie kunnen vinden.

4.1.4 Terugkoppeling theorie

Aan de hand van de categorieën (1) *meldingen*, (2) *instellingen* en (3) *voorlichting* kan gesteld worden dat Chrome een aantal punten waarborgt en een aantal niet. Na het onderzoeken van de interface blijkt dat Chrome meldingen geeft over de aantal *trackers* die aanwezig zijn op websites. Dit gebeurt niet vanzelf; gebruikers moeten achter de mogelijkheid komen. Ook is de melding niet helemaal volgens de richtlijnen van het *value-sensitive design* (Friedman & Kahn, 2002, pp. 1171 -1201). Deze categorie draagt daarom gedeeltelijk bij aan de *affordance user-agency* over data. Gebruikers hebben de handelsmogelijkheid om door het designelement (1) *meldingen* in te zien dat er data verzameld wordt, maar niet welke data en wat er mee gebeurt. Ook moet er zelf actie ondernomen worden in plaats dat het designelement de gebruiker hierin meeneemt. De meldingen zijn daarom ook relationeel (Curinga, 2014); de geoefende gebruiker zal een stuk sneller achter deze mogelijkheid komen.

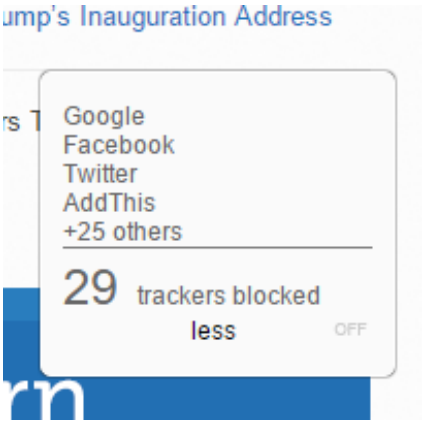
De instellingen van Chrome dragen ook gedeeltelijk bij aan de *affordance user-agency* om veilig met hun data om te gaan. Er zijn genoeg mogelijkheden om privacy-instellingen aan te passen en de opties worden overzichtelijk weergegeven. Wel staan deze opties al standaard niet in het voordeel van de gebruiker ingesteld. Ondanks dat dit niet per se nadelig is voor het behalen van de *affordance* is er wel sprake van een relationeel probleem: wederom zal de geoefende gebruiker eerder de instellingen aanpassen dan iemand die minder verstand heeft van software. Het designelement (2) *instellingen* draagt dus wel bij aan de handelingsmogelijkheid voor gebruikers maar zou dit beter kunnen doen door al standaard in het voordeel van de gebruiker te staan.

De designelementen in de categorie (3) *voorlichting* dragen ook gedeeltelijk bij aan het behalen van de *affordance*. Er is wel voorlichting over veilig browsen maar wederom moet de gebruiker hier zelf achter komen. Daarbij zijn de twee documenten over het verzamelen van gegevens onoverzichtelijk, vol vakjargon en incompleet. Gebruikers worden beperkt door de designelementen om de *affordance user-agency* te behalen: de documenten zijn moeilijk om te begrijpen. Daarnaast zouden de designelementen binnen (3) *voorlichting* idealiter de gebruiker al tijdens het browsen moeten voorlichten over wat veilige websites zijn.

4.2 Epic browser

4.2.1 Meldingen

Bij de installatie van Epic komt er geen privacy melding zoals besproken in de paragraaf over Chrome. Na het installeren zijn wederom de websites *dictionary.com*, *msn.com* en *photobucket.com* bezocht. De Epic browser heeft een functie die standaard ingeschakeld staat en gebruikers toont hoeveel *trackers* er op dat moment zijn (afbeelding 7). Epic doet dit proactief. Volgens de browser waren er op dictionary.com 29 *trackers*, op msn.com 7 *trackers* en op photobucket.com 33 *trackers*.



(Afbeelding 7)

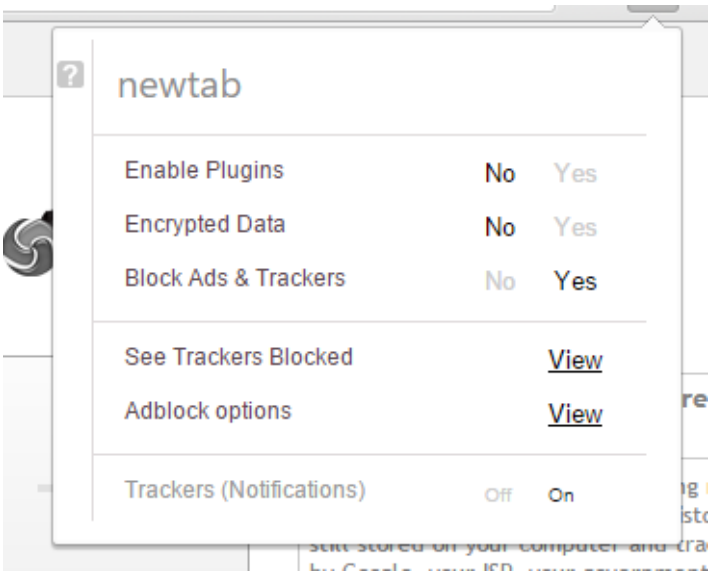
(Afbeelding 8)

