De eerste evaluatie van de cookiewet door de OPTA

Citeersuggestie: T. Geerlof, De eerste evaluatie van de cookiewet door de OPTA, IT 842.

De OPTA, toezichthouder van de Telecommunicatiewet (Tw), heeft op 2 augustus 2012 op haar website een verslag[1] gepubliceerd over een rondetafelbijeenkomst over de cookiewet tussen de OPTA en brancheorganisaties Dutch Dialogue Marketing Association (DDMA) en Interactive Advertising Bureau (IAB).

De cookiewet regelt (in artikel 11.7a Tw) dat websites hun bezoekers moeten informeren en toestemming vragen voordat zij een cookie of ander gegeven op de computer, laptop of mobiele telefoon plaatsen of uitlezen.

Op de agenda van het overleg stonden de volgende punten:

1) Wordt de cookiebepaling uit de Telecommunicatiewet nageleefd?
2) OPTA geeft uitleg over de informatieplicht;
3) OPTA over toestemming en bijbehorende bewijslast;
4) OPTA over wat functionele cookies zijn;
5) De branche over de cookiebepaling in relatie tot gebruiksvriendelijkheid van websites en mogelijke oplossing middels Do Not Track (DNT);
6) Branche over de informatieplicht;
7) Vervolg

Ad 1) Naleving

OPTA stelt voorop dat de resultaten van een *quick scan* van de top 25 websites aantonen dat nog maar weinig websites voldoen aan de wettelijke vereisten. Bij een aansluitend bezoek van de 25 sites in een browsersessie worden 298 cookies geplaatst. Zes van de 25 websites informeren de internetgebruiker over het feit dat zij cookies plaatsen en slechts 1 site vraagt vooraf om toestemming voor het plaatsen van de cookies.

OPTA merkt op dat de sector wel bezig is met de cookiewet, maar dat modellen om te informeren en toestemming te vragen langzaam tot stand komen. OPTA meent dat dit komt doordat organisaties eerst duidelijk willen weten wat er van hen verlangd wordt, alvorens zij hun systemen aanpassen.

Waarschijnlijk is ook niet uitgesloten dat de afwachtende houding van de branche verband houdt met de niet-naleving van de wet door de websites van de (rijks-)overheid, hoewel de rijksoverheid per kennisgeving van 9 augustus 2012 heeft aangegeven dat ook haar websites inmiddels in overeenstemming met de cookiewet zijn.

Ad 2) Informatieplicht

De eerste plicht die voortvloeit uit de cookiebepaling is dat de bezoeker door de website moet worden geïnformeerd over de werking van de cookies die door de website zullen worden geplaatst (na verkregen toestemming). OPTA doet in dat verband de volgende concrete aanbevelingen:

a) Plaats **duidelijk** leesbare informatie over de plaatsing van cookies op een **zichtbare** plaats op de website en niet door een **vage verwijzing** naar een privacy statement;

b) als *best practice* ziet OPTA het om zo gedetailleerd mogelijk over de werking en het doel van cookies te informeren. Bijvoorbeeld: *"wij maken gebruik van Analyticscookies om bij te houden welke pagina's van onze website u bezoekt en hoe lang u op die pagina's blijft."*;

c) als de website toestaat dat derden cookies plaatsen op de website, benoem deze derden (*"reisverzekeraars*") en wees daarover niet vaag (*"met zorg geselecteerde partners"*);

[1] Verslag rondetafelbijeenkomst over cookiebepaling (i.s.m. DDMA en IAB), 2 augustus 2012 <http://www.opta.nl/nl/actueel/alle-publicaties/publicatie/?id=3635>

d) geef aan waarom je als site-eigenaar *third party* cookies gebruikt en wijs erop dat de derde deze ook voor andere doeleinden kan gebruiken, zoals *profiling*. Verwijs de internetgebruiker naar de voorwaarden van de derde en neem niet de voorwaarden van de derde over op de eigen site.

Ad 3) Toestemmingsvereiste en bewijslast

Impliciete toestemming voor de plaatsing van cookies vindt geen steun in de wet. Oftewel, het adagium "*wie zwijgt, stemt toe"* gaat niet op. Er is een actieve handeling van de internetgebruiker vereist, alvorens mag worden overgegaan tot de plaatsing van de cookie: opt-in via bijvoorbeeld "ja, ik wil".

Bovendien moet je als website kunnen bewijzen dat je toestemming hebt verkregen en dus strekt het tot aanbeveling om de toestemming te "loggen" en om hierbij de op dat moment geldende privacystatement aan te hechten en welke informatie werd gegeven. Het loggen van de toestemming kan, aldus OPTA, plaatsvinden in de cookie. Gaat het om *third party* cookies, spreek dan (contractueel) af met deze derde welke informatie hij wel en niet mag verzamelen. Een vlucht naar andere technieken, denk bijvoorbeeld aan *browser fingerprinting*, om het toestemmingsvereiste te ontlopen is ongewenst (aldus OPTA) en bovendien zonder het gewenste effect, omdat alle technieken waarmee gegevens worden geplaatst of uitgelezen onder het bereik van de cookiewet vallen.

Ad 4) Functionele cookies

Artikel 11.7a lid 3 Tw noemt twee uitzonderingen op het toestemmingsvereiste. Uitgesloten zijn de cookies die noodzakelijk zijn om de communicatie over een elektronisch communicatienetwerk uit te voeren (sub a) en *first party* cookies die nodig zijn om een door de gebruiker gevraagde dienst te leveren (sub b). Klassiek voorbeeld sub b is de *user input cookie* die het mogelijk maakt om verder te winkelen in een webwinkel terwijl de geselecteerde producten in het winkelmandje blijven.

OPTA refereert wat betreft voorbeelden van cookies vallend onder de sub b-vrijstelling aan de recent gepubliceerde opinie van de artikel 29-werkgroep[2].

Deze opinie is verhelderend: het werkt uit waarom bepaalde cookies onder de uitzondering van sub b vallen:

a. *User input* (zie hiervoor over het winkelmandje). Deze worden overigens geacht slechts gedurende een browsersessie nodig te zijn. Die laatste beperking is begrijpelijk als we de parallel maken met de wereld van *brick and mortar*: als ik besluit mijn boodschappenmandje bij Albert Heijn niet af te reken en de winkel te verlaten, ga ik er vanuit dat ik bij terugkomst het door mij gevulde mandje niet meer zal aantreffen;

b. Authenticatie cookies: denk aan het inloggen door een klant op de site van een bank om zijn persoonlijke pagina's te raadplegen (rekeningoverzicht, betalingen, beleggingen, etc.). Cookies zijn daar nodig om de gebruiker de mogelijkheid te geven om bij het opvragen van die verschillende pagina's toegang te geven zonder iedere keer opnieuw in te hoeven loggen (en dus om de door hem gevraagde dienst te leveren). Let op: in beginsel geldt dit slechts voor een browsersessie. Als de webpagina is afgesloten, mag de gebruiker erop vertrouwen dat hij niet wordt "onthouden", tenzij hij dit expliciet aangeeft door bijvoorbeeld "*remember me*" aan te vinken.

   De werkgroep merkt daarbij op, dat de functie van de cookie in dit geval ook wel beperkt moet blijven tot dat doel en niet mag worden aangewend voor *profiling* en/of *behavioural advertising*;

c. *User centric* cookies: cookies die dienen ter vergroting van de online veiligheid op verzoek van de gebruiker. Denk daarbij aan cookies die herhaalde mislukte inlogpogingen op sites registreren. Deze cookies worden bovendien geacht permanent gewenst te zijn, in die zin dat de internetgebruiker deze zal willen blijven gebruiken als hij zelf de browsersessie heeft beëindigd;

d. *Multimedia player session* cookies: worden gebruikt om technische data op te slaan om

[2] Opinion 04/2012 on Cookie Consent Exemption, 7 juni 2012, 00879/12/EN, WP 194 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf>

video- en audiocontent terug te spoelen. Deze worden ook aangeduid als “flash cookies”, omdat de meest gebruikte videotechniek online Adobe Flash is.

e. And last but not least: de *social plug-in content sharing* cookies: door het grote publiek met name gekend vanwege de “vind-ik-leuk”-knop van Facebook die je tegenwoordig onder (nagenoeg) alle content op het internet aantreft. Wat velen misschien niet weten, is dat Facebook een cookie plaatst zodra je (ook als niet-lid van Facebook) een pagina met de like-/share-button passeert en dat Facebook je vanaf dat moment volgt langs alle pagina’s waarop de button is afgebeeld en het aantal websites met button neemt sinds 2009 exponentieel toe.

   Naar mijn idee, terecht, onderscheidt de werkgroep hier twee scenario’s waarvan moet worden beoordeeld of deze onder de vrijstelling van criterium sub b vallen.

   Ten eerste de Facebook-gebruiker die aan het surfen is en die tegelijkertijd ingelogd is op zijn persoonlijke Facebook-pagina. Als hij op de like-/share-button klikt onder willekeurig welke content, mag verondersteld worden dat hij dat doet om zijn Facebook-vrienden op deze content te wijzen. Oftewel: het is noodzakelijk in het kader van de door Facebook te leveren dienst dat de cookie wordt geplaatst en wordt uitgelezen.

   A-contrario gaat die redenering niet op voor uitgelogde Facebook-leden of internetters die niet over een Facebook-account beschikken. Aan hen moet dus wel degelijk toestemming worden gevraagd alvorens het *social plug-in* cookie mag worden geplaatst.

Ad 5) De branche over de cookiebepaling in relatie tot gebruiksvriendelijkheid van websites

De branche geeft aan dat het moeilijk is om een balans te vinden tussen toestemming vragen en het waarborgen van gebruiksvriendelijkheid. Online onderzoeksbureau Invest Online heeft aangetoond dat een strikte naleving van de wet kan leiden tot een drastische terugloop in het aantal bezoekers[3]. Mijn inziens is dit effect ontegenzeggelijk het gevolg van deze strenge wet.

Op dit moment kan de bezoeker slechts worden gevraagd of hij wel of niet toestemt met het plaatsen van cookies, ongeacht welk type cookie. Dat is onwenselijk. De branche zou het wenselijker vinden om toestemming gespecificeerd per type cookie te vragen (men spreekt van een “drietrapsraket”): *“stemt u in met het plaatsen van cookies voor een optimale werking van de website, cookies ten behoeve van onze statistiek en reclamecookies?”*. De branche stelt dat zo’n drietrapsraket aan de architectuur van het internet raakt en moeilijk te implementeren is. Bovendien twijfelt de branche of dit nog wel een beheersbare keuze is voor de webbezoeker, omdat de lijst met cookies waarvoor hij toestemming moet geven mogelijk erg lang wordt.

De branche (en de politiek, aldus de OPTA in het verslag) is daarom voorstander van een oplossing waarbij de besturingssystemen van de browser een keuze voor het accepteren van cookies kunnen registreren. Uit de overwegingen bij de geconsolideerde Privacyrichtlijn, wisten wij al dat de Europese wetgever het niet ondenkbaar vond dat men via de browserinstellingen zijn toestemming kon geven. Gelet op de strenge implementatie door de Nederlandse wetgever, verbaast het enigszins dat de OPTA in haar verslag stelt dat ook “de politiek” hiervan voorstander zou vinden. Hoe dat ook zij, de branche biedt als oplossing aan de zogenaamde Do Not Track (DNT) standaard. DNT verstuurt via http een *header* aan de bezochte website met daarin de aangegeven voorkeuren van de gebruiker over het gebruik van cookies. De website zou zich aan deze instelling moeten conformeren. Op dit moment is DNT nog niet fijnmazig genoeg om de gedetailleerde voorkeuren van gebruikers op te slaan en te communiceren. Hoewel ook OPTA in beginsel positief lijkt te staan ten opzichte van DNT, benadrukt zij dat websites aan de wet moeten voldoen in afwachting van een goed functionerend DNT-systeem.

Ad 6) Branche over de informatieplicht

De sector is van mening dat de informatievoorziening beter kan en moet en presenteert twee voorstellen om dit in de praktijk te brengen. Ten eerste stelt de branche voor om gelijkluidende en –ogende meldingen op websites op te nemen, onder verwijzing

[3] <http://www.investonline.nl/testresultaten_cookiewet>

naar een algemene informatiepagina en de cookiepolicy van de betrokken website. Ten tweede stelt men een branchebrede voorlichtingscampagne voor in samenwerking met het platform voor de informatiesamenleving, ECP-ECN, om de burger over cookies en de cookiewet te informeren.

OPTA sluit af met de mededeling dat deze bijeenkomst moet worden gezien als een aftrap van een structureel overleg over *compliance* en voorlichting en naleving van de wet.

Samenvatting

De rondetafelbijeenkomst heeft nauwelijks tot nieuwe inzichten over de cookiewet geleid. Behoudens de verwijzing naar de opinie van de artikel 29-werkgroep wat betreft een kwalificatie van verschillende functionele cookies als zodanig, kenden wij de verwoorde standpunten al: de cookiewet wordt niet of nauwelijks nageleefd, websites moeten, na volledige en duidelijk informatieverschaffing, kunnen bewijzen dat zij over de vereiste toestemming van de gebruiker beschikken, de branche heeft hier bezwaren tegen en iedereen kijkt reikhalzend uit naar een *new and improved* DNT-systeem.

Wel mogen wij misschien voorzichtig aannemen, dat het verzoek van Minister Verhagen aan OPTA om pas in 2013 te beginnen met handhaving van de cookiewet, door OPTA lijkt te worden ingewilligd.

Overigens was naar mijn idee de grote afwezige bij het overleg privacywaakhond CBP. Immers, vanaf 1 januari 2013 wordt een tweede lid toegevoegd aan artikel 11.7a Tw, inhoudende het wettelijk vermoeden dat het plaatsen van (in het bijzonder) een *tracking* cookie, een verwerking is van persoonsgegevens, waarop de Wet Bescherming Persoonsegevens van toepassing is. Veronderstellend dat er eind 2012 een DNT-protocol is dat de goedkeuring van Eurocommissaris Kroes kan dragen, dan laat dat onverlet de verplichtingen die de Wbp oplegt aan websites als verantwoordelijke voor de verwerking van persoonsgegevens en de vragen die dat met zich meebrengt.

Timme Geerlof, Ploum Lodder Princen