WAXTRAPP BV
Van Diemenstraat 278
1013 CR Amsterdam
Tel: 020 67 22 308
Fax: 020 67 22 488
www.waxtrapp.com
info@waxtrapp.com
ING Bank 6667.05.194
KvK nr. 33285688
BTW nr. 809944340

Commissie Wetsvoorstel Implementatie NRF
mr. J.W. Dijkman
Ministerie van Economische zaken
Den Haag

Amsterdam, 13-5-2010

Geachte commissiue implementatie wetsvoorstel NRF,

Ik ben technisch directeur/ondernemer, van een bedrijf dat software ontwikkelt waar gepersonaliseerde websites mee gebouwd worden, en heb een technische achtergrond.

Ik wil graag gebruik maken van de mogelijkheid om een bijdrage te leveren aan de vorming van technische bepalingen rond deze wetgeving. Ik ben ook gaarne bereid om mijn voorstellen toe te lichten, als u daar behoefte aan heeft. Neem contact op met 020-6722308 of e-mail naar: bas.groot@waxtrapp.com

Synopsis van mijn voorstel

Omschrijf privacy klasse A t/m G bij wet.
A=veilig, G=alles ligt op straat.

Zorg dat de aanbieder alles op zijn site aan dezelfde klasse moet laten voldoen, dus voor klasse C moeten ook reclame-banners en statistiek-software e.d. aan klasse C voldoen.

Wie slechts aan de laagste klasse G voldoet, lapt privacy duidelijk aan zijn laars en moet verplicht opt-in doen.

Als een deel van de site aan een lagere privacy klasse voldoet, moet je daar alleen via opt-in toestemming gebruik van kunnen maken. (bijvoorbeeld een site van niveau B, met een enquete op niveau E)

Voordelen

- Duidelijk en simpel voor de burger: 1 letter zegt alles.
- Stimuleert investeringen en kwaliteit, ipv Nederland op achterstand zetten
- Conform de Europese richtlijn niet alleen cookies, maar allerlei soorten privacy-schendingen met de nieuwe, opkomende alternatieven voor cookies worden tegengegaan.
- Handhaving is automatiseerbaar, dus relatief goedkoop

Inhoudsopgave

Waarom mijn schrijven?

Allereerst ben ik belanghebbende. Mijn bedrijf levert gepersonaliseerde websites en webapplicaties.

Cookies zijn een noodzakelijk onderdeel van elke vorm van internet-diensten waarbij personaliatie en voorkeuren van de gebruiker bijhouden, een rol spelen.

We zouden het jammer vinden als onze producten en diensten door de nieuwe wetgeving onverkoopbaar worden.

De geest van de wetgeving is het beschermen van de privacy van de burger, maar in haar poging dat te doen, wordt een nuttige technologie min of meer verboden.

De wetgeving zou niet moeten gaan over het verbieden van de technische wegen waarlangs privacy-overtredingen begaan worden. De wetgeving zou moeten gaan over het verbieden van ongeoorloofd delen van informatie.

In de stukken van de internetconsultatie:
http://www.internetconsultatie.nl/nrfimplementatie/document/126
wordt vermeld dat er veel debat is geweest over cookies door burgerrechten-belanghebbenden, maar ik vrees dat daarbij missie en idealisme het heeft gewonnen van objectieve kennis.

Al sinds cookies in 1995 zijn bedacht hebben sommigen het merkwaardige idee postgevat dat cookies “Slecht” zijn. Dat is net zo min onwaar als dat cookies “Veilig” zijn.
Het is een middel dat voor legitiem gebruik en misbruik kan zorgen, dat zegt u zelf ook.

Mijn privacy standpunt

Allereerst ben ik een groot voorstander van meer privacy op internet. Juist als technisch deskundige op internet-gebied met 14 jaar hands-on ervaring, zie ik hoe makkelijk het is om informatie bijeen te graaien en hoezeer je maar moet accepteren dat je als consument je gegevens te grabbel moet gooien om iets van een bedrijf of dienst gedaan te krijgen.

En vind ik dat met name de internet-multinationals op grote schaal gegevens toe-eigenen waar ze geen recht op hebben.

Ik heb mij dan ook in diverse media kritisch uitgelaten over de handelwijze van Google, wier beleid zich kenschetst door een informatie- en privacy-veelvraat die luidkeels roept “wij hoeven niet transparant te zijn want we zijn ok!”.

Elke burger heeft ongemerkt te maken met Google Analytics en Google Advertenties die informatie van alles en iedereen opzuigen en daar van alles mee doen wat u en ik niet weten.

Maar vergeet de vrolijke blokjes “share this” buttons van sociale sites als LinkedIn, Facebook, StumbleUpon en dergelijke niet, die vriendelijke kleine sneaky knopjes versturen ook bezoekers-informatie naar hun eigen site, ook als je er -niet- op klikt! Jaja, boefjes, dat zijn het.

Dat deugt niet en daar mag de wetgeving best tegen optreden.

Nogmaals, niet het **middel** dat gebruikt wordt om privacy te schenden moet verboden worden, het **schenden zelf** moet verboden worden.

Het effect van de huidige wetgeving

Het effect van het huidige opt-in, wat neerkomt op een bijna- verbod, is averechts. Nederland zal als internet-technologieland moet meerennen met de rest van de wereld met één been in het gips.

Het schaadt de industrie op internationaal niveau en drukt innovatie naar het buitenland.
En Nederland loopt al achter.

Het is ook onnodig, want het Nederlandse voorstel is veel strenger dan de Europese richtlijn, en de Europese richtlijn richt zich op waar het om gaat. Dit onderbouw ik verderop.

Daarnaast drijft de wetgeving slechts aanbieders richting minder geoorloofde technieken. Ook dit zal ik nader verklaren, uit hoofde van mijn kennis over internettechnologie.

Effecten in de internationale concurrentiepositie

Bijvoorbeeld: stel je bent een Nederlandse webwinkel. Handel is op internet vaak internationaal, voor veel producten doet het er voor de consument weinig toe of je die in Japan, de VS, Duitsland of Nederland bestelt.

De moderne consument gaat rondshoppen op allerlei verschillende websites om iets te kopen.

De websites waar hij eerst een toestemming popup krijgt voordat hij de site op kan, klikt hij meteen weg, wat da's irritant en roept twijfel op of het wel deugt, ten faveure van buitenlandse sites die dat allemaal niet hebben. Na enige tijd zal er zelfs gedrag ontstaan bij regelmatige webwinkel gebruikers, om alle sites met .nl in het URL gewoon niet eens meer heen te gaan.

Het effect is dus dat de concurrentiepositie van de internet-handel in Nederland geschaad wordt. Hetzelfde geldt voor bijna alle internet-gerelateerde bedrijfstakken, en allerlei content-gerelateerde internet-intiatieven zoals informatieve en culturele sites, online magazines en blogs, die zonder advertentie-inkomsten niet kunnen overleven en inmiddels onmiskenbaar hun nut en gunstige invloed op het culturele en maatschappelijke landschap hebben gehad.

De wetgeving drijft aanbieders naar andere technieken

Deze wetgeving neigt een oorlog uit het verleden te willen winnen. En verplaatst het probleem alleen maar. Hij lokt uit tot creatief omzeilen van de cookie opt-in regeling met middelen waar je veel minder blij mee moet zijn.

Het netto effect van een totaal opt-in regime is dat legitieme én malafide aanbieders van websites geforceerd worden naar andere middelen van individuen volgen, waar alsnog hetzelfde misbruik kan plaatsvinden.

Het drijft innovatie naar buitenland

Wanneer cookies voor een bedrijf van levensbelang zijn om de website te laten functioneren en geld te verdienen, en de wetgeving van het eigen land is veel strenger dan die in omringende landen, dan ligt het voor de hand om de site gewoon in een buurland te hosten, eventueel onder de vlag van een buitenlands BV'tje voor juridische dekking.

Bij internet maakt het immers meestal totaal niet uit in welk land de server staat.