De Epic browser heeft net als Chrome een aantal icoontjes waar meer informatie wordt getoond over de website. In de linkerbovenhoek is er een icoon die een pop-up opent waar staat of de website en de connectie veilig zijn (afbeelding 8). Het icoontje is niet opvallend en kan makkelijk over het hoofd worden gezien. Aan de rechterkant van de URL-balk zijn twee ander icoontjes te vinden; een paraplu en een rode stekker. Deze icoontjes zullen besproken worden in de sub paragraaf over (2) *instellingen*.

De categorie (2) *meldingen* wordt gedeeltelijk gewaarborgd binnen de Epic browser. Gebruikers krijgen proactief te zien wanneer er data wordt verzameld en welke *trackers* hier verantwoordelijk voor zijn. Net als bij Chrome mist er wel informatie over welke data er uitgezonden wordt en waar dit heen gaat. Ook is het icoontje dat informatie toont over de veiligheid van de website makkelijk over het hoofd te zien.

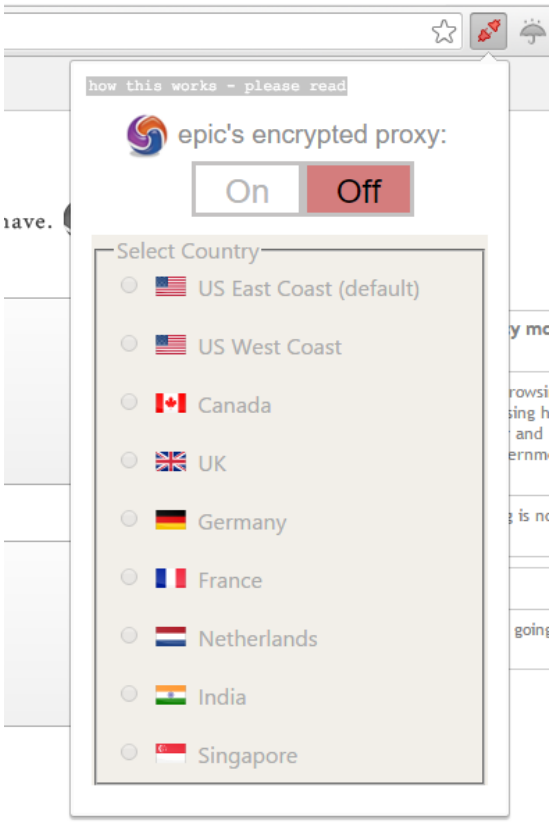
4.2.2 Instellingen

De Epic browser heeft net als Chrome een optie om middels een *short-cut* belangrijke instellingen te tonen. Het grote verschil met Chrome is dat Epic deze *short-cut* aan de rechterkant van de URL-balk toont en dit doet middels een paraplu. Dit valt de gebruiker al direct op; het icoontje roept op tot vragen. Op het moment dat men op het parapluutje drukt, verschijnt er een menu waarin de veiligheidsinstellingen aangepast kunnen worden (afbeelding 9). Hierin staan de instellingen *enable plug-ins*, *block ads & trackers* en *tracker notifications* standaard in het voordeel van de gebruiker. Zoals gesteld in de vorige paragraaf zijn plug-ins potentieel gevaarlijk en *ads en trackers* de reden van dataverzameling. Daarbij notificeert Epic de gebruiker als er *trackers* aanwezig zijn.



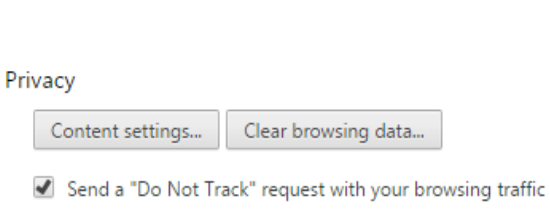
(Afbeelding 9)

Het rode icoontje waarbij stekkers worden afgebeeld leidt tot de mogelijkheid om een proxy in te schakelen. Dit is een mogelijkheid waarbij gebruikers anoniem en beveiligd kunnen browsen. De browser communiceert een ander IP-adres naar de websites. Hierdoor is het moeilijker voor websites en *trackers* de gebruiker te volgen (afbeelding 10).

