



Afstudeeronderzoek

S. Eppinga

Studentnummer: 335577

Aecius Juridisch Advies

Mr. A.E.C. Punt

HBO – Rechten

Hanzehogeschool Groningen

Mr. H.W.J Smeltekop

Groningen, februari 2014

“Wat app ik nu aan mijn broek hangen?”

De relatie tussen het gebruik van apps en het beroepsgeheim van advocaten

Afstudeeronderzoek HBO – Rechten

“Wat app ik nu aan mijn broek hangen?”

De relatie tussen het gebruik van apps en het beroepsgeheim van advocaten

Door:

S. Eppinga

Student HBO – Rechten, Hanzehogeschool Groningen

Studentnummer: 335577

Opdrachtgever:

Aecius Juridisch Advies

Mr. A.E.C. Punt

Afstudeerdocent:

Hanzehogeschool Groningen

Mr. H.W.J Smeltekop

Groningen, februari 2014

Tegenwoordig zijn smartphones niet meer weg te denken in het dagelijks gebruik van de consument op zowel privé als zakelijk gebied. Om deze smartphones zo gebruiksvriendelijk mogelijk te houden zijn er apps (applicaties) ontwikkeld. Dit zijn programma's welke de gebruiker via een platform zoals de App Store of Google Play Store kan downloaden en gebruiken op zijn smartphone. Tussen deze twee Stores zit een verschil in het aanbieden en downloaden van de apps. Bij de App Store hoeft een consument niet installatievoorwaarden te accepteren en bij de Google Play Store wel. Aecius Juridisch Advies (hierna: Aecius) is gezien de berichten in de media zich ervan bewust dat apps gegevens van de smartphone verzamelen en doorsturen. Daarnaast is Aecius van mening dat de installatie- en gebruiksvoorwaarden welke de Google Play Store op een Android toestel presenteert in strijd kan zijn met de Nederlandse wet- en regelgeving, aangezien een app vaak toestemming vraagt voor toegang tot meerdere functies in het toestel dan dat de app nodig heeft. Hierdoor is de app in staat om met de toestemming van de gebruiker gegevens van de smartphone te verwerken. Tegenwoordig worden smartphones ook veel zakelijk gebruikt, zowel binnen Aecius als andere kantoren waar advocaten en juridisch adviseurs werkzaam zijn. Advocaten hebben jegens hun cliënten te maken met het beroepsgeheim. Wanneer gegevens van een cliënt zonder toestemming van deze door een app wordt verwerkt zou het beroepsgeheim van de advocaat in het geding kunnen komen.

Aecius wil hierover meer duidelijkheid krijgen en heeft mij als doel gesteld om dit probleem te onderzoeken en aanbevelingen te schrijven of er een relatie is tussen het gebruik van apps conform de installatie- en gebruiksvoorwaarden en mogelijke schending van beroepsgeheim binnen de advocatuur. In dit onderzoek heb ik mij zoveel mogelijk gericht op de wetgeving inzake apps alsmede de risico's hiervan. In deze scriptie wordt het probleem verder uitgelegd aan de hand van de opgestelde hoofd- en deelvragen.

Om dit onderzoek van verschillende kanten te belichten is er een (niet-) literatuuronderzoek en een empirisch onderzoek verricht. Binnen het (niet-) literatuuronderzoek is de toepasbare wet- en regelgeving betreffende apps en het beroepsgeheim uitgezocht en toegepast. Daarnaast zijn de installatie- en gebruiksvoorwaarden van vijf apps nader onder de loep genomen en er is onderzocht wat deze apps aan gegevens verwerken en of dit in strijd is met de Nederlandse wetgeving. Tevens is aan de hand van andere onderzoeken een beeld gegeven van de privacy risico's van apps. Binnen het empirische onderzoek zijn er privacy experts, advocatenkantoren en app-ontwikkelaars geïnterviewd. De privacy experts zijn geïnterviewd om een duidelijk beeld van de risico's en problemen van apps te geven. De advocatenkantoren en app-ontwikkelaars zijn geïnterviewd om de huidige situatie vast te stellen. Onder de huidige situatie wordt verstaan: het gebruik, de kennis en het bewustzijn van de risico's van apps.

De belangrijkste resultaten uit het onderzoek zijn:

- Er zit een verschil in het aanbieden van apps door de App Store en de Google Play Store. Bij de App Store worden apps van tevoren gecontroleerd door medewerkers van Apple voordat zij in de Store worden aangeboden. Bij de Google Play Store wordt een app van tevoren minimaal gecontroleerd en kan deze vrijwel meteen in de Store verschijnen. Google Play Store heeft ervoor gekozen om apps installatievoorwaarden te laten presenteren terwijl apps uit de App Store geen voorwaarden presenteren aan de gebruiker.
- De installatie- en gebruiksvoorwaarden van de vijf onderzochte apps voldoen veelal niet aan de wettelijke regels betreffende algemene voorwaarden, Wet bescherming persoonsgegevens (Wbp) en Telecommunicatiewet (Tw).
- De apps verzamelen veel gegevens uit de smartphone van de gebruiker, zonder dat de gebruiker dit doorheeft en hier toestemming voor geeft. Deze verzamelde gegevens worden hoofdzakelijk gebruikt voor commerciële doeleinden.

- De privacy experts geven aan dat veel mensen zich wel bewust zijn van de risico's maar ze niet precies weten wat de risico's zijn. Dit komt vooral doordat apps niet goed communiceren welke gegevens zij precies verwerken en waarvoor ze deze gegevens gebruiken.
Daarnaast is er een snelle technologische ontwikkeling die de wetgeving niet kan bijhouden, hierdoor dient de wetgeving sneller te worden aangepast.
- De advocatuur geeft aan zich wel bewust te zijn van het feit dat apps gegevens verwerken en dit risico's met zich meebrengt. Desondanks gaan advocatenkantoren er vanuit dat deze gegevens goed en veilig worden verwerkt en dat het voor een derde lastig is om daaraan te komen. Ze zien de uitvoering van het beroepsgeheim tevens als een eigen verantwoordelijkheid. Daarnaast lezen de meeste advocaten niet de voorwaarden van de app door, zodat zij niet weten welke gegevens precies worden verwerkt. Dit kan inhouden dat er gegevens zonder toestemming van de cliënt worden verzameld en verwerkt door een derde, waardoor alsnog onbewust het beroepsgeheim wordt geschonden.
- App-ontwikkelaars beweren dat zij op een nette en verantwoordelijke manier omgaan met de verwerkte gegevens, omdat zij niet in een kwaad daglicht neergezet willen worden. Ze zijn zich bewust van de privacyrisico's van apps, maar welke precies weten ze niet. Qua kennis op het gebied van Nederlandse wetgeving betreffende apps zijn ze niet volledig op de hoogte. Daarnaast geven ze aan dat de mogelijkheden, om via een app gegevens te verwerken voor 'kwade' doeleinden, eindeloos zijn.

Uit de resultaten zijn aanbevelingen voor Aecius ontstaan. De belangrijkste aanbevelingen zijn:

- Binnen Aecius zelf het app gebruik op de smartphone tot het minimum beperken wanneer er cliëntgegevens op staan.
- De bekendheid betreffende de risico's van apps is zeer gering en gezien de maatschappelijke relevantie is het belangrijk om deze bekendheid te vergoten door middel van het houden van workshops of het schrijven van een artikel.
- Verder onderzoek doen binnen meerdere advocatenkantoren naar apps en het bewustzijn van de risico's, om zo een nog breder beeld te krijgen. Daarnaast kan er een verder onderzoek worden gedaan naar andere beroepsgroepen met beroepsgeheim en hoe zij met apps omgaan en of ze bewust zijn van de risico's.

Begin september 2013 zou ik aanvankelijk starten met mijn onderzoek bij een andere organisatie, CUBE050. Ondanks het feit dat mijn onderzoeksvoorstel aan alle eisen voldeed, is vanwege het missen van voldoende juridische aspecten helaas het onderzoek afgeblazen. Om het afstuderen nog enigszins te kunnen redden heeft CUBE050 mij doorgestuurd naar Aecius met de vraag of mr. Arnoud Punt nog een “beter juridisch” onderwerp wist binnen CUBE050 waardoor ik daar kon afstuderen. Aecius is bekend met CUBE050 door het af en toe geven van workshops. Tijdens het gesprek met mr. Arnoud Punt kwam hij met een nieuw onderwerp naar voren, hierop zijn wij samen gaan brainstormen en aan het einde liep ik met een compleet nieuwe opdracht de deur uit. Mijn afstudeerplek bij CUBE050 heb ik opgezegd en ben half september van start gegaan bij Aecius. Hiervoor wil ik allereerst graag CUBE050 bedanken voor het meedenken in mogelijkheden. Tot slot wil ik bij het uitvoeren van mijn onderzoek mr. Arnoud Punt bedanken die mij telkens in de goede richting heeft gestuurd wanneer mijn onderzoek te lang dreigde te worden en mr. Harry Smeltekop die mij als afstudeerdocent heeft begeleid tijdens het afstuderen.

Sanne Eppinga

Groningen, februari 2014

Samenvatting	3
Hoofdstuk 1. Inleiding	8
Hoofdstuk 2. Methodologische verantwoording	15
2.1 Onderzoeksmethoden	15
2.2 Onderzoeksubjecten	16
2.3 Analyse gegevens	16
Hoofdstuk 3. Theorie	17
3.1 Deelvraag 1.	17
3.1.1. subvraag a.	22
3.1.2. subvraag b.	27
3.1.3. subvraag c.	30
3.2 Deelvraag 2.	34
3.3 Deelvraag 3.	36
Hoofdstuk 4. Gegevens en resultaten uit praktijkonderzoek	38
4.1 <i>Interviews met experts</i>	
Deelvraag 4.1	38
Deelvraag 4.2	39
4.2 <i>Interviews met de advocatuur</i>	
Deelvraag 5.1	41
Deelvraag 5.2	42
4.3 <i>Interviews met app-ontwikkelaars</i>	
Deelvraag 6.1	43
Deelvraag 6.2	44
Deelvraag 6.3	45
4.4 <i>Overkoepelende analyse</i>	
Deelvraag 7.1	45
Hoofdstuk 5. Conclusies en aanbevelingen	47
5.1 Conclusies	47
5.2 Aanbevelingen	51
Lijst van afkortingen en begrippen	52
Literatuurlijst en jurisprudentielijst	55
Bijlagen	60
Bijlage 1.	60
Bijlage 2.	63
Bijlage 3.	65
Bijlage 4.	67
Bijlage 5.	67
Bijlage 6.	70
Bijlage 7.	79
Bijlage 8.	82
Bijlage 9.	87
Bijlage 10.	91
Bijlage 11.	100
Bijlage 12.	104
Bijlage 13.	108

Bijlage 14.	110
Bijlage 15.	115
Bijlage 16.	116
Bijlage 17.	118
Bijlage 18.	121
Bijlage 19.	123
Bijlage 20.	124
Bijlage 21.	126
Bijlage 22.	128

Hoofdstuk 1. Inleiding

Definitie van het probleem

In dit onderzoeksrapport staat het volgende probleem centraal: Het is onduidelijk of advocaten weten welke problemen en risico's er zijn met betrekking tot apps aangaande de voorwaarden, in relatie tot het beroepsgeheim binnen de advocatuur. Daarnaast is het onduidelijk welke problemen en risico's er precies zijn met betrekking tot de voorwaarden en het functioneren van apps.

Wat is een app?

App is de afkorting van het woord applicatie. Een app is een programma die te downloaden is op apparaten zoals smartphones en tablets. Een app heeft het doel om (kleine) functies aan een telefoon of tablet toe te voegen zo zijn er; zaklamp-apps, nieuws-apps, hardloop-apps, bankier-apps, etc. Een app is een stukje software dat op het apparaat wordt gedownload en wordt "verweven" met het Operating System (OS) in het toestel.

Type praktijkgericht onderzoek

Dit onderzoek zal zich richten op het signaleren van het probleem omschreven onder: "definitie van het probleem." Er zal in de praktijk moeten worden onderzocht wat het probleem is om daarna met een oplossing te kunnen komen. Tot dusver is het onduidelijk welke risico's de voorwaarden van apps met zich mee brengen en of dit een risico is voor advocaten met beroepsgeheim.

Onderzoekskader

Het onderzoekskader is hieronder terug te lezen wordt uitgelegd door middel van de volgende punten: aanleiding, fase en cyclus, relevantie, actoren, wet- en regelgeving en eerdere onderzoeken.

Aanleiding

De aanleiding voor dit onderzoek is in beginsel ontstaan doordat er bij Aecius de vraag was ontstaan of de installatievoorwaarden welke de Facebook app hanteert bij het downloaden, in strijd zijn met het Nederlandse privacy recht. Facebook en andere soorten Social Media zoals Twitter, LinkedIn, Whatsapp en Path zijn platforms waar gebruikers een persoonlijke pagina hebben of persoonlijke informatie delen. Deze persoonlijke informatie is in sommige gevallen zowel toegankelijk via de websites of via apps op de smartphone en of tablet. Wanneer een app wordt gedownload door de gebruiker op zijn/haar smartphone, moet de gebruiker in sommige gevallen akkoord gaan met de algemene voorwaarden of de installatievoorwaarden die de apps stellen. Platforms voor apps beheren persoonlijke digitale informatie van miljoenen gebruikers en al deze persoonlijke informatie wordt digitaal getransporteerd en opgeslagen. Wanneer gebruikers akkoord gaan met de algemene voorwaarden kan het dat de app meer persoonsgegevens van het toestel haalt dan dat nodig is. De aanleiding voor dit onderzoek is dat Aecius bezorgd is naar de problemen en risico's die er spelen met betrekking tot het gebruik van apps. Aecius is zelf een Juridisch Advies bureau en heeft jegens cliënten te maken met de geheimhoudingsplicht. Naast advocaten hebben andere beroepsgroepen zoals medici, notarissen, politiebeamten, accountants, etc.¹ zich te houden aan een contractuele geheimhoudingsplicht en/of het beroepsgeheim. Aecius wil graag weten of er problemen zijn bij het gebruik van apps in relatie tot het beroepsgeheim waar bepaalde beroepsgroepen zich aan hebben te houden. Binnen het onderzoek wordt er alleen gekeken binnen de advocatuur.

¹ www.wikipedia.nl geraadpleegd op 18 september 2013 (zoek op: *beroepsgeheim*)

Fase en cyclus

De interventiecyclus bestaat uit de volgende fases: probleemsignalering, diagnosefase, ontwerpfase, interventiefase en evaluatiefase. Dit onderzoek zal vooral plaatsvinden binnen de probleemsignalering. In deze fase zal moeten worden onderzocht wat het probleem/knelpunt is alvorens te komen met een oplossing. Er kan worden vastgesteld dat er sprake is van een knelpunt, omdat er bij Aecius onduidelijkheid is over de gebruiksvoorwaarden van apps en of door middel van de betreffende voorwaarden risico's ontstaan voor beroepsgroepen met beroepsgeheim. Met behulp van dit onderzoek zal hopelijk een groot deel van deze onduidelijkheid worden weggenomen.

Relevantie

Tegenwoordig is bijna iedereen in bezit van een smartphone en/of tablet. Zo'n 8 miljoen mensen in Nederland bezitten een smartphone en 5,6 miljoen Nederlanders bezitten een tablet². Om snel en makkelijk op het relatief kleine scherm van een smartphone informatie te kunnen bekijken wordt er gebruik gemaakt van apps. Gebruikers van een smartphone/tablet kunnen apps downloaden vanuit een online distributieplatform zoals App Store, Google Play of Windows Phone Store. Alvorens een app wordt geïnstalleerd kan aan de gebruiker worden gevraagd of deze akkoord gaat met de installatievoorwaarden. Later kan een app de gebruiker vragen om akkoord te gaan met de algemene voorwaarden. De installatievoorwaarden zijn hetzelfde als app-machtigingen, de app wil bij het installeren toegang tot een aantal programma's en gegevens op het toestel. Wat er vervolgens met de gegevens gebeurt die apps verkrijgen bij toegang, is nog onduidelijk. Uit een opinie³ van Europese Privacytoezichthouders blijkt dat apps enorme hoeveelheden persoonsgegevens verwerken. Daarnaast verkrijgen ze toegang tot andere apps op de smartphone. *"Dit gebeurt vaak zonder dat gebruikers goed worden geïnformeerd en zonder toestemming. Dit is in strijd met de Europese Privacywetgeving."* Aldus voorzitter van de Artikel 29-werkgroep Jacob Kohnstamm. Aecius wil daarom graag een onderzoek naar de risico's van de installatievoorwaarden en gebruiksvoorwaarden die de apps stellen richting de gebruikers en of deze niet in strijd is met het beroepsgeheim van advocaten. Aecius heeft richting haar cliënten te maken met een geheimhoudingsplicht aangezien er bij Aecius geen advocaten werken. Een geheimhoudingsplicht is een mondelinge of schriftelijke afspraak tussen de cliënt en jurist waarbij de jurist/juridisch adviseur de plicht heeft om bepaalde opgedane kennis niet aan derden mede te delen, tenzij hier expliciet toestemming voor is gegeven. Een op een smartphone gedownloade app kan toegang krijgen tot persoonsgegevens in de smartphone⁴. Daarmee is de kans zeer groot dat tussen deze gegevens ook gegevens van cliënten zitten die op grond van de geheimhoudingsplicht of beroepsgeheim niet zonder toestemming van de cliënt aan derden mogen worden verstrekt. Daarom wil Aecius zowel voor zichzelf als voor andere juridische beroepsgenoten die zich hebben te houden aan de geheimhoudingsplicht of beroepsgeheim, een onderzoek naar de problemen en de daaruit voortvloeiende eventuele risico's van het gebruik van apps in kaart worden gebracht.

Actoren

- **Aecius Juridisch Advies:** heeft zich gespecialiseerd in het ICT-Recht en houdt zich daarom nauw bezig met de zaken die rondom software, ICT en internet gelden waaronder apps en voorwaarden. Voor Aecius wordt het onderzoek verricht, zij kunnen de daaruit voortvloeiende aanbevelingen gebruiken in de dienstverlening richting cliënten.
- **Beroepsgroepen met geheimhoudingsplicht:** De beroepsgroepen die zich aan de geheimhoudingsplicht hebben te houden zijn: medici, advocaten, notarissen, politiebeambten, accountants, priesters, paramedici, tolken, maatschappelijke assistenten, ambtenaren in fiscale en inlichtingendiensten, medewerkers van psychologische diensten⁵. In dit onderzoek ligt de focus op de advocatuur.

