Je geld of je gegevens

De keuze tussen privacybescherming en gratis internetdiensten

Bart van der Sloot[1]

In plaats van geld vragen veel internetbedrijven (ongemerkt) persoonsgegevens voor hun diensten, op basis waarvan zij persoonsgerichte reclames tonen. In een bij de Tweede Kamer aanhangige wet wordt deze methode aan banden gelegd. Maar een te stringent model kan de huidige infrastructuur van het internet schaden daar veel internetbedrijven hun diensten slechts gratis kunnen leveren bij de gratie van een verdienmodel gebaseerd op persoonsgerichte reclames.

Stel, u heeft hard gewerkt, besluit een avondje vrij te nemen en vraagt zich af of er een aardig programma op tv is. U surft naar de gratis internetdienst tvgids.nl om zich te verwittigen van het aanbod van die avond. Zonder dat u daar erg in heeft, plaats tvgids een klein tekstbestand (cookie) op uw computer om die een uniek herkenningsteken te geven.[2] Hiermee kan een site uw computer herkennen en kan zij bepaalde gegevens opslaan, zodat u bij herhaald bezoek niet telkenmale uw gebruikersnaam en wachtwoord hoeft in te vullen of uw taalinstellingen hoeft te wijzigen. Echter, naast het feit dat de tvgids een cookie plaatst, worden er bij een bezoek aan de site tevens 68 cookies van derde-partijen geplaatst,[3] die zodoende tevens uw internetgedrag kunnen registreren. Facebook plaatst bijvoorbeeld via elke site waarop een 'Vind ik leuk'- of 'Aanraden'-knop valt te zien een cookie op uw computer.[4] Dientengevolge verkrijgt Facebook een schat aan informatie over uw websitebezoek en uw interesses. Ook Google, die de meeste advertenties toont die u op het internet ziet, zoals op Telegraaf.nl en Funda.nl, plaatst middels elk van deze advertenties een cookie op uw computer.[5]

Doordat deze bedrijven zo een nauwkeurig beeld krijgen van welke websites u bezoekt, op welke artikelen of items u klikt, hoe vaak u deze sites bezoekt en hoelang, krijgen zij een nauwkeurig beeld van uw interesses. De reclames

Facebook plaatst via elke site waarop een 'Vind ik leuk'- of 'Aanraden'-knop valt te zien een cookie op uw computer

die op internetpagina's worden getoond, zijn dan ook in toenemende mate gekoppeld aan een uniek persoonsprofiel dat op basis van het geregistreerde internetgedrag wordt vervaardigd. Zo kan het voorkomen dat twee personen die dezelfde website op hetzelfde moment bezoeken een verschillende advertentie te zien krijgen. Deze persoonsgebonden reclames zijn effectiever dan algemene reclames: een modefetisjist zal zich immers eerder laten verleiden door de nieuwe collectie van Zara dan door afgeprijsde Zeemanshirtjes.

Met het op grote schaal verzamelen van persoonsgegevens zijn vele gevaren gemoeid; zo bestaat er het gevaar voor misbruik, voor datalekken en voor het feit dat organisaties persoonsgegevens doorverkopen aan derde-partijen.[6] Bovendien komt de autonomie en zelfbeschikking van internetgebruikers in het gedrang nu zij

Auteur

1. Mr. drs. B. van der Sloot is onderzoeker aan het Instituut voor Informatie Recht (IViR) van de UvA. Hij is medeauteur van de onlangs verschenen studie voor de OPTA: L. Kool, A. van der Plas, N. van Eijk, N. Helberger & B. van der Sloot, 'A bite too big: Dilemma's bij de implementatie van de Cookiewet in Nederland', www.ivir.nl/publicaties/vaneijk/A_bite_too_big.pdf.

Noten

2. ENISA, 'Bittersweet cookies. Some security and privacy considerations', www.enisa.europa.eu/act/it/library/pp/cookies/at_download/fullReport.

3. www.consumentenbond.nl/test/elektronica-communicatie/internet-en-software/veiligonline/extra-informatie/cookies-test/.

4. A. Roosendaal, 'Facebook tracks and traces everyone: Like this!', SSRN 2011-1717563.

5. www.google.com/doubleclick/.

6. Het is dan ook zuiverder om van data-protectie- in plaats van privacyproblemen te spreken. B. van der Sloot, 'Het plaatsen van cookies ten behoeve van behavioural targeting vanuit privacyperspectief', *P&I* 2011-2.

doorgaans geen weet hebben van dit fenomeen. Naar aanleiding van nieuwe Europese regelgeving[7] vereist een wet ter wijziging van de Telecommunicatiewet,[8] die thans aanhangig is bij de Tweede Kamer, dat voordat er een cookie mag worden geplaatst, de internetgebruiker moet worden geïnformeerd en hij zijn toestemming moet hebben gegeven.[9] Er woedt momenteel zowel op Europees als op nationaal niveau een verhit debat over de wijze waarop het informatie- en toestemmingsvereiste in de praktijk moet worden ingevuld, waarbij moet worden bedacht dat de Wet bescherming persoonsgegevens (WBP) op beide punten extra vereisten stelt, daar de door de cookies verzamelde gegevens doorgaans naar een persoon zijn te herleiden en die wet derhalve tevens van toepassing is.[10] Het dilemma bestaat eruit dat indien er wordt gekozen voor een stringente, privacybeschermende invulling van de eisen, dit mogelijke consequenties kan hebben voor de internetomgeving zoals zij thans bestaat, maar dat indien er wordt gekozen voor het in stand houden van de huidige praktijk, dit grote gevolgen heeft voor de gegevensbescherming van de internetgebruikers. In plaats van een radicale keuze voor het een of het andere, dient er te worden geopteerd voor een gedifferentieerd model, dat onderscheid maakt tussen het soort en de aard van de geplaatste cookies.

Informatievereiste

Het informatievereiste uit de aanhangige wet bepaalt dat eenieder die een cookie wenst te plaatsen 'de gebruiker duidelijke en volledige informatie [dient] 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'.[11]

Het kan gebeuren dat twee personen die dezelfde website op hetzelfde moment bezoeken een verschillende advertentie te zien krijgen

De WBP eist daarenboven dat degene die persoonsgegevens verwerkt in ieder geval zijn identiteit dient te vermelden.[12] In de huidige praktijk worden internetgebruikers doorgaans van deze zaken op de hoogte gesteld middels de 'privacy policy' op een website, die vaak slecht te vinden en moeilijk leesbaar is. De memorie van toelichting bij de thans aanhangige wet stelt dan ook dat deze praktijk in de toekomst onvoldoende zal zijn om aan het wettelijk kader te voldoen.[13]

Om de transparantie en informatieverstrekking te bevorderen, hebben een aantal marktpartijen een zogenoemd I-Icon ontwikkeld.[14] Als dit icoon op een website wordt getoond, betekent dit dat er een advertentie op basis van persoonlijke voorkeuren wordt getoond. Door op het icoon te klikken, krijgt de gebruiker informatie over de advertentie, de adverteerder en de wijze waarop de reclame-uiting tot stand is gekomen. Alhoewel dit initiatief valt toe te juichen, is het onwaarschijnlijk dat hiermee aan het juridische kader wordt voldaan daar de logica achter zowel het informatie- als het toestemmingsvereiste is dat de consument zijn autonomie en zelfbeschikking herkrijgt. De regeling vereist dan ook dat de informatie dient te worden verstrekt vóór het moment dat een cookie wordt geplaatst en de gegevens worden benut voor reclamedoeleinden, waarvan bij het getoonde I-Icon geen sprake is.

Door privacyvoorvechters wordt dan ook geopperd om met een zogenoemde pop-up te werken, een beeld dat verschijnt zodra er een cookie wordt geplaatst en waarop valt te lezen door wie dit geschiedt en voor welke doeleinden. Zo is verzekerd dat de gebruiker per cookie wordt geïnformeerd vóór of tijdens het moment dat deze wordt geplaatst. Echter, als er meerdere cookies per webpaginabezoek worden geplaatst dan komt dit noch het gebruikersgemak ten goede, noch draagt het zorg voor een betere bescherming van de autonomie van de internetgebruikers, nu het de vraag is of de gebruiker zich de moeite zal getroosten alle informatie ook daadwerkelijk tot zich te nemen. Ook deze methode is derhalve onbevredigend, temeer daar zulk een stringente regeling wel eens de doodsklap voor persoonsgerichte internetreclame zou kunnen betekenen, aangezien het plaatsen van cookies het internetgebruik dan hindert.