De bedoeling van Europese richtlijnen is juist een gelijk speelveld voor ondernemers in alle landen. Onnodig strenge wetten gaan tegen de geest van Europese samenwerking in.

Het drijft bedrijven naar profiling

Het identificeren van individuen gaat dan niet meer via cookies maar via profiling. De porno-industrie doet dit al een hele tijd, omdat de slimmere burger bij dergelijke sites zijn browser in privacy-mode zet, en daarmee cookies uitschakelt als hij dergelijke sites bezoekt.

Profiling betekent in jip-en-janneketaal: alle unieke kenmerken van de browser in kwestie bij elkaar optellen en dat verhaspelen tot een getal. En dat getal is dan per bezoeker min of meer uniek. Cookies komen er niet aan te pas, het is ietsje minder betrouwbaar, maar de mogelijkheid tot privacy-schending is onverlet.

Met IPv6 wordt de cookie opt-in een dode letter

Zodra het nieuwe basisprotocol van het hele internet, IPv6 ingeburgerd raakt, wat naar verwachting de komende paar jaar zal gebeuren, is de hele cookie-discussie volkomen vervallen.

Want in IPv6 wordt bij elke connectie naar een website twee nummers meegestuurd:

- het aansluitnummer bij de internetprovider (wat nu ook al gebeurt bij het huidige IPv4)
- het unieke nummer van de netwerkkaart in de computer van de gebruiker

(technisch zit het iets ingewikkelder, maar voor de privacy-praktijk komt het daar op neer)

Gevolg is dat internetgebruikers te allen tijde individueel te volgen zijn, ongeacht hoe vaak ze hun browser afsluiten of hun browser in privacy-modus zetten of wat dan ook. Want dit gegeven komt niet uit de browser maar uit de computer.

Kortom, het hindert de industrie nu en het dwingt tot andere oplossingen die veel minder wenselijk zijn.

Vergeleken met de Europese richtlijn is het onnodig streng

Als we de Europese richtlijn pagina 34, artikel (66) erbij pakken:

Third parties may wish to store information on the equipment of a user, or gain access to information already stored, for a number of purposes, ranging from the legitimate (such as certain types of cookies) to those involving unwarranted intrusion into the private sphere (such as spyware or viruses). It is therefore of paramount importance that users be provided with clear and comprehensive information when engaging in any activity which could result in such storage or gaining of access.

The methods of providing information and offering the right to refuse should be as user-friendly as possible. Exceptions to the obligation to provide information and offer the right to refuse should be limited to those situations where the technical storage or access is strictly necessary for the legitimate purpose of enabling the use of a specific service explicitly requested by the subscriber or user.

Where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user's consent to processing may be expressed by using the appropriate settings of a browser or other application. The enforcement of these requirements should be made more effective by way of enhanced powers granted to the relevant national authorities.

Dan staat daar dat het medium waarlangs de intrusion plaatsvindt, er niet toe doet. Of dat nou cookies zijn of spyware en viruses, de er moet een mogelijkheid zijn om te weigeren en dat moet zo gebruikersvriendelijk mogelijk gebeuren.

De tekst van de wetgever stelt niet dat een opt-in noodzakelijk is, maar dat je glashelder moet uitleggen wat je doet en de optie bieden om dat te weigeren. Om daar een opt-in van te maken is objectief niet in overeenstemming met de EU richtlijn. Dat staat er gewoon niet.

De wet heeft tegenstrijdigheden

De grootste tegenstrijdigheid is dat ALLE cookies van een opt-in moeten worden voorzien, terwijl tegelijk wordt gezegd dat het niet de bedoeling is dat de gebruiker met die opt-in lastig gevallen wordt.

Dat wordt gezegd in:

http://www.internetconsultatie.nl/nrfimplementatie/document/123

Het is vanuit het perspectief van de werking van het internet en het gebruiksgemak van de eindgebruiker niet praktisch om bij ieder bezoek van een site waarbij een cookie wordt geplaatst de eindgebruiker wordt geconfronteerd met een scherm waarop deze om toestemming wordt gevraagd alvorens er verder kan worden gesurft.

Nu wordt dus feitelijk gesteld: Toestemming vragen moet, maar steeds toestemming moeten vragen is irritant en niet wenselijk. Branche, kom met een oplossing waar 1 ongelijk is aan 1.

De wet veroorzaakt kip-ei kwesties

Het lastige van cookies is ook, dat de bezoeker geen keus heeft dan zijn browser in privé modus zetten.

Via de website kan een aanbieder weinig doen tot niets doen.

Je kunt immers op een site niet een voorkeur voor “geen cookies” bijhouden, want voorkeuren bijhouden doe je met cookies.

Hetzelfde geldt voor sessies: bijna alle moderne sites houden sessie-ID's bij. Ze betekenen niks, het is niet meer dan een getalletje waarmee de server zijn bezoekers uit elkaar kan houden, en het getalletje wordt meestal de server ook weer vergeten na een tijdje. Maar hoe onthoud je welke bezoekers geen sessie-ID willen zonder sessie-ID? Die allemaal sessie ID '0' geven is nog steeds een cookie, wettelijk gezien, en geeft weer rare bij-effecten die je niet wilt.

Een alternatief wat wel eens geopperd wordt is om sessie-ID en voorkeuren via het URL mee te geven in plaats van via cookies, maar dat is in feite nog privacy-gevoeliger. Want browsers geven de vorige pagina die je bezocht mee (de zg Referrer). Veel (oudere) webapplicaties gebruiken die referrer ook, dus veel van zulke applicaties gaan ook stuk met je browser in privé modus.

Maar dat soort sessie- en voorkeuren-gegevens via het URL doorgeven is ergerlijk, en geeft ongewild gegevens aan anderen door zonder intrusie en zonder iets op de browser op te slaan, en bovendien is het hinderlijk voor zoekmachines. Het is namelijk voor iedere site anders en ze moeten dus 'begrijpen' hoe het in elkaar zit om rommel weer uit het URL te kunnen filteren.

Cookies hebben dat probleem niet. Die zijn, in weerwil van wat niet-onderlegde activisten soms denken, veiliger dan sessie- en voorkeurs-informatie in URLs.

De wet biedt echter ook mogelijkheden

De huidige wet biedt een aantal mogelijkheden waaronder legitiem gebruik van cookies gewoon is toegestaan als het nodig is voor het functioneren van de dienst.

Toestemming hoeft alleen te worden gevraagd:

- Als het technisch nodig is
- Als het gaat om opslaan van gegevens,

Alleen laat de wetgever in het midden wanneer het “nodig” is en wanneer “opslaan”

Bovendien is de wens van de wetgever dat het vooral duidelijk is, zo duidelijk mogelijk.
Daarom wil ik een voorstel doen, wat volgens mij vrijwel geheel in het huidige wetsvoorstel past.

Mijn voorstel: privacy klassering!

Klasseer websites in diverse privacy-niveaus, die bij wet omschreven staan.
Dit is geïnspireerd op het milieukeurmerk voor auto's en huizen. Maak daarmee duidelijk en simpel voor de gebruiker om te weten wat er met je gegevens gebeurt. De klassen moeten dan wel zo simpel mogelijk omschreven zijn.

Basisvoorwaarden

Sites die geen privacy klassering hebben, moeten voldoen aan de strenge opt-in regeling.
Sites die een privacy klasse hebben, hoeven geen opt-in te bieden, onder de volgende voorwaarden:

- De privacy klasse moet duidelijk op de homepage vermeldt worden als tekst-link of wettelijk vastgesteld logo

- Klikken op link/logo leidt naar een pagina waar de aanbieder glashelder uitlegt wat hij qua privacy doet en uitleggen hoe de gebruiker de site kan gebruiken met extra bescherming.
  - dat is simpel te doen, kwestie van de wettelijke tekst die bij de privacy-klasse hoort, knippen/plakken

- Op de pagina waar de privacy-uitleg staat, moet een link zitten: “ik ga niet akkoord met dit privacy-niveau” waarmee:
  - de cookies die deze site geschreven heeft, direct worden weggehaald of leeg gemaakt,
  - de browser een nieuw leeg scherm opent
  - en het scherm met de huidige site afsluit
  - (een dergelijk scriptje heeft een junior ontwikkelaar in 5 minuten geschreven)

- Op elke vervolgpagina waar navigatie aanwezig is, moet de klikbare privacy klasse vermeld staan, of anders een link die duidelijk verwijst naar de privacy-informatie
  - Veel mensen komen op een site via zoekmachines, en komen dan meestal niet op een homepage. Ze moeten dan meteen kunnen zien wat voor vlees ze in de kuip hebben.

- De privacy-klasse informatie moet goed leesbaar zijn
  - Aanbieders zullen een slechte klassering graag wit-op-wit of in een onleesbaar klein lettertype vermelden.

- Aanbieders die zichzelf uitgeven met een te hoge privacy klasse moet gelden als valsheid in geschrifte op dezelfde manier als het voeren van een keurmerk dat je nooit is toegekend, of een te gunstig milieukeurmerk.

- Aanbieder betracht volledige transparatie en verleent medewerking aan inspecties die moeten uitwijzen of het privacy-niveau nageleefd wordt, met name of er geen gegevens met derden gedeeld worden of gegevens over dezelfde bezoeker van derden gebruikt worden.

Laagste klassering geldt voor de hele site

Het idee is dat de aanbieder van websites een bepaalde privacy klasse alleen kan behalen als de hele site eraan voldoet, inclusief de reclamebanners, statistieksoftware, targeting software en wat dies meer zij.

Gevolg: Simpele statische sites die geen cookies gebruiken en niks bijhouden, zijn klasse A en dus brandschoon. Maar zodra zo'n site Google advertenties, Google analytics of Facebook-share buttons op je site zet, bepaalt het onveiligste onderdeel op je site je privacy klasse.

Gebruik je op je site onderdelen van derden die geen privacy-klasse kunnen afgeven, dan kun je zelf ook geen privacy-klasse krijgen, en moet je automatisch aan het opt-in regime voldoen.

Wat een aanbieder wel mag: Gebruik je op een specifiek onderdeel van je site iets wat van een lagere privacy klasse is dan de privacy klasse van de rest van je site, dan MOET je toestemming vragen voordat de gebruiker toegang krijgt tot dat privacy-gevoelige deel gebruik kan maken.

Bijvoorbeeld: stel dat de site helemaal klasse B is, maar je gaat een enquete invullen waarvan de gegevens gedeeld worden met een derde partij, dan kun je op de eerste pagina van de enquete vermelden: deze enquete voldoet aan privacy klasse D (+link wat dat betekent). Wilt u doorgaan?

Privacy klasse A

- Cookies of andere middelen van gebruikers traceren worden **helemaal niet** gebruikt.
- Aanbieder deelt **nooit** via de site verkregen gegevens met derden
- Aanbieder gebruikt **nooit** gegevens over dezelfde bezoeker van derden
- Aanbieder garandeert dat site-onderdelen van derden 100% voldoen aan Privacy klasse A.

Privacy klasse B

- Cookies worden gebruikt
- Cookies worden gewist na afsluiten browser
- Cookies bevatten geen informatie die betekenisvol is voor derden
- Aanbieder deelt nooit verkregen gegevens met derden
- Aanbieder gebruikt nooit gegevens over dezelfde bezoeker van derden
- Aanbieder garandeert dat site-onderdelen van derden 100% voldoen aan Privacy klasse B.

Privacy Klasse C

- Cookies worden gebruikt
- Cookies worden **niet** gewist na afsluiten browser, blijven langer bestaan
- Cookies bevatten geen informatie betekenisvol is voor derden (zie B)
- Aanbieder deelt nooit verkregen gegevens met derden
- Aanbieder gebruikt nooit verkregen gegevens van derden
- Aanbieder gebruikt nooit gegevens over dezelfde bezoeker van derden
- Aanbieder garandeert dat site-onderdelen van derden 100% voldoen aan Privacy klasse C.

Privacy klasse D

- Cookies worden gebruikt
- Cookies worden wel of niet gewist, dat maakt niet uit
- Cookies bevatten **wel** informatie bevatten die betekenisvol is voor derden (zie B)
- Aanbieder deelt nooit verkregen gegevens met derden.
  - Dus anderen kunnen wel via malware gegevens uit je cookies lezen
- Aanbieder gebruikt nooit gegevens over dezelfde bezoeker van derden
- Aanbieder garandeert dat site-onderdelen van derden 100% voldoen aan Privacy klasse D.

Privacy klasse E

- Cookies worden gebruikt
- Cookies worden wel of niet gewist, dat maakt niet uit

- Cookies bevatten **geen** informatie bevatten die betekenisvol is voor derden (zie B)
- Aanbieder mag **wel** verkregen gegevens delen met derden
- Aanbieder mag **wel** gegevens over dezelfde bezoeker van derden gebruiken
- Aanbieder garandeert dat site-onderdelen van derden 100% voldoen aan Privacy klasse E.

Privacy klasse F

- Cookies worden gebruikt
- Cookies worden wel of niet gewist, dat maakt niet uit
- Cookies bevatten **wel** informatie bevatten die betekenisvol is voor derden (zie B)
- Aanbieder mag **wel** verkregen gegevens delen met derden
- Aanbieder mag **wel** gegevens over dezelfde bezoeker van derden gebruiken
- Aanbieder garandeert dat site-onderdelen van derden 100% voldoen aan Privacy klasse F.

Privacy klasse G

- Alles wat niet 100% aan een bovenstaande klassering voldoet.
- Opt-in regime voor cookies is verplicht.

Nadere specificatie

Betekenisvolle informatie voor derden nader gespecificeerd

bijv WEL: Sessie-ID's, lettergrootte voorkeuren, andere voorkeuren
bijv NIET: info over bezochte pagina's, inhoud van winkelmandje, login-gegevens, wachtwoorden, rekeningnummer, eerder gebruikt zoekwoord, NAW gegevens

Of de betekenisvolle informatie versleuteld is of niet, doet niet ter zake. Immers, professioneel geschreven spyware zal versleutelde informatie direct herkennen en proberen te kraken. Aangezien het versleutelingsniveau van cookies al gauw zal achterlopen op de algemeen aanvaardbare standaard, krijg je al snel

Het opslaan van privacy-gevoelige informatie in versleutelde vorm in cookies is veel te verleidelijk voor aanbieders.

Gegevens delen nader gespecificeerd

- Bij het delen van gegevens met derden doet het niet ter zake of er al dan niet betaling in geld, gegevens of in andere natura tegenover staat.
- Bij het delen van gegevens met derden maakt het niet uit of de gegevens herleidbare informatie bevatten of alleen sessie-ID's. Delen is delen.
- Bij het gebruiken van gegevens van derden over dezelfde bezoeker, geld dat ook voor "vermoedelijk" dezelfde bezoeker. (bijvoorbeeld op basis van browser-profiling, IP adres etc)

Voordelen van deze regeling

Voor aanbieders

- Het wordt voor de aanbieders aantrekkelijk gemaakt om mee te doen aan de regeling, want een goede site heeft een hoog keurmerk straalt en betrouwbaarheid richting de klanten. Dat is wat aanbieders willen

- Het is voor aanbieders mogelijk om personalisatie en andere prettige voorkeuren e.d. aan

te bieden zonder de bezoeker weg te jagen met ergerlijke popups en toestemmingsschermen

- Aanbieders die banners of software van derden gebruiken, kunnen hen vragen om een oplossing die aan een bepaald keurmerk voldoet.

- Er ontstaat een nieuwe markt voor aanbieders van banner- en statistieksoftware die een hogere privacy klasse hebben dan de huidige marktleiders als Google, Yahoo en Microsoft.

- De meeste reclamebanner en statistiek-software bedrijven zijn bonafide en houden slechts betekenisloze informatie zoals sessie-nummers bij, en kunnen dat blijven doen.

- Het dwingt de marktleiders om betere privacy-afschermende alternatieven voor hun banner- en statistiek-technologie te leveren, omdat ze anders omzet kwijtraken aan concurrenten die dat wél doen.

Voor de bezoekers

- Superduidelijk: De bezoeker hoeft zich niet door obscure en juridische teksten te worstelen om te begrijpen wat er met zijn gegevens gebeurt: 1 letter van A...G geeft uitsluitsel.

- De bezoeker kan zich vooraf vergewissen met wat voor partij hij van doen heeft en wat er met zijn gegevens gebeurt.

- De consument kan meteen bij het zien van een te laag privacy-niveau meteen zijn browser in privé modus zetten, of de site verlaten.

- De bezoeker wordt niet tijdens het browsen lastig gevallen wordt met irritante toestemmingsschermen en popups.

- De bezoeker weet dat er geen stiekeme dingen gebeuren waar hij geen weet van heeft.

Voor de overheid

- De technische details worden samen met de branche geregeld zonder dat de overheid op de stoel van de technici of de branche hoeft te gaan zitten, wat doorgaans leidt tot een achterhoedegevecht.

- De technische details van het keurmerk kunnen aangepast worden terwijl echte excessen altijd onder de strenge regeling zullen vallen.

- De regeling zorgt eerder voor een verbetering van het betrouwbaarheidsimago van Nederlandse websites ten opzichte van andere landen, in plaats van een verslechtering.

- De regeling stimuleert aanbieders om te investeren in goede privacy in plaats van ze te stimuleren om te vluchten in minder aantrekkelijke alternatieven.

- Naleving van de privacy-klasse is merendeels met relatief eenvoudige, (vrijwel) geheel geautomatiseerde systemen te controleren. Je hebt software nodig die lijkt op een een "crawler-robot" zoals zoeksites die gebruiken om het internet te indexeren.

- Door geautomatiseerde controle vallen malafide sites die zichzelf openlijk een veel te hoge privacy-klasse toedichten, snel door de mand en is controle en handhaving vergt dus

weinig mankracht en kosten. Alleen het niet-delen van informatie zal dan inspectie vergen.

Een mogelijk simpeler alternatief voor privacy-klassen A-G

Een nadeel van deze regeling is dat er een hele privacy klasse en keurmerk-santenkraam moet worden opgetuigd.

Het gaat een grote kunst worden om de privacy-klassen zoals door mij omschreven, zo te omschrijven dat een burger het nog kan begrijpen, maar dat het juridisch wel klopt wat er staat.
Ik heb er een klein beetje verstand van maar ben geen jurist.
Een praktisch eenvoudiger alternatief is dat er op een website op -elke- pagina een duidelijke link moet staan "over cookies op deze site" (of iets anders)

Klik je op deze link, dan staat daar glashelder uitgelegd wat er met cookies gebeurt op de site.

Op de pagina waar de privacy-uitleg staat, moet een link zitten: "ik ga niet akkoord met dit privacy-niveau" waarmee:

- de cookies die deze site gemaakt heeft, direct worden weggehaald of leeg gemaakt,
- de browser een nieuw leeg scherm opent
- en het scherm met de huidige site afsluit

(een dergelijk scriptje heeft een gemiddelde ontwikkelaar in 5 a 10 minuten geschreven)

Het nadeel van deze regeling is echter wel, dat het weer een soort opt-out regeling is, alleen dan met verplichte vermelding op alle pagina's.

Tot slot

Ik hoop met mijn voorste een zinnige bijdrage te leveren aan het debat en de vorming van goede wetgeving rond privacy, maar wel vanuit een voor aanbieders haalbare en technisch objectieve handelwijze, die bovendien ook ergernis bij de surfende burger vermijdt.

Ik ben graag bereid mijn voorstel toe te lichten.
U kunt mij daarvoor contacteren op 020-6722308 of bas.groot@waxtrapp.com

Met vriendelijke groet,

Bas Groot
Directeur
WAXTRAPP BV