² 'GfK: Nederland telt 5,6 miljoen tablet gebruikers' *Tweakers* 20 juni 2013, www.tweakers.nl (zoek op *Tabletgebruikers*)

³ 'Gebruik persoonsgegevens door app alleen toegestaan met toestemming gebruiker' *College Bescherming Persoonsgegevens* 14 maart 2013 www.cbpweb.nl (zoek op *privacy apps*)

⁴ www.mijnprivacy.nl (zoek op: *privacyrisico's van apps*)

⁵ www.wikipedia.nl (zoek op: *beroepsgeheim*)

- **Clënten van de omschreven beroepsgroepen:** cliënten verstrekken persoonsgegevens aan bijv. een advocaat of arts. Deze cliënten mogen er vanuit gaan dat de desbetreffende arts of advocaat conform het beroepsgeheim met de persoonsgegevens omgaat.
- **App-ontwikkelaars:** deze bedrijven ontwikkelen apps die vervolgens te downloaden zijn vanaf een online platform. App-ontwikkelaars hebben zich te houden aan privacy regels en zijn daarmee een actor binnen dit onderzoek.

Wet- en Regelgeving

Er zal binnen het onderzoek gebruik gaan worden gemaakt van verschillende soorten wet en regelgeving.

- Europees Recht: Op Europees niveau is er wetgeving ontworpen met betrekking tot het beschermen van persoonsgegevens. Dit heeft er mee te maken dat er in Europa een vrij verkeer van informatie en gegevens heeft. Het Verdrag van Straatsburg, art. 8 EVRM en Europese richtlijnen hebben voor een groot deel de inhoud van de Wet bescherming persoonsgegevens bepaald. Alsmede de toepassing en de implementatie.⁶
- Wet bescherming persoonsgegevens (Wbp): is geregeld in het Bijzonder Bestuursrecht. De wet is conform artikel 2 lid 1 Wbp van toepassing op de geheel of gedeeltelijke geautomatiseerde verwerking van persoonsgegevens, alsmede de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.
- Algemene voorwaarden en contractrecht: Hier speelt boek 6 Burgerlijk Wetboek een rol alsmede de jurisprudentie en de wettelijke bepalingen die toepasbaar zijn op algemene voorwaarden en contracten.
- ICT-Recht: heeft onder andere toepassing op elektronische overeenkomsten en bescherming van elektronische informatie.
- Regels met betrekking tot het beroepsgeheim van beroepsgroepen: het schenden van ambts-/beroepsgeheim is strafbaar⁷. Voor advocaten is het beroepsgeheim opgenomen in de Gedragscode Centrale Controle Verordeningen van de Nederlandse Orde van Advocaten en lokale Orden van Advocaten. Voor andere ambt- en beroepsgroepen is de inhoud van het beroepsgeheim geregeld in andere stukken.

De wet- en regelgeving wordt verder uitgewerkt in deelvraag 1 van Hoofdstuk 3. Theorie.

Eerdere onderzoeken m.b.t. het voorgenomen onderzoek

- Op 14 maart 2013 heeft het College Bescherming Persoonsgegevens een artikel vrijgegeven over het gebruik van persoonsgegevens bij de mobiele app. In dit artikel hebben Europese Privacytoezichthouders een opinie geschreven over dit onderwerp⁸.
- The Wall Street Journal (hierna: The Journal) heeft een onderzoek⁹ gestart naar de soort informatie die apps verzamelen en gebruiken. The Journal onderzocht 101 populaire iOS en Android-apps en 56 daarvan gaven het unieke identificatienummer van het toestel door aan andere bedrijven. De gebruiker werd niet op de hoogte gebracht en er werd ook geen toestemming gevraagd door de app. Daarnaast gaven 47 apps de locatie van de telefoon door, 5 apps verstuurden leeftijd, geslacht en andere persoonlijke details van buitenstaanders.
- 20 augustus 2013, de MEF (Mobile Entertainment Forum) heeft onderzoek gedaan naar het privacybeleid van mobiele apps.¹⁰

⁶ H.R. Kranenburg en L.F.M. Verhey, *Wet bescherming persoonsgegevens in Europees Perspectief*, Deventer: Kluwer 2011, p. 11 en 12

⁷ artikel 272 Wetboek van Strafrecht

⁸ 'Gebruik persoonsgegevens door app alleen toegestaan met toestemming gebruiker', *College Bescherming Persoonsgegevens* 14 maart 2013 www.cbpweb.nl (zoek op *privacy apps*)

⁹ 'Hoe veilig zijn smartphone apps?' *Redactie Computerworld.nl* 14 juli 2011, www.computerworld.nl (zoek op: *Privacy Apps*)

¹⁰ 'Mobiele apps hebben vaak nog vaag privacy-beleid' 29 augustus 2013, www.telecomnieuwsnet.wordpress.com (zoek op: *Privacy Apps*)

Er zijn verder geen onderzoeken die zich specifiek richten tot het privacybeleid van apps en de risico's daarvan voor het beroepsgeheim van bepaalde beroepsgroepen.

Doelstelling

(a.)

Het doel van dit onderzoek is het doen van aanbevelingen aan Aecius Juridisch Advies, betreffende de relatie tussen het gebruik van apps conform de installatie - en gebruiksvoorwaarden en het handelen daarnaar, door zowel de gebruiker als de app-ontwikkelaar en de mogelijke schending van beroepsgeheim binnen de advocatuur.

door;

(b.)

Het in kaart brengen van de eventuele problemen en risico's van de gebruiksvoorwaarden van apps en het handelen daarnaar, in relatie tot het beroepsgeheim van advocaten. Dit is gebaseerd op de uitkomsten van interviews met experts, de advocatuur, app-ontwikkelaars, en het doen van (niet)-literatuuronderzoek.

Centrale vraag

Welke conclusies zijn er af te leiden uit de in kaart gebrachte problemen en risico's van de (gebruiks)voorwaarden van apps en het handelen daarnaar, in relatie tot het beroepsgeheim van advocaten, blijkens het literatuuronderzoek en interviews?

Deelvragen

Theoretisch

1. Welke wet- en regelgeving en jurisprudentie spelen een rol bij de voorwaarden van apps?
 - a. Wat betekent het akkoord gaan met voorwaarden van een app? *(In het bijzonder wordt er gekeken naar de meest voorkomende installatievoorwaarden van de app, welke de app toegang geeft tot andere apps in het toestel. Bijvoorbeeld email, foto's, camera, contactgegevens etc.)*
 - b. Welke gegevens verzamelen apps volgens de gebruiksvoorwaarden en hoe werkt de praktijk?
 - c. Zijn de voorwaarden die worden geaccordeerd bij installatie van apps (bijv. vragen om toegang tot foto's) in strijd met de Nederlandse wetgeving?
2. Wat zijn conform (niet-)literatuurbronnen en onderzoeken de problemen en risico's die er spelen met betrekking tot de veiligheid van vertrouwelijke informatie bij het gebruik van apps?
3. Wat houdt het beroepsgeheim van de advocatuur in en wanneer wordt het beroepsgeheim geschonden in combinatie met het werken met apps?

Methoden van onderzoek: de theoretische deelvragen vallen onder deskresearch. Deskresearch wordt toegepast als basis van het onderzoek, dit is de theoretische kant van het onderzoek waar het onderzoek onderbouwd worden aan de hand van relevante niet-literatuur en literatuur. De bovenstaande deelvragen van dit onderzoek zijn theoretisch. Het is namelijk belangrijk om eerst een basis te leggen waarin de relevante wet- en regelgeving, jurisprudentie en het onderwerp goed wordt uitgelegd.

2. Empirisch

Interviews met experts:

- Wat zijn de risico's en eventuele privacyproblemen van apps?

Interviews met advocaten:

- Hoe wordt er binnen het advocatenkantoor rekening gehouden met het gebruik van apps en de eventuele risico's?

Interviews met app-ontwikkelaars:

- In hoeverre houden app-ontwikkelaars zich bezig met de veiligheid van vertrouwelijke informatie in de gebruiksvoorwaarden van apps?

- In hoeverre hebben app-ontwikkelaars invloed op de voorwaarden die platforms stellen wanneer zij een app willen aanbieden op het platform?

Methoden van onderzoek: de bovenstaande deelvragen vallen onder de onderzoeksmethode: het houden van interviews. De deelvragen zijn in drie stukken opgedeeld, er zijn deelvragen ontwikkeld voor experts, voor advocaten en voor app-ontwikkelaars. Met deze partijen worden de interviews gehouden. Deze interviews zijn nodig om informatie via de praktische kant van het onderzoek te verkrijgen. Voor de interviews worden vragen opgesteld die de deelvragen uit het empirische gedeelte beantwoorden. Het houden van interviews en gesprekken valt onder kwalitatief onderzoek. Het doel van de interviews is om zowel een weergave te kunnen schetsen van de risico's en eventuele problemen van het gebruik van apps als om de huidige situatie binnen de advocatenkantoren en app-ontwikkelaars duidelijk te krijgen. Binnen de huidige situatie vallen het gebruik, de kennis en het bewustzijn van de risico's van apps. De risico's en eventuele problemen worden besproken met de experts. De huidige situatie en de bevestiging van de risico's en problemen worden besproken met de advocaten en app-ontwikkelaars.

3. Analytisch

- Wat leert ons de vergelijking tussen de werkelijkheid volgens de experts en de theorie binnen dit onderzoek?
- Welke relatie is er tussen het gebruik van apps door de kantoren en het beroepsgeheim van advocaten?
- Zijn er overeenkomsten en verschillen tussen het handelen van de app-ontwikkelaar in de praktijk en de resultaten uit de theorie?
- Wat leert ons de vergelijking van de resultaten van elk van de drie onderzoeksobjecten?

Methoden van onderzoek:

De bovenstaande drie deelvragen vallen onder het analytische gedeelte van het onderzoek. De uitkomsten van het deskresearch en interviews met experts, advocaten en app-ontwikkelaars zullen worden verzameld en geanalyseerd. Uit de drie analyses vloeit een conclusie voort. Binnen de analyse wordt er geen nieuwe informatie toegevoegd, maar informatie uit het theoretische gedeelte en empirische gedeelte samengevoegd en geanalyseerd.

Toelichting op de afbakening van het onderzoek

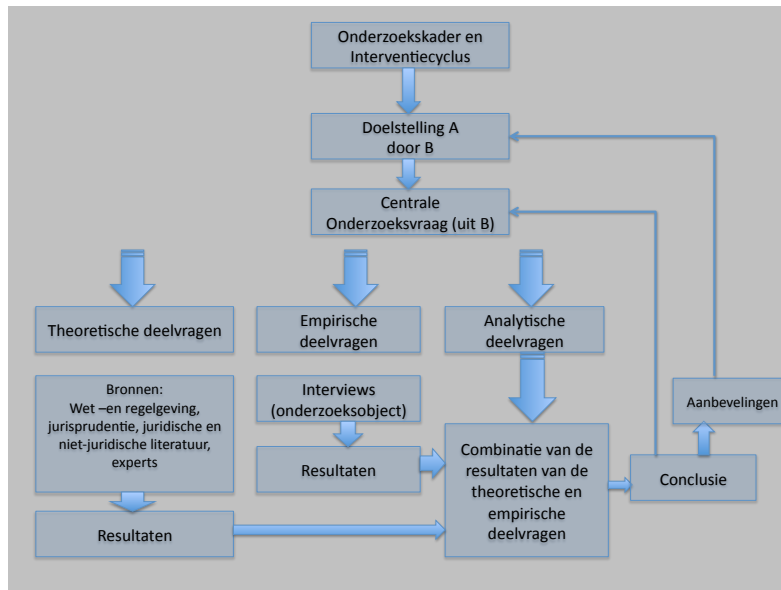
Onderzoeksobjecten: de onderzoeksobjecten welke worden gebruikt in dit onderzoek zijn experts, advocatenkantoren en app-ontwikkelaars. Er is voor deze drie partijen gekozen om een duidelijk beeld te krijgen van verschillende kanten. De experts worden gebruikt als "hoofd"-object om de risico's duidelijk te krijgen. Er wordt binnen advocatenkantoren gekeken hoe er wordt omgegaan met het gebruik van apps, in relatie tot het beroepsgeheim. Bij app-ontwikkelaars wordt gekeken in hoeverre zij bij het ontwikkelen van apps daar rekening mee houden. Dit is nodig omdat het onderzoek op deze manier van meerdere kanten wordt belicht zodat uiteindelijk de conclusie van het onderzoek op meerdere bronnen is gebaseerd.

Actuele theorieën: Het gebruiken van apps kan nodige risico's met zich meebrengen. Advocaten hebben zich te houden aan het beroepsgeheim en door deze nieuwe ontwikkelingen is het moeilijk voor advocaten om in te schatten of ze hun beroepsgeheim schenden. Tevens wordt de scheidingslijn tussen het gebruik van apps en het beroepsgeheim vager. Het is op dit moment onduidelijk welke risico's en problemen er spelen met betrekking tot het gebruik van apps en de relatie tot het beroepsgeheim.

Afbakening onderzoek: het onderzoek is afgebakend binnen één beroepsgroep, namelijk de advocatuur. Hiervoor is gekozen omdat het lastig wordt om alle beroepsgroepen met beroepsgeheim te interviewen. Daarnaast is er binnen Aecius ook makkelijk contact te krijgen met advocatenkantoren en experts. Ook worden er interviews gehouden met app-ontwikkelaars, deze onderzoeksobjecten worden gebruikt om alle kanten van het verhaal duidelijk te krijgen.

Onderzoeksmodel

In onderstaande afbeelding staat een schematische weergave van het onderzoeksmodel. In bijlage 22 van dit onderzoek staat de uitgebreide vorm van het onderzoeksmodel.



Afbeelding 1.

Uitleg onderzoeksmodel:

Het onderzoek begint bovenaan bij het onderzoekskader en interventiecycclus. Vanuit daar vloeit de doelstelling voort die uit twee delen is opgebouwd. Deel A is de omschrijving van het doel en deel B is hoe het deel A bereikt gaat worden. De centrale onderzoeksvraag vloeit voort uit het B gedeelte en als laatste zal ook de conclusie moeten aansluiten op de centrale onderzoeksvraag. De onderzoeksvraag wordt beantwoord door drie soorten deelvragen: theoretisch, empirisch en analytisch. De theoretische deelvragen worden beantwoord door middel van bronnen (zie afbeelding 1.). De empirische deelvragen worden beantwoord door middel van de onderzoekobjecten, namelijk interviews. De analytische deelvragen zijn een combinatie van de resultaten van de theoretische en empirische deelvragen. Op basis van deze resultaten wordt een analyse gemaakt die een heldere weergave geeft van alle onderzoeksresultaten. Vanuit de analyse vloeit de conclusie voort welke de centrale onderzoeksvraag moet beantwoorden. Vanuit de conclusie kunnen ook de aanbevelingen worden geschreven die een antwoord geven op de doelstelling van het onderzoek. Als dit allemaal is gedaan dan is de cirkel rond. Het begint namelijk bij een doelstelling en een centrale onderzoeksvraag die worden beantwoord door de conclusie en de aanbevelingen aan het einde van het onderzoek.

Uitleg lezer en introductie hoofdstukken

Het onderzoeksrapport is opgebouwd uit verschillende componenten. Het eerste gedeelte bestaat uit het voorblad, titelpagina, samenvatting en voorwoord. Het tweede gedeelte zijn de eerste vier hoofdstukken. En het derde gedeelte is het laatste hoofdstuk. In hoofdstuk 1. De inleiding, wordt een inleiding gegeven op het onderzoeksrapport. In dit hoofdstuk wordt de basis gelegd voor het onderzoek. Er is bepaald hoe het onderzoek verricht wordt, het onderwerp is afgekaderd, de onderzoeksobjecten bepaald en doelstelling en hoofd- en deelvragen geformuleerd. In hoofdstuk 2. wordt de methodologische verantwoording beschreven. In dit hoofdstuk wordt een gemotiveerde toelichting gegeven op de gemaakte keuzes voor de gebruikte onderzoeksmethoden.

In hoofdstuk 3, het theoretische hoofdstuk van het onderzoek, wordt het onderzoek onderbouwd doormiddel van de theoretische bronnen. De deelvragen uit het theoretische gedeelte worden hier uitgewerkt. Hoofdstuk 3 maakt automatisch een koppeling met hoofdstuk 4. Het empirische gedeelte van het onderzoek. In dit hoofdstuk worden de gegevens en resultaten uit het praktijkonderzoek besproken. De verkregen resultaten worden vervolgens geanalyseerd en gekoppeld met de informatie uit het theoretische gedeelte van het onderzoek. De analyse leidt vervolgens tot een heldere weergave van de onderzoeksresultaten.

Tot slot komt het derde gedeelte met het laatste hoofdstuk, hoofdstuk 5. In hoofdstuk 5. Zijn de conclusies en aanbevelingen naar de organisatie terug te lezen. De conclusie heeft betrekking op de resultaten uit het onderzoek. De aanbevelingen vloeien vervolgens logischerwijs uit de conclusie voort. De conclusie beantwoord uiteindelijk de centrale onderzoeksvraag en de aanbevelingen geven antwoord op de doelomschrijving van het onderzoek. Na hoofdstuk 5 is het onderzoeksrapport aangevuld met een lijst van afkortingen en begrippen, literatuur- en jurisprudentielijst en bijlagen.

Hoofdstuk 2. Methodologische verantwoording

Binnen dit hoofdstuk wordt in drie delen de methodologische verantwoording besproken. Onder 2.1 Onderzoeksmethoden wordt de onderzoeksbenadering en de onderzoeksmethoden toegelicht. Binnen de onderzoeksmethoden wordt gemotiveerd wat de theoretische en empirische bronnen zijn. Onder 2.2 Onderzoeksubjecten wordt er uitgelegd waarom er is gekozen voor meerdere onderzoeksubjecten. Onder 2.3 Analyse gegevens wordt er uitgelegd hoe de verkregen informatie geanalyseerd wordt en wat het uiteindelijke doel van de analyse is.

