VMC Studiemiddag

Verslag

Frederik Zuiderveen Borgesius*

De Vereniging voor Media- en Communicatierecht en de Vereniging voor Reclamerecht organiseerden op 25 juni 2010 een gezamenlijke studiemiddag over het onderwerp 'behavioral targeting'. Onder dit begrip valt onder meer het vastleggen van surfgedrag op het internet (bijvoorbeeld middels cookies) en het gebruik van deze gegevens om gericht te adverteren. Vanwege het steeds frequenter wordende gebruik van behavioral targeting en het feit dat er nieuwe Europese regels zijn opgesteld, is het debat over behavioral targeting weer opgelaaid.

Inleiding

Behavioral targeting blijft de gemoederen bezig houden en er was dan ook zoveel belangstelling voor de studiemiddag dat uitgeweken moest worden naar een grotere locatie. Arnoud Engelfriet (ICTRecht en Iusmentis) legde uit hoe behavioral targeting technisch in zijn werk gaat. María Verónica Pérez Asinari (European Data Protection Supervisor) behandelde de laatste ontwikkelingen op Europees niveau. Jeroen Koëter (De Brauw Blackstone Westbroek) besprak de Nederlandse rechtspraktijk. Professor Dennis Hirsch (Capital University Law School, Columbus, Ohio) ging in op de juridische aspecten van behavioral targeting in de Verenigde Staten. De middag werd voorgezeten door professor Jan Kabel (Instituut voor Informatierecht, Universiteit van Amsterdam). Hieronder volgt een verslag van de middag.

Engelfriet: wat zijn cookies en hoe werkt behavioral targeting?

Arnoud Engelfriet gaf een heldere uiteenzetting over de technische aspecten van cookies en behavioral targeting. '*Cookies*' zijn kleine tekstbestandjes die websitehouders op de computer van een internetgebruiker kunnen installeren. Op deze manier kan (de computer van) een gebruiker herkend worden. Dit kan praktisch zijn bij het onthouden van de inhoud van een virtueel winkelwagentje of het feit dat iemand is ingelogd bij een online e-maildienst. Zogenoemde '*session cookies*' worden automatisch verwijderd als de browser wordt afgesloten. '*Persistent cookies*' blijven daarentegen ook bewaard als de browser wordt afgesloten of de computer wordt uitgezet.

Elementen van een webpagina zijn doorgaans afkomstig van meerdere servers. Zo staan op nu.nl advertenties die worden geplaatst door Doubleclick, een dochterbedrijf van Google.[1] Sites zoals nu.nl worden in dit verband wel '*publishers*' genoemd. Bedrijven als Doubleclick, die een netwerk van websites van advertenties voorzien, worden wel '*ad network providers*' genoemd. Niet alleen publishers plaatsen cookies, maar ook derden zoals ad network providers doen dit. Deze cookies worden wel '*third party cookies*' genoemd.

Ad network providers plaatsen doorgaans persistent cookies en gebruiken die om het surfgedrag van een internetgebruiker te volgen. Als websites worden bezocht waar Doubleclick advertenties aan levert, dan registreert Doubleclick dat het om dezelfde internetgebruiker gaat. Op deze manier wordt het surfgedrag over sites die behoren tot een advertentienetwerk vastgelegd.[2]

Het is mogelijk om persoonsgegevens toe te voegen aan het surfprofiel dat wordt vastgelegd. Engelfriet gaf als voorbeeld Facebook, dat alle informatie uit het profiel dat iemand zelf heeft samengesteld, kan toevoegen aan het surfprofiel dat wordt vastgelegd aan de hand van sites waarop Facebook ook een functie aanbiedt.

Tegenwoordig bieden alle bekende browsers meer of minder geavanceerde mogelijkheden om cookies te beheren. Zo kan er voor worden gekozen alleen third party cookies te weren.[3]

* F.J. Zuiderveen Borgesius is student Onderzoeksmaster Informatierecht aan de Universiteit van Amsterdam en werkzaam bij SOLV Advocaten te Amsterdam.

1 Zie www.doubleclick.com.

2 Bij '*on-site behavioral targeting*' wordt het surfgedrag van internetgebruikers binnen één website vastgelegd. Deze vorm van behavioral targeting wordt hier niet verder behandeld.

3 Het vastleggen van surfgedrag kan overigens ook op andere manieren geschieden, bijvoorbeeld door het dataverkeer van een internetgebruiker bij de internet access provider te monitoren (deep packet inspection). Voor zover bekend wordt deze techniek in Europa momenteel niet (meer) toegepast.

Pérez Asinari: geamendeerde e-Privacyrichtlijn

María Verónica Pérez Asinari behandelde de geamendeerde e-Privacyrichtlijn,[4] de Dataprotectierichtlijn[5] en de recente opinie over behavioral targetingvan de Artikel 29 Werkgroep, het advies- en overlegorgaan van Europese privacytoezichthouders.[6] Indien een door middel van cookies aangelegd surfprofiel aangevuld wordt met de naam van een internetgebruiker, bijvoorbeeld nadat deze zijn naam ergens heeft ingevuld, dan is uiteraard de Dataprotectierichtlijn van toepassing. Er is dan immers sprake van de verwerking van persoonsgegevens.[7] Veel ad network providers betogen dat zij alleen weten dat een internetgebruiker met cookie '2vesgazbej45va555xsenyvs' op zijn computer bepaalde interesses heeft. Omdat zij de naam van die gebruiker niet weten, zouden zij geen persoonsgegevens verzamelen. De Artikel 29 Werkgroep is echter van mening dat er bij behavioral targeting doorgaans wel sprake is van de verwerking van persoonsgegevens. Een cookie kan immers gebruikt worden ter onderscheiding van een individu binnen een groep. Een naam is niet steeds noodzakelijk om een persoon te identificeren, aldus de Werkgroep.[8] Uit de reacties van het publiek bleek dat dit standpunt van de Werkgroep omstreden is. Velen waren van mening dat de regels van de Dataprotectierichtlijn niet toegepast zouden moeten worden op behavioral targeting.

Eind 2009 heeft de Richtlijn Burgerrechten[9] de e-Privacyrichtlijn gewijzigd. Volgens het geamendeerde lid 3 van artikel 5 van de de e-Privacyrichtlijn dient er een opt-in regel te gelden: cookies mogen slechts worden geplaatst indien de internetgebruiker toestemming heeft verleend, na te zijn voorzien van duidelijke en volledige informatie.[10] Er zijn twee uitzonderingen op deze opt-in regel. Ten eerste kan toestemming achterwege blijven indien een cookie wordt geplaatst met het enkele doel verzending van communicatie mogelijk te maken. Ten tweede kan toestemming achterwege blijven indien een cookie strikt noodzakelijk is om een uitdrukkelijk gevraagde dienst te leveren. Voor cookies die nodig zijn om in te loggen bij een e-maildienst of om een virtueel winkelwagentje te vullen, hoeft derhalve geen toestemming gevraagd te worden.

Deze opt-in regel wordt verder genuanceerd door overweging 66 van de Richtlijn Burgerrechten: 'Wanneer dit technisch mogelijk en doeltreffend is, kan, overeenkomstig de desbetreffende bepalingen van [de Dataprotectierichtlijn], de toestemming van de gebruiker met verwerking worden uitgedrukt door gebruik te maken van de desbetreffende instellingen van een browser of een andere toepassing'.

Volgens de Artikel 29 Werkgroep legt de nieuwe regeling ten aanzien van cookies samen met de Dataprotectierichtlijn mogelijk verplichtingen op aan drie categorieën partijen in de context van behavioral targeting. Ten eerste zijn er verplichtingen voor ad network providers. Deze plaatsen (third party) cookies en de regels ten aanzien van cookies gelden dus primair voor hen, ook als er geen persoonsgegevens worden verwerkt.[11] Daarnaast zijn zij verantwoordelijke in de zin van de Dataprotectierichtlijn indien zij persoonsgegevens verwerken.[12]

Ten tweede kunnen publishers een rol hebben als medeverantwoordelijke. De verantwoordelijkheid van de publisher hangt af van de manier waarop de publisher en de ad network provider samenwerken. Van geval tot geval moet worden beoordeeld hoe deze samenwerking is vormgegeven. Medeverantwoordelijkheid van de publishers houdt vooral in dat zij websitebezoekers goed moeten informeren over hun samenwerking met ad network providers en over het plaatsen van cookies.[13]

Ten derde is het mogelijk dat ook de adverteerders persoonsgegevens verwerken. In dat geval zijn zij te kwalificeren als een (mede)verantwoordelijke in de zin van de Dataprotectierichtlijn.[14]

Koëter: behavioral targeting en de Nederlandse rechtspraktijk

Jeroen Koëter besprak de Nederlandse rechtspraktijk.[15] In Nederland zijn de Telecommunicatiewet, de daarop gebaseerde regelgeving en de Wet Bescherming Persoonsgegevens kernregelingen ten aanzien van behavioral targeting. Op 24 mei 2011 dient de geamendeerde e-Privacyrichtlijn te zijn doorgevoerd in de nationale wetgeving.[16] Artikel 5 lid 3 zal worden geïmplementeerd in artikel 11.3a van de Telecommunicatiewet.[17]

Sommige organisaties in de marketingbranche gaan er op grond van overweging 66 van de Richtlijn Burgerrechten van uit dat er niets zal veranderen, omdat toestemming kan blijken uit browserinstellingen: business as usual.[18] Ook de Neder-

4 Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 7 maart 2002 van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (*PbEG* 2002, L 201/37).

5 Richtlijn 95/46/EG van het Europees Parlement en de Raad van de Europese Unie van 23 november 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (*PbEG* 1995, L 281/31).

6 Groep Gegevensbescherming Artikel 29, *Opinion 2/2010 on online behavioural advertising* (WP 171), Brussel: 22 juni 2010 (Verder: Artikel 29 Werkgroep, WP 171, 2010). Aangeraden wordt de Engelse versie te raadplegen, daar in de Nederlandse vertaling onder meer een ontkenning is weggevallen.

7 Artikel 1 lid 1 en artikel 2 sub a van de Dataprotectierichtlijn.

8 Artikel 29 Werkgroep, WP 171, 2010, p. 9.

9 Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische communicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming (*PbEU* 2009, L 337/11).

10 Het regime geldt niet alleen voor cookies, maar ook voor bijvoorbeeld adware en spyware.

11 Artikel 29 Werkgroep, WP 171, 2010, p. 10.

12 Artikel 2 (d) van de Dataprotectierichtlijn en artikel 1 (d) van de Wet bescherming persoonsgegevens.

13 Artikel 29 Werkgroep, WP 171, 2010, p. 11-12.

14 Artikel 29 Werkgroep, WP 171, 2010, p. 12.

15 Koëter heeft in 2009 een goed artikel geschreven over behavioral targeting: J. Koëter, 'Behavioral targeting en privacy: een juridische verkenning van internet gedragsmarketing', *Tijdschrift voor internetrecht* 2009-4, p. 104-111, http://bit.ly/a81tNa (verder: Koëter 2009).

16 Artikel 4 lid 1 van de Richtlijn Burgerrechten.

17 Zie www.internetconsultatie.nl/nrfimplementatie. Daarmee vervalt artikel 4.1 van het Besluit universele dienstverlening en eindgebruikersbelangen, waar momenteel de Nederlandse regeling ten aanzien van cookies (een opt-outsysteem) te vinden is.

18 Out-Law, 'Advertisers say that new cookie law is met by browser settings', *Out-Law News* 24 november 2009, www.outlaw.com.

landse regering lijkt inmiddels van mening te zijn dat de toestemming van de gebruiker kan blijken uit zijn browserinstellingen.[19]

Uit dezelfde overweging 66 blijkt echter dat toestemming in overeenstemming moet zijn met de Dataprotectierichtlijn. In die richtlijn is toestemming gedefinieerd als een 'vrije, specifieke en op informatie berustende wilsuiting'.[20] Volgens Koëter is het dan ook slechts in een zeer beperkt aantal gevallen mogelijk om toestemming te geven door middel van browserinstellingen.[21] Aangezien de gebruiker actief dient aan te geven dat hij een cookie accepteert, is de toestemming door middel van browserinstellingen alleen geldig, als een browser standaard alle cookies weigert. Momenteel worden door de meeste browsers echter standaard alle cookies geaccepteerd. Het is twijfelachtig of gesproken kan worden van toestemming als een internetgebruiker de standaardinstellingen van zijn browser niet aanpast.[22] Ook als een internetgebruiker zijn browser zo aanpast dat alle cookies (inclusief third party cookies) worden geaccepteerd, zijn niet alle problemen opgelost. Een dergelijke toestemming voor alle toekomstige, onbepaalde verwerkingen zou moeilijk te rijmen zijn met de eis dat toestemming 'specifiek' dient te zijn. Bovendien dient een internetgebruiker alvorens toestemming te geven geïnformeerd te worden. Ook dat is niet goed voorstelbaar als toestemming wordt gegeven middels browserinstellingen. Koëter is het dan ook met de Artikel 29 Werkgroep eens dat doorgaans geen toestemming voor cookies gegeven kan worden door middel van browserinstellingen. Meerdere aanwezigen spraken echter hun vrees uit voor de strenge interpretatie van de Artikel 29 Werkgroep.

Volgens Koëter, Pérez Asinari en de Artikel 29 Werkgroep moet de marketingbranche creatieve oplossingen bedenken om de praktijk in lijn te brengen met de nieuwe regelgeving. Koëter noemde drie mogelijke oplossingen, die afzonderlijk of gecombineerd overwogen zouden kunnen worden. Ten eerste zouden browserfabrikanten verplicht kunnen worden om de standaardinstellingen aan te passen.[23] Indien een browser als standaardinstelling heeft dat alle cookies worden geweigerd, is er in ieder geval een actieve handeling nodig van de internetgebruiker om cookies te accepteren. Een probleem blijft echter hoe de internetgebruiker geïnformeerd dient te worden.

Ten tweede zou een vorm van '*white listing*' kunnen worden overwogen.[24] Er zou een lijst samengesteld kunnen worden van cookies die niet geplaatst worden om het surfgedrag van internetgebruikers te monitoren. Gebruikers die er geen prijs op stellen dat hun surfgedrag wordt gevolgd zouden dan alleen cookies die op die lijst staan kunnen accepteren. Er zou dan bijvoorbeeld een plug-in voor browsers kunnen worden ontwikkeld die cookies die op de whitelist staan automatisch accepteert. Cookies die niet op die lijst staan moeten dan handmatig worden geaccepteerd. Een nadeel van deze oplossing is echter dat alleen internetgebruikers met afdoende technische kennis een dergelijke plug-in zouden gebruiken.

Een derde mogelijkheid is het aanbieden van een opt-outmogelijkheid via advertenties. Hierin kan worden aangegeven dat de advertenties worden geplaatst op grond van behavioral targeting, hetgeen de transparantie vergoot. Via de advertentie zou men dan ook direct moeten kunnen doorklikken naar het profiel dat de ad network provider heeft aangelegd, alsmede naar een pagina met een opt-outmogelijkheid.[25]

Hirsch: behavioral targeting in de Verenigde Staten

Professor Dennis Hirsch gaf een overzicht van de benadering van privacyregulering in de afgelopen dertien jaar in de Verenigde Staten, waar men geen met de Wet bescherming persoonsgegevens (Wbp) vergelijkbare privacywet kent.[26] Hirsch schetste een juridisch landschap waarin wetgeving niet wordt ingevoerd en zelfregulering niet wordt uitgevoerd.

In 1998 publiceerde de marketingbranche een zelfreguleringscode: de *Guidelines for Online Privacy Policies*.[27] Deze Guidelines schreven, behoudens enkele uitzonderingen, een opt-outsysteem voor. Hoewel de Guidelines niet bijzonder streng waren, werden ze grotendeels genegeerd. Ook het zelftoezicht verwaterde. In 2003 onderschreven nog slechts twee bedrijven de Guidelines.

Rond het jaar 2000 veranderde het klimaat in de Verenigde Staten en riep de Federal Trade Commission de regering op behavioral targeting wettelijk te reguleren.[28] In hetzelfde jaar werd de Children's Online Privacy Protection Act (COPPA) van kracht die de privacy van kinderen op het internet diende te beschermen.[29] Om de privacy op het internet te beschermen zijn er in de jaren die volgden tien wetsvoorstellen gedaan, die echter alle vroegtijdig sneuvelden.

Vervolgens spoorde de Federal Trade Commission in 2007 de marketingbranche opnieuw aan zichzelf te reguleren.[30] Dit leidde in 2009 tot de Self-Regulatory Principles for Online Behavioral Advertising.[31] Wederom wordt daarbij uitgegaan van een opt-outsysteem. De Principles bevatten geen systeem

19 Na de studiemiddag is dit bevestigd in een persbericht op Rijksoverheid.nl: 'Daarnaast moeten de internetbedrijven toestemming hebben verkregen voor het plaatsen van de cookie. Deze bepaling is zo uitgewerkt dat als het internetbedrijf de gebruiker goed heeft geïnformeerd, de toestemming van de gebruiker kan blijken uit de instellingen van het programma waarmee de gebruiker het internet op gaat. Hiermee is een en ander werkbaar voor internetbedrijven, maar wordt recht gedaan aan het goed informeren van de consument over zijn privacy.' (Rijksoverheid, 'Kabinet wil veilige en toegankelijke telecom', *Rijksoverheid* 2 juli 2010, www.rijksoverheid.nl.)

20 Artikel 2(h) van de Dataprotectierichtlijn.

21 Aldus ook Artikel 29 Werkgroep, WP 171, 2010, p. 13.

22 Aldus ook Artikel 29 Werkgroep, WP 171, 2010, p. 13-14.

23 Aldus ook: Europese Toezichthouder voor Gegevensbescherming, *Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy* (EDPS/10/6), Brussel: 22 maart 2010, www.edps.europa.eu, kantlijnnummer 92-98.

24 Aldus ook: O. van Daalen, 'Nieuwe regels voor cookies: wenselijk of niet?', *Bits of Freedom* 7 juni 2010, www.bof.nl.

25 Zie voor een voorbeeld: Interactive Advertising Bureau, *CLEAR Ad Notice (Control Links for Education and Advertising Responsibly)*, New York: IAB & NAI april 2010, www.iab.net/clear.

26 Zie voor een uitgebreide uiteenzetting van het Amerikaanse privacyrecht: D.J. Solove en P.M. Schwarz, *Privacy, Information and Technology*, Austin: Wolters Kluwer/Aspen 2009.

27 Zie www.privacyalliance.org/resources/ppguidelines.shtml.

28 Federal Trade Commission, *Online Profiling: A Report to Congress. Part 2*, Washington: July 2000, www.ftc.gov/os/2000/07/onlineprofiling.htm, par. III.

29 Zie www.ftc.gov/ogc/coppa1.htm.

30 Zie www.ftc.gov/opa/2007/12/principles.shtm.

31 Zie www.iab.net/media/file/ven-principles-07-01-09.pdf.

van onafhankelijk toezicht. Onder bedrijven lijkt er meer animo om deze Principles te onderschrijven dan het geval was ten aanzien van de Guidelines uit 1999.

Dit jaar is er echter weer hernieuwde aandacht voor regulering bij wet. Zo is er een wetsvoorstel gedaan door congreslid Rick Boucher.[32] Dit voorstel bevat voor de meeste categorieën persoonsgegevens een opt-outsysteem. Volgens de digitale burgerrechtenorganisatie Electronic Frontier Foundation zou de wet niet veel bescherming bieden.[33]

Samenvattend heeft in de Verenigde Staten zelfregulering tot nu toe nog weinig effect gehad om de privacy te beschermen, en lijkt de kans klein dat er op federaal niveau binnen afzienbare tijd een effectieve internetprivacywet wordt ingevoerd.

Hirsch heeft de eerste helft van 2010 onderzoek verricht naar Nederlandse privacyregulering bij het Instituut voor Informatierecht van de Universiteit van Amsterdam. Tijdens de studiemiddag presenteerde hij zijn eerste voorlopige onderzoeksresultaten. Na zijn onderzoek neigt Hirsch ernaar om de mogelijkheden van coregulering in de Verenigde Staten verder te onderzoeken. Hirsch verwees naar de Nederlandse praktijk, waarbij het College Bescherming Persoonsgegevens kan verklaren dat een gedragscode een juiste uitwerking vormt van de Wbp.[34] Coregulering biedt wellicht kansen om de impasse in de Verenigde Staten te doorbreken. Een voordeel van coregulering is dat regels meer draagvlak in de branche zouden kunnen hebben dan wetgeving. Ook zou coregulering wellicht kunnen leiden tot regelgeving die meer op de praktijk is toegesneden. Enkele mogelijke nadelen van coregulering zijn het gebrek aan democratische controle en de onduidelijke juridische status. Tot slot was Hirsch er niet zeker van of coregulering – een aanpak die goed past bij het Nederlandse poldermodel – wel gemakkelijk toegepast kan worden in de Verenigde Staten.

Aan beide kanten van de oceaan wordt nog volop geworsteld met privacybescherming op het internet en de effectiviteit van die bescherming laat te wensen over. Het ziet er niet naar uit dat het debat spoedig zal verstommen.

32 Zie www.boucher.house.gov/images/stories/Privacy__Draft__5-10.pdf.

33 R. San Miguel, 'The Draft Legislation That Could Make the Privacy Problem Worse', *E-Commerce Times* 6 juni 2010, www.ecommercetimes.com.

34 Hoofdstuk 3 van de Wet bescherming persoonsgegevens.