SMART Privacy
Actualiteiten internetrecht 28 november 2013
Robert Kreuger & Lars Leemeijer

Inleiding

SMART devices[1] verzamelen een enorme hoeveelheid data waaronder het e-mailadres van de gebruiker, locatiegegevens, contactlijsten, agenda en foto's. Deze gegevens worden gekoppeld aan een uniek ID nummer van het SMART device.[2] Doordat Apps interacteren met de besturingssystemen van SMART devices, kan veel meer data verzameld worden dan met de traditionele internetbrowser.[3] Zo kunnen zelfs microfoons en camera's door Apps worden aangezet. Tegelijkertijd is sprake van een ontwikkeling waarbij (persoonlijke) data wordt prijsgegeven in ruil voor (gratis) diensten (*data als betaalmiddel*).[4] Problematisch wordt het wanneer deze 'transactie' wordt gesloten terwijl de App-gebruiker niet of slecht geïnformeerd is over welke data wel en welke niet wordt overgedragen'.[5] Het behoeft weinig uitleg dat dit privacy problemen met zich meebrengt. In deze paper staat de impact van SMART devices op de persoonlijke levenssfeer centraal. De volgende hoofdvraag wordt in de onderstaande paragrafen beantwoord: ***Welke privacyrechtelijke normen moeten van toepassing zijn op Apps?*** Doel is te komen tot een *global approach*, echter zonder daarbij aandacht te besteden aan het jurisdictieprobleem.[6] Om de centrale probleemstelling te beantwoorden wordt in paragraaf 1 het begrip privacy uitgelicht. Vervolgens wordt in paragraaf 2 de ontwikkeling rondom SMART devices beschreven. In paragraaf 3 wordt een aanzet gedaan tot een *global approach.*

1. Juridisch kader

Privacy is geen nieuw begrip en bovendien tijd-, plaats- en contextafhankelijk.[7] Privacy is van oudsher van belang in het kader van de woning en het intieme leven.[8] Problematisch is dat het intieme leven zich in toenemende mate online afspeelt en dat gezien de hoeveelheid privacygevoelige data die zich op een SMART device kan bevinden, betoogd kan worden dat een doorzoeking hiervan een minstens even zware impact kan hebben op de persoonlijke levenssfeer als een doorzoeking van

[1] Hiermee bedoelen wij onder andere smartphones en tablets. Met oog op snelle technologische ontwikkelingen (met het bijbehorende fenomeen *"Internet of Things*" (zie bijvoorbeeld H. Kopetz, *Real-Time System Design Principles for Distributed Embedded Applications*, Real-Time Systems Series 2011, p. 307-323.) prefereren wij de overkoepelende term '*SMART devices'*. Deze term staat voor "an electronic device, generally connected to other devices or networks via different protocols such as Bluetooth, NFC, WiFi, 3G, etc, that can operate to some extent interactively and autonomously", *Wikipedia.com*, <bit.ly/chkNA1>.
[2] 'Mobile Data Privacy Is Terra Incognita to Users and Developers', *PCWorld.com* 24 februari 2012, <bit.ly/xrToOY>.
[3] Article 29 Data Protection Working Party (27 februari 2013), *Opinion 02/2013 on apps on smart devices*, p. 5, <bit.ly/WJnjzC>; Bovendien draagt de smartphone gebruiker het device bijna altijd bij zich en staat het bijna altijd aan, zie FTC Staff Report (februari 2013), *Mobile Privacy Disclosures. Building Trust Through Transparency*, p. 2. <1.usa.gov/U8mcby>.
[4] 'Data als betaalmiddel: de nieuwe privacy', *Emerce.nl* 12 november 2013, <bit.ly/1brabDR>; Zie over het benaderen van persoonsgegevens als eigendomsrecht: C. Prins, "When personal data, behavior and virtual identities become a commodity: Would a property rights approach matter?", (2006) 3:4 *SCRIPTed* 270, p. 270-303. <bit.ly/17U1EIg>.
[5] Zie M. Hildebrandt, *Recht en markt: met falen en opstaan*, in: L. Mommers et al. (red.), *Het binnenste buiten*, Leiden: Meijers-Instituut 2010, p. 275-289.
[6] Omdat de spelers rondom SMART devices (App ontwikkelaars, Appstores, telecom-aanbieders en eindgebruikers), zich veelal geografisch op verschillende plaatsen bevinden, zijn er problemen rondom jurisdictie. Door deze mondiale insteek en een beperking in het aantal te gebruiken woorden in deze paper, is het afbakenen van deze paper door jurisdictieaspect uit te sluiten gerechtvaardigd.
[7] P.H. Blok, *Het recht op privacy: een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht*, Den Haag: Boom Juridische uitgevers 2002, p.25. Blok nuanceert deze in de literatuur veel gemaakte bewering door te stellen dat het niet de privacy zelf is die plaats en contextafhankelijk is, maar dat er per plaats en context op een verschillende manier wordt omgesprongen met de rechtvaardigingsgronden voor een inbreuk op privacy.
[8] P.H. Blok. "Het recht op privacy: een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht.", Den Haag: Boom Juridische uitgevers 2002, p.25.