2.1 Onderzoeksmethoden

Onderzoeksbenadering: Er zijn verschillende soorten onderzoeksbenaderingen namelijk: deductief onderzoek of inductief onderzoek. Bij een deductief onderzoek wordt de theorie getoetst en bij een inductief onderzoek wordt een theorie opgesteld. Creswell (1994) noemt praktische criteria om het verschil tussen inductief en deductief onderzoek uit te drukken. Op basis hiervan wordt er binnen dit onderzoek gebruik gemaakt van de inductieve methode. Creswell (1994) stelt dat “een onderwerp waar een grote hoeveelheid literatuur over bestaat, van waaruit je een theoretisch kader en een hypothese kunt definiëren, zich makkelijker leent voor deductie. Bij onderzoek over een onderwerp dat nieuw is, dat veel discussie losmaakt en waarover nog weinig literatuur bestaat, is het waarschijnlijk beter om inductief te werken door gegevens te genereren en de analyseren, en na te denken over de vraag welke theoretische ideeën deze gegevens suggereren.”¹¹ Bij een inductieve methode wordt voor het verzamelen van gegevens vaak de kwalitatieve methode (interviews gebruikt). Het onderwerp van dit onderzoek is nieuw en er bestaat nog weinig literatuur over. Daarnaast maakt het onderwerp veel discussie los zie: “eerdere onderzoeken met betrekking tot dit onderzoek”. Desondanks de inductieve benadering is het onderzoek niet compleet inductief er zijn ook overeenkomsten met de deductieve methode. Er is sprake van een hypothese, namelijk of het onduidelijk is of de advocatuur bewust is van de risico's van het gebruik van apps. Mijns inziens denk ik dat de advocatuur hier niet van op de hoogte is, aangezien nog niet duidelijk in de media naar voren is gekomen dat advocaten geen smartphones etc. meer mogen gebruiken, omdat dit een eventueel risico zou kunnen opleveren. Tijdens dit onderzoek wordt deze hypothese door middel van de onderzoeksmethoden getoetst en daarmee bevestigd of ontkracht.

Onderzoeksmethoden: om de uiteindelijke doelstelling beantwoord te krijgen moet er gebruik worden gemaakt van onderzoeksmethoden. De onderzoeksmethoden kunnen bestaan uit een kwalitatieve onderzoeksmethode en de kwantitatieve onderzoeksmethode. De kwalitatieve onderzoeksmethode is een onderzoeksmethode waarbij meer diepgaande informatie verkregen wordt. Het houden van bijvoorbeeld een interview valt onder de kwalitatieve onderzoeksmethode. Bij een kwantitatieve onderzoeksmethode wordt er vaak gebruik gemaakt van grote hoeveelheden verkregen informatie waarbij de resultaten in een cijfermatig overzicht worden geplaatst, bijvoorbeeld het houden van een enquête.

Naast deze methoden zijn er ook meerdere methoden namelijk: deskresearch, inhoudsanalyse en observatie.

Binnen dit onderzoek wordt er gebruik gemaakt van de volgende onderzoeksmethoden:

Deskresearch: om een basis te kunnen leggen in het theoretische gedeelte van het onderzoek wordt deskresearch toegepast. Dit betekent het doen van (niet-)literatuuronderzoek. Binnen dit onderzoek wordt er gebruik gemaakt van theoretische bronnen namelijk: literatuur, niet-literatuur, internetbronnen/tijdschriften en rapporten. Er is gekozen voor deze theoretische bronnen omdat,

¹¹ M. Saunders, P. Lewis en A. Thornhill, *Methoden en technieken van onderzoek*, Amsterdam: Pearson Education Benelux 2008, p. 31 en 35

via deze bronnen de meest relevante informatie kan worden verkregen. Vooral internetbronnen en vakbladen zijn voor dit onderzoek relevant. Er is namelijk meer op internet en in vakbladen informatie te vinden over apps en de problemen en risico's daarvan dan in literatuur, omdat het nog een jong onderwerp is waar nog niet veel in de literatuur over is geschreven.

Interviews: naast deskresearch wordt er ook informatie verkregen door middel van de interviews. Interviews vallen onder de kwalitatieve onderzoeksmethode zoals hierboven staat beschreven en worden gevoerd met de onderzoeksobjecten. De reden waarom er gebruik wordt gemaakt van interviews binnen dit onderzoek is omdat via interviews dieper op informatie in kan worden gegaan dan bij enquêtes en er kan worden doorgevraagd op verkregen informatie. De informatie die uit de interviews wordt verzameld zijn de empirische bronnen binnen het onderzoek. Er wordt namelijk op een praktijkgerichte manier informatie verkregen. Daarnaast is observeren of een laboratoriumonderzoek verrichten niet toepasbaar op dit onderzoek. Het houden van interviews als empirische bron is daarom binnen dit onderzoek de meest logische manier om informatie te verzamelen.

2.2 Onderzoeksobjecten

De onderzoeksobjecten binnen dit onderzoek zijn de experts op privacy en ICT – Recht gebied, medewerkers binnen de advocatuur en app-ontwikkelaars. De experts gelden als “hoofd” – object. De advocatenkantoren en app-ontwikkelaars worden gebruikt om het beleid en gebruik van apps duidelijk te krijgen in de praktijk. De keuze om voor meerdere onderzoeksobjecten te kiezen is om zo een beter beeld te krijgen van de situatie. De resultaten worden namelijk vanuit meerdere kanten bekeken.

Bovenstaand de experts die een weergave kunnen geven van de risico's en eventuele privacyproblemen van apps. De resultaten die uit deze interviews voortvloeien gelden als inhoudelijke resultaten. Deze resultaten worden gebruikt voor de analyse met de resultaten uit het literatuuronderzoek. Onder de experts komen de advocatenkantoren en app-ontwikkelaars. Met deze onderzoeksobjecten wordt de huidige situatie omtrent het gebruikt, kennis en bewustzijn van de risico's van apps vastgesteld.

Binnen dit onderzoek worden meerdere onderzoeksobjecten gebruikt. Het risico van het kiezen voor één onderzoeksobject is dat er bij de resultaten maar een enkele kant belicht wordt in plaats van meerdere kanten. De resultaten zouden dan als niet-objectief kunnen worden aangemerkt. De resultaten vanuit de interviews met experts worden aangevuld met de resultaten uit de interviews met advocatenkantoren en app-ontwikkelaars. De resultaten uit het laatste worden gebruikt om de huidige situatie vast te stellen en te bevestigen.

2.3 Analyse gegevens

Het doel van de analyse is dat het tot een heldere weergave van de onderzoeksresultaten moet geven. De resultaten van het deskresearch en de resultaten die vanuit de onderzoeksobjecten zijn verkregen worden eerst apart beschreven. De resultaten uit het theoretische gedeelte: deskresearch worden beschreven in hoofdstuk 3. De resultaten uit het empirische gedeelte: interviews, waar informatie vanuit de onderzoeksobjecten wordt verkregen, worden beschreven in hoofdstuk 4. Daarnaast vindt er een onderlinge vergelijking van resultaten plaats die vanuit de onderzoeksobjecten komt, omdat er gebruik wordt gemaakt van meerdere onderzoeksobjecten en dus meerdere resultaten. Vervolgens worden deze gegevens geanalyseerd waarbij de resultaten uit het theoretische gedeelte erbij worden betrokken.

De gegevens worden op deze manier geanalyseerd omdat gebruik wordt gemaakt van verschillende bronnen, namelijk theoretische en empirische bronnen. Binnen de empirische bronnen wordt er vervolgens informatie verzameld vanuit meerdere onderzoeksobjecten. Elk van deze bronnen hebben eigen resultaten. De resultaten zullen daarom eerst moeten worden vergeleken, wil er daarna een analyse worden uitgevoerd. Wanneer de analyse wordt uitgevoerd, worden ook de resultaten uit het theoretische gedeelte erbij betrokken.

3.1 Deelvraag 1.

Welke wet- en regelgeving en jurisprudentie spelen een rol bij de voorwaarden van apps?

Terminologie

Het doel van deze deelvraag is om uitleg te geven over de toepasbare wet- en regelgeving wat betreft de voorwaarden bij de overeenkomst tussen een app en een consument. Op dit moment bestaat er verwarring of de voorwaarden die apps hanteren algemene voorwaarden, gebruiksvoorwaarden of servicevoorwaarden zijn. De terminologie die apps gebruiken op websites en bij installatie is niet eenduidig. Het is namelijk onduidelijk of de specifieke app-machtigingen, bij installatie, gedefinieerd kunnen worden als gebruiksvoorwaarden of algemene voorwaarden. Hetzelfde geldt voor de termen: servicevoorwaarden, algemene gebruiksvoorwaarden, leveringsvoorwaarden etc. Deze verwarring zorgt ervoor dat gebruikers niet weten of bijvoorbeeld servicevoorwaarden hetzelfde zijn als algemene voorwaarden en daardoor juridisch hetzelfde kunnen worden gekwalificeerd.

Algemene voorwaarden zijn voorwaarden die bij meerdere overeenkomsten worden gebruikt. De bedingen die in algemene voorwaarden zijn opgenomen mogen niet de kern van de prestatie aangeven¹². Gebruiksvoorwaarden zijn algemene voorwaarden die toegespitst zijn op het gebruik van een dienst of product.

Wanneer een gebruiker een app downloadt uit een platform (App Store of Google Play Store) is er in eerste instantie een overeenkomst tussen de gebruiker en het platform. Wanneer de gebruiker een app downloadt en installeert vanuit het platform is er tevens een overeenkomst tussen de gebruiker en de app. In dit onderzoek wordt de tweede verbintenis onderzocht, namelijk de overeenkomst tussen de gebruiker en de app. Als de gebruiker een app downloadt moet hij akkoord gaan met voorwaarden, zogeheten app-machtigingen, anders kan hij niet verder met installeren. Deze voorwaarden zijn op alle gebruikers van toepassing wanneer deze de app installeren. Daarnaast verklaart de app bij het downloaden dat de 'terms of service', 'algemene voorwaarden' of 'gebruiksvoorwaarden' van toepassing zijn op de overeenkomst tussen de app en de gebruiker. Wat betreft de terminologie is hier het punt waar verwarring kan ontstaan. Het antwoord is ondanks dat de voorwaarden verschillende termen hebben, kunnen ze allemaal gekwalificeerd worden als algemene voorwaarden, omdat de voorwaarden van toepassing zijn op elke overeenkomst tussen de gebruiker en de specifieke app. Daarnaast zijn de (gebruiks- en installatie)voorwaarden voor alle gebruikers hetzelfde. Welke naam er aan de voorwaarden wordt gegeven, doet niet af aan het feit dat het algemene voorwaarden zijn, danwel een onderdeel daarvan. Gebruiksvoorwaarden zijn algemene voorwaarden welke zijn toegespitst op het gebruik van een app. Installatievoorwaarden zijn algemene voorwaarden welke zijn toegespitst op de installatie van een app. Dit blijkt uit het feit dat het standaardvoorwaarden zijn waarmee de gebruiker pas na het downloaden mee akkoord gaat en daarmee is voldaan aan artikel 231 boek 6 Burgerlijk Wetboek.

Wetgeving

Europees Recht

Platforms moeten zich aan de Europese wetgeving houden wanneer er apps worden aangeboden binnen de landen die deel uitmaken van de Europese Unie. In Europa is een vrij verkeer van informatie. Dit betekent dat alle informatie en gegevensstromen zich vrij kunnen bewegen van en naar de Europese lidstaten. De Europese en nationale wetgeving dient op dit vrije verkeer te zijn aangepast. De hieronder genoemde richtlijnen zijn van toepassing op de Telecom markt, een markt waar het aanbieden van apps en de apps zelf deel van uitmaken. Een richtlijn is een Europees bindende uitspraak waarvan iedere lidstaat zelf mag bepalen hoe deze in de nationale wetgeving

¹² artikel 6:231 sub a Burgerlijk Wetboek

wordt geïmplementeerd. Een lidstaat moet deze richtlijn uiteindelijk hebben geïmplementeerd binnen een bepaalde termijn.

De richtlijnen:

95/46/EG¹³ is een richtlijn die toepassing heeft op de bescherming van natuurlijke personen in verband met verwerking van persoonsgegevens en het vrije verkeer van die gegevens. Er wordt gestreefd naar een evenwicht tussen een hoog beschermingsniveau van de persoonlijke levenssfeer en het vrije verkeer van persoonsgegevens in de Europese Unie. Uit deze richtlijn is de Wet bescherming persoonsgegevens (Wbp) ontstaan in het Nederlands Recht. Deze richtlijn is op Europees niveau een referentiekader voor de bescherming van persoonsgegevens. Op dit moment wordt er door de Europese Commissie een nieuwe verordening ontworpen welke betrekking heeft op de Nederlandse Wbp. Deze richtlijn is regelgevend kader die bestaat uit een algemene verordening bescherming persoonsgegevens en een richtlijn die betrekking heeft op bescherming van persoonsgegevens die worden verwerkt van politie en justitiele activiteiten¹⁴.

Er zijn vijf richtlijnen die het bestaande regelgevingkader vormen voor de elektronische communicatienetwerken en –diensten in Europa:

2002/21/EG¹⁵ is de kaderrichtlijn inzake een gemeenschappelijk regelgevingkader voor elektronischecommatienetwerken en –diensten. Er is wetgeving uitgewerkt die aansluit op de technologische vooruitgang en de eisen binnen deze markt. De reden is om snelle veranderingen die plaatsvinden binnen deze markt bij te houden. Daarnaast is binnen dit kader een regelgevingkader ontworpen voor de elektronische communicatie. Het hoofddoel is mededingen te versterken door de toetreding van nieuwkomers te vergemakkelijken en investeringen in deze sector te bevorderen.

2002/19/EG¹⁶ is een toegangsrichtlijn tot interconnectie van elektronische communicatienetwerken en bijbehorende faciliteiten.

2002/20/EG¹⁷ is een machtigingsrichtlijn waarbij het noodzakelijk is dat tussen verschillende elektronische communicatienetwerken en –diensten en de daarbij gebruikte technieken een machtigingssysteem is waarin alle vergelijkbare diensten op vergelijkbare wijze worden behandeld. Deze richtlijn strekt tot het ontwerpen van een juridisch kader waarbij de vrijheid van elektronische communicatienetwerken en –diensten en de daarbij gebruikte technieken wordt gewaarborgd. Voor de aanbieders van elektronische communicatienetwerken moeten dezelfde transparante, objectieve en niet-discriminerende en evenredige rechten, voorwaarden en procedures gelden.

2002/22/EG¹⁸ is de universele richtlijn voor diensten. Deze richtlijn moet de levering van alle diensten garanderen. Deze richtlijn moet bij blijven met de veranderingen op het gebied van technologische vooruitgang, de marktontwikkelingen en de behoeften van de gebruiker.

Richtlijn privacy en elektronische communicatie: **2002/58/EG**¹⁹ is een richtlijn wat de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie betreft. Binnen de ICT en met name het internet en maildiensten worden er specifieke voorschriften geleverd om de bescherming van persoonlijke levenssfeer te waarborgen. Deze regelgeving is bedoeld om gebruikers een vertrouwd gevoel te geven wanneer zij gebruik maken van elektronische diensten en technologieën. Onder deze richtlijn vervalt het verbod op spam, het stelsel van voorafgaande toestemming van de gebruiker (opt-in) en regeling inzake de installatie van cookies.

¹³ www.eur-lex.europa.eu (zoek op: *samenvatting 95/46/EG*)

¹⁴ Voorstel voor een verordening betreffende de bescherming van individuen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, versie behandelfase Eerste Kamer januari 2014

¹⁵ www.eur-lex.europa.eu (zoek op: *samenvatting 2002/21/EG*)

¹⁶ www.eur-lex.europa.eu (zoek op: *richtlijn 2002/19/EG*)

¹⁷ www.eur-lex.europa.eu (zoek op: *richtlijn 2002/20/EG*)

¹⁸ www.eur-lex.europa.eu (zoek op: *richtlijn 2002/22/EG*)

¹⁹ www.eur-lex.europa.eu (zoek op: *samenvatting 2002/58/EG*)

Het aanschaffen van een app via een website of platform gebeurt online. Om deze elektronische handel zo goed mogelijk te reguleren is de richtlijn **2000/31/EG**²⁰ in werking getreden. Hierin staan de juridische aspecten van de elektronische handel. De aanpassingswet inzake elektronische handel voorziet in een implementatie van deze richtlijn in de Nederlandse wetgeving. De richtlijn heeft betrekking op alle diensten van de informatiemaatschappij. Er bestaat nog onduidelijkheid of de gebruiker bij het aanschaffen van een app een product of dienst aanschaft. Deze vraag zal worden beantwoord op de volgende pagina.

Nederlands Recht

Binnen het Nederlands recht zijn er een aantal soorten wet- en regelgeving die een rol spelen bij installatie- en gebruiksvoorwaarden van apps. Wanneer een platform een app aanbiedt en de gebruiker deze app downloadt en installeert, is er sprake van aanbod en aanvaarding hierdoor komt een overeenkomst tot stand²¹. De meeste apps van bedrijven zoals Facebook en Twitter zijn internationaal gevestigd. Het is lastig om te bepalen welk recht van toepassing is. Het Nederlands recht bepaalt dat wanneer de wederpartij, een consument, in Nederland woont afdeling 6.5.3 van het Burgerlijk Wetboek aangaande de algemene voorwaarden van toepassing is²². In subvraag c wordt afdeling 6.5.3 Burgerlijk Wetboek getoetst aan de installatievoorwaarden.

Op veel overeenkomsten zijn algemene voorwaarden van toepassing, zo ook tussen de app en de gebruiker. Voor de algemene voorwaarden geldt in eerste instantie contractsvrijheid, de inhoud mag door de opstellende partij zelf worden ingevuld. Desondanks heeft een partij zich wel te houden aan wettelijke regels. Zo mogen de algemene voorwaarden niet onredelijk bezwarend zijn²³ en moet de gebruiker een redelijke mogelijkheid hebben om van de algemene voorwaarden kennis te nemen²⁴. In dit geval is de overeenkomst tussen de consument en de app een elektronische overeenkomst, omdat het via de elektronische weg geschiedt. De app moet de algemene voorwaarden voor of bij het sluiten van de overeenkomst ter beschikking stellen aan de gebruiker. De gebruiker moet de mogelijkheid hebben om de voorwaarden op te slaan ten behoeve van latere kennisneming. Wanneer dit niet mogelijk is moet de app de gebruiker laten weten waar de voorwaarden zijn te vinden of dat de app, de gebruiker de voorwaarden opstuurt²⁵.

Naast de wetgeving over de algemene voorwaarden is ook de Wet bescherming persoonsgegevens (Wbp) van toepassing. Deze wetgeving is een implementatie uit de Europese richtlijn: 95/46/EG. De wet is van toepassing op de geheel of gedeeltelijke geautomatiseerde verwerking van persoonsgegevens, alsmede de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen²⁶. Een app is software die persoonsgegevens verkrijgt en deze gegevens volledig geautomatiseerd verwerkt. Wanneer een gebruiker de gebruiksvoorwaarden accepteert en de app gaat gebruiken moet de app zo zorgvuldig mogelijk de verkregen persoonsgegevens verwerken. Daarnaast vraagt een app bij installatie vaak om een aantal machtigingen om toegang te krijgen tot andere functies op het toestel. De app heeft daardoor toegang tot persoonlijke gegevens waar de app zorgvuldig mee moet omgaan. Wanneer dit niet gebeurd is, is het in strijd met de Nederlandse Wbp. Vanwege de snelle technologische ontwikkelingen is er een nieuw wetvoorstel ingediend bij de Tweede Kamer inzake “meldplicht datalekken”. Deze meldplicht wordt toegevoegd in de Wbp. Het Cbp krijgt de bevoegdheid om bestuurlijke boetes op te leggen wanneer bij bedrijven een inbreuk wordt gemaakt op de beveiligingsvoorschriften voor persoonsgegevens. Bedrijven hebben een meldplicht wanneer er een datalek wordt geconstateerd, wanneer zij dit niet doen kunnen ze een boete opgelegd krijgen van het Cbp²⁷.

²⁰ www.europa.eu (zoek op: *samenvatting 2000/31/EG*)

²¹ artikel 6:217 Burgerlijk Wetboek

²² artikel 6:247 lid 4 Burgerlijk Wetboek

²³ artikel 6:236 jo 237 Burgerlijk Wetboek

²⁴ artikel 6:234 Burgerlijk Wetboek

²⁵ artikel 6:234 lid 1 sub c Burgerlijk Wetboek

²⁶ artikel 2 lid 1 Wet bescherming persoonsgegevens

²⁷ Wijziging Wet bescherming persoonsgegevens (meldplicht datalekken), *Kamerstukken II 2013/14*, 33 662

Naast de Wbp is ook het ICT – Recht van toepassing dit is het alomvattende recht omtrent de juridische aspecten binnen de ICT zoals elektronische overeenkomsten en bescherming van elektronische informatie. De Telecommunicatiewet is van toepassing aanbieders van (openbare) elektronische communicatienetwerken en diensten²⁸. De eigenaren van elektronische communicatienetwerken (bijvoorbeeld KPN) dienen zorg te dragen voor de bescherming van persoonsgegevens van de gebruikers van het netwerk²⁹. Dit geldt ook voor de aanbieders van elektronische communicatie diensten zoals Telfort of Hi³⁰. Dit zijn internet en mobiele telefoonproviders die hun eigen diensten aanbieden en gebruik maken van het netwerk van KPN. Nu is het alleen nog de vraag of een app kan worden aangemerkt als een product of dienst. Een app is software. Software is in eerste instantie niet tastbaar en kan daardoor eerder aangemerkt worden als een dienst dan een product.

Het verschil zit hem in eerste instantie in het ‘stoffelijke’: een product/goed kan men aanraken een dienst niet. Toch kan software worden uitgeschreven in codes waardoor het wel tastbaar wordt. Tevens kan software op een CD worden gezet waardoor het geheel als product kan worden aangemerkt. Er zijn ontzettend veel discussies of de software zelf een product of dienst is. In het Elektriciteitsarrest (HR 23 mei 1921) werd elektriciteit aangemerkt als ‘eenig goed’, hierdoor kon de voor diefstal verdachte tandarts voor diefstal van elektriciteit worden veroordeeld³¹. Hier werd elektriciteit als goed aangemerkt ondanks dat elektriciteit niet stoffelijk is. De Hoge Raad heeft in een ander arrest bepaald dat het wegnemen van belminuten en sms’jes van een ander, beoordeeld kan worden als diefstal. De belminuten en sms’jes zijn economisch van aard en zijn daarom juridisch gezien een goed dat wederrechtelijk is verkregen³². Civielrechtelijk gezien kan dit toch anders worden beoordeeld. Gezien de aard van een app is men geneigd te denken dat een app gedefinieerd kan worden als dienst. Een app wordt namelijk niet aangeschaft via een materiële drager zoals een CD of USB. De apps wordt aangeschaft over het internet en wanneer het geïnstalleerd is staat het op een materiële drager zoals een tablet of smartphone. Daarnaast is de aard van de apps diensten zoals Facebook, Twitter, Dropbox en Whatsapp zijn internetdiensten omdat, zij via het internet een dienst aanbieden waar consumenten gebruik van kunnen maken en zelf kunnen personaliseren. Daarnaast definiëren deze bedrijven hun aanbod als ‘dienst’: de consument koopt een app niet, maar verkrijgt alleen het gebruiksrecht/licentie op een app. Er is hierdoor geen sprake van een eigendomsoverdracht van de aanbieder naar de gebruiker op de app. Samenvattend kan een app gedefinieerd worden als een dienst. Hierdoor is de dienst van de informatiemaatschappij van toepassing. Deze wet is van toepassing op degene die een dienst van de informatiemaatschappij verleent³³. In dit geval is dat het platform degene die een dienst verleent. Zij verlenen een dienst (aanbieden van de app), tegen vergoeding (in casu niet altijd, er zijn ook gratis apps), langs elektronische weg (via internet), op afstand (wereldwijd) en op individueel verzoek van de afnemer (de gebruiker verzoekt zelf met zijn account de app aan te schaffen).

Regelgeving

Dit onderzoek is toegespitst op het beroepsgeheim van advocaten. In de wet is het schenden van ambts-/beroepsgeheim strafbaar gesteld³⁴. Voor beroepsgroepen met beroepsgeheim zijn regels met betrekking tot geheimhoudingsplicht vastgesteld. Voor advocaten is deze regelgeving opgenomen in de Gedragscode Centrale Controle Verordeningen van de Nederlandse Orde van Advocaten en lokale Orden van Advocaten³⁵. Wat het beroepsgeheim voor advocaten verder inhoudt wordt uitgelegd in deelvraag 3.3. Naast regelgeving wat betreft het beroepsgeheim heeft de Rijksoverheid het Nationaal Cyber Security Center (hierna: NCSC) opgericht. Deze heeft als doel het gezamenlijk vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale

²⁸ artikel 1.1 sub e jo. f Telecommunicatiewet

²⁹ artikel 11.2 Telecommunicatiewet

³⁰ www.kpn.nl (zoek op: *Merken KPN*)

³¹ ‘Electriciteits-arrest’ 5 november 2013, www.recht.nl (zoek op: *Nieuws, Strafrecht, Electriciteits-arrest*)

³² LJN: BQ6575, HR 31-01-2013, www.rechtspraak.nl

³³ artikel 3:15d lid 1 Burgerlijk Wetboek

³⁴ artikel 272 Wetboek van Strafrecht

³⁵ D.J. Hesermans, *Advocatenwet*, Deventer: Kluwer 2009

domein³⁶. NCSC stelt onder andere ook beveiligingsrichtlijnen voor mobiele apparaten en ICT – beveiligingsrichtlijnen voor webapplicaties. Hoofdstuk 5 van de beveiligingsrichtlijn voor mobiele apparaten is toegespitst op applicaties³⁷. In dit hoofdstuk zijn 14 richtlijnen opgenomen voor het gebruik van applicaties op smartphones. De opgestelde richtlijnen van NCSC zijn niet wettelijk verplicht maar zijn adviserend van aard. Deze richtlijnen gelden overigens voor de gebruikers van apps en degenen die bij organisaties en de Rijksoverheid betrokken zijn bij de beveiliging van mobiele apparaten.

Jurisprudentie

In Nederland is er geen jurisprudentie te vinden die te maken heeft met het schenden van privacy door middel van apps op smartphones. Onder het kopje ‘Nederlands Recht’ is het Elektriciteitsarrest en het belminuten en smsjes – arrest toegelicht. Wat betreft het schenden van privacy door middel van apps is jurisprudentie wereldwijd te vinden over privacyschending in de telecomunicatiesector. In deelvraag 3 worden drie arresten toegelicht betreffende het schenden van het beroepsgeheim.

- In USA betaalde Facebook 10 miljoen dollar in een zaak rond het schenden van privacy voor reclamadoeleinden aldus webwereld.nl. De rechtszaak is aangespannen door vijf gebruikers van Facebook omdat hun “vind-ik-leuks” aan bedrijven werden gekoppeld aan de producten en aangeboden aan andere Facebook vrienden. Voor deze medewerking werd vooraf geen toestemming gevraagd.³⁸
- Google en Microsoft klagen de Amerikaanse overheid aan om meer informatie te mogen vrijgeven over het aantal verzoeken om gebruikersgegevens dat de Amerikaanse overheid doet bij Google. Google en Microsoft willen meer transparantie in de informatievergaring. De Amerikaanse overheid wil niet dat bekend wordt hoe vaak zij verzoeken indienen bij Google.³⁹ Volgens een artikel op zdnet.nl werd Google beschuldigd van illegaal datamining, Google’s advocaten stelden tijdens de rechtszaak dat gebruikers ‘geen legitieme verwachting van privacy hebben’. Via de gebruiksvoorwaarden hebben de gebruikers van Gmail ingestemd met het feit dat e-mails worden gescand voor het filteren van spam en het afleveren van gerichte advertenties.⁴⁰
- In maart 2012 werden 18 bedrijven aangeklaagd voor de rechter in Amerika over de App Privacy, het gaat onder andere om Apple, Twitter en Facebook. Apps van deze bedrijven verzamelden, uploaden en stalen bewust het adresboek van de gebruiker zonder dat de gebruiker werd geïnformeerd.⁴¹

Conclusie deelvraag 1:

In deze eerste deelvraag van het onderzoek is de relevante wet- en regelgeving en jurisprudentie besproken welke betrekking heeft op dit onderwerp. Het was in het begin onduidelijk of de installatievoorwaarden hetzelfde zijn als algemene voorwaarden. Deze vraag is in het begin van deze deelvraag opgehelderd; installatievoorwaarden zijn hetzelfde als algemene voorwaarden en kunnen daardoor als zijnde algemene voorwaarden juridisch worden gekwalificeerd. Op het gebied van Europese wetgeving zijn een aantal richtlijnen uitgelegd welke toepassing hebben op het elektronisch verwerken van persoonsgegevens dan wel alle diensten welke via internet worden aangeboden en verwerkt. Vooral de nieuwe verordening waar de Europese Commissie nog mee bezig is wordt gezien als belangrijke nieuwe regelgeving op het gebied van verwerken van

³⁶ ‘Organisatie’ www.ncsc.nl

³⁷ ‘Beveiligingsrichtlijnen voor mobiele apparaten’, 14 november 2012, www.ncsc.nl (zoek op: *beveiligingsrichtlijnen mobiele apparaten*)

³⁸ ‘Facebook betaald miljoenen voor privacy-misstap’ 18 juni 2012, www.webwereld.nl (zoek op: *rechtszaak Facebook*)

³⁹ ‘Microsoft en Google starten rechtszaken over dataverzoeken’ 31 augustus 2013, www.webwereld.nl (zoek op: *rechtszaak Google*)

⁴⁰ ‘Google: Gmail-gebruikers hoeven niet te rekenen op privacy’ 14 augustus 2013, www.zdnet.nl (zoek op: *rechtszaak Google*)

⁴¹ ‘18 Firms sued over App Privacy, Including Apple, Twitter, Facebook’ 15 maart 2012, www.pcmag.com (zoek op: *lawsuit app privacy*)

persoonsgegevens in de toekomst. Op het gebied van Nederlands recht is wetgeving betreffende algemene voorwaarden en Wbp van toepassing omdat de installatievoorwaarden welke apps presenteren na het downloaden moeten voldoen aan afdeling 6.5.3 Boek 6 Burgerlijk Wetboek. Installatievoorwaarden zijn immers algemene voorwaarden. De Wbp is van toepassing omdat apps (persoons)gegevens verwerken, de verwerking van deze gegevens dient conform de Wbp te gebeuren. De Telecommunicatiewet is van toepassing omdat het digitale gegevensverkeer over de elektronische communicatienetwerken gaat en hebben de providers de plicht om de persoonsgegevens welke over het netwerk gaan te beschermen. Een app is een dienst gezien de aard van de app en het feit dat het niet stoffelijk is. Tot slot is uitgelegd waarom de dienst van de informatiemaatschappij van toepassing is, deze wetgeving is van toepassing op het platform.

3.1.1 subvraag a.

Wat betekent het akkoord gaan met voorwaarden van een app? (In het bijzonder wordt er gekeken naar de meest voorkomende installatievoorwaarden van de app, welke de app toegang geeft tot andere apps in het toestel. Bijvoorbeeld email, foto's, camera, contactgegevens etc.)

Soorten apps

Binnen het onderzoek worden vijf apps aan het licht gesteld. De reden waarom er voor vijf apps is gekozen is omdat het onmogelijk is alle miljoenen apps die wereldwijd worden aangeboden te onderzoeken. De vijf apps zijn:

- Facebook: Facebook is een social netwerk site waar gebruikers een persoonlijk profiel hebben en interesses en gebeurtenissen delen met anderen. Gebruikers kunnen met hun profiel vrienden worden met andere gebruikers. In het tweede kwartaal van 2013 heeft Facebook op de smartphone wereldwijd 469 miljoen gebruikers per dag en 819 miljoen gebruikers per maand.⁴²
- Twitter: Twitter is een internetdienst waar gebruikers een profiel kunnen aanmaken en korte berichtjes met maximaal 140 tekens kunnen plaatsen. Twitter is te gebruiken op de PC of via een te downloaden app op de smartphone. In Nederland maken 3,3 miljoen gebruikers van Twitter.⁴³
- Whatsapp: Whatsapp is een gratis berichtendienst in een vorm van een app die te downloaden is op de smartphone. In augustus 2013 staat de teller op 300 miljoen gebruikers. Per dag worden er 31 miljard berichten gestuurd en 325 miljoen foto's.⁴⁴
- Dropbox: Dropbox is een cloud-dienst waar je van gebruik kan maken via je computer, laptop, smartphone en tablet. In de dropbox kun je bijvoorbeeld foto's, video's en documenten zetten waar je automatisch via de apparaten toegang tot hebt. Zo heeft de gebruiker overal en altijd zijn documenten en gegevens bij zich.⁴⁵ In juli 2013 had Dropbox 175 miljoen gebruikers⁴⁶.
- Dirkzwager KennisBoek app: Dirkzwager is een advocaten en notarissen kantoor in Nijmegen en Arnhem. Zij hebben een Dirkzwager kennis app⁴⁷ ontwikkeld waar allerlei juridische artikelen te lezen zijn over verschillende rechtsgebieden geschreven door de juristen van Dirkzwager. Op deze manier wil Dirkzwager actief haar kennis delen. Het is niet te herleiden hoeveel gebruikers er zijn van de Dirkzwager KennisBoek app.

Deze apps zijn te downloaden op twee soorten systemen namelijk, Apple apparaten met als besturingssysteem iOS, dit gaat via de App Store of iTunes Store en Samsung apparaten met als besturingssysteem Android dit gaat via de Google Play Store. In onderstaande worden alle vijf apps onderzocht op een iPhone 4S (iOS) en een Samsung SIII mini (Android). Op deze twee verschillende toestellen wordt gekeken of de gebruiker akkoord moet gaan met installatievoorwaarden.

⁴² 'Earnings Slides' Second Quarter 2013, 24 juli 2013, www.investor.fb.com

⁴³ "Social media in Nederland 2013: Groei van gebruik Twitter en Facebook afgevlakt" 18 februari 2013, www.marketingfacts.nl (zoek op: *Social Media in Nederland 2013*)

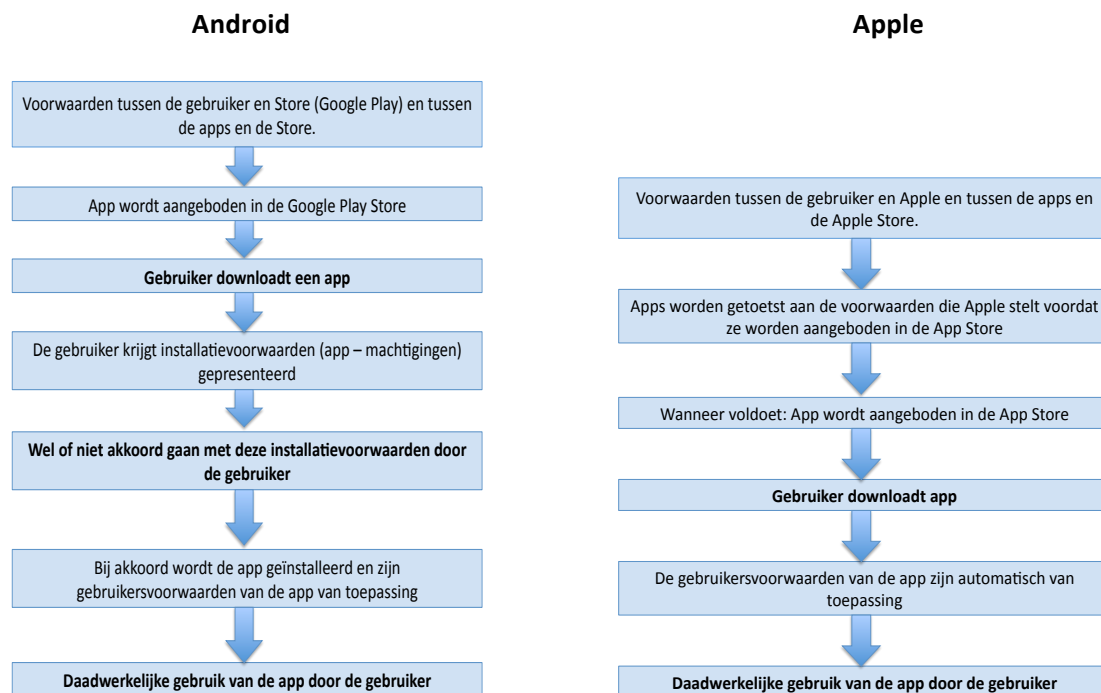
⁴⁴ 'Alle cijfers over het socialmediagebruik in Nederland medio 2013' 30 augustus 2013, www.marketingfacts.nl (zoek op: *Social Media gebruikers*)

⁴⁵ www.dropbox.com, 22 oktober 2013

⁴⁶ 'Dropbox now has 175 milion users, up from 100M in November 2012', 9 juli 2013, www.techcrunch.com (zoek op: *Users Dropbox*)

⁴⁷ www.kennisboek.nl, 22 oktober 2013

Voordat deze apps worden behandeld wordt er in de onderstaande afbeelding globaal uitgelegd hoe de structuur en de fases van de voorwaarden van apps vanaf de Store tot het daadwerkelijk gebruik eruit ziet. De linker afbeelding geeft de structuur weer van een gebruiker die Android software op zijn toestel heeft staan, de rechter afbeelding is de structuur van Apple Software.



Afbeelding 2.

Uit de afbeelding is te herleiden dat Android en Apple verschillende werkwijzen hanteren betreffende het aanbieden van apps vanuit de Stores en de voorwaarden bij het downloaden. In een artikel op computerwereld.nl⁴⁸ wordt uitgelegd wat de achterliggende gedachte is waarom Apple geen app-machtigingen communiceert bij de gebruiker. Apple controleert namelijk zelf alle apps die worden aangeboden in de AppStore op een aantal zaken, zoals: doet de app wat hij zegt te doen? En werkt deze naar behoren? (zie afbeelding 2.) Ook worden er beperkingen opgelegd door Apple in de functies van een app. Apple probeert over het algemeen de ontwikkelaars te van weerhouden dat zij volledige toegang krijgen tot het apparaat. Dit kan ermee te maken hebben dat Apple de privacy van haar gebruikers wil beschermen. De gebruiker kan zelf met iOS bepalen in de instellingen of een app toegang krijgt tot bijvoorbeeld contactenlijst, foto's of microfoon. Dit betekent dat een app bij voorbaat op een Apple toestel geen machtiging krijgt, maar dat de gebruiker toestemming moet geven. Bij Android wordt een app aangeboden in de Google Play Store, maar de gebruiker bepaalt zelf of hij akkoord wil gaan met de app-machtigingen in de installatievoorwaarden. Wanneer een app is gedownload uit een van de Stores zijn altijd de gebruiksvoorwaarden en het privacy beleid van de app van toepassing op overeenkomst tussen de app en de gebruiker.

In deze subvraag wordt er gekeken naar de installatievoorwaarden die de apps hanteren en wat het betekent voor de gebruiker wanneer hij ermee akkoord gaat. Apple hanteert zoals eerder beschreven geen installatievoorwaarden, dit betekent dat er alleen naar de installatievoorwaarden van Android wordt gekeken.

Facebook

De installatievoorwaarden van Android voordat de Facebook app geïnstalleerd kan worden staan in de blauwe balk. De app krijgt bij acceptatie van de machtigingen toegang tot bepaalde functies/programma's in het toestel. De gebruiker moet deze machtigingen accepteren anders kan

⁴⁸ 'Hoe veilig zijn smartphone apps?' 14 juli 2011, www.computerwereld.nl (zoek op: *app machtigingen*)

deze de app niet gebruiken.

In bijlage 1 van dit onderzoek staan deze app-machtigingen bij installatie en deze zijn genummerd van afbeelding 1 t/m 6. In onderstaande blauwe balk staat de opsomming van de app-machtigingen.

De Facebook app wil gemachtigd worden voor de volgende zaken: “actieve applicaties ophalen, camera, gebruikersinterface van andere applicaties, netwerkcommunicatie, batterijstatistieken wijzigen, telefoonoproepen, en sociale informatie.” (afbeelding 1.)

Dit zijn nogal een aantal machtigingen en binnen dit onderzoek worden niet alle machtigingen behandeld; gebruikersinterface, netwerkcommunicatie en batterijstatistieken worden erbuiten gelaten. De app heeft namelijk sommige functies nodig om te kunnen werken. De app wil actieve applicaties ophalen, dit betekent dat de app informatie kan ophalen over huidige en recent uitgevoerde taken (bijlage 1 afbeelding 2). Er staat niet over welke taken er informatie wordt opgehaald. Daarnaast mag de app, na akkoord, op elk gewenst moment foto's en video's maken met de camera (bijlage 1 afbeelding 3). Deze machtiging is zeer opvallend omdat het niet de intentie kan zijn van de gebruiker dat deze toestemming geeft aan de app om op elk moment foto's te gaan maken met de camera. Er wordt niet door de app in de machtiging vermeld wat er met de foto's en video's gebeurt, waar ze worden opgeslagen, de termijn, waar ze voor worden gebruikt etc. De app machtigt zichzelf om de telefoonfuncties van het apparaat te openen (bijlage 1 afbeelding 4). Dit betekent dat de app het telefoonnummer, serienummer, actieve oproepen (inclusief telefoonnummers) enzovoort kan ophalen. Daarnaast kan de app telefoonnummers bellen zonder tussenkomst van de gebruiker. De woorden “zonder tussenkomst van de gebruiker” baart zorgen. De app kan nummers gaan bellen zonder dat de gebruiker dit wil of überhaupt weet, de gebruiker wordt immers niet voorafgaand om toestemming gevraagd. Net als bij de camera kan het niet de intentie van de gebruiker zijn dat hij toestemming geeft aan de app om elk moment nummers te gaan bellen en daarbij de kosten voor de gebruiker maken. De app kan er achter komen met wie de gebruiker aan het bellen is en wat het telefoonnummer is van die persoon. Volgens de Nederlandse Wbp mag alleen informatie worden verzameld die overeenstemt met de gerechtvaardigde doeleinden⁴⁹. Er kunnen tevens vraagtekens worden geplaatst bij de machtiging dat de app toegang heeft om de contactgegevens te kunnen lezen (bijlage 1, afbeelding 5). Dit betekent dat de contactgegevens automatisch worden verwerkt, een app kan niet tegelijkertijd miljoenen contactgegevens gaan lezen. Het zal eerst moeten worden verwerkt alvorens het gelezen kan worden. Facebook is een platform waar veel persoonsgegevens actief door de gebruiker wordt gedeeld. Alle bovenstaande machtigingen kunnen getoetst worden aan artikel 9 lid 1 en lid 2 en artikel 11 Wbp. Er kan getoetst worden of de verwerking van alle informatie door de app onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. Gezien de hoeveelheid informatie die Facebook via de achterkant van de app wil verzamelen kan men zich afvragen waarom er geen ondubbelzinnige toestemming wordt gevraagd⁵⁰. De gebruiker kan zonder te lezen de installatievoorwaarden accepteren en wordt later geen toestemming gevraagd wanneer de gegevens daadwerkelijk worden verwerkt. Het lijkt gezien de voorwaarden hierboven er niet op dat Facebook rekening houdt met de gevolgen van de verwerking voor de gebruiker, de wijze waarop de gegevens zijn verkregen, de aard van de gegevens en de bewaartermijn. Wanneer de installatievoorwaarden van Facebook aan de Wbp wordt getoetst kan er gesteld worden dat de hoeveelheid gegevens die de app verwerkt niet noodzakelijk⁵¹ is voor de werking van de app.

Twitter

Wanneer een gebruiker met een Android toestel Twitter wil installeren moet hij akkoord gaan met een aantal voorwaarden. Het aantal installatievoorwaarden bij Twitter liggen lager dan bij Facebook. De afbeeldingen van Twitter zijn opgenomen in bijlage 2. en genummerd van

⁴⁹ artikel 7 Wet bescherming persoonsgegevens

⁵⁰ art. 8 sub a Wet bescherming persoonsgegevens

⁵¹ artikel 8 Wet bescherming persoonsgegevens

afbeelding 7 t/m 10. Twitter heeft tot de volgende zaken toegang nodig:

Twitter heeft toegang nodig tot: "Contactgegevens lezen, volledige internettoegang, inhoud van USB-opslag wijzigingen of verwijderen, gedetailleerde (GPS) locatie, accounts toevoegen of verwijderen en uw profielgegevens lezen." (afbeelding 7.)

Er wordt alleen ingegaan op contactgegevens lezen, gedetailleerde (GPS) locatie en profielgegevens lezen. Net als bij de Facebook app wil deze app toegang tot het adresboek van de gebruiker op het apparaat om de contactgegevens te lezen (bijlage 2 afbeelding 8). Twitter vermeldt niet wat er met de contactgegevens gebeurt en waarom zij het willen lezen. Bij de Facebook app is beschreven waarom het lezen van contactgegevens in strijd kan zijn met het Nederlandse privacy recht. De app wil toegang tot de gedetailleerde GPS locatie van de gebruiker (bijlage 2 afbeelding 9). De app kan hierdoor de precieze locatie van de gebruiker traceren of netwerkbronnen zoals zendmasten en wifi. De GPS werkt alleen wanneer de gebruiker dit aanzet op het toestel. De app motiveert niet waarom zij de gedetailleerde locatie willen hebben en waarvoor ze deze willen gebruiken. Het is overigens logisch dat de app wil weten waar de telefoon zich bevindt om verbinding te maken met zendmasten of wifi, zodat de dienst werkt. Twitter is een internetdienst en kan alleen functioneren met een internetverbinding. Net als bij Facebook kan er getoetst worden volgens artikel 8 b Wbp of het noodzakelijk is dat de GPS locatie moet worden gebruikt voor de uitvoering van de app. Een nauwkeurige GPS locatie kan namelijk leiden tot een persoon en is daarmee een persoonsgegeven conform artikel 1 a Wbp. Tot slot kan de app persoonlijke profielgegevens lezen die op het apparaat zijn opgeslagen (bijlage 2, afbeelding 10). Hiermee bedoelt de app gegevens zoals naam en contactgegevens uit het toestel. Deze gegevens zijn volgens artikel 1a Wbp, net als GPS locatie, persoonsgegevens aangezien deze leiden tot een identiteit van een persoon⁵². De verwerking van deze gegevens dienen op een zorgvuldige manier te worden behandeld conform artikel 6 Wbp. De app vermeldt dat zij de gegevens gebruiken om de gebruiker te identificeren en om profielgegevens naar anderen kan verzenden. Wat er met "anderen" wordt bedoeld wordt niet verteld en wat deze "anderen" vervolgens met de gegevens van gebruikers doen is niet bekend.

Whatsapp

Whatsapp heeft bij installatie machtiging tot veel gegevens op het toestel. De machtigingen staan in de blauwe balk op de volgende pagina vermeld en in bijlage 3 afbeelding 11 t/m 15 staan de afbeeldingen.

Whatsapp heeft de machtiging om: "directe telefoonnummers bellen, SMS verzenden en ontvangen, audio opnemen, GPS locatie, contactgegevens lezen en opslaan, profielgegevens lezen, inhoud van USB-opslag wijzigingen of opslaan, accountsgegevens toevoegen of verwijderen, facturering, actieve applicaties ophalen, slaapstand van toestel voorkomen en synchronisatie instellingen lezen." (afbeelding 11/12/13.)

In het stuk over Facebook en Twitter is al behandeld wat het inhoudt wanneer de app een machtiging wil voor het adresboek, GPS locaties en telefoonnummers rechtstreeks bellen. Whatsapp heeft naast deze machtigingen ook 'Audio Opnemen'. "De app mag een pad (bestand) voor geluidsopname openen." Er staat niet dat dit ook met tussenkomst van de gebruiker moet gebeuren of dat de app zomaar geluidsfragmenten kan gaan opnemen. De app heeft de functie 'Audio opnemen' omdat gebruikers geluidsfragmenten naar elkaar kunnen sturen in een chat. Wanneer de app alleen audio opneemt als de gebruiker de app hiervoor toestemming geeft door op de button te drukken, is er geen probleem maar wanneer de app uit eigen beweging audio kan gaan opnemen, wordt het een ander verhaal. Er kunnen dan opnames worden opgenomen van gesprekken of handelingen die zich in een vertrouwelijke sfeer bevinden. Geluidsopnames waar

⁵² artikel 1 sub a Wet bescherming persoonsgegevens

iemands stem duidelijk op is te horen is een persoonsgegeven conform artikel 1a Wbp. Wanneer de Audio wordt opgenomen om als doel afgespeeld te worden in de chatfunctie. Voldoet deze handeling aan artikel 7 Wbp.

Whatsapp vraagt bij de installatie ook toegang tot het adresboek die de gebruiker op zijn toestel heeft staan. Wanneer de gebruiker hiermee akkoord gaat worden alle contacten uit het adresboek doorgestuurd naar de Whatsapp servers⁵³. Voor iPhone bezitters is er een andere manier ontwikkeld. Vanaf iOS 6 is het mogelijk voor iPhone gebruikers om deze machtiging te weigeren (bijlage 3, afbeelding 14⁵⁴). Whatsapp is dan gewoon te gebruiken zonder dat er met deze installatievoorwaarden akkoord wordt gegaan. De iPhone bezitter met software iOS 6 of hoger kan zelf beslissen of Whatsapp toegang heeft tot het adresboek op de telefoon of niet (bijlage 3, afbeelding 15). Wanneer de gebruiker weigert of in Privacyinstellingen Whatsapp niet meer toegang geeft tot de contactenlijst kan de gebruiker zelf in Whatsapp contacten gaan toevoegen. Een gebruiker met een toestel met Android software kan niet bij de installatie van Whatsapp weigeren dat Whatsapp automatisch toegang heeft tot het adresboek.

Dropbox

De installatievoorwaarden die Dropbox geeft op een Android toestel richten zich minder op persoonsgegevens van de gebruiker. Er wordt bijvoorbeeld toegang gevraagd tot de inhoud van de USB opslag te wijzigen of verwijderen, accounts toevoegen of verwijderen, gegevens van internet ontvangen, automatisch starten bij opstarten, slaapstand van telefoon voorkomen, synchronisatie instellingen lezen en toegang tot beveiligde gegevensopslag testen (bijlage 4, afbeelding 16). Dit zijn niet meteen machtigingen die toegang verkrijgen tot bijvoorbeeld het adresboek of de camera. Het is veel waarschijnlijker dat de omschreven machtigingen daadwerkelijk noodzakelijk zijn om de app te kunnen laten functioneren.

KennisBoek

De app is te downloaden en te installeren zonder installatievoorwaarden op een iPhone. De gebruiker kan zich registreren bij de KennisBoekapp om de app te personaliseren. De gebruiker moet dan akkoord gaan met de voorwaarden. De gebruiker kan zich laten registreren door in te loggen met Facebook-account, Google-account of zich laten registreren bij KennisBoekapp zelf (bijlage 5, afbeelding 17 t/m 20 en 21 t/m 23).

“Kennis heeft toegang nodig tot: netwerkcommunicatie, telefoonoproepen, en opslag.” Onder het kopje “meer weergeven” staat tevens dat de Kennis app toegang nodig heeft tot “systeemhulpmiddelen en netwerkcommunicatie.” (afbeelding 21 en 22)

De afbeeldingen van de bovenstaande app machtigingen op een Android toestel zijn opgenomen in bijlage 5, afbeelding 21. Er wordt in dit onderzoek alleen ingegaan op telefoonoproepen. De KennisBoek app kan net als de Facebook app de telefoonfuncties van het apparaat openen (bijlage 5, afbeelding 22). De KennisBoek app kan het telefoonnummer het serienummer van de telefoon bepalen, of een oproep actief is en het nummer waarmee de oproep is verbonden. De toelichting hiervan is hetzelfde als bij de Facebook app. De overige machtigingen heeft de app nodig om te kunnen functioneren.

Conclusie subvraag a.

Er zijn in deze subvraag vijf apps onderzocht welke bij Android installatievoorwaarden presenteren. Eerst is toegelicht op wat voor manier de twee platforms de apps aanbieden, daarmee wordt ook

⁵³ ‘Overtredingen Whatsapp deel beëindigd na onderzoek CBP en Canadese Privacytoezichthouder’ 28 januari 2013, www.cbpweb.nl pag. 11

⁵⁴ ‘Overtredingen Whatsapp deel beëindigd na onderzoek CBP en Canadese Privacytoezichthouder’ 28 januari 2013, www.cbpweb.nl pag. 13

duidelijk dat Android wel voorwaarden presenteert en Apple niet. De gebruiker moet met deze voorwaarden akkoord gaan, anders kan deze de app niet gebruiken. Wanneer de installatievoorwaarden goed worden gelezen, wordt het steeds duidelijker dat de machtigingen die apps vragen af en toe dubieus zijn. Enkele machtigingen zijn logisch om de app te kunnen laten functioneren. De Facebookapp staat bovenaan wanneer het gaat om gegevensverzameling via de machtigingen. In de volgende subvraag wordt de gebruiksvoorwaarden die apps presenteren op hun websites onderzocht en gekeken welke gegevens de apps verzamelen volgens deze gebruiksvoorwaarden.

3.1.2. subvraag b.

Welke gegevens verzamelen apps volgens de gebruiksvoorwaarden en hoe werkt de praktijk?

Wanneer de gebruiker heeft besloten om de installatievoorwaarden te accepteren (bij Android) en de app te gaan gebruiken zijn de gebruiksvoorwaarden tussen de app en de gebruiker van toepassing. In de gebruiksvoorwaarden vermelden de apps wat zij doen met de gegevens die zij verkrijgen van de gebruiker dan wel actief (gebruiker geeft zelf gegevens) of in-actief (app haalt gegevens zelf vanaf het toestel). In deze subvraag wordt behandeld wat de belangrijkste punten zijn uit de gebruiksvoorwaarden van apps en dan vooral wat zij pretenderen te verzamelen van de gebruiker en wat er in de praktijk wordt verzameld of een keer fout is gegaan. De gebruiksvoorwaarden van de vijf genoemde apps zijn opgenomen in de bijlagen. De gebruiksvoorwaarden die de vijf apps hanteren hebben veel overeenkomsten wat betreft het verzamelen van data, ondanks dat er verschillen zitten in de soorten apps. Alle apps verzamelen zogenaamde Log Data, dit zijn data die van het device wordt gehaald wanneer een gebruiker 'iets doet' met de app. Deze data worden ongemerkt verwerkt door de apps, zij vragen namelijk geen toestemming wanneer zij Log Data willen verwerken. Onder Log Data vallen o.a. het IP-adres, type browser, besturingssysteem, gelinkte websites, bezochte websites, locaties, toestel en app ID's en cookie-informatie (bijlage 7 art 3.1/3.3, bijlage 9 artikel 8, bijlage 10 artikel 5, bijlage 12 artikel 1 en bijlage 13 artikel 6). Het opstarten van een app en eventueel aanmelden geldt ook als Log Data. Op deze manier kunnen apps nauwlettend de bewegingen van gebruikers vaststellen. Sommige soorten Log Data mag de app verwerken wanneer het voor statistische doeleinden wordt gebruikt⁵⁵, zoals bezochte besties en cookieinformatie. De apps verklaren in haar gebruiksvoorwaarden deze gegevens te gebruiken om hun service en diensten beter op de gebruikers te kunnen afstemmen. Dit is een erg breed argument dat kan indekken dat gegevens ook voor advertentie doeleinden kunnen worden gebruikt. Advertenties kunnen theoretisch gezien ook vallen onder service en diensten.

De gebruiksvoorwaarden van Facebook bestaan uit drie delen: verklaring van rechten en verantwoordelijkheden (bijlage 6), een beleid inzake gegevensgebruik (bijlage 7) en richtlijnen voor de community (deze richtlijnen zijn niet relevant voor dit onderzoek)⁵⁶. Twitter vermeldt de gebruiksvoorwaarden (bijlage 8) en privacybeleid (bijlage 9) op haar website. Bij beide partijen blijft de gebruiker eigenaar van de gegevens die deze op het netwerk plaatst. Facebook en Twitter krijgen een gebruiksrecht op alle gegevens (bijlage 6 artikel 2.1, bijlage 8 artikel 5). Dit betekent dat de partijen de gegevens mogen gebruiken en de vruchten daarvan mogen genieten. De gebruiker moet bij het aanmelden enkele persoonlijke gegevens aan de partijen verstrekken die worden gebruikt om een profiel op te starten. Het is mogelijk om via beide diensten foto's en video's te plaatsen. Facebook verwerkt en slaat deze foto's en video's op in haar servers, dit is enigszins logisch omdat anders deze gegevens niet kunnen worden afgebeeld. Wat minder 'logisch' klinkt, is dat zowel Facebook als Twitter metagegevens verzamelen van deze foto's. (bijlage 7 artikel 3.2, en bijlage 9 artikel 4). Metagegevens zijn gegevens over: tijd, datum en plaats waar de foto is gemaakt.

⁵⁵ artikel 9 lid 3 Wbp

⁵⁶ Gebruiksvoorwaarden, 24 oktober 2013 www.facebook.nl

Gebruikers van Twitter kunnen instellen of zij wel/niet hun locatie in een bericht willen weergeven. Desondanks verzamelt Twitter via de Log Data de locaties van gebruikers, ongeacht zij dit aan of uit hebben staan. Twitter vermeldt niet hoelang de locatiegegevens bewaard blijven en of Twitter deze definitief verwijderd wanneer de gebruiker de Tweet met locatie verwijderd. (bijlage 9, artikel 5). Bij het verzamelen van de Log Data vermeldt Twitter wel een bewaringstermijn namelijk 18 maanden, daarna wordt de Log Data verwijderd (bijlage 9, artikel 8).

De diensten verklaren zelf dat zij dit gebruiken om haar service naar de klanten toe te verbeteren. In de praktijk zijn er andere conclusies getrokken. Volgens professor Mireille Hildebrandt legt Facebook in de praktijk het gedrag van de gebruikers vast om zo een profiel te creëren, aan de hand van dit profiel worden bepaalde advertenties weergegeven die in eerste instantie onschuldig lijken (bijlage 7, artikel 3.6)⁵⁷. Wanneer een gebruiker een website bezoekt, een website of product 'liked' dan verschijnen er op zijn Facebook profiel advertenties die met de website of product te maken hebben. Wanneer een gebruiker vermeldt dat hij bijvoorbeeld is wezen skiën, passen de advertenties zich daar op aan en laten skiproducten zien of aanbiedingen voor wintersportgebieden⁵⁸. Gebruikers vullen zelf persoonlijke informatie in zoals 'vrijgezel' of 'in een relatie'. Het komt voor dat gebruikers die vrijgezel zijn meer reclame voorbij zien komen van datingsites. Op deze manier probeert Facebook toch aan zijn dienst geld te verdienen.

Twitter verzamelt in praktijk meer informatie dan dat het lijkt. Een gebruikster van Twitter heeft al haar gegevens opgevraagd en ze ontving een bestand van 50 MB met informatie die Twitter over haar had verzameld, meer dan 1000 emailcontacten en 150 telefoonnummers had Twitter van haar mobiele telefoon geïmporteerd en bewaard⁵⁹. Max Schremers, een rechtenstudent uit Oostenrijk, had een verzoek bij Facebook ingediend tot inzage van zijn gegevens welke Facebook had opgeslagen. Hij kreeg 1.222 pagina's met informatie van de afgelopen drie jaar. Daarin zat genoeg aanleiding om 22 klachten in te dienen bij de Ierse Data Protection Commissioner. Deze 22 klachten zijn ingediend door de Europe versus Facebook-groep die Max Schremers had opgericht. Schremers wijst erop dat Facebook informatie welke door de gebruiker in het verleden is verwijderd, bewaart. Daarnaast was het antwoord op het inzageverzoek onvolledig omdat Facebook nog niet alle gegevens naar Schremers had gestuurd⁶⁰.

Whatsapp heeft op haar website haar algemene voorwaarden en het privacybeleid gepubliceerd (bijlage 10 en bijlage 11). Whatsapp vermeldt in haar voorwaarden wat zij wel en niet verzamelen (bijlage 11, artikel 6). Ze geven aan alleen telefoonnummers te verzamelen en geen inhoud van de berichten te kopiëren, bewaren of archiveren. Daarnaast worden berichten niet bewaard in de servers wanneer deze zijn afgeleverd. Whatsapp fungeert als berichtendienst en om te kunnen functioneren, verzamelt het telefoonnummers van de gebruikers. In de algemene voorwaarden wordt vermeld dat Whatsapp periodieke toegang heeft tot het adresboek van de gebruiker. Whatsapp verklaart dat zij alleen nummers verzamelen en geen andere gegevens zoals namen en emailadressen (bijlage 11, artikel 6). Whatsapp verzamelt de telefoonnummers uit de contactenlijst als in-network numbers en out-network numbers. In-network numbers zijn nummers van personen die Whatsapp gebruiken, out-network numbers zijn nummers van personen die geen Whatsapp gebruiken (bijlage 11, artikel 3). Whatsapp verklaart dat de gebruiker bepaalde persoonlijke en identificeerbare informatie verschaft zoals mobiele telefoonnummer, naam, betalingsinformatie (wanneer toegankelijk) en informatie over het apparaat. Wanneer een Whatsapp bericht is verzonden of ontvangen wordt er een statusupdate bijgehouden van de tijd en datum van verzending. Whatsapp geeft aan dat zij de verzamelde informatie via de website of de service gebruiken om te kunnen opereren, te blijven bestaan en om de service beter op de consument aan te passen. Ze geven aan persoonlijke informatie niet te gebruiken voor commerciële doeleinden en advertenties. Ze gebruiken het wel om de gebruiker op de hoogte te houden van eigen veranderingen aan bijvoorbeeld de website. De Log Data gebruikt Whatsapp om de dienst beter aan

⁵⁷ 'Wat weten facebook en Google over je?', 27 december 2011, www.security.nl

⁵⁸ 'Facebook gebruikt updates en likes voor reclame', 22 september 2011, www.nu.nl

⁵⁹ '50 MB aan Tweets, adressen en al je nummers. Dit is wat Twitter van je weet' 18 april 2012, www.nrc.nl

⁶⁰ 'Tweentwintig klachten na inzage gegevens op Facebook', 27 oktober 2011, www.bof.nl

te kunnen bieden aan haar gebruikers (bijlage 11, artikel 7). Whatsapp verklaart wel persoonlijke informatie te delen met derden wanneer het gaat om hun eigen service te verbeteren (bijlage 11, artikel 8). Er worden per dag zo'n 31 miljard berichten verzonden. Een bericht wordt 30 dagen vastgehouden in de servers wanneer de ontvanger niet online is om het bericht te ontvangen. Na de 30 dagen wordt het bericht verwijderd (bijlage 11, artikel 6). Daarnaast verklaart Whatsapp niet dat ze de berichten niet lezen, ze verklaren alleen dat ze de berichten niet kopiëren, bewaren of opslaan. Tot slot worden de gegevens naar de Verenigde Staten gestuurd, daar is Whatsapp gevestigd en heeft het zijn servers (bijlage 11, artikel 13). Wat dit voor consequenties heeft voor het Nederlandse privacyrecht wordt besproken in de volgende subvraag.

In de gebruiksvoorwaarden lijkt Whatsapp zich in eerste instantie aan de regels te houden. Zo vermelden zij netjes wat zij wel en niet verzamelen en de verzamelde gegevens worden alleen voor de gestelde doeleinden gebruikt. In de praktijk is Whatsapp in 2012 grondig onderzocht door het CBP en de Canadese privacytoezichthouder naar verwerking van persoonsgegevens door Whatsapp⁶¹. Er zijn enkele overtredingen geconstateerd waarvan inmiddels een aantal zijn verholpen en een aantal nog voortduren. Tijdens het onderzoek zijn er een aantal bevindingen geconstateerd. Zoals eerder vermeld moet de gebruiker toestemming geven aan Whatsapp om toegang te verlenen tot het hele adresboek (behalve bij iOS 6 of hoger). Het CBP heeft geconstateerd dat Whatsapp niet deze mogelijkheid tot weigeren biedt aan andere gebruikers met andere software. Daarnaast kunnen gebruikers niet instellen wie zij wel of niet in hun Whatsapplijst willen hebben. Van niet-gebruikers verkrijgt Whatsapp geen ondubbelzinnige toestemming om hun telefoonnummers te gebruiken. Deze drie zaken zorgen ervoor dat Whatsapp artikelen 8 en 11 lid 1 Wbp overtreedt. Het CBP heeft ook twee beveiligingstekerkomingen geconstateerd *“ten aanzien van het aanmaken van de wachtwoorden en ten aanzien van de verzending van berichten.”*⁶² Naar aanleiding van het onderzoek heeft Whatsapp een versleuteling aangebracht op de berichten zodat deze in de toekomst beter beveiligd verstuurd worden.

De gebruiksvoorwaarden van Dropbox⁶³ zijn net als de voorwaarden van Twitter en Whatsapp in het Engels opgesteld. De voorwaarden van Dropbox die in dit onderzoek relevant zijn, zijn de gebruiksvoorwaarden (bijlage 11) en het privacybeleid (bijlage 12). Dropbox verklaart dat alles wat de gebruiker in Dropbox plaatst eigendom is en blijft van de gebruiker (bijlage 11, artikel 2). Om Dropbox te kunnen gebruiken moet de gebruiker een account aanmaken. Dropbox verzamelt een aantal persoonsgegevens (bijlage 12, artikel 1). Dropbox is een cloud opslaglocatie waar gebruikers hun bestanden kunnen plaatsen, dit is ook het doel van Dropbox. Dropbox heeft een apart stuk in het privacy beleid opgenomen met een uitleg wat er met de verkregen informatie gebeurt. Dropbox verzamelt persoonlijke informatie om de gebruiker te contacteren of te identificeren. Persoonlijke informatie wordt gebruikt om de Service te verbeteren, om bij te houden of er gebruik wordt gemaakt van de Service, beter inzicht te krijgen in behoeftes en interesses, om de ervaring te personaliseren en om de gebruiker te voorzien van updates. Dropbox verzamelt cookies die soms vermengd worden met persoonlijke informatie. Deze informatie gebruikt Dropbox om een analyse met behulp van Google Analytics te maken over het gebruik van de Service (bijlage 12, artikel 2). In de praktijk heeft Dropbox zich niet altijd netjes gehouden aan het privacybeleid. Drs. Christopher Soghoian heeft in 2011 onderzocht dat Dropbox medewerkers toegang hadden tot bestanden van gebruikers. De bestanden waren gecodificeerd, maar de codes konden teruggedraaid worden door de medewerkers. Dropbox beweerde dat de codes die zij gebruiken net zo veilig zijn als de codes van banken en defensie. Daarnaast kon Dropbox bestanden de-dupliceren, dit betekent dat wanneer dubbele bestanden van verschillende gebruikers in Dropbox stonden Dropbox maar één bestand in de cloud hield en de rest verwijderde. De reden hiervoor was dat Dropbox zo de 2GB ruimte kon garanderen. Het tegenstrijdige is dat 'maximaal' encryptie bestanden niet gededupliceerd kunnen worden. Wanneer een bestand gecodificeerd is opgeslagen kan het niet

⁶¹ 'Overtredingen Whatsapp deels beëindigd na onderzoek CBP en Canadese Privacytoezichthouder' 28 januari 2013, www.cbpweb.nl (zoek op: *Nieuws en publicaties*)

⁶² 'Overtredingen Whatsapp deels beëindigd na onderzoek CBP en Canadese Privacytoezichthouder' 28 januari 2013, www.cbpweb.nl pag. 3

⁶³ 'Dropbox Terms & Conditions' 26 maart 2013, www.dropbox.com

worden gededupliceerd omdat het door de encryptie van Dropbox zelf niet mogelijk is de inhoud van het bestand te lezen. Medewerkers moesten dus de codes hebben om bestanden daarmee te dedupliceren.^{64 65}

KennisBoek hanteert disclaimer en een privacybeleid voor de KennisBoek app (bijlage 13). Ze verklaren dat ze de persoonlijke informatie die wordt verstrekt vertrouwelijk en in overeenstemming met de Wet bescherming persoonsgegevens wordt behandeld (bijlage 13, artikel 1). Dirkzwager verzamelt verschillende persoonsgegevens, namelijk actieve en technische persoonsgegevens (bijlage 13, artikel 2). Actieve persoonsgegevens zijn o.a. naam en contactgegevens bij de registratie.

De KennisBoek app verzamelt persoonlijke informatie die ze zoals zij zelf verklaren in overeenstemming met het Wbp behandelen. Het verwerken van persoonsgegevens anders dan de doeleinden van verwerking gebeurt alleen wanneer de gebruiker Dirkzwager ondubbelzinnig toestemming heeft verleend (bijlage 13, artikel 4).

Dirkzwager maakt net als Dropbox gebruik van Google Analytics in de app en op de website. Zo kan Dirkzwager bijhouden hoeveel mensen gebruik maken van de app en website. Het verwerken van gegevens voor statistische doeleinden wordt niet als onverenigbaar beschouwd⁶⁶. Toch geeft Dirkzwager de gebruiker de mogelijkheid om Google Analytics te blokkeren door een link te geven naar de website in de disclaimer (bijlage 13, artikel 6).

Conclusie subvraag b:

In deze deelvraag zijn van alle apps zijn de voorwaarden doorgenomen. Het is opvallend dat alle apps naast registratiegegevens ook veel gegevens over de apparaten verzameld zoals Log Data, IP adres, browser type en in sommige gevallen de bezochte websites voordat de website van de app werd bezocht. Wat apps doen met gegevens motiveren zij in de voorwaarden. De ene app is duidelijker in het vermelden welke informatie er wordt verzameld en welke niet en hoelang dit wordt bewaard. Per app is een praktijkvoorbeeld gegeven om te laten zien dat de werkelijkheid soms anders is dan het lijkt. In deelvraag 2 komen meerdere onderzoeken aan het licht. Facebook gaat vrij open om met persoonlijke gegevens, zij versturen deze gegevens bijvoorbeeld naar derden en adverteerders. Twitter is duidelijker in het aangeven van termijnen hoelang zij gegevens bewaren van de gebruikers. Daarnaast presenteert Twitter zichzelf ook als een open medium waardoor de gebruiker ook bewust moet zijn van het feit dat alles wat hij op Twitter zet openbaar is. Whatsapp geeft zelf aan niet veel gegevens van gebruikers te verzamelen en op te slaan. Daarnaast hebben zij duidelijk in de algemene voorwaarden opgenomen welke gegevens Whatsapp niet bewaard. Dropbox geeft aan geen GPS – locaties van het apparaat op te slaan en wanneer een gebruiker een foto uploadt in Dropbox met metagegevens is dit de ‘keuze’ van de gebruiker zelf. Tot slot KennisBoek app, deze door Dirkzwager ontwikkelde app geeft aan dat deze in overeenstemming met de Wbp omgaat met het verwerken van persoonsgegevens.

3.1.3 subvraag c.

Zijn de voorwaarden die worden geaccordeerd bij installatie van apps (bijv. vragen om toegang tot foto's) in strijd met de Nederlandse wetgeving?

Er wordt nadrukkelijk niet gekeken naar de inhoud van de complete sets algemene voorwaarden omdat dit het doel en de scope van dit onderzoek te buiten gaat. Daarnaast wordt de wet-en regelgeving betreffende het beroepsgeheim er buiten gelaten omdat deze in deelvraag 3 en de analyse wordt behandeld. Daarentegen wordt hier gekeken naar de installatievoorwaarden die worden gepresenteerd bij het installeren van de app. In deelvraag 1 is uitgelegd dat de installatievoorwaarden deel uitmaken van de algemene voorwaarden. De volgende Nederlandse wet- en regelgeving is op dit vraagstuk van toepassing: de wetgeving rond algemene voorwaarden, de Wbp en de Telecommunicatiewet (Tw.). Eerst wordt er ingegaan op de vraag of de apps

⁶⁴ C. Soghoian 'How Dropbox sacrifices user privacy for cost savings', 12 april 2011, paranoia.dubfire.net

⁶⁵ 'Dropbox in de knoop met privacy' 16 mei 2012, www.automatiseringgids.nl (zoek op: *Dropbox in de knoop met privacy*)

⁶⁶ artikel 9 lid 3 Wet bescherming persoonsgegevens

betreffende de algemene voorwaarden zich houden aan de Nederlandse wetgeving en daarna de Wbp en de Tw.

In deelvraag 1. is kort uitgelegd wat verschillende punten zijn met betrekking tot algemene voorwaarden in de Nederlandse wetgeving. Zo is het duidelijk dat in Nederland het beginsel van contractsvrijheid tussen partijen geldt. De gebruiker mag zelf bepalen wat hij opneemt in de algemene voorwaarden (m.u.v. de kernprestatie), het is vervolgens aan de wederpartij of hij er mee akkoord gaat. Ondanks dat de bedrijven van apps hoofdzakelijk zijn gevestigd in de VS is het Nederlands recht betreffende de algemene voorwaarden (afdeling 6.5.3 van Boek 6) toch van toepassing⁶⁷. De reden hiervan is dat de Nederlandse burger goed moet worden beschermd tegen onredelijke voorwaarden. In de algemene voorwaarden kan het bedrijf opnemen dat het Californische recht van toepassing is, dit is de vrijheid van rechtskeuzebevoegdheid. Er is geen beperking met betrekking tot het rechtsstelsel dat op de overeenkomst of algemene voorwaarden als toepasselijk kan worden verklaard. Partijen hebben vrijheid wanneer het gaat om het kiezen van het toepasselijk recht dan wel Forumkeuze in de voorwaarden⁶⁸⁶⁹. In het geval van algemene voorwaarden is de wederpartij geen partij in het opstellen / onderhandelen van de bedingen in de algemene voorwaarden. Wanneer de wederpartij een geschil aanhangig maakt op grond van het schenden van de open norm of een artikel uit de Wbp moet de Californische rechter dit aan het Nederlands recht toetsen, omdat deze van dwingend recht zijn en ter bescherming van de consument. In beginsel kijkt de rechter niet naar de verhoudingen tussen partijen.

De installatievoorwaarden bij Android worden na het downloaden van de app automatisch gepresenteerd. Er staat duidelijk “(naam app) heeft toegang nodig tot:....” met daaronder een aantal punten. Met behulp van de knop met “accepteren” laat de wederpartij weten dat hij akkoord gaat met de installatievoorwaarden. De app voldoet hiermee aan de informatieplicht omdat deze de wederpartij een redelijke mogelijkheid geeft om kennis te nemen van de voorwaarden⁷⁰. Aangezien de overeenkomst via elektronische weg tot stand komt moet de consument de voorwaarden kunnen opslaan voor latere kennisneming. Wanneer dit niet mogelijk is moeten de voorwaarden hem worden toegezonden⁷¹. Op een Android toestel is het mogelijk om van de installatievoorwaarden kennis te nemen onder het kopje “Instellingen”.

De bedingen die zijn opgenomen in de installatievoorwaarden kunnen als onredelijk bezwarend worden aangemerkt. Er zijn verscheidende criteria voor de rechter om te toetsen wanneer een beding onredelijk bezwarend is, variërend van de open norm tot de gesloten norm. De open norm is opgenomen in artikel 233 sub a Boek 6 Burgerlijk Wetboek. Aan de hand van de open norm kan de rechter breed toetsen of bedingen onredelijk bezwarend zijn aangezien veel algemene voorwaarden verschillend van elkaar zijn. Aangezien het aanbieden van apps zich op de consument markt bevindt wordt er strenger getoetst door de rechter aan de hand van de zwarte of grijze lijst. Dit is de gesloten norm omdat er specifieke bepalingen zijn opgenomen in de lijsten. De bepalingen op de zwarte lijst zijn altijd onredelijk bezwarend en daardoor zonder meer vernietigbaar. De bepalingen op de grijze lijst worden als vermoedelijk onredelijk bezwarend gezien, tegenbewijs is hierbij mogelijk. Een beding dat op een van deze lijsten staat kan door de rechter worden getoetst en vernietigd.

In de open norm zijn de volgende criteria opgenomen: er kan worden gelet op de aard en de overige inhoud van de overeenkomst, de wijze waarop de voorwaarden tot stand zijn gekomen en de wederzijds kenbare belangen van partijen en overige omstandigheden van het geval⁷². De aard en de overige inhoud van de overeenkomst kan breed worden beoordeeld. Er kan naar een aantal factoren worden gekeken bijvoorbeeld de duur van de overeenkomst, soort overeenkomst (arbeid, koop, huur, dienst) en de factoren van de markt⁷³. Bij de wijze waarop de voorwaarden tot stand zijn gekomen wordt gekeken of het eenzijdig of met overleg tot stand is gekomen⁷⁴. De wederzijds

⁶⁷ artikel 247 lid 4 Boek 6 Burgerlijk Wetboek

⁶⁸ Alnati arrest, HR 13 mei 1966

⁶⁹ L. Strikwerda, *Inleiding tot het Nederlandse Internationaal Privaatrecht*, Deventer: Kluwer 2000

⁷⁰ artikel 233 sub b jo 234 lid 2 Boek 6 Burgerlijk Wetboek

⁷¹ artikel 234 lid 1 sub c Boek 6 Burgerlijk Wetboek

⁷² artikel 233 sub a Boek 6 Burgerlijk Wetboek

⁷³ B. Wessels, *Contracten maken*, Deventer: Kluwer 2007

⁷⁴ E.M. Bruggeman, *Praktijkboek Koop/-aannemingsovereenkomst*, Instituut voor Bouwrecht 2006

kenbare belangen van partijen bij de algemene voorwaarden; het kan voor de gebruiker van groter belang zijn om procedures te voorkomen terwijl het belang de wederpartij (consument) kan zijn dat in een beding is opgenomen dat zijn gegevens niet naar derden worden verstuurd. Tot slot de overige omstandigheden van het geval, dit is een erg breed begrip waarbij een aantal omstandigheden in acht kunnen worden genomen: de deskundigheid van partijen, maatschappelijke positie, onderlinge verhoudingen, etc.⁷⁵.

Onderstaand worden de installatievoorwaarden (niet inhoudelijk) getoetst aan de hand van de open norm en de zwarte en grijze lijst. (1.) Aard en overige inhoud van de overeenkomst: alle overeenkomsten zijn tussen de app en de wederpartij, de kern van de overeenkomst is het aanschaffen van een app om deze dienst te kunnen gebruiken. Het varieert per consument of de overeenkomst lang of kort duurt. Zo zullen Whatsapp en Facebook langer worden gebruikt dan sommige spelletjes. De factoren van de markt bepalen o.a. de gedragsregels hoe de voorwaarden tot stand komen. Het is vrij duidelijk dat dit eenzijdig gebeurt aangezien partijen niet gaan overleggen voordat de consument een app downloadt. Dit sluit direct aan bij (2.) de wijze waarop de voorwaarden tot stand komen. (3.) De wederzijds kenbare belangen van partijen zouden bij de meeste voorwaarden als onredelijk bezwarend kunnen worden aangemerkt. Er wordt over het algemeen namelijk geen rekening gehouden met het belang van de gebruiker. Er is gezegd geen sprake meer van een gezonde verhouding tussen het gebruiken van een app en de app toegang geven tot belangrijke informatie op het toestel waarbij niet wordt vermeld waarvoor het wordt gebruikt. Sommige voorwaarden, zoals die van Facebook, welke het recht verlenen om zonder tussenkomst of wetenschap van de gebruiker telefoonnummers te bellen of de contactenlijst te lezen, zijn tegenstrijdig met het belang van de wederpartij omdat de wederpartij niet zelf kan bepalen of zij dit Facebook wel of niet wil toestaan. (4.) Bij de overige omstandigheden van het geval ligt de verhouding bij de deskundigheid en de onderlinge verhouding van beide partijen erg scheef. De consument is vrij onwetend wat betreft voorwaarden en zal wanneer deze langs komen ze snel accepteren. Daarnaast worden de voorwaarden gesloten tussen een 'normale' burger en een grote multinational zoals Facebook, die sociaal-economisch en maatschappelijk veel sterker staat. De open norm is erg ruim gedefinieerd en zo kan het toetsen ervan ook geschieden. De reden voor een ruime definiëring is omdat veel algemene voorwaarden van elkaar verschillen, hierdoor is een algemene norm moeilijk te geven⁷⁶. Het is uiteindelijk aan de rechter om te toetsen of specifieke bedingen in de installatievoorwaarden als (kennelijk) onredelijk bezwarend kunnen worden aangemerkt. Naast de open norm worden bedingen getoetst aan de bepalingen in de zwarte en grijze lijst. In de installatievoorwaarden van de apps staan geen bedingen die getoetst kunnen worden aan de zwarte of grijze lijst. De bepalingen op deze lijsten zien meer op algemene voorwaarden of gebruiksvoorwaarden dan installatievoorwaarden. Wanneer een rechter de installatievoorwaarden zou gaan toetsen, lijkt het mij daarom waarschijnlijker dat de rechter eerder via de open norm gaat beoordelen of bepaalde bedingen onredelijk bezwarend zijn.

In deelvraag 1 en in andere subvragen is al verwezen naar de Wbp. Voor de Nederlandse burger geldt de Wbp, de persoonsgegevens van de Nederlandse burger dienen in overeenstemming met deze wet te worden behandeld. Daarmee is de Wbp van dwingend recht: een contractuele bepaling of een voorwaarde mag hier niet van afwijken. Zie artikel 8 Wbp, alleen op deze gronden mogen persoonsgegevens worden verwerkt, een voorwaarde mag hier niet van afwijken⁷⁷. De Wbp heeft artikel 4 lid 2 Wbp opgenomen waarin wordt vermeld dat de Wbp toepassing heeft op verwerking van persoonsgegevens door een verantwoordelijke die een vestiging buiten de EU heeft en waarbij gebruik wordt gemaakt van geautomatiseerde middelen die zich in Nederland bevinden.

Geautomatiseerde middelen is een breed begrip waar veel onder kan vallen zoals: computers, smartphones, servers, etc. De meeste bedrijven of app-ontwikkelaars hebben een vestiging buiten de EU. Ondanks de vestiging zijn zij toch gebonden aan de Wbp wanneer persoonsgegevens door Nederland worden verwerkt dan wel via smartphones of het transporteren naar servers. Tevens is

⁷⁵ B. Wessels, *Contracten maken*, Deventer: Kluwer 2007

⁷⁶ 'Algemene voorwaarden' 20 oktober 2013 www.iusmentis.nl (zoek op: *algemene voorwaarden*)

⁷⁷ A. Engelfiet 'Wanneer is een wet nu optioneel?' 19 juli 2013, www.iusmentis.nl

het Safe Harbor principe opgesteld, deze regelgeving geldt voor de bescherming voor persoonlijke data welke tussen de EU en de VS worden uitgewisseld. De reden hiervoor is dat in de VS een andere standaard bestaat voor privacy dan in de EU. Safe Harbor is voortgevloeid uit de EU richtlijn: 95/46/EG, net als de Nederlandse Wbp. Bedrijven in de VS kunnen een Safe Harbor certificaat aanvragen, zij moeten kunnen garanderen dat zij de persoonlijke data en de privacy van gebruikers net zo goed beschermen als dat gebeurt in de EU⁷⁸. Facebook⁷⁹, Twitter (bijlage 9, artikel 17) en Dropbox (bijlage 12, artikel 10) hebben apart in het privacy beleid opgenomen dat gegevensverwerking geschiedt in overeenstemming met het VS – EU Safe Harbor principe.

Er zijn een aantal voorwaarden voor de rechtmatigheid van de verwerking van persoonsgegevens: (1) het gebeurt in overeenstemming met proportionaliteit en subsidiariteit⁸⁰, het (2) stemt overeen met het beschreven doel (doelbinding)⁸¹ en (3) er moet sprake zijn van een rechtvaardigingsgrond⁸². Verder zijn er nog aanvullende artikelen in de Wbp die bepalen welke persoonsgegevens niet mogen worden verzameld en wat bijvoorbeeld de bewaartermijnen zijn.

Alle vijf de apps vragen bij de installatie toegang tot bepaalde informatie op een Android-toestel. Facebook kan o.a. toegang tot de camera en het telefoonboek krijgen wanneer deze is gemachtigd bij de installatie. Twitter kan o.a. toegang krijgen tot de contactgegevens en de GPS locatie en Whatsapp kan gemachtigd worden voor het telefoonboek. Deze gegevens worden volgens het Nederlands Recht aangemerkt als persoonsgegevens, de gegevens kunnen leiden tot de identiteit van een persoon. De verwerking van deze gegevens mag alleen op een behoorlijke en zorgvuldige wijze (proportionaliteitsbeginsel). Wat er niet bij installatievoorwaarden uitdrukkelijk wordt uitgelegd is het doel van de te verzamelen gegevens. Er staat bij de bepaling namelijk geen uitleg wat het doel van Facebook is om toegang te krijgen tot de camera en op elk moment foto's te maken, of het doel van Twitter om toegang te krijgen tot de GPS locatie. Daarmee handelen de apps in strijd met de Wbp. Daarnaast kan getoetst worden of de gegevensverwerking noodzakelijk is voor de uitvoering van de apps. Whatsapp is een berichtendienst en wil daarom toegang tot alle telefoonnummers. Het is enigszins logisch dat Whatsapp een telefoonnummer nodig heeft om contact te kunnen leggen, maar daarom hoeft niet de hele contactenlijst te worden verwerkt. In deelvraag a. is al uitgelegd dat het mogelijk is om Whatsapp niet meer te machtigen op een iPhone, desondanks kan de gebruiker toch Whatsapp blijven gebruiken. De gebruiker kan zelf bepalen welke nummers hij toevoegt in Whatsapp, daardoor is de machtiging niet meer nodig. Het CBP had in deelvraag a. al geconstateerd dat Whatsapp in strijd met artikelen 8 en 11 Wbp heeft gehandeld. Hoe noodzakelijk is het voor Facebook om op elk moment foto's te maken? Of voor Twitter om de GPS locatie te verkrijgen? De aard van de gegevens wegen namelijk niet op tegen de noodzakelijkheid van de verwerking van de gegevens. Ook lijkt het dat de gevolgen voor de gebruiker niet in overweging worden genomen. De KennisBoek app vraagt op een apparaat met Android software enkele machtigingen. De KennisBoek app verklaart in haar disclaimer dat persoonlijke informatie die wordt verstrekt door de gebruiker vertrouwelijk is en in overeenstemming met de Wbp wordt behandeld. Een telefoonnummer, serienummer van een telefoon en oproepen zijn persoonsgegevens. Het is namelijk een gegeven die tot een identiteit van persoon leidt⁸³. In eerste instantie zou de KennisBoek app de gegevens mogen verwerken, zolang dit maar op een behoorlijke en zorgvuldige wijze gebeurt⁸⁴. De persoonsgegevens, zoals het telefoonnummer en de oproepgegevens, mogen slechts worden verwerkt indien: de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend⁸⁵. Er wordt eenmalig aan de gebruiker medegedeeld dat de app toegang wil hebben tot deze gegevens bij installatie maar het is niet duidelijk wanneer de app daadwerkelijk toegang tot de gegevens wil hebben. Er wordt bij installatie niet vermeld wat de

⁷⁸ R. Niamat 'Safe Harbor – een korte opfris cursus (column)' 24 maart 2011, www.ispam.nl (zoek op: *Safe Harbor*)

⁷⁹ 'Een aantal andere dingen die je moet weten' Beleid inzake gegevensgebruik Facebook, www.facebook.nl

⁸⁰ artikel 6 Wet bescherming persoonsgegevens

⁸¹ artikel 7 Wet bescherming persoonsgegevens

⁸² artikel 8 Wet bescherming persoonsgegevens

⁸³ artikel 1 sub a Wet bescherming persoonsgegevens

⁸⁴ artikel 6 Wet bescherming persoonsgegevens

⁸⁵ artikel 8 sub a Wet bescherming persoonsgegevens

KennisBoekapp met de verkregen gegevens doet die zij verkrijgt door de machtiging. De app vermeldt niet of zij de verkregen gegevens daadwerkelijk gaat verzamelen en opslaan. Desondanks heeft de app wel toegang tot de telefoonfuncties en kan de app de gegevens lezen. De KennisBoekapp beweert toegang nodig te hebben tot de telefoonfuncties om te kunnen functioneren. Er kan worden betwist of de app dit noodzakelijkerwijs nodig heeft voor de uitvoering van de overeenkomst conform artikel 8 Wbp. In dit geval kan de app-machtiging in strijd zijn met de Nederlandse wet- en regelgeving. Het is mogelijk dat de app de verkregen gegevens in overeenstemming met de Wbp verwerkt, zoals zij zelf vermelden in de disclaimer. Alleen kan worden betwijfeld of de persoonsgegevens worden verwerkt in overeenstemming met de doeleinden van de app.

Tot slot de Telecommunicatiewet (Tw.) in artikel 11.7a is opgenomen dat eenieder die door middel van elektronische communicatienetwerken toegang wenst te krijgen tot een smartphone om gegevens te lezen of op te slaan (a) de gebruiker duidelijke en volledige informatie te verstrekken overeenkomstig de Wbp met daarbij de doeleinden waarvoor de gegevens worden opgeslagen en (b) toestemming moet hebben gekregen van de gebruiker voor de desbetreffende handeling. De toestemming van de gebruiker is gedefinieerd in artikel 11.1 onder g Tw. en omvat toestemming in de zin van artikel 1 onder i Wbp. De apps willen toestemming van de gebruiker om gegevens van de smartphone te lezen of op te slaan. Hiervoor vraagt de app toestemming doormiddel van het accepteren van de installatievoorwaarden door de gebruiker. De doeleinden van het lezen of opslaan worden hierbij vaak niet vermeld door de app. Wat betreft de toestemming in de Tw. wordt het Wbp aangehaald. In artikel 1 onder i Wbp wordt toestemming gedefinieerd als: "elke vrije, specifieke en op informatie beruste wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt." Het kan worden betwijfeld of de machtigingen hieraan voldoen. De gebruiker kan namelijk niet in algehele vrijheid zijn wil uiten, alleen beperkt. De gebruiker kan de voorwaarden accepteren of niet, maar er kan niet per machtiging worden ingesteld of de gebruiker daar wel of niet mee akkoord gaat. De machtigingen zijn daarnaast niet specifiek geformuleerd, maar zeer algemeen "mag alle adressen die op uw apparaat zijn opgeslagen, lezen" (bijlage 2, afbeelding 8). Deze formulering is toepasbaar op alle machtigingen die de app wil verkrijgen. Tot slot wordt de gebruiker niet volledig geïnformeerd over de noodzakelijke inlichtingen voor goede oordeelsvorming.⁸⁶ De machtigingen worden summier beschreven waardoor er betwijfeld kan worden of de beschrijving bijdraagt aan de goede oordeelsvorming.

Conclusie subvraag c.

In deze vraag werden niet alle installatievoorwaarden aan het Nederlands Recht getoetst maar hoofdzakelijk de aard en de manier van presenteren naar de gebruiker toe. Het is duidelijk dat sommige bedingen in de installatievoorwaarden niet overeenstemmen met de open norm. Het is erg onduidelijk wat het doel is van de apps om bepaalde gegevens te verzamelen. Ook lijkt het niet noodzakelijk dat de apps toegang mag hebben tot bepaalde gegevens om te kunnen functioneren. Daarnaast werkt de manier van toestemming geven door de gebruiker automatisch in het nadeel van de gebruiker, dit is in strijd met de Telecommunicatiewet en de Wbp. In de volgende deelvraag wordt ingegaan op de problemen en risico's bij het gebruik van apps.

3.2 Deelvraag 2.

Wat zijn conform (niet-)literatuurbronnen en onderzoeken de problemen en risico's die er spelen met betrekking tot de veiligheid van vertrouwelijke informatie bij het gebruik van apps?

In de vorige deelvraag en subvragen is uitgebreid uitgelegd dat apps zich vaak anders gedragen dan doet vermoeden. In deze deelvraag wordt uitgelegd aan de hand van eerdere onderzoeken wat na de installatie en tijdens het gebruik de problemen en risico's zijn van apps.

⁸⁶ 'Onderzoek naar de verwerking van persoonsgegevens in het kader van de mobiele applicatie whatsapp door Whatsapp Inc.' 28 januari 2013, www.cbppweb.nl pag. 30

De artikel 29-werkgroep van Europese privacytoezichthouders heeft begin 2013 een onderzoek uitgevoerd over de privacyrisico's van apps. Er is een opinie geplaatst waarin concrete verplichtingen op grond van de Europese privacywetgeving voor app-ontwikkelaars is uitgewerkt. *“Een smartphone-gebruiker heeft gemiddeld zo'n 37 apps gedownload. Apps kunnen enorme hoeveelheden persoonsgegevens van die gebruiker verwerken, onder meer door toegang tot het fotoalbum of het gebruik van locatiegegevens. Dit gebeurt nu vaak zonder dat gebruikers hierover goed zijn geïnformeerd en zonder dat zij hiervoor vrijelijk toestemming hebben kunnen geven. Dat is in strijd met Europese privacywetgeving, aldus de voorzitter van de Artikel 29-werkgroep Jacob Kohnstamm.”*⁸⁷ Deze conclusie is in de vorige deelvraag ook door de onderzoeker getrokken. De opinie stelt dat de risico's van apps hoog ligt aangezien het in directe verbinding staat met het gehele Operating System (OS) van de smartphone. Hierdoor heeft de app veel makkelijker toegang tot het OS in vergelijking met een normale internet browser in relatie tot het OS van een PC en kan daardoor het grote hoeveelheden data verzamelen.⁸⁸

Op de website van het Cbp: www.mijnprivacy.nl wordt ook aandacht besteed aan de privacy risico's van apps. Het Cbp somt een aantal risico's op: (1) apps verkrijgen vaak geen geldige toestemming, (2) apps verzamelen meer gegevens dan nodig, (3) onvoldoende beveiligingsmaatregelen van apps en (4) zowel gratis als betaalde apps brengen risico's met zich mee⁸⁹.

De Australische software architect en beveiligingsexpert Troy Hunt heeft een onderzoek gedaan naar iOS apps. Hunt ontdekte dat veel iOS apps spyware met zich meedragen waardoor apps gebruikers precies kunnen volgen tijdens het gebruik. Dit zijn ook apps die gewoon uit de App Store kunnen worden gedownload. Apple pretendeert apps van te voren compleet te hebben doorgelicht, maar blijkt niet goed genoeg. Zo blijkt maar weer dat zelfs apps uit de 'beveiligde' App Store risico's met zich mee brengen. Deze apps kunnen privacygevoelige informatie overdragen naar o.a. Flurry. Flurry is een bedrijf waar apps zich op kunnen aansluiten om analyses van het app gebruik te kunnen vaststellen. Flurry registreert zo'n 3,5 biljoen app sessies per dag. Flurry gebruikt niet alleen iOS apps maar ook apps op Android, Blackberry en Windows toestellen. Hierdoor kan het bedrijf enorme hoeveelheid data verwerken en verzamelen. Deze data gebruikt Flurry vervolgens weer om profielen te maken en te verkopen aan derde partijen, waaronder veel advertentiebureaus⁹⁰. Uit het onderzoek blijkt tevens dat de data slecht wordt gecodeerd waardoor persoonlijke informatie slecht beveiligd wordt doorgestuurd, met als gevolg dat internetcriminelen eenvoudig aan inloggegevens kunnen komen. Gebruikers gebruiken hun toestel tegenwoordig steeds vaker met zakelijke informatie.

Zakelijke contacten worden opgeslagen op telefoons en zakelijke telefoontjes worden gepleegd, hierdoor wordt het veiligheidsrisico alleen maar groter⁹¹.

In Groot-Britannië is door de nieuwszender Channel 4 in samenwerking met MWR InfoSecurity een onderzoek gedaan naar de data-uitwisselingen van een smartphone. Channel 4 had een virtuele – niet bestaande – persoon aangemaakt en 24 uur lang de datastromen gevolgd. Op de telefoon hebben ze 30 van de populairste apps gedownload. In de 24 uur dat de telefoon aanstond zijn er meer dan 144.000 'pakketjes' met informatie verstuurd naar ongeveer 315 servers over de hele wereld. Sommige bevatten informatie over bezochte websites en anderen over de precieze locatie van de telefoon en waar deze was geweest. Zelfs wanneer de telefoon 45 minuten lang niet werd gebruikt waren er toch 30.000 verzoeken naar 76 servers om informatie te versturen. Veel informatie over de locatie werd verstuurd naar zigi.com. Dit zijn adverteerders in de VS en Oekraïne. Mr. Miller van MWR zegt dat het veel mensen verrast dat de telefoon altijd actief is, zelfs wanneer er niets mee wordt gedaan. Een smartphone heeft altijd verbinding met het internet en de apps. De apps kunnen er voor kiezen om door te gaan met informatie te verzenden zelfs wanneer de gebruiker de telefoon heeft neergelegd⁹².

⁸⁷ “Europese privacytoezichthouders publiceren opinie over mobiele apps *Gebruik persoonsgegevens door app alleen toegestaan met toestemming gebruiker*” 14 maart 2013, www.cbpweb.nl

⁸⁸ ‘CBP opinion on Mobile Apps’ 14 maart 2013, pag. 5, www.cbpweb.nl

⁸⁹ ‘Apps’ www.mijnprivacy.nl (zoek op: *ik heb een vraag over apps*)

⁹⁰ Uitzending TROS Radar, TROS Nederland 2, 18 november 2013

⁹¹ ‘Vrijwel elke iPhone besmet met spyware’ 12 juni 2013, www.repairking.nl (zoek op: *spyware iPhone*)

Conclusie deelvraag 2:

Wat inmiddels de problemen en risico's zijn is wel duidelijk. Apps doen meer dan alleen het 'leuke spelletje' laten draaien of mooie foto's bewerken. Veel apps sturen persoonlijke data door naar grote bedrijven zoals Flurry die profielen samenstelt uit deze data en deze delen met adverteerders (bijlage 14, artikel 2.3). Tegenwoordig gebruiken veel mensen hun telefoon naast privé ook zakelijk. Er worden zakelijke contacten opgeslagen en via email, Whatsapp, sms of telefonisch gecommuniceerd. Uit de sub en deelvragen is naar voren gekomen dat de apps deze gegevens verzamelen. Het probleem is dat weinig mensen hier vanaf weten en de risico's zijn dat slecht beveiligde data kan worden onderschept door internetcriminelen. Daarnaast gaat de smartphone 24 uur per dag door met data verzamelen en versturen, zelfs al heeft de gebruiker deze in zijn broekzak zitten.

3.3 Deelvraag 3.

Wat houdt het beroepsgeheim van de advocatuur in en wanneer wordt het beroepsgeheim geschonden in combinatie met het werken met apps?

Het beroepsgeheim houdt in dat wanneer iemand bij het uitoefenen van zijn beroep over feiten en gegevens van derden zwijgt die zijn verkregen bij het uitoefenen van zijn beroep⁹³. Het beroepsgeheim geldt niet als de betrokkene toestemming geeft om aan derden inlichtingen te verstrekken. De beroepen die een beroepsgeheim hanteren zijn: Medici, Advocaten, Notarissen, Politiebeambten, Accountants, Priesters, Paramedici, Tolken, Maatschappelijk assistenten, Ambtenaren in fiscale en inlichtingendienst en Medewerkers van psychosociale diensten. Schending van het beroepsgeheim is strafbaar conform artikel 272 Wetboek van Strafrecht. Dit artikel is van toepassing op alle beroepsgroepen met beroepsgeheim. Per beroepsgroep is het beroepsgeheim verder uitgewerkt. Zo staat in artikel 88 Wet BIG (Beroepen in individuele Gezondheidszorg) en artikel 7:457 Burgerlijk Wetboek het beroepsgeheim voor medici uitgewerkt. In dit stuk zal ik vooral ingaan op het beroepsgeheim van advocaten.

Jurisprudentie

Het beroepsgeheim kan worden geschonden door bijvoorbeeld een arts of advocaat. In het verleden is dit voorgekomen. In een arrest van de Hoge Raad op 14 mei 2013⁹⁴ heeft een arts/psycholoog zich willen beroepen op het verschoningsrecht. In deze zaak bezat zij een videoband met de verklaring van een minderjarige jongen die tijdens een speltherapie verklaarde dat hij is misbruikt door zijn vader. De rechter-commissaris beval in het belang van de zaak de arts tot uitlevering ter inbeslagneming van de videoband, de arts beriep zich op de medische geheimhoudingsplicht en zag geen grond om deze geheimhoudingsplicht te doorbreken. De rechtbank heeft besloten dat op grond van de aard en de ernst van het strafbare feit en het belang dat de geheimhouding moet wijken voor het belang dat de waarheid aan het licht komt. Het beroep op het verschoningsrecht door de arts is afgewezen door de rechtbank en Hoge Raad. In sommige gevallen is het op grond van maatschappelijk belang gegrond dat een beroepsuitoefenaar met geheimhoudingsplicht deze mag doorbreken.

Door de Raad van Discipline in Den Bosch is een klacht jegens een advocaat gegrond verklaard dat deze de geheimhoudingsplicht uit de mediation overeenkomst heeft geschonden. Hierbij heeft de advocaat art. 7.1 van het NMI Mediationreglement 2008 geschonden. De advocaat heeft een waarschuwing en een passende maatregel gekregen⁹⁵.

⁹² 'Secret lifes of phones, how yours contacts 315 servers a day' 14 november 2013, www.channel4.com (zoek op: *Data Baby*)

⁹³ definitie beroepsgeheim, www.encyclo.nl

⁹⁴ LJN: BZ9943, HR 14-05-2013, www.jure.nl

⁹⁵ YA1772, Raad van Discipline 's – Hertogenbosch H258 – 2010, www.juridischdagblad.nl

In het arrest van de Hoge Raad op 4 april 2006 was een advocaat verdacht van het medeplegen dan wel uitlokken van doen plegen van schending van geheimhoudingsplicht. De advocaat werd verdacht van het aanbieden van geld aan een informatiebureau om in ruil daarvoor, in strijd met de wet, vertrouwelijke gegevens te verschaffen over personen tegen wie zijn cliënt een vordering wilde instellen. Bij de advocaat zijn stukken in beslag genomen door de rechter-commissaris in belang van het onderzoek. De advocaat deelde bij inbeslagname mede dat de stukken onder zijn geheimhoudingsplicht vielen en zich beriep op het verschoningsrecht. De advocaat is door de Rechtbank als verdachte aangemerkt van het schenden van zijn geheimhoudingsplicht. Desondanks moeten de stukken worden teruggegeven aan de advocaat⁹⁶.

Advocaten

Alle advocaten zijn conform artikel 1 Advocatenwet inschreven bij de Orde van Advocaten. Dit betekent dat de advocaat zich aan de Advocatenwet moet houden en aan de eisen die de Orde van Advocaten stelt⁹⁷. De Raad van Toezicht van de Orde van Advocaten heeft de Gedragscode 1992 opgesteld. “Deze gedragscode biedt een leidraad voor hoe de besturen en de medewerkers van de Nederlandse en lokale Orden van Advocaten dienen te handelen in uitvoering van hun werkzaamheden.”⁹⁸ De gedragscode heeft als doel om een balans te zoeken tussen enerzijds het beschermen van privacy van degenen van wie persoonsgegevens worden verwerkt en anderzijds de noodzaak respectievelijk het belang van de Nederlandse Orde van Advocaten en de lokale Orden van Advocaten om bepaalde persoonsgegevens te verwerken⁹⁹. Het uitgangspunt is de Wbp, deze wet is van toepassing op de gedragscode. In regel 6 van de Gedragscode 1992 staat dat de advocaat verplicht is tot geheimhouding (bijlage 15, sub 1) Deze geheimhouding duurt voort tot het einde van de relatie tussen de cliënt en de advocaat (bijlage 15, sub 4). De advocaat dient te zwijgen over de persoon van de cliënt en de omvang van diens belangen (bijlage 15, sub 1). Dit betekent dat de advocaat geen persoonsgegevens mag verstrekken aan derden zonder de toestemming van zijn cliënt. Het beroepsgeheim kan worden geschonden wanneer dit wel gebeurt. Voor klachten over schending van de geheimhoudingsplicht door de advocaat wordt vaak de tuchtrechter ingeschakeld. Wanneer een advocaat zich op het verschoningsrecht beroept tijdens een strafzaak toetst de rechter dit marginaal. Dit betekent dat de rechter het oppervlakkig en niet inhoudelijk toetst. In het Notaris Maas arrest is door de rechter bepaald dat wanneer er bij een beroep op verschoningsrecht ten minste een redelijke twijfel bestaat dat hier sprake van is, het verschoningsrecht moet worden gehonoreerd¹⁰⁰.

Communicatie tussen de cliënt en de advocaat is vertrouwelijk, vooral wanneer het inhoudelijk over de zaak gaat. Doordat het beroepsgeheim voor het ambt van de advocaat wettelijk is vastgesteld mag er verwacht worden dat advocaten hier op een juiste wijze mee om gaan. Tegenwoordig gebruiken veel advocaten smartphones zakelijk als communicatiemiddel. Daarnaast gebeurt steeds meer communicatie over de email en soms whatsapp of sms. De gegevens van de cliënt op het toestel van de advocaat kunnen risico lopen wanneer er (bepaalde) apps op staan. Uit de vorige deelvragen is gebleken welke risico's hier aan vast zitten. Het is mogelijk dat persoonsgegevens van cliënten, zoals namen, telefoonnummers, emailadressen, documenten etc. die over de smartphone worden gecommuniceerd in handen komt van derde partijen. Hierdoor kan het beroepsgeheim geschonden worden. Ongeacht of de verwerking van deze gegevens veilig gebeurt door partijen staat tegenover het feit dat zij de gegevens in handen hebben en daarmee schendt de advocaat zijn beroepsgeheim. In de volgende deelvragen worden de uitkomsten van interviews met o.a. advocatenkantoren toegelicht. Er wordt besproken hoe advocatenkantoren omgaan met smartphones in de zakelijke context en of zij bewust zijn van de risico's van de apps en of zij denken dat hierdoor het beroepsgeheim wordt geschonden.

⁹⁶ LJN: 2006, 248, 5-04-2006, www.rechtspraak.nl

⁹⁷ ‘Regels voor advocaten’ www.advocatenorde.nl (zoek op: *beroepsgeheim*)

⁹⁸ D.J. Hesermans, *Advocatenwet*, Deventer: Kluwer 2009 pag. 174

⁹⁹ D.J. Hesermans, *Advocatenwet*, Deventer: Kluwer 2009 pag. 175

¹⁰⁰ F.A.W. Bannier, N.A.M.E.C. Fanoy, J.M. Tempelaar, W.L.J.M. Duijst, A.P.H. Meijers, *Beroepsgeheim en verschoningsrecht*, Sdu Uitgevers: 2008

In het empirische gedeelte van het onderzoek worden de deelvragen beantwoord op basis van de uitkomsten uit de interviews. Drie verschillende beroepsgroepen zijn geïnterviewd: experts op het gebied van ICT recht en/of privacy, advocatenkantoren en app-ontwikkelaars. Bij elke beroepsgroep wordt in het begin toegelicht waarom er is gekozen voor twee personen/kantoren per beroepsgroep en waarom deze een goed beeld van de werkelijkheid kunnen geven. Bij de experts worden risico's van apps vastgesteld en een analyse gemaakt tussen werkelijkheid volgens de experts en de theorie binnen het onderzoek. Binnen de advocatenkantoren wordt de huidige situatie vastgesteld en vergeleken met een daaropvolgende analyse tussen de huidige situatie en het beroepsgeheim volgens de theorie. Tot slot worden de app-ontwikkelaars behandeld. Hier wordt de huidige situatie van de twee bedrijven vastgesteld en vergeleken en er wordt een analyse gemaakt tussen het handelen van de app-ontwikkelaars volgens de interviews en de praktijk. Voor de leesbaarheid van het onderzoek en de structuur van de drie onderzoeksobjecten wordt er per onderzoeksobject door middel van deelvragen de vergelijking, vaststelling en apart de analyse behandeld. Tot slot wordt in deelvraag 7.1 een overkoepelende analyse gegeven op basis van de verkregen gegevens welke zijn verkregen door de drie onderzoeksobjecten.

4.1 Deelvraag 4.1 De experts

Om deze deelvraag te kunnen beantwoorden zijn er interviews gehouden met Janneke Sloetjes advocaat en medewerkster van Bits of Freedom en Aramis Jean-Pierre, functionaris gegevensbescherming bij DUO. De uitwerkingen van de interviews zijn terug te lezen in bijlage 16 en 17.

Wat zijn de risico's en de eventuele privacyproblemen van apps?

Bij het benaderen van experts hebben twee van de vier benaderde experts aangegeven dat zij tijd hadden om mee te werken aan mijn onderzoek. De experts waarmee de interviews zijn gehouden, zijn gezien hun functie en werkveld absoluut experts op het gebied van privacy (en apps). Hierdoor hebben zij een goed beeld kunnen geven van de werkelijkheid wat betreft de privacyrisico's van apps. De meerwaarde om nog een derde te interviewen is er hierdoor niet.

Volgens Janneke Sloetjes is het grote risico van apps dat deze grote hoeveelheden persoonsgegevens kunnen verzamelen en deze opslaan op de servers. Sommige organisaties geven geen duidelijkheid waar hun servers staan, wat er gebeurt met de gegevens en wie er toegang tot hebben. Daarnaast speelt de onwetendheid van de gebruikers een rol, zij drukken vaak zonder goed te lezen op 'accepteren' en weten daardoor niet wat ze nou precies hebben geaccepteerd en wat er gebeurt met de gegevens. Toch kunnen gebruikers niet alles kwalijk worden genomen, veel apps zijn onduidelijk qua uitleg waarvoor zij de gegevens gebruiken of waar de gegevens worden opgeslagen. De servers staan wereldwijd en de meeste gegevens worden verknipt en over de hele wereld verstuurd. De bedrijven weten hierdoor ook niet altijd waar gegevens staan. Aramis Jean – Pierre is van mening dat vooral gratis apps zoals spelletjes veel risico's met zich mee dragen, hij ziet deze apps vooral als doorgeefluik die grote hoeveelheden informatie doorsturen naar de bedrijven achter de apps. Het is mogelijk dat een gebruiker op zijn toestel 9 veilige apps heeft staan maar dat 1 app onveilig is en alsnog informatie kan doorsturen. Daarnaast zijn gratis apps geen gratis apps, deze bedrijven achter de apps verzamelen gegevens via de apps van gebruikers welke deze bedrijven kunnen doorverkopen (voor commerciële doeleinden).

Volgens Janneke Sloetjes handelen de meeste app-ontwikkelaars volgens de regels en de meeste apps ook, desondanks zijn er ontwikkelaars en landen die kwaad willen en onprofessioneel handelen. Wanneer data op het grondgebied van de VS komen, mogen deze op grond van de Patriot Act de data doorzoeken wanneer de inhoud van de data verdacht wordt van terrorisme. Men gaat er van uit dat dit niet met de nodige terughoudