

ELAW KEUZEVAK TELECOMRECHT

*privacy en bescherming persoonsgegevens (incl.  
spam, telemarketing en cookies)*

Gerrit-Jan Zwenne — 10 mei 2019



Universiteit Leiden  
The Netherlands



*roadmap*

- *vertrouwelijkheid en beveiliging*
- *anoniem bellen en gebeld worden, geheim nummer*
- *verkeers- en locatiegegevens, bewaarplicht en aftappen*
- *cookies, spam en telemarketing*

## vertrouwelijkheid en beveiliging

- bescherming persoonsgegevens en privacy van abonnees en gebruikers
- vertrouwelijkheid van communicatie
- beveiliging én meldplicht beveiligingsinbreuk

melden bij AP én bij abonnees en gebruikers!

- niet aftappen, af luisteren enz., tenzij
- met uitdrukkelijke toestemming
  - integriteit netwerk
  - overbrengen communicatie
  - wettelijk voorschrift of bevel

Deep Packet Inspection (DPI)

## anoniem bellen en gebeld worden

- nummerherkenning
- specificatie telefoonrekening

recht op gespecificeerde rekening (KPN), en recht op ongespecificeerde rekening

- recht op anoniem bellen
- recht om niet anoniem te worden gebeld
- recht om wel anoniem te worden gebeld maar beperkingen m.b.t. alarmnummers

## 'geheim nummer'

- toestemming vereist voor opname gegevens in telefoongids of abonnee informatiedienst
- voor standaardgids of -informatiedienst moet Telco toestemming vragen

18xy: 1880, 1800, 1801

zoeken op naam in combinatie met adres en woonplaatsgegevens

hoe zit het met 'omgekeerd zoek-diensten (reversed search)..?

## verkeersgegevens

- anonimiseren, zodra niet meer nodig voor overbrengen verkeer en facturering
- met toestemming ook voor value added services en marketing van elektronische communicatie-diensten

gegevens die worden verwerkt voor overbrengen van communicatie of facturering ervan

Bijv. tijdstip en duur, oproep, oproepnummer, Cell-ID, omvang e-mailbericht, etc.

Let op! GPS gegevens worden niet gebruikt voor overdracht van communicatie, zijn dus locatiegegevens maar géén verkeersgegevens (art. 11.5a Tw)

## bewaarplicht ..?!

Wat?

- verkeer- en lokatiegegevens
- nawijsgegevens

Hoe lang?

- 12 mndn voor de politie
- 06 mndn voor de justitie

Waarvoor?

- onderzoek, opsporing en vervolgen ernstige misdrijven



HvJEU 8 april 2014 C-293/12 en C594/12

- inmenging in fundamentele rechten op bijzonder ernstige wijze
- wél sprake van een algemeen belang, nl. strijd tegen ernstige criminaliteit en uiteindelijk openbare veiligheid
- maar met richtlijn 2006/24/EG zijn niettemin grenzen overschreden die ingevolge het evenredigheidsbeginsel in acht moeten worden genomen



buitenwerkingstelling..!

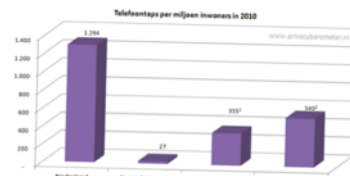
## aftappen

- telecomnetwerk en diensten moeten aftapbaar zijn
- medewerkings- en geheimhoudingsplicht
- en beveiligingsplan



### Nederland nog steeds wereldkampioen afluisteren

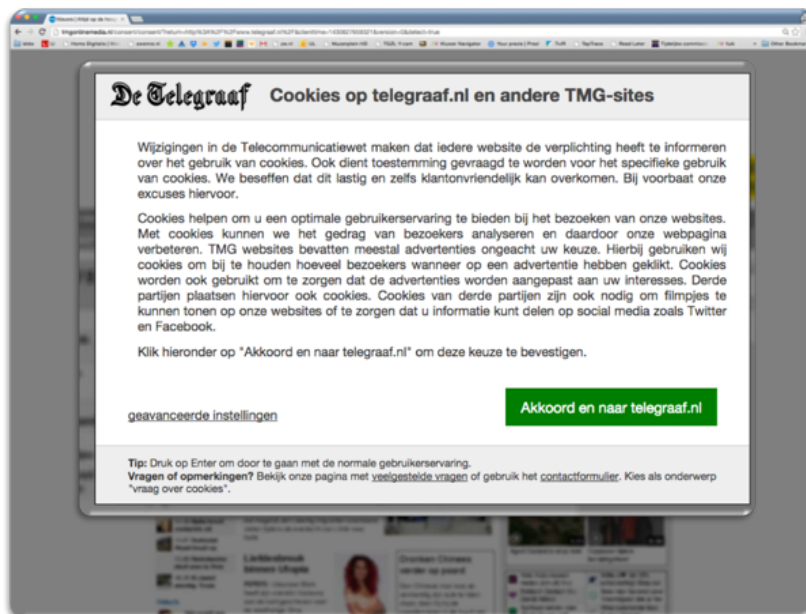
Vanmiddag verscheen een rapport van de onderzoeksafdeling van het ministerie van Justitie. In het rapport wordt de Nederlandse afluisterpraktijk vergeleken met die van Engeland, Duitsland, en Zweden. De opsporings- en rechtssystemen in die landen zijn anders dan in Nederland, dus een precieze vergelijking is lastig. Maar duidelijk is wel dat Nederland nog steeds 'wereldkampioen' afluisteren is.



<http://bit.ly/dxA9Zz>

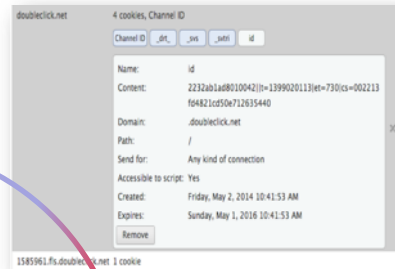


## COOKIES (EN DERGELIJKE)



## cookies: object van regelgeving

gebruik van elektronische communicatie voor opslag van informatie of voor verkrijgen van toegang tot informatie die reeds is opgeslagen in eindapparatuur van een abonnee of gebruiker”



door eindgebruiker gebruikt apparaat aangesloten op een elektronisch communicatienetwerk, zoals computer, smartphone, set-top box, enz.(art. 1.1(jj)(i) Tw)

## ‘cookiebepaling’

art. 11.7a, eerste lid, Telecomwet

- duidelijke en volledige informatie overeenkomstig de Wbp, en in ieder geval over de doeleinden van de cookies
- toestemming van de gebruiker

Art. 13-14 AVG: o.a. eigen identiteit, doeleinden en ‘nadere informatie voor zover nodig om zorgvuldige verwerking te waarborgen’

Vgl. art. 7 en overw. 32, 42-43 AVG

### ICTRecht incasseert €8200 dankzij cookiepopup met incassotoestemming

9 april 2013 door [Arnoud Engelen](#)

Dankzij het gemak waarmee mensen online akkoord gaan met cookiepopups heeft ICTRecht een bedrag van €8200 mogen incasseren via automatische incasso. Dat maakte het juridisch adviesbureau vandaag bekend. Naast de bekende teksten over Analyticscookies en sociale media bevatte de cookiepopup ook de tekst “Tevens geeft u toestemming €100 van uw bankrekening te laten afschrijven”. Een dergelijke tekst is rechtsgeldig, nu bezoekers expliciet op “Akkoord” moesten klikken.

(32) Toestemming dient te worden gegeven door middel van een duidelijke actieve handeling, bijvoorbeeld een schriftelijke verklaring, ook met elektronische middelen, of een mondelinge verklaring waaruit blijkt dat de betrokkene vrijwillig, specifiek, geïnformeerd en ondubbelzinnig instemt met de verwerking van zijn persoonsgegevens. Hiertoe zou kunnen behoren het klikken op een vakje bij een bezoek aan een internetwebsite, het selecteren van technische instellingen voor diensten van de informatiemaatschappij of een andere verklaring of een andere handeling waaruit in dit verband duidelijk blijkt dat de betrokkene instemt met de voorgestelde verwerking van zijn persoonsgegevens. Stilzwijgen, het gebruik van reeds aangekruiste vakjes of inactiviteit mag derhalve niet als toestemming gelden. De toestemming moet gelden voor alle verwerkingsactiviteiten die hetzelfde doel of dezelfde doeleinden dienen. Indien de verwerking meerdere doeleinden heeft, moet toestemming voor elk daarvan worden verleend. Indien de betrokkene zijn toestemming moet geven na een verzoek via elektronische middelen, dient dat verzoek duidelijk en beknopt te zijn en niet onnodig storend voor het gebruik van de dienst in kwestie.

↓  
duidelijke actieve handeling – dus niet stilzwijgend!

in vrijheid gegeven...

specifiek, geïnformeerd en ondubbelzinnig

afzonderlijke toestemming voor verschillende doeleinden

op duidelijke en beknopte wijze gevraagd en niet onnodig storend

(42) Indien de verwerking plaatsvindt op grond van toestemming van de betrokkene, moet de verwerkingsverantwoordelijke kunnen aantonen dat de betrokkene toestemming heeft gegeven voor de verwerking. Met name in de context van een schriftelijke verklaring over een andere zaak dient te worden gewaarborgd dat de betrokkene zich ervan bewust is dat hij toestemming geeft en hoever deze toestemming reikt. In overeenstemming met Richtlijn 93/13/EEG van de Raad (10) stelt de verwerkingsverantwoordelijke vooraf een verklaring van toestemming op in een begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal; deze verklaring mag geen oneerlijke bedingen bevatten. Opdat toestemming met kennis van zaken wordt gegeven, moet de betrokkene ten minste bekend zijn met de identiteit van de verwerkingsverantwoordelijke en de doeleinden van de verwerking van de persoonsgegevens. Toestemming mag niet worden geacht vrijelijk te zijn verleend indien de betrokkene geen echte of vrije keuze heeft of zijn toestemming niet kan weigeren of intrekken zonder nadelige gevolgen.

↓  
bewijsplicht m.b.t. toestemming

bewustheid dat toestemming is gegeven en hoever die reikt

begrijpelijk en gemakkelijk toegankelijk, duidelijke en eenvoudige taal

identiteit van de toestemmingvragers en de verwerkingsdoeleinden

'echte keuze' en weigering of intrekking kan zonder 'nadelige gevolgen'...

↓

(43) Om ervoor te zorgen dat toestemming vrijelijk wordt verleend, mag toestemming geen geldige rechtsgrond zijn voor de verwerking van persoonsgegevens in een specifiek geval wanneer er sprake is van een duidelijke wanverhouding tussen de betrokkene en de verwerkingsverantwoordelijke, met name wanneer de verwerkingsverantwoordelijke een overheidsinstantie is, en dit het waarschijnlijk maakt dat de toestemming in alle omstandigheden van die specifieke situatie vrijelijk is verleend. De toestemming wordt geacht niet vrijelijk te zijn verleend indien geen afzonderlijke toestemming kan worden gegeven voor verschillende persoonsgegevensverwerkingen ondanks het feit dat dit in het individuele geval passend is, of indien de uitvoering van een overeenkomst, daaraan behorende het verlenen van een dienst, afhankelijk is van de toestemming ondanks het feit dat dergelijke toestemming niet noodzakelijk is voor die uitvoering.

*geen 'duidelijke wanverhouding' tussen toestemmingvrager en -gever...*

*afzonderlijke toestemming voor verschillende gegevensverwerkingen...*

*bij aangaan van overeenkomst geen toestemming verlangen voor verwerkingen die niet nodig zijn voor de uitvoering van die overeenkomst...*

*Echter, uit art. 7(4) AVG blijkt dat er in zo een geval alleen goed moet worden onderzocht of de toestemming in vrijheid is gegeven*

## bewijsvermoeden

Amendement  
Kamerstukken II 2011/12,  
32 549, nr. 39

- cookies gebruikt voor verzamelen, combineren of analyseren van gegevens over het gebruik van verschillende diensten van de informatiemaatschappij
- worden vermoed persoonsgegevens verwerkingen te zijn

AVG van toepassing en in dat geval verwerkingsgrondslag vereist, zoals

- toestemming, of
- uitvoering overeenkomst, of
- gerechtvaardigd belang



## uitzonderingen

### geen toestemming of informatieplicht als:

- cookies strikt noodzakelijk zijn om de gevraagde dienst van de informatiemachtigheid te leveren
- én privacy ongevaarlijke effectiviteits- of kwaliteitscookies...
- cookies die nodig zijn om de communicatie over een elektronisch communicatienetwerk uit te voeren, of als;

taalinstellingen, voorkeuren, opslaan wachtwoord, betalingen via ideal, enz.  
Kamerstukken II 2010/11, 32 549, p. 78

analytics, A/B-testing, affiliate cookies, e.d.

## cookiemuren-verbod

Art 11.7(5) Tw

*De toegang van de gebruiker tot een dienst van de informatie-maatschappij die wordt geleverd door of namens een krachtens publiekrecht ingestelde rechtspersoon wordt niet afhankelijk gemaakt van het verlenen van toestemming*



## cookiemuren-discussie

Text proposed by the Commission

(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, end-users are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, end-users are overwhelmed with requests to provide consent. The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should provide for the possibility to express consent by using the appropriate settings of a browser or other application. The choices made by end-users when establishing its general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties. Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the end-user and the website. From this perspective, they are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers may be used as gatekeepers, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.

Amendment

(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, users are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, users are overwhelmed with requests to provide consent. **This Regulation should prevent the use of so-called "cookie walls" and "cookie banners" that do not help users to maintain control over their personal information and privacy or become informed about their rights.** The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should provide for the possibility to express consent by **technical specifications, for instance by using the appropriate settings of a browser or other application. These settings should include choices concerning the storage of information on the user's terminal equipment as well as a signal sent by the browser or other application indicating the user's preferences to other parties.** The choices made by users when establishing the general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties. Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the user and the website. From this perspective, they are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers, or applications or operating systems may be used as the executor of a **user's choices,** thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.

*Text proposed by the Commission*

(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, **end-users** are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, **end-users** are overloaded with requests to provide consent. The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should provide for the possibility to express consent by using the appropriate settings of a

browser or other application. The choices made by **end-users** when establishing **its** general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties. Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the **end-user** and the website. From this perspective, they are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers may be used as **gatekeepers**, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.

*Amendment*

(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, **users** are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, **users** are overloaded with requests to provide consent. **This Regulation should prevent the use of so-called "cookie walls" and "cookie banners" that do not help users to maintain control over their personal information and privacy or become informed about their rights.** The use of technical means to provide consent, for

this Regulation should provide for the possibility to express consent by **technical specifications, for instance by** using the appropriate settings of a browser or other application. **Those settings should include choices concerning the storage of information on the user's terminal equipment as well as a signal sent by the browser or other application indicating the user's preferences to other parties.** The choices made by **users** when establishing **the** general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties. Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the **user** and the website. From this perspective, they are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers, **or applications or operating systems** may be used as **the executor of a user's choices**, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.



Alle antwoorden op mijn vragen

## Vragen van organisaties over cookiewalls

### Mag ik als organisatie een cookiewall gebruiken?

Nee, dat mag niet. Op grond van de Algemene verordening gegevensbescherming (AVG) is een cookiewall (cookiemuur) niet toegestaan. Dat komt omdat u met een cookiewall géén geldige toestemming kunt krijgen van uw bezoekers of gebruikers voor het plaatsen van tracking cookies.

#### Toestemming voor tracking cookies

U moet toestemming vragen om tracking cookies te plaatsen. Dit geldt als u een website heeft, maar ook bij apps of andere diensten. Met tracking cookies kunt u het (internet)gedrag van mensen door de tijd heen volgen. Vaak zijn dit advertentiecookies.

#### Cookiewall

Een cookiewall houdt in dat mensen die een website willen bezoeken of app willen gebruiken, de vraag krijgen om cookies te accepteren voordat zij toegang krijgen tot de website. Geven zij geen toestemming, dan krijgen zij geen toegang.

Let op: het verbod op cookiewalls ziet niet alleen op het plaatsen van cookies. Niet alleen cookies vallen onder deze beschrijving, maar ook daarmee vergelijkbare technieken waarvoor eveneens toestemming gevraagd moet worden. Dit zijn technieken zoals Javascripts, Flash cookies, HTML5-local storage en/of web beacons.

#### Geldige toestemming

De AVG stelt strenge eisen aan geldige toestemming. Een belangrijke eis is dat mensen vrij moeten zijn om toestemming te geven. En dus ook om toestemming te weigeren. De AVG ziet toestemming niet als 'vrij' als iemand geen echte of vrije keuze heeft. Of als diegene toestemming niet kan weigeren zonder nadelige gevolgen.

Bij een cookiewall hebben websitebezoekers geen echte of vrije keuze. Weliswaar kunnen ze tracking cookies weigeren, maar dat kan niet zonder nadelige gevolgen. Want tracking cookies weigeren, betekent dat ze geen toegang krijgen tot de website. Daarom zijn cookiewalls onder de AVG verboden.

Zie ook: [Hoe vraag ik als organisatie toestemming zonder cookiewall?](#)

**NEE**

Géén ongevraagde  
commerciële elektronische  
communicatie

**NEE**

Art. 11.7-11.8 Telecomwet

*ongevraagde elektronische communicatie zonder menselijke tussenkomst*

**SPAM**



"Greetings, friend. Do you wish to look as happy as me?"

Well, you've got the power inside you right now.

**So use it.**

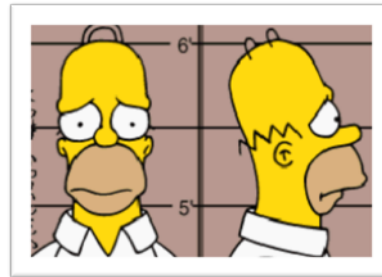
And send \$1 to Happy Dude, 742 Evergreen Terrace, Springfield. Don't delay; eternal happiness is just \$1 away!"

"Greetings friend, this is Homer Simpson, aka, Happy Dude.

The courts have ordered me to call everyone, and apologize for my telemarketing scam...

**I'm sorry.**

If you can find it in your heart to forgive me, send \$1 to Sorry Dude, 742 Evergreen Terrace, Springfield. You have the power!"



## waar gáát het over?

ongevraagde elektronische communicatie voor commerciële ideële of charitatieve doeleinden met en zonder menselijke tussenkomst

A guaranteed delivery of 50 million e-mails for under a thousand bucks

And you need only one sucker in a million to recover your start-up costs

oproepautomaat, fax, spam! e-mail, sms, wallposts

lagere kosten, dus opt-in

telemarketing

hogere kosten, dus opt-out

## *commercieel (ideëel of charitatief):*

*elke vorm van communicatie bestemd voor het aanprijzen van de goederen, diensten of het imago van een onderneming, instelling of persoon die een commerciële, industriële of ambachtelijke activiteit of een gereguleerd beroep uitoefent*

## *regels voor ongevraagde commerciële elektronische communicatie*

*zonder menselijke tussenkomst...*

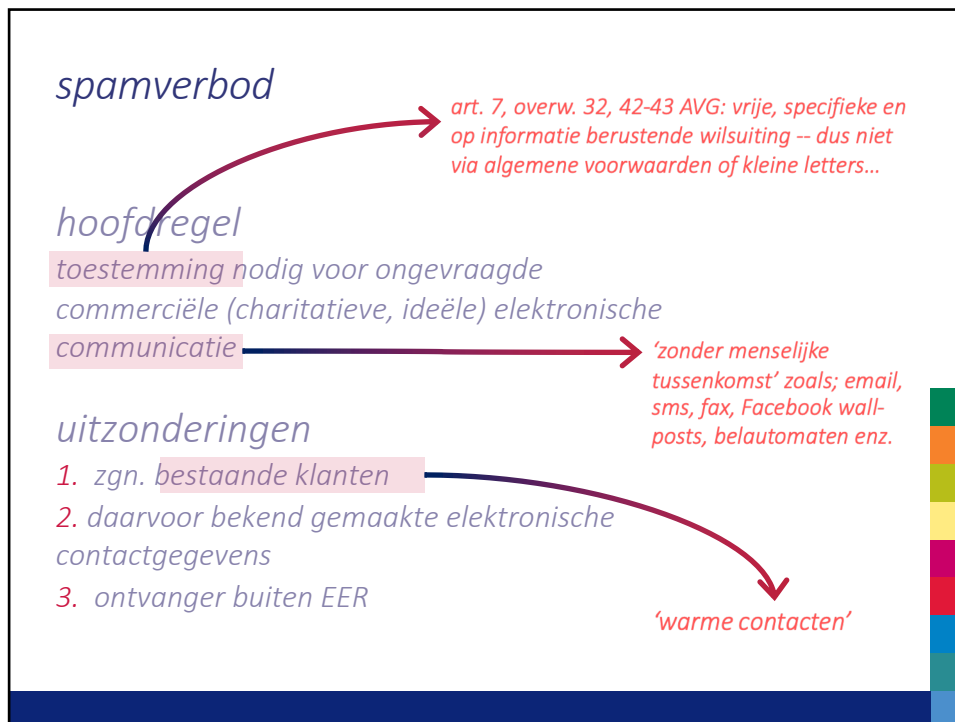
*art.11.7 jo. 11.8 Tw  
ongevraagde elektronische  
communicatie*

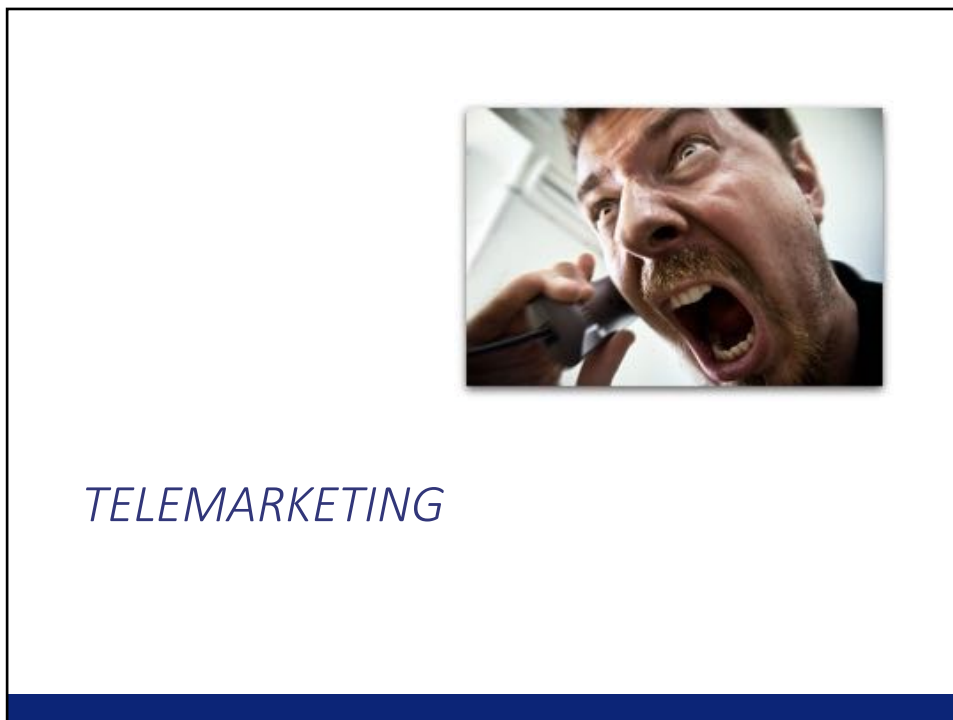
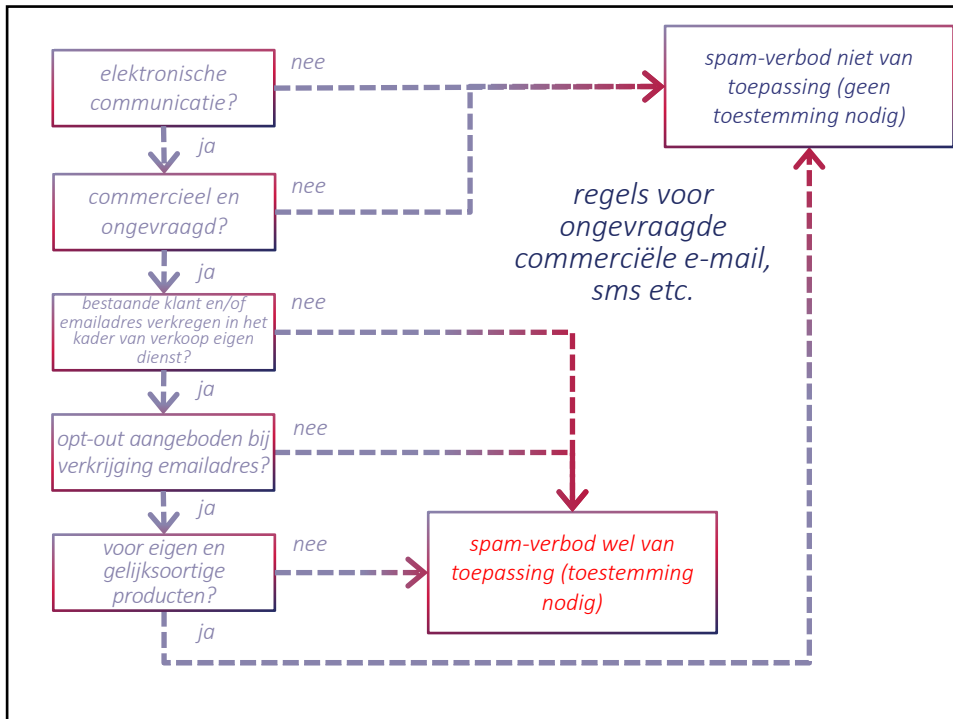
*art.3:15e BW  
dienst van de informatiemaatschappij*

*art. 21.2 AVG  
verwerking persoonsgegevens t.b.v. direct  
marketing*

*art. 7:46h -2 BW  
ongevraagde e-mail ter bevordering van  
koop op afstand*

*zelfregulering  
DDMA RCC Code Email*







# telemarketing

## hoofregel

ongevraagd bellen van natuurlijke personen voor commerciële (ideële, charitable) doeleinden is toegestaan

niet alleen consumenten maar ook zzp-ers, eenmanszaken, maten in een maatschap, vof's enz.

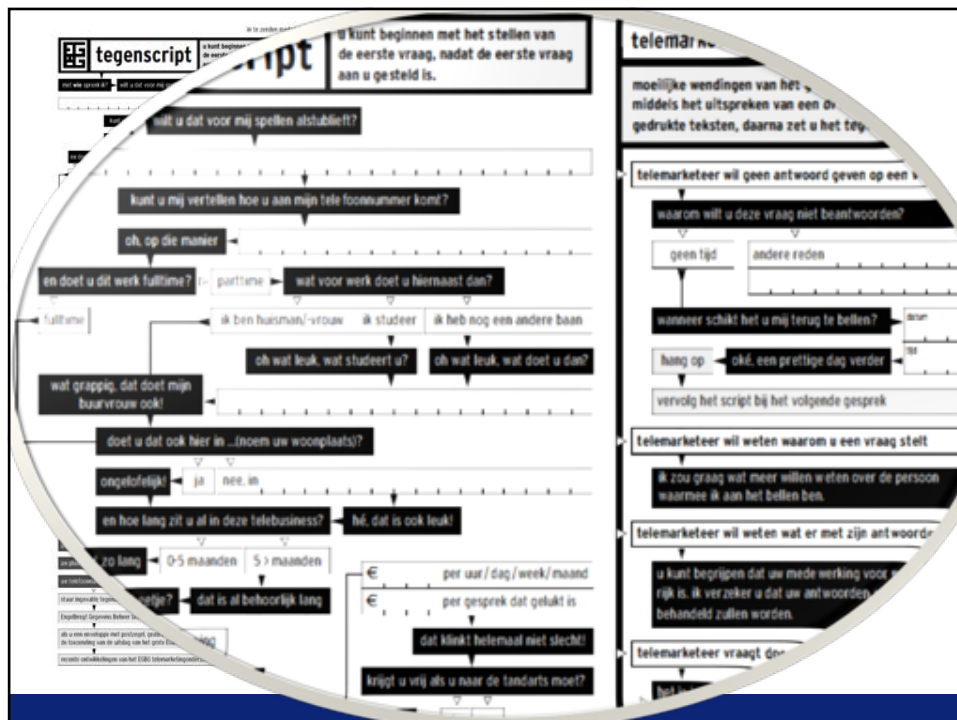
direct of indirect promoten van product, organisatie of onderneming...

- op basis van opt-out, en
- gebruikmaking van een 'ontdubbeld' belbestand

opschonen aan de hand van bestanden van bel-me-niet

## uitzondering

- zgn. 'bestaande klanten' met betrekking tot eigen gelijksoortige producten



## Cie voorstel (10 januari 2017)

- *niet alleen regels voor telcos & ISPs maar ook voor OTTs!*
- *meer aandacht voor vertrouwelijkheid van onlinegedrag*
- *cookietoestemming kan ook worden gegeven via browserinstellingen*
- *bij telemarketing moet call center het gebruikte nummer bekend maken*
- *één toezichthouder: Ap*

Over the Top: Netflix, Whatsapp etc.

maar gebruikers moeten er iedere zes maanden op worden gewezen dat toestemming kan worden ingetrokken...

of een special telemarketing-nummer gaan gebruiken...

niet meer ook ACM



## discussies

- *hoe nodig zijn specifieke ePrivacy-regels, in aanvulling op de AVG?*
- *content is nodig om nieuwe diensten te ontwikkelen*
- *moeten cookiemuren worden verboden..?*

Bijv. Artificial Intelligence based support, vertaalssoftware, enz.

individuele gebruiker niet geneigd toestemming te geven

contractsvrijheid?

zelfrijdende auto's en andere devices...

*vragen?*

[g.j.zwenne@law.leidenuniv.nl](mailto:g.j.zwenne@law.leidenuniv.nl)