de woning. De problematiek rondom de impact van technologie op privacy is al vroeg beschreven.[9] Om deze reden is het van belang te bezien of, en zo ja in hoeverre, het concept van privacy heroverwogen dient te worden in de huidige informatiesamenleving.[10] In deze paragraaf wordt daarom getracht het privacybegrip te duiden. Om tot een goede duiding te komen, moet gekeken worden naar de losse kernbeginselen zoals die zijn neergelegd in verschillende wet- en regelgeving. Deze losse elementen overlappen echter, en grijpen in elkaar. Op basis van hetgeen is gedistilleerd uit de bestaande literatuur en wet- en regelgeving, wordt vervolgens een aanzet gedaan tot een *global approach* van privacy met betrekking tot SMART devices.

In het kader van een *global approach*, is ons vertrekpunt niet artikel 8 lid 1 EVRM,[11] maar artikel 17 IVBPR.[12]

> *1. Niemand mag worden onderworpen aan willekeurige of onwettige inmenging in zijn privé leven, zijn gezinsleven, zijn huis en zijn briefwisseling, noch aan onwettige aantasting van zijn eer een goede naam.*
> *2. Een ieder heeft recht op bescherming door de wet tegen zodanige inmenging of aantasting*

Hoewel het IVBPR niet door alle staten is ondertekend (en geratificeerd), vindt het in tegenstelling tot het EVRM, wereldwijde toepassing.[13] Grosso modo gaat privacy om het afschermen van het eigen leven tegen ongewenste inmenging van buitenaf met als onderliggend belang de autonomie en zelfbeschikking[14] om zodoende de onafhankelijkheid van het individu te waarborgen.[15] Dit volgt ook uit de begripsomschrijving van Westin (1967): "*Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others".*[16]

In het kader van SMART devices staat in de literatuur en relevante wet- en regelgeving voornamelijk het (min of meer zelfstandig) recht op bescherming van persoonsgegevens centraal,[17] waarbij vaak een onderscheid wordt gemaakt tussen 'normale' en 'bijzondere' gegevens.[18] Bescherming van

[9] Het *juridische* begrip 'privacy'; "*the right to be let alone*", is voor het eerst in 1890 beschreven door Samuel D. Warren en Louis D. Brandeis in "The right to privacy." *Harvard law review* 4.5 (1890). P. 193-2200. "*Numeruous mechanical devices threaten to make good the prediction that what is whispered in the closet shall be proclaimed from the house tops*", p. 194. De informatietechnologie die toen centraal stond was met telelenzen de privésfeer binnendringen door foto opnames te maken.
[10] Vergelijk A.F. Westin, "Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I--The Current Impact of Surveillance on Privacy." *Columbia Law Review* 66.6 (1966), p. 1017.
[11] Artikel 8 lid 1 Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, Rome, 04-11-1950.
[12] Artikel 17 Internationaal Verdrag inzake burgerrechten en politieke rechten, New York, 16-12-1966.
[13] Zie voor een overzicht van de landen die het IVBPR ondertekend en geratificeerd hebben: *Minbuza.nl*, <bit.ly/IoJSUB>.
[14] Vergelijk E.J. Dommering. "Privacy als het zelfbeschikkingsrecht van de 21e eeuw." *Mediaforum-Amsterdam* 2009-11/12, p. 382.
[15] A.F. Westin, "Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I--The Current Impact of Surveillance on Privacy." *Columbia Law Review* 66.6 (1966), p. 1024. Uit jurisprudentie volgt nog dat het recht op een persoonlijke levenssfeer zich ook uitstrekt tot de werkvloer (EHRM 16 december 1992, nr. 13710/88 (*Niemitz/Duitsland*).
[16] A.F. Westin, *Privacy and Freedom*, New York: Atheneum 1967, p. 7.
[17] Het is van belang te constateren dat privacy en de bescherming van persoonsgegevens niet hetzelfde zijn: het recht op (informationele) privacy is breder en omvat onder andere de bescherming van persoonsgegevens. In het kader van *SMART devices* staan echter voornamelijk persoonsgegevens centraal, zoals neergelegd in 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).
[18] 'Persoonsgegevens' zijn gegevens die betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon (zie HvJ EU 9 november 2010, nr. C-92/09 en C-93/09 (*Schecke en Eifert*)). 'Bijzondere persoonsgegevens' zijn gegevens met een intiem karakter of waarvan het gebruik het risico van discriminatie in zich draagt. Dit zijn gegevens betreffende iemands godsdienst, levensovertuiging, politieke gezindheid, gezondheid, sexuele leven, lidmaatschap van een vakbond en strafrechtelijke gegevens (vergelijk artikel 8 Richtlijn 45/96/EG, in Nederland geïmplementeerd in artikel 16 Wbp).

persoonsgegevens bestaat ons inziens uit de volgende kernelementen.[19] *Rechtsgrondslag*: er moet een wettelijke grondslag zijn die (persoons-) gegevensverwerking rechtvaardigt.[20] In het kader van gegevensverwerking bij Apps bestaat deze rechtsgrondslag doorgaans uit *toestemming.*[21] Het tweede element is *transparantie*: de betrokkene moet voorafgaand aan de verwerking van zijn gegevens op de hoogte worden gesteld van de identiteit van de verwerker en het doel waarvoor zijn gegevens worden verwerkt. Het moet inzichtelijk zijn welke gegevens worden verzameld en tussen wie deze informatie wordt uitgewisseld (*accountability*).[22] Het derde component is *doelbinding*: gegevensverwerking zou beperkt moeten worden tot een vooraf vastgesteld doel. Verder is van belang dat de kwaliteit en kwantiteit van de verzamelde gegevens toereikend is, ter zake dienend en niet bovenmatig (data-minimalisatie).[23] Bovendien moeten de gegevens afdoende worden beveiligd (dataprotectie)[24] en moet er een mogelijkheid zijn de gegevens aan te vullen, te verbeteren of te verwijderen.[25]

2. Apps & Privacy

Om een goed beeld te schetsen betreffende de omvang en de juridische aspecten rondom Apps en privay zal kort de ontwikkeling van de App en Appmarket worden beschreven, waarna zal worden ingegaan op problemen veroorzaakt door de mogelijkheden van Apps.

In 2007 kwam de iPhone op de markt. Dit was de eerste smartphone die aansloeg bij het brede publiek.[26] Op 10 juli 2008 werd de App Store geopend, het eerste platform voor Apps, welke de ontwikkeling van Apps in een stroomversnelling heeft gebracht. In de eerste paar dagen werden er meer dan 10 miljoen Apps gedownload.[27] Kort nadat Apple de App Store lanceerde werd er door de concurrentie soortgelijke platforms opgezet.[28] Momenteel zijn de App Market en Google Play de belangrijkste App-aanbieders.[29] Technologische ontwikkelingen brengen mee dat steeds meer Apps voor verschillende doeleinden gebruikt zullen worden.[30] Uit onderzoek van Forrester[31] blijkt dat de hoeveelheid en significantie van Apps in hoog tempo zal toenemen. Er wordt dan ook wel van *App*

[19] Deze componenten zijn ontleend uit literatuur omtrent bescherming van persoonsgegevens (zie bijvoorbeeld: Article 29 Data Protection Working Party (27 February 2013), *Opinion 02/2013 on Apps on SMART devices*,<bit.ly/WJnjzC>; P.H. Blok, *Het recht op privacy: een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht*, Den Haag: Boom Juridische uitgevers 2002 en bestaande regelgeving.

[20] Deze wettelijke grondslag moet aan de vereisten van '*accessibility'* en '*foreseeability'* voldoen (EHRM 26 april 1979, ECHR Series A, 30, *NJ* 1980, 146, par. 49 (*Sunday Times/ Verenigd Koninkrijk*).

[21] Vergelijk artikel 8 lid 2 (a) Richtlijn 45/96/EG; Article 29 Data Protection Working Party (13 juli 2011), *Opinion 15/2011 on the definition of consent*, <bit.ly/1aTKZVz>.

[22]Vergelijk artikel 10 Richtlijn 45/96/EG.

[23] The data minimization principle derives from Article 6.1(b) and (c) of Directive 95/46/EC and Article 4.1(b) and (c) of Regulation EC (No) 45/2001, which provide that personal data must be "collected for specified, explicit and legitimate purposes" and must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed". <bit.ly/1dwzR5y>.

[24] Zie artikelen 16 en 17 Richtlijn 45/95/EG.

[25] Vergelijk artikel 12 Richtlijn 45/96/EG.

[26] Twintig jaar eerder (1993) is de eerste smartphone op de markt gebracht, de IBM Simon Personal Communicator. Met de Simon werden ook de eerste Apps (kalender, adresboek, klok, rekenmachine, notitieblok, email en games) ontwikkeld. Echter, bij het brede publiek is de iPhone de eerste smartphone welke massaal in gebruik werd genomen.

[27] 'iPhone App Store Downloads Top 10 Million in First Weekend', *Apple.com* 14 juli 2008, <bit.ly/GX3sia>.

[28] Google (Android Market), Microsoft (Marketplace), Blackberry (App World) en Nokia (Ovi).

[29] Apple heeft dit jaar bekend gemaakt dat er meer dan 50 miljard downloads zijn gedaan in de App Store. Voor Google Play gelden gelijke cijfers, hetgeen betekent dat er in totaal over de 100 miljard Apps zijn gedownload door consumenten. Hiernaast blijkt dat de App Store gebruiker gemiddeld 83 Apps en de Google Play gebruiker 53 Apps installeert. 'Apple's App Store Marks Historic 50 Billionth Download', *Apple.com* 16 mei 2013, <bit.ly/13osUZk> en '100 billion App downloads', *Asymco.com* 31 mei 2013, <bit.ly/1aJmKqr>.

[30] Door de innovatie rondom SMART Devices (denk aan Google Glasses, Near field communication of bijvoorbeeld medische Apps) wordt de kans op eventuele schending van het recht op de persoonlijke levenssfeer aanzienlijk vergroot.

[31] A BT Futures Report (maart 2011), *Mobile App Internet Recasts The Software And Services Landscape*, <bit.ly/1i9Mfub>.

Internet gesproken.[32] Het probleem ligt in de veelheid aan data die Apps kunnen verwerken. Een trend die is ontstaan bij de ontwikkeling van Apps is die van data maximalisatie.[33] Apps proberen zoveel mogelijk persoonsgegevens te verwerken met als doel deze door te verkopen aan derden (denk aan advertentie- of analytische bureaus).

Deze trend van data maximalisatie staat haaks op het recht op de bescherming van privacy. Big Data is een verdienmodel geworden.[34] Dit geldt ook voor Apps op SMART devices. Apps verwerken gegevens[35] en verkopen deze door, maar vaak ontbreekt het aan een wettelijke grondslag. Niet alleen de gegevensverwerking van een persoon wordt gebruikt maar ook de gegevens van alle personen er omheen. Naarmate er meer gegevens over een persoon worden verwerkt, wordt het profiel van een persoon meer waard. Data is hiermee een product geworden. Afgevraagd kan worden in hoeverre dit strookt met bovengenoemde zelfbeschikking. Personen beschikken niet over hun eigen data, of hebben in ieder geval geen (tot weinig) macht over hun eigen data. De controle ligt bij de partijen die de gegevens van een persoon verwerken en kunnen verkopen.[36] Potentieel gevaar ligt in het doel van de massale gegevensverwerking. Bedrijven koppelen het gedrag van een persoon met andere profielen zodat ze een voorspelling kunnen maken en het gedrag kunnen beïnvloeden. Door kleine gedragsveranderingen waar te nemen, maken computers patronen die niet zichtbaar zijn voor mensen en kunnen zij het gedrag van de consument bepalen. Big Data leidt dus tot een voorspellend systeem.[37] Op deze manier worden mensen gestuurd en onbewust beperkt in wat men ziet en wil.

De normering dient te worden afgestemd op de bescherming van de consument tegen bovenstaande geleidelijke beïnvloeding van beslissingen door middel van gegevensverwerking.[38] Privacy binnen de informatiemaatschappij moet worden geïnterpreteerd als een zelfstandig te waarderen belang – met de nadruk op zelfbeschikking en autonomie – van gegevensbescherming.

Bij de gegevensverwerking door Apps komt dat ons inziens op het volgende neer: er dient sprake te zijn van geïnformeerde toestemming voor een bepaalde vorm van dataverwerking, welke niet voor een ander dan het aangegeven doel wordt gebruikt. De praktijk van SMART devices blijkt echter weerbarstig ten aanzien van de in de vorige paragraaf genoemde beginselen van gegevensbescherming. Ten eerste kunnen vraagtekens geplaatst worden bij de rechtsgrondslag voor gegevensverwerking bij Apps. Zoals hierboven gezegd wordt in de praktijk 'toestemming' als rechtsgrondslag voor gegevensverwerking gekozen. Om tot toestemming te komen dient het doel van

---

[32] 'The App Internet is an application architecture of native Apps on a range of SMART mobile devices, cars, televisions, and appliances linked to a broad array of cloud-based services to provide a optimized, context-rich experience anytime, anywhere…', The Mobile "App Internet" Recasts the Software & Services Landscape by Ellen Daley, Forrester, slide 5. <slidesha.re/1c5vlaT>.
[33] Zie bijvoorbeeld 'How much is your personal data worth?', *Ft.com* 12 juni 2013, <on.ft.com/1cLMLrd>.
[34] Er zijn bedrijven met marktwaarden van ver boven de honderd miljard die (enkel) verdienen aan het verkopen van data aan derden. 'Marktwaarde Facebook boven 100 miljard dollar', *Adformatie.nl* 27 augustus 2013, <bit.ly/1dLaNVz>. Zie ook bijvoorbeeld Branham Group (juni 2012), *Maximizing the Value Provided by a Big Data Platform - IBM*, <bit.ly/1brfZPp>.
[35] Het gaat om technische data; de naam en landcode van de gebruiker, de naam en landcode van het toestel, de code van het mobile netwerk van de provider, het soort connectie die gebruikt, het soort toestel (specifieke model en versie) dat gebruikt wordt, het IP-adres van het toestel, de tijdzone, etc. en persoonlijke data; gegevens welke op het SMART Device staan zoals: adresboek, kalender, locatiegegevens, fotobestanden. Ook kunnen de gegevens die door de gebruiker zijn ingevoerd worden verwerkt. Hierbij gaat het om de geboortedatum, e-mail adres, voor- en achternaam, geslacht, profielfoto, telefoonnummer, social media account, gebruikersnaam en websites. Ook kunnen Apps cookies plaatsen welke niet zichtbaar zijn voor de gebruiker en niet verwijderd kunnen worden.
[36] Er kan beargumenteerd worden dat privacy in onze informatiesamenleving als een commercieel product gezien moet worden. Mensen moeten zelf over hun data kunnen beschikken en eventueel kunnen verkopen aan derden. Zie bijvoorbeeld <Datacoup.com> of <Personal.com>.
[37] M. Hildebrandt. "Privacy na de 'computationele wending'", *De transparante samenleving. Jaarboek ICT en samenleving 2011*. Ed. Valerie Frissen, Linda Kool en Marc van Lieshout. Media Update, TNO, ECP-EPN, 2011, p.5. <bit.ly/Ih3VUG>.
[38] TILT (januari 2005), *Veiligheid en privacy in 2030: twee toekomstscenario's*, p. 30. <bit.ly/1ifo8tX>.

de gegevensverwerking duidelijk omschreven en begrijpelijk te zijn voor de gemiddelde consument. In de praktijk ontbreekt vaak deze cruciale informatie voor de gebruiker om tot een bewuste toestemming te komen.[39] Deze informatie wordt soms niet verstrekt, of "verstopt" in algemene voorwaarden die vervolgens vaak niet ondubbelzinnig worden geaccepteerd door de eindgebruiker. Omdat de meeste Apps (indien om toestemming gevraagd wordt) enkel gebruik maken van het aanvinken van een verklaring de algemene voorwaarden – zonder dat de gebruiker bewust is van de gevolgen – te accepteren, is er doorgaans onvoldoende sprake van een naar wil en verklaring overeenstemmende overeenkomst in de zin van het civiele recht. Er kan, door het ontbreken van transparantie (vanwege onduidelijkheid en onoverzichtelijkheid) bij dergelijke aanvaardingen (die vaak impliciet wordt geacht te zijn door het gebruiken van de dienst),[40] sprake zijn van een gebrekkige wil. Daarnaast is in het kader van de algemene voorwaarden van Apps in veel gevallen niet voldaan aan de informatieplicht[41] en kan er sprake zijn van onredelijk bezwarende bedingen.[42] Bovendien worden algemene voorwaarden regelmatig gewijzigd. Een op het gebied van gegevensverwerking goed geïnformeerde consument zou sommige Apps niet downloaden,[43] bijvoorbeeld omdat hun gegevens aan derden worden doorverkocht. Ten tweede kunnen vraagtekens geplaatst worden bij de doelen waarvoor gegevens worden verwerkt door Apps. Een groot deel van de Apps verzamelt gegevens met een onduidelijk of onvoldoende duidelijk omschreven doel. Zij verzamelen bijvoorbeeld gegevens onder de noemer van 'marktonderzoek', wat niet uitsluit dat gegevens worden doorverkocht aan derden.[44]

3. Naar een *global approach*

Vanwege het mondiale karakter van internet is ook de problematiek rondom Apps grensoverschrijdend. In deze paragraaf wordt getracht de in paragraaf 1 genoemde kernelementen van bescherming van persoonsgegevens om te zetten in een leidraad voor een *global approach*, waarbij rekening wordt gehouden met de in paragraaf 2 genoemde problematiek rondom SMART devices. Wij stellen voorop dat de hierboven door ons genoemde kernelementen inherent zijn aan artikel 17 IVBPR. Ze kunnen worden gelezen als een modern uitvloeisel van artikel 17 IVBPR in de informatiemaatschappij. Dit betekent dat staten zich moeten inspannen aan deze speerpunten te voldoen. De vraag is op welke manier dit het beste vertaald kan worden naar concrete normen voor de praktijk. Met andere woorden: wat zijn de *best practices* om de consument meer controle en zelfbeschikking te geven over haar persoonlijke data?

Privacy moet worden ingebouwd tijdens het ontwikkelen van Apps (*privacy by design*). Daarbij is het ons inziens van belang dat de standaardinstellingen van Apps zo moeten zijn ingesteld, dat ze zo min mogelijk data oogsten (data-minimalisatie) bij de SMART-device gebruiker. Vervolgens moet de gebruiker de keuze hebben om naar tijd en context bepaalde data te verstrekken (*privacy by default).* Hierbij is cruciaal dat deze keuze geïnformeerd is. Om dit te bewerkstelligen moet de App duidelijke en toegankelijke informatie verschaffen over welke gegevens worden verwerkt en welke

[39] Art. 29 Data Protection Working Party over toestemming: *Ec.europa.eu*, <bit.ly/sFOLVV>.
[40] Zie bijvoorbeeld *9gag.com*, <bit.ly/AbOYAx>.
[41] De verplichting van de gebruiker om de wederpartij een redelijke mogelijkheid te bieden om van de algemene voorwaarden kennis te nemen.
[42] Gebruikers van Apps zijn consumenten en worden beschermd op grond van art. 6:233 BW (gelet op de aard en de overige inhoud van de overeenkomst, de wijze waarop de voorwaarden zijn tot stand gekomen, de wederzijds kenbare belangen van partijen en de overige omstandigheden van het geval, onredelijk bezwarend is voor de wederpartij). Algemene voorwaarden zijn – ook als de wederpartij ze niet gelezen heeft – bindend. Echter, deze mogen niet onredelijk bezwarend zijn.
[43] 'Report: Majority of app users will uninstall over privacy concerns', *Fiercedeveloper.com* 6 september 2012, <bit.ly/QE6aht>.
[44] Zie Art. 29 Data Protection Working Party (13 July 2011), *Opinion 15/2011 on the definition of consent*, p.6. Zie verder 'How much is your personal data worth?', *Ft.com* 12 juni 2013, <on.ft.com/1cLMLrd> of 'How much are you worth?', *Inria.fr* (geen datum), 'Privatics', <bit.ly/1grnSVl>.

niet (transparantie).[45] Deze informatie moet beknopt en begrijpelijk worden weergegeven in de Appstore, en op een later moment raadpleegbaar zijn in de App. De informatie in dergelijke End User License Agreemtens (EULA's) verwerken is echter niet voldoende. Hierom wordt gepleit voor *just-in-time disclosures*,[46] waarbij de gebruiker expliciet toestemming kan geven voor een bepaalde gegevensverwerking. Bij Apple Apps worden dergelijke toestemmingen reeds gevraagd, maar hier is het doel waarvoor de gegevens worden verwerkt ons inziens vaak niet duidelijk en/of expliciet genoeg gecommuniceerd. Om een goed geïnformeerde keuze te maken, moet de consument inzicht krijgen in welke gegevens worden verwerkt en voor welk doel en aan welke partijen ze worden doorgespeeld. Een stap in de goede richting om het *privacy by design*-ideaal te realiseren is een *privacy-dashboard,* waarbij een visueel overzicht wordt gemaakt welke Apps welke data verwerken en waarbij de gebruiker (per App) de keuze heeft om bepaalde data wel of niet te delen.[47] In het verlengde hiervan kunnen ook icoontjes worden getoond die bijvoorbeeld aangeven wanneer locatiegegevens worden gedeeld.[48]

Nu is vastgesteld welke normen dienen te gelden en op welke wijze deze dienen te worden geoperationaliseerd, is het de vraag wie verantwoordelijk gehouden kan worden voor de handhaving hiervan. Ons inziens zijn er meerdere redenen om Appstores verantwoordelijk te maken. Ze opereren op mondiaal niveau, hebben controle over de aard en inhoud van de Apps en handhaven, bijvoorbeeld op het gebied van intellectuele eigendom en aanstootgevende content reeds door Apps niet toe te laten in hun winkel zolang ze niet aan de wet- en regelgeving voldoen. Ze zijn de laatste partij die inhoudelijke (juridische) kwaliteitseisen kunnen stellen aan Apps, voordat de eindgebruiker ze aanschaft. Momenteel sluiten Appstores hun aansprakelijkheid op het gebied van privacy tegenover de eindgebruiker uit.[49] Tegelijkertijd stelt de Apple Appstore reeds kwaliteitsvoorwaarden aan Apps die worden gehandhaafd middels ex-ante reviews.[50] Ons inziens ligt het meer voor de hand hieraan een aansprakelijkheid te koppelen. Effectieve handhavingsmogelijkheden liggen derhalve in het aansprakelijk maken van Appstores die geen Apps mogen verkopen die niet aan de privacyrechtelijke normen voldoen. Voordeel van het verantwoordelijk maken van Appstores is dat niet alleen privacy beter gereguleerd wordt (dan handhaving te richten op individuele ontwikkelaars), maar dat de kwaliteit van Apps in brede zin gewaarborgd blijft.[51] De door ons voorgestelde vorm van zelfregulering[52] is echter ook niet vrij van haken en ogen. Voorwaarde is bijvoorbeeld dat het reviewproces van Apps transparant(er) wordt gemaakt, beslissingen tot afwijzingen goed gemotiveerd worden en dat deze openbaar zijn. Op deze punten zou nader onderzoek gedaan kunnen worden, maar het is van belang de privacyrechtelijke normen rondom apps globaal te operationaliseren om het recht op zelfbeschikking en autonomie van de gebruiker te waarborgen.

[45] DDMA (september 2013), *Praktische juridische tips mobile*, p. 5. <bit.ly/17XAlPB>; GSMA (februari 2012), *Mobile and Privacy*, p. 4. <bit.ly/KhDiu8>.
[46] FTC Staff Report (maart 2012), *Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers*, p. 15. <1.usa.gov/H3LgcC>.
[47] FTC Staff Report (februari 2013), *Mobile Privacy Disclosures. Building Trust Through Transparency*, p. 16. <1.usa.gov/U8mcby>.
[48] FTC Staff Report (februari 2013), *Mobile Privacy Disclosures. Building Trust Through Transparency*, p. 17. <1.usa.gov/U8mcby>.
[49] *Apple.com* (geen datum), 'Licensed Application for end user license agreement', <bit.ly/114qnoG>.
[50] *Developer.apple.com* (geen datum), 'App Store Review Guidelines', <bit.ly/b5S9rl>.
[51] Denk aan filtering van lage kwaliteitsApps met malware, aanstootgevende content, of anderszins inbreukmakend materiaal.
[52] Zie over privacy en zelfregulering: P.H. Blok, *Het recht op privacy: een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht*, Den Haag: Boom Juridische uitgevers 2002, p.310 ev.