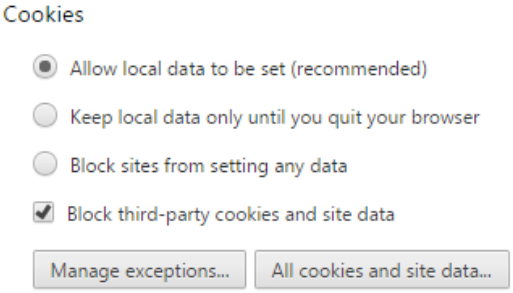


(Afbeelding 10)

Het daadwerkelijke menu is precies hetzelfde als Chrome. Dit komt omdat de browsers op hetzelfde raamwerk zijn gebouwd: *Chromium*. Dit houdt in dat qua basale werking de browsers overeenkomen. Er zijn twee belangrijke verschillen te vinden tussen de instellingen van Chrome en Epic. Ten eerste wordt er al standaard het verzoek tot niet volgen verstuurd tijdens het browsen (afbeelding 11). Ten tweede worden cookies van derde partijen geblokkeerd (afbeelding 12). Wel worden er door Epic *cookies* geaccepteerd.



(Afbeelding 11)

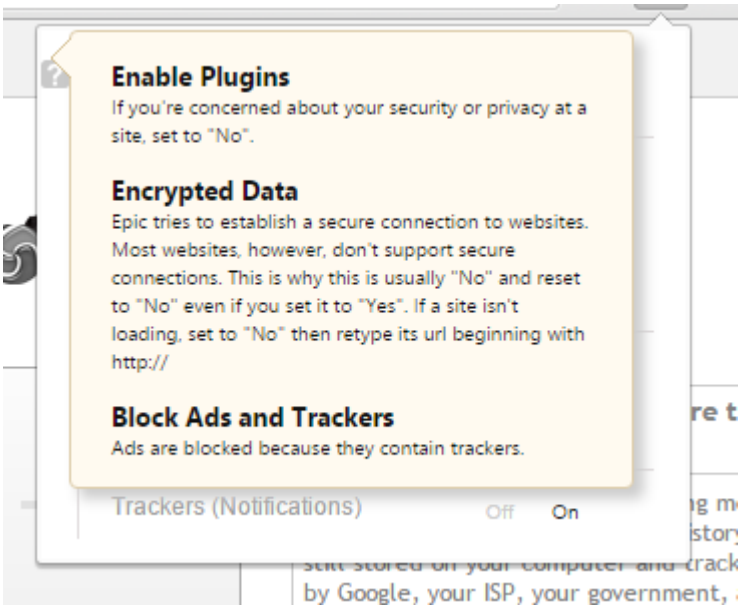


(Afbeelding 12)

Er kan gesteld worden dat Epic bijna hetzelfde scoort als Chrome binnen de categorie (2) *instellingen*. Gebruikers hebben de mogelijkheid om alle opties te veranderen en deze instellingen worden goed weergeven. Wel doet Epic het beter als het aankomt op standaardinstellingen: alle opties staan in het voordeel van de gebruiker. De *short-cuts* van Epic zijn ook beter dan Chrome; er is meer te veranderen zonder naar het instellingen menu te hoeven gaan.

4.2.3 Voorlichting

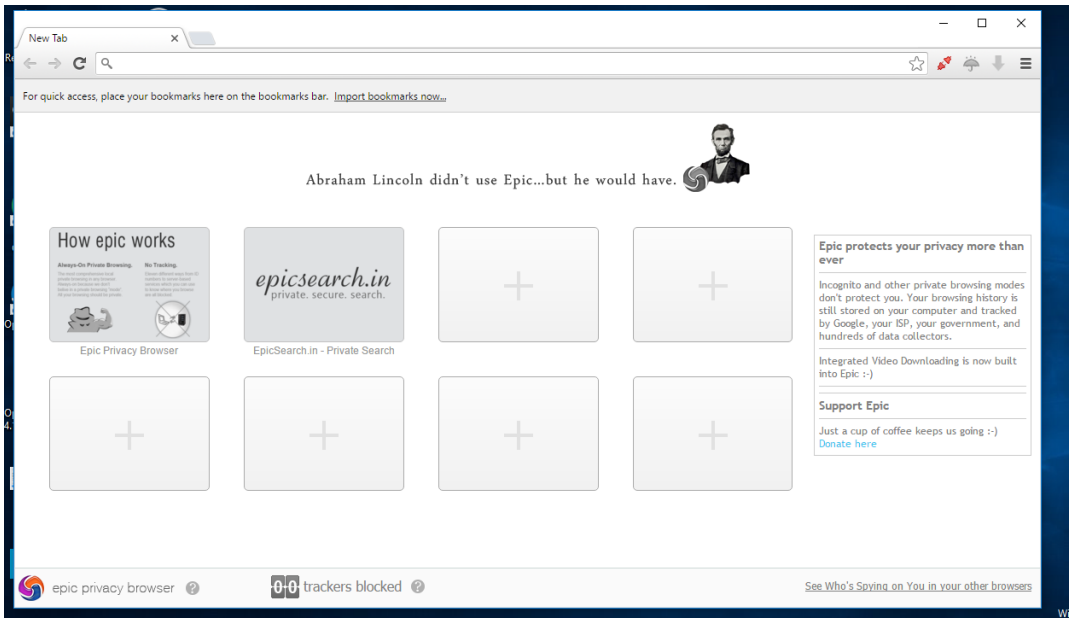
In de categorie (3) *voorlichting* doet Epic het goed vanwege een aantal redenen. Allereerst wordt er bij iedere instelling een linkje met extra informatie getoond. Een voorbeeld is het paraplu icoontje. Na het klikken op het parapluutje verschijnen er instellingen over veilig browsen. Op het moment dat de gebruiker op het vraagtekentje drukt (afbeelding 13) wordt er informatie getoond over wat de opties inhouden.



(Afbeelding 13)

Daarnaast toont Epic bij het openen van de browser direct een aantal links waar gebruikers informatie kunnen opdoen over veilig browsen en de werking van Epic (afbeelding 14). De links leiden tot pagina's waar zeer duidelijk, zonder het gebruik van vakjargon uitgelegd wordt hoe Epic werkt en wat het belang is van het beschermen van privacy.

De Epic browser waarborgt de laatste categorie door al in de browser gebruikers te informeren over het gebruik van bepaalde instellingen. De browser doet dit op een actieve manier door de informatie direct te implementeren in plaats van de gebruiker door te sturen naar een website. Ook is de informatie zoals getoond op de startpagina interessant: gebruikers worden uitgenodigd om kennis op te doen van veilig browsen.



(Afbeelding 14)

4.2.4 Terugkoppeling theorie

De Epic browser waarborgt een aantal punten goed en een aantal punten minder als het aankomt op het behalen van de *affordance* user-agency over data. Er wordt op een actieve manier gebruikt gemaakt van designelementen om de categorie (1) *meldingen* te ondervangen. Gebruikers hebben de mogelijkheid tot handeling, omdat er proactief meldingen worden getoond. Wel mist Epic de mogelijkheid om in te zien welke data er verzameld wordt en waar de data heen gaat. Kennis speelt hierbij geen rol; gebruikers hoeven niet zelf achter de optie tot inzage te komen (Curinga, 2014). Er kan gesteld worden dat de designelementen in categorie (1) *meldingen* zorgen voor het behalen van de *affordance* user-agency over data; informatie wordt op een proactieve, duidelijke manier getoond. Een minpunt is wel het nietszeggende icoontje aan de rechterkant van de URL-balk. Deze kan over het hoofd worden gezien.

De instellingen van Epic dragen bij aan de *affordance user-agency* over data. Dit komt door het feit dat alle instellingen in het voordeel van de gebruiker staan. Gebruikers zonder kennis hoeven zich hier niet druk om te maken. Daarnaast kunnen gebruikers door middel van de *short-cuts* snel

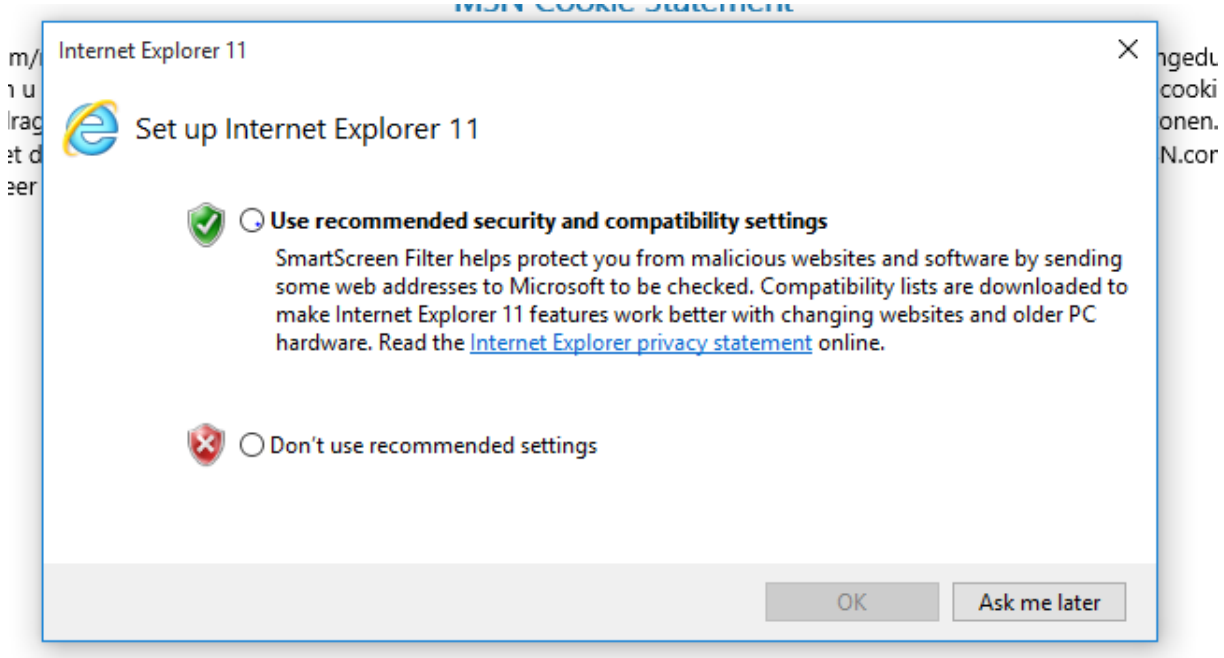
belangrijke instellingen veranderen. De designelementen binnen (2) *instellingen* dragen bij aan de *affordance* vanwege het gemak, overzicht en standaardinstellingen.

De laatste categorie wordt ook gewaarborgd door Epic. Gebruikers worden aan de hand van de designelementen meegenomen in welke keuze ze moeten maken en krijgen daarbij ook de mogelijkheid tot het opdoen van kennis. Dit versterkt de handelingsmogelijkheid van gebruikers. Ook lost dit het relationele probleem op: gebruikers kunnen ook al is er geen kennis van software of browsers, een weloverwogen keuze maken.

4.3 Internet Explorer

4.3.1 Meldingen

Internet Explorer geeft tijdens het installeren een melding over veilig browsen. Er wordt gevraagd of de gebruiker de standaardinstellingen wilt inschakelen. Dit zou volgens Internet Explorer gebruikers helpen om zich tegen kwaadaardige website te beschermen. Er wordt hier gesproken in duidelijke termen (afbeelding 15). De hyperlink die leidt tot uitleg van de privacy-statement van Internet Explorer wordt besproken in (3) *voorlichting*.



(Afbeelding 15)

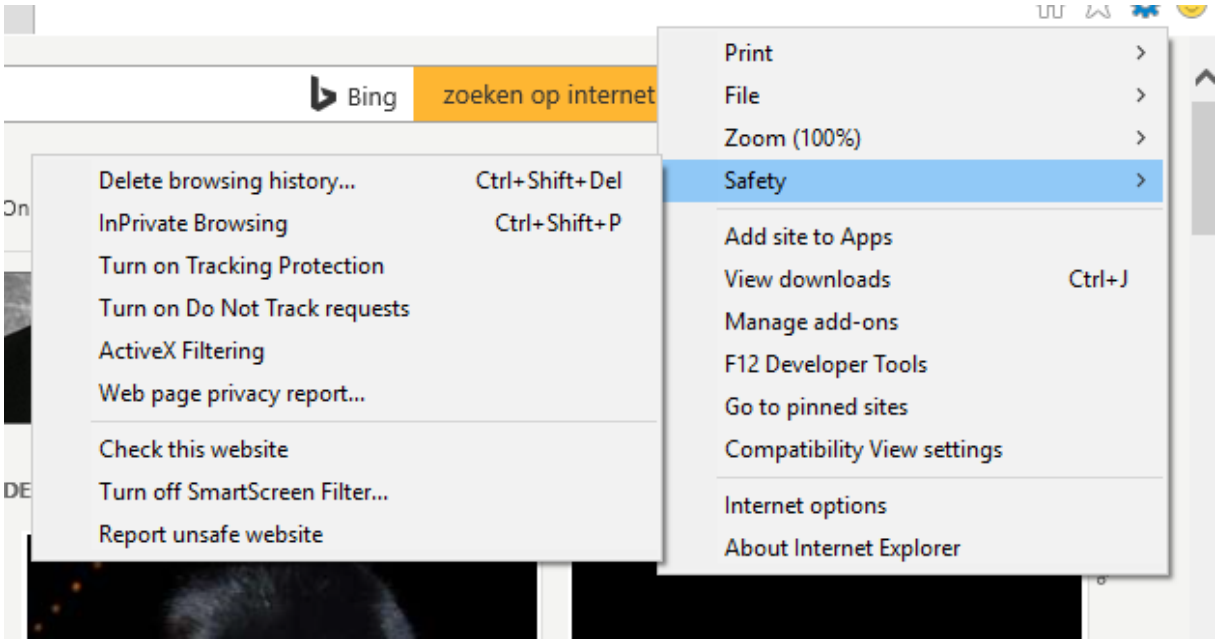
Tijdens het browsen met Internet Explorer viel er op dat er geen meldingen worden getoond over *trackers* of dataverzameling. Er zijn ook geen icoontjes te vinden waar meer informatie op gedaan kan

worden over de website. Internet Explorer mist de visuele hulpmiddelen die Chrome en Epic wel hebben.

Er kan aan de hand van de richtlijnen voor het *value-senstive design* (Friedman & Kahn, 2002, pp. 1171-1201) gesteld worden dat Internet Explorer niet voldoet aan de categorie (1) *meldingen*. Er is geen enkele informatie te vinden over veiligheid van websites of dataverzameling. Daarbij toont Internet Explorer ook geen mogelijkheid om in te zien wanneer er data verzameld wordt.

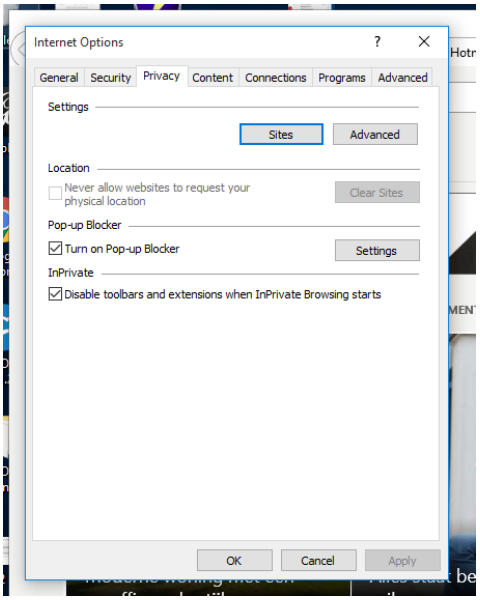
4.3.2 Instellingen

Zoals gesteld in de vorige sub-paragraaf mist Internet Explorer icoontjes met daarachter instellingen over privacy. Wel is er aan de rechterkant een drop-down menu te vinden waar er een aantal opties over privacy te vinden zijn. In dit menu staan *tracking protection* en *do not track* standaard uitgeschakeld. Op het moment dat gebruikers op *tracking protection* drukken, volgt er een lege pagina waar plug-ins geïnstalleerd kunnen worden. De optie wekt de indruk dat plug-ins die betrekking hebben op *tracking protection* al standaard geïnstalleerd zijn (afbeelding 16).

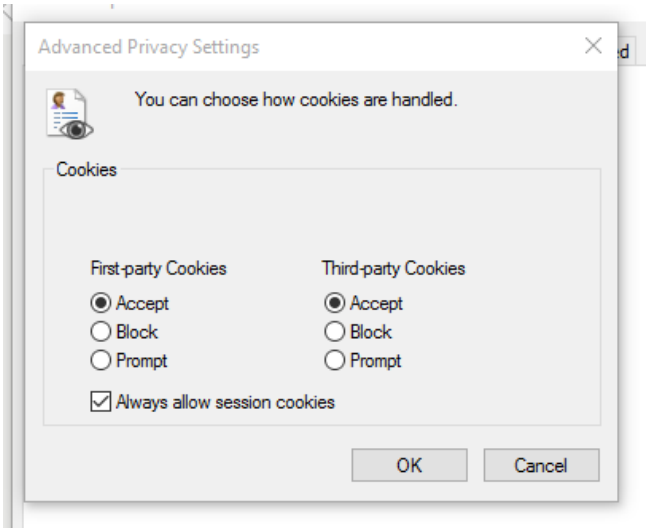


(Afbeelding 16)

Het instellingen-menu van Internet Explorer ziet er in verhouding met de twee andere browsers verouderd uit. Wel zijn de instellingen overzichtelijk ingedeeld (afbeelding 17). Op het moment dat de gebruiker naar de instellingen over privacy gaat, zijn de mogelijkheden beperkt. Het is alleen mogelijk om *cookies* en *cookies* van derde partijen in - en uit te schakelen. In verhouding met de andere twee browsers mist Internet Explorer de geavanceerde opties zoals het inzien van *cookies* en het blokkeren van bijvoorbeeld plug-ins. Daarnaast staan de instellingen standaard in het nadeel van de gebruiker. Wel zijn Epic en Internet Explorer de enige browsers die de mogelijkheid bieden om cookies van derde partijen te blokkeren. Chrome heeft deze instelling niet.



(Afbeelding 17)



(Afbeelding 18)

Internet Explorer scoort in de categorie (2) *instellingen* matig: standaard staan de opties niet in het voordeel van de gebruiker en zijn deze minder uitgebreid dan bijvoorbeeld Chrome en Epic. Ook mist er enige vorm van bescherming tegen *trackers*. Er wordt wel gebruik gemaakt van *short-cuts* om de privacy instellingen te tonen, alleen blijkt dat een van de *short-cuts* leidt tot een lege pagina. De opties zijn wel overzichtelijk weergegeven.

4.3.3 Voorlichting

Bij het installeren toont Internet Explorer een link naar de privacy-overeenkomst die gebruikers moeten accepteren op het moment dat ze gebruik maken van de browser. In dit document wordt er uitgelegd waar gebruikers mee akkoord gaan. Dit document bevat net als de overeenkomst van Chrome vakjargon en is daarom moeilijk te begrijpen. Tijdens het gebruik van de browser viel op dat er nergens uitleg is gegeven over dataverzameling. Ook mist Internet Explorer hulppagina's over veilig

browsen en opties die hierbij toepasselijk zijn. Er kan gesteld worden dat Internet Explorer de categorie (3) *voorlichting* helemaal niet waarborgt: gebruikers worden op geen enkel moment meegenomen in de voor - en nadelen van keuzes en het fenomeen dataverzameling.

4.3.4 Terugkoppeling theorie

In verhouding met de twee andere browsers doet Internet Explorer het slecht. Twee van de drie categorieën worden niet of slecht gewaarborgd. In de categorie (1) *meldingen* en de categorie (3) *voorlichting* presteert Internet Explorer het slechtst. De designelementen binnen (1) *meldingen* informeren gebruikers niet over dataverzameling. (1) *meldingen* draagt daarom niet bij aan de handelingsmogelijkheid voor gebruikers om veilig met hun data om te gaan. Bij de designelementen van (3) *voorlichting* doet Internet Explorer het ook slecht. Er zijn geen hulppagina's te vinden over veilig browsen en het document wat wordt getoond is moeilijk te begrijpen. Internet Explorer scoort wel punten als het aankomt op instellingen; gebruikers hebben de mogelijkheid om *cookies* van derde partijen te blokkeren.

Concluderend kan er gesteld worden dat de designelementen binnen de drie categorieën er niet voor zorgen dat gebruikers handelingsmogelijkheid hebben om veilig met data om te gaan. De *affordance user-agency* over data wordt daarom ook niet behaald.

5. Conclusie

De hoofvraag van dit onderzoek is: *op welke manieren waarborgen de designelementen in browsers de mogelijkheid voor gebruikers om de affordance user-agency over data te behalen.* De browsers waarborgen middels designelementen de hoofdvraag op een aantal manieren. Ten eerste zijn (1) *meldingen* een belangrijk designelement die gebruikers helpt om veilig met data om te gaan. De Epic browser presteert in deze categorie het best. Epic informeert gebruikers proactief over dataverzameling. Dit zorgt ervoor dat er *user-agency* kan ontstaan omdat een gebruiker aan de hand van de meldingen kan beslissen of zijn data veilig genoeg is. Google Chrome staat op de tweede plek. De browser geeft informatie over *trackers* en dataverzameling maar doet dit niet uit zichzelf. Internet Explorer scoort het slechts binnen (1) *meldingen*: er is geen enkele vorm van waarschuwing bij de uitwisseling van data.

De categorie (2) instellingen is een andere manier waarmee browsers gebruikers kunnen helpen om de *affordance* te behalen. De Epic browser en Google Chrome scoren goed omdat er *short-cuts* naar de privacy-instellingen zijn. Daarnaast is het menu overzichtelijk en wordt er uitleg gegeven. Wel scoort Epic beter dan Chrome omdat de instellingen in het voordeel van de gebruiker staan. Dit zorgt ervoor dat gebruikers zonder technische kennis ook veilig zijn. De designelementen binnen (1) *instellingen* bij Chrome en Epic dragen daarom bij aan het behalen van de *affordance*. Internet Explorer presteert wederom slechter. Dit komt vanwege het gebrek aan *short-cuts*, het verouderde interface en de standaardinstellingen. Wel geeft Internet Explorer de optie om *cookies* van derde partijen te blokkeren, Chrome heeft deze instelling niet.

De laatste categorie (3) *voorlichting* is mogelijk het meest belangrijk voor gebruikers. Dit is vanwege het feit dat browsers gebruikers kunnen informeren over veilig internet gebruik. De Epic browser scoort binnen deze categorie het best. Bij alle belangrijke instellingen is er uitleg gegeven in termen van voor - en nadelen. Daarnaast is er op de startpagina van Epic informatie te vinden over de werking van de browser en veilig internetgebruik. Chrome staat op de tweede plek; de browser geeft wel informatie maar gebruikers moeten hier zelf achter komen. Wel is het belangrijk om te noemen dat de documenten waarin uitleg wordt gegeven over dataverzameling, moeilijk te begrijpen zijn. Internet Explorer scoort ook binnen deze categorie het slechts. Er is geen enkele vorm van uitleg te vinden over instellingen en de veilige omgang met data.

Concluderend wordt er gesteld dat er een aantal manieren zijn die ervoor zorgen dat gebruikers de *affordance user-agency* over data kunnen behalen. Ten eerste zouden browsers gebruikers proactief moeten informeren over *trackers* en dataverzameling. Ten tweede moeten

instellingen overzichtelijk zijn en in het voordeel van de gebruiker. Als laatste moet voorlichting ervoor zorgen dat gebruikers kennis op kunnen doen van veilig browsen.

5.2 Discussie

Tijdens het onderzoek zijn er een aantal pijnpunten ontdekt. Allereerst is het onderzoek zeer beperkt van schaal. Er zijn nog veel verschillende browsers die niet zijn meegenomen in dit onderzoek. Een voorbeeld is Mozilla Firefox. Deze browser staat ook bekend als veilig. Daarnaast was er nog verdiepende theorie aanwezig over software. Hiermee had het theoretisch kader versterkt kunnen worden. Ook is de bias van de onderzoeker een belangrijk punt om te noemen. Al voor het onderzoek had ik kennis van browsers en software; dit zorgt ervoor dat er niet helemaal met een objectieve blik naar de browsers is gekeken.

Voor vervolgonderzoek is het interessant om te kijken hoe een grote groep mensen de browsers ervaren. Dit zou zorgen voor een betere afspiegeling van hoe browsers de *affordance* waarborgen. Ook zouden de gegevens hiermee gegeneraliseerd kunnen worden.

6. Bronnenlijst

Bilbao, B. (2016, April 8). Which Is the Most Secure Browser for 2016 – Firefox, Chrome, Internet Explorer, Safari - SensorsTechForum.com. Retrieved from http://sensorstechforum.com/which-is-the-most-secure-browser-for-2016-firefox-chrome-internet-explorer-safari-2

Curinga, M. X. (2014). Critical analysis of interactive media with software affordances. *First Monday*, *19*(9). Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/4757/4116

Dunn, J. (2016, February 25). The best 8 secure browsers | Security | Techworld. Retrieved from http://www.techworld.com/security/best-8-secure-browsers-2016-3246550/

Friedmanm, B., & Kahn, P. (2002). Human values, ethics and design. In *The Human-Computer Interaction Handbook* (pp. 1177-1201). Hillsdale: Erlbaum associates.

Gibson, J. J. (2015). Theory of affordances. In *The Ecological Approach to Visual Perception* (pp. 119-137). New York, NY: Psychology Press.

Gomez, M. L. (2016, January 22). Why Internet Explorer Is Getting More Dangerous. Retrieved from https://www.maketecheasier.com/internet-explorer-more-dangerous/

Henry, A. (2014, December 18). The Best Privacy and Security-Focused Web Browsers. Retrieved from http://lifehacker.com/the-best-privacy-and-security-focused-web-browsers-1672758270

Keizer, G. (2015, May 5). Chrome reaches major user share milestone, climbs above 25% | Computerworld. Retrieved from http://www.computerworld.com/article/2918996/web-browsers/chrome-reaches-major-user-share-milestone-climbs-above-25.html

Most popular U.S. multi-platform web properties 2016 | Statistica. (2016). Retrieved from https://www.statista.com/statistics/271412/most-visited-us-web-properties-based-on-number-of-visitors/

Norman, D. A. (2009). Natural interaction. In *The design of future things* (pp. 57-91). New York: Basic Books.

Norman, D. A., & Norman, D. (2013). Knowing what to do: constraints discoverability, and feedback. In *The Design of Everyday Things: Revised and Expanded Edition* (pp. 80-134). New York: Basic Books.

Shah, R. C., & Kesan, J. P. (2009). Recipes for cookies: how institutions shape communication technologies. *New Media & Society*, *11*(3), 315-336.

Stalder, F., & Mayer, C. (2009). The Second Index. Search Engines, Personalization and Surveillance |Future Non Stop. Retrieved from http://future-nonstop.org/c/609e8e4fa58aa59f8310958c4d2e4e37

Tsalis, N., Mylonas, A., & Gritzalis, D. (2016). An Intensive Analysis of Security and Privacy Browser Add-Ons. *Lecture Notes in Computer Science*, 258-273.

United States. (2016). *The CIA world factbook 2017*. New York: Skyhorse publishing.

Van Dijck, J. (2013). Facebook and the imperative of sharing. In *The culture of connectivity: A critical history of social media* (pp. 57-58). Oxford: Oxford University Press.

What They Know - WSJ. (2016). Retrieved from http://blogs.wsj.com/wtk/