Toestemmingsvereiste

Eenzelfde dilemma doet zich voor ten aanzien van het toestemmingsvereiste. In de thans aanhangige wet wordt vereist dat een ieder die een cookie wenst te plaatsen 'van de gebruiker toestemming [dient] te hebben verkregen voor de desbetreffende handeling'.[15] Daarbij dient voor het begrip toestemming aansluiting te worden gezocht bij de WBP,[16] die toestemming definieert als elke ondubbelzinnige 'vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt'.[17] In de huidige

Cookies

Door de computer van iedere gebruiker van een uniek herkenningsteken (een cookie) te voorzien, kunnen bedrijven het internetgedrag van gebruikers minutieus volgen. In een bij de Tweede Kamer aanhangige wet wordt deze methode aan banden gelegd door te eisen dat vóór plaatsing van een cookie de geïnformeerde toestemming van de internetgebruiker moet zijn verkregen. Over de praktische invulling van dit vereiste bestaat echter discussie nu een te soepele invulling de privacy van internetgebruikers kan ondermijnen en een te stringent model de huidige infrastructuur van het internet kan schaden daar veel internetbedrijven hun diensten slechts gratis kunnen leveren bij de gratie van een verdienmodel gebaseerd op persoonsgerichte reclames. Daarom dient er voor een gedifferentieerd model te worden gekozen, dat cookies afhankelijk van hun soort en aard aan banden legt of toestaat.

© Corbis

praktijk kan de gebruiker slechts achteraf een geplaatst cookie weigeren door deze te verwijderen. Dit zal echter onvoldoende zijn om aan de te implementeren bepaling te voldoen, die voorafgaande toestemming vereist.

Marktpartijen wijzen op de mogelijkheid om middels browserinstellingen bepaalde of alle cookies van tevoren te weigeren, wat een vorm van toestemming met zich mee zou brengen.[18] Echter, gezien het feit dat deze instellingen doorgaans standaard alle cookies accepteren en de gemiddelde gebruiker niet weet dat hij door middel van zijn browserinstellingen toestemming geeft voor het plaatsen van cookies, zal dit niet afdoende zijn om aan het toestemmingsvereiste te voldoen.[19] Dit is niet anders nu er nieuwe browsers worden vervaardigd waarbij de gebruiker bij het eerste gebruik de browser zelf moet instellen, daar deze 'browsertoestemming' hoogstens een generieke vorm van toestemming met zich meebrengt, dat wil zeggen alle mogelijk te plaatsen cookies betreft, terwijl de WBP een specifieke vorm van toestemming vereist.[20]

Ook ten aanzien van het toestemmingsvereiste pleiten privacyvoorvechters voor een pop-up per cookie, waarbij de gebruiker per keer moet aanklikken of hij akkoord gaat met het plaatsen ervan of niet. Deze methode draagt zorg voor een specifieke toestemming of weigering per cookie en voldoet zodoende aan het wettelijk kader. Toch is het wederom de vraag of dit het gebruikersgemak en de autonomie van de internetgebruiker ten goede zal komen.[21] Sommige internetdiensten zullen slecht toegankelijk worden, het huidige verdienmodel van veel deze diensten wordt bemoeilijkt en het is de vraag of gebruikers inderdaad ten aanzien van elk cookie een afgewogen oordeel zullen vormen over de wenselijkheid van de plaatsing daarvan.

Een gedifferentieerd model

De invulling van zowel het informatie- als het toestemmingsvereiste is derhalve problematisch als wordt uitgegaan van een uniform systeem voor alle cookies. Een

7. Richtlijn 2009/136/EG (Richtlijn burgerrechten) ter wijziging van Richtlijn 2002/58/EG (e-Privacyrichtlijn). P. Traung, 'EU Law on Spyware, Web Bugs, Cookies, etc., Revisited: Article 5 of the Directive on Privacy and Electronic Communications', *Business Law Review* 2010-10. M. Bolhuis, 'Regulering van cookies – papier of praktijk?', *Mediaforum* 2011-3.

8. Wijziging van de Telecommunicatiewet ter implementatie van de herziene telecommunicatierichtlijnen, *Kamerstukken II* 2010/11, 32 549, nr. 2.

9. De huidige, niet minder stringente regels uit het Besluit universele dienstverlening en eindgebruikersbelangen hebben tot nu toe nauwelijks handhavingprioriteit gekregen. Uitzondering is Rb. Rotterdam 3 februari 2010, *LJN* BL2092. OPTA onderzoekt momenteel hoe de toekomstige bepaling het best kan worden gehandhaafd. www.opta.nl/nl/actueel/alle-publicaties/publicatie/?id=3334.

10. Groep gegevensbescherming artikel 29, Advies 2/2010 over online reclame op basis van surfgedrag ('behavioural advertising'), *WG* 171, 2010, Brussel. (WG 171).

11. Art. 11.7a lid 1 WBP, *Kamerstuk* 32 549/2.

12. Art. 33-34 WBP.

13. *Kamerstuk* 32 549/3, p. 78.

14. www.aboutads.info/. M. Hastak & M. J. Culnan, 'Future of Privacy Forum. Online Behavioral Advertising "Icon" Study', http://futureofprivacy.org/final_report.pdf.

15. Art. 11.7a lid 1 WBP, *Kamerstuk* 32 549/2.

16. Art. 2 onderdeel f e-Privacyrichtlijn.

17. Art. 1 onderdeel i jo. 7 WBP.

18. Daarbij verwijzend naar overweging 66 Richtlijn burgerrechten.

19. *Kamerstuk* 32 549/3, p. 79.

20. F.J. Zuiderveen Borgesius, 'De nieuwe cookieregels: alwetende bedrijven en onwetende internetgebruikers?', *P&I* 2011-1. Daarbij moet tevens worden bedacht dat de normadressant van de wet degene is die het cookie plaatst.

21. F. Sickinghe & M. Geus 'Implementatie van de herziene Europese telecomrichtlijnen (deel I): De vrijheid van de nationale wetgever in het nieuwe woud van regulering', *Mediaforum* 2010-7/8.

Door privacyvoorvechters wordt geopperd om met een pop-up te werken, een beeld dat verschijnt zodra er een cookie wordt geplaatst

gedifferentieerd model lijkt dan ook beter op zijn plaats. De cookiebepaling in de thans aanhangige wet maakt reeds onderscheid tussen twee soorten cookies; slechts met betrekking tot niet-functionele cookies geldt de informatie- en toestemmingsverplichting, terwijl functionele cookies, die het gebruik van een internetdienst ondersteunen door bijvoorbeeld wachtwoorden of taalinstellingen op te slaan, hiervan zijn uitgezonderd.[22] Daarnaast laat de wet ruimte om verder te differentiëren door bij algemene maatregel van bestuur nadere regels te stellen met betrekking tot het informatie- en toestemmingsvereiste.[23]

Voor zogenoemde First Party-cookies, die worden geplaatst door de eigenaar van de bezochte website, zou in een gedifferentieerd model een licht regime kunnen gelden, waarbij het I-Icon en niet-voorgeprogrammeerde browserinstellingen zouden volstaan, terwijl voor Third Party-cookies,[24] die worden geplaatst door derden, er wel degelijk pop-ups zouden moeten verschijnen. De gemiddelde internetgebruiker weet immers niet en hoeft ook niet te weten dat er bij een bezoek aan de tvgids 68 cookies van derdepartijen worden geplaatst. Door pop-ups wordt hij daarvan op de hoogte gesteld en kan hij besluiten deze te weigeren.

Daarenboven kan er worden gedifferentieerd tussen zogenoemde http-cookies en overige cookies, zoals flash-cookies[25] en ever-cookies.[26] Http-cookies zijn de 'normale' cookies, die worden geplaatst in de browser en die relatief eenvoudig zijn te verwijderen en te blokkeren. Daarnaast zijn er echter tevens cookies die zich nestelen in verborgen plekken op de computer, zoals de flash player of elders. Naast het feit dat er weinig kennis bestaat over het bestaan van dit soort cookies, hoe ze kunnen worden verwijderd en geblokkeerd, zijn ze soms haast onverwijderbaar en worden ze gebruikt voor evident onrechtmatige praktijken zoals respawning, het ongemerkt herstellen van expliciet verwijderde http-cookies.[27] Door slechts http-cookies toe te staan, worden dit soort praktijken onmogelijk.

Tot slot kan er een onderscheid worden gemaakt tussen zogenoemde session-cookies, die na het afsluiten van de browser automatisch worden verwijderd, en persistent-cookies, die langer dan vijftig jaar op een computer kunnen blijven staan en ook gedurende die tijd het gedrag van een internetgebruiker kunnen volgen. Hieraan zou de wetgever een halt moeten toeroepen door het plaatsen van persistent-cookies geheel te verbieden of de toegestane levensduur sterk te begrenzen. Zodoende blijven de cookies slechts voor een beperkte periode staan, kan er slechts een beperkt persoonsprofiel worden opgebouwd en verliest het informatie- en toestemmingsprincipe niet aan belang. Dat dit geenszins een belemmering hoeft te vormen voor de reclamemogelijkheden van internetbedrijven blijkt wel uit het feit dat er steeds meer met zogenoemde 'liveprofielen' wordt gewerkt, die slechts worden opgebouwd gedurende één internetsessie, actueler zijn en daarom vaak effectiever dan langdurig opgebouwde profielen.[28]

Conclusie

In plaats van geld vragen veel internetdiensten (ongemerkt) persoonsgegevens voor hun gratis diensten, op basis waarvan zij persoonsgerichte reclames tonen.
De methode om deze gegevens te registreren, het plaatsen van cookies, wordt in een thans aanhangige wet aan banden gelegd door te eisen dat alvorens plaatsing de geïnformeerde toestemming van de gebruiker moet zijn ontvangen. De praktische invulling hiervan ligt echter gevoelig daar een te stringente uitleg het gebruiksgemak en het verdienmodel van internetbedrijven hindert en een te vrijblijvende invulling nadelige consequenties heeft voor de privacybelangen van internetgebruikers. Een gedifferentieerd model kan een oplossing bieden door functionele cookies vrij te stellen van verplichtingen, First Party-cookies aan een licht en Third Party-cookies aan een zwaar regime te onderwerpen, andere dan http-cookies te verbieden en persistent-cookies te verbieden of hun levensduur sterk aan banden te leggen. Door niet voor een uniforme, maar voor een gedifferentieerde benadering te kiezen, worden de privacybelangen van internetgebruikers veiliggesteld en wordt het internetbedrijven desondanks niet onmogelijk gemaakt om middels advertentie-inkomsten een lucratief verdienmodel te exploiteren. Doordat veel bedrijven die zich op deze markt begeven in Nederland zijn gevestigd, de cookies op in Nederland staande computers worden geplaatst en de daarmee verkregen gegevens meestentijds binnen Nederland of Europa worden verwerkt, is het Nederlandse recht niet alleen van toepassing, maar ook zeer goed handhaafbaar.[29] Ook op bedrijven, zoals Google en Facebook, die hun belangrijkste vestigingen en activiteiten in de Verenigde Staten ontplooien, is het nationale recht van toepassing en handhaafbaar, zoals bijvoorbeeld blijkt uit de onlangs gewezen dwangsom van het College bescherming persoonsgegevens (CBP) aan Google voor het overtreden van de Nederlandse wet[30] en het feit dat Google in Duitsland onder druk van de nationale handhavingsautoriteit een apart, extra beschermend regime heeft moeten implementeren ten aanzien van Street View.[31] Een gedifferentieerd model ten aanzien van cookies is derhalve niet alleen wenselijk, ook wat betreft de toepasselijkheid van het Nederlandse recht en de handhavingsmogelijkheden daarvan staat niets hieraan in de weg. •

22. Art. 11.7a lid 3 WBP, *Kamerstuk* 32 549/2.
23. Art. 11.7a lid 4 WBP, *Kamerstuk* 32 549/2.
24. Functionele Third Party-cookies zijn er nauwelijks.
25. A. Soltani e.a., 'Flash Cookies and Privacy', *SSRN* 2009-1446862.
26. http://samy.pl/evercookie/.
27. *WG* 171, p. 7.
28. Daarnaast zijn er mogelijkheden voor contextuele reclames.
29. L. Kool, A. van der Plas, N. van Eijk, N. Helberger & B. van der Sloot, 'A bite too big: Dilemma's bij de implementatie van de Cookiewet in Nederland', p. 33-34.
30. www.cbpweb.nl/pages/pb_20110419_google.aspx.
31. http://googlepolicyeurope.blogspot.com/2010/10/how-many-german-households-have-opted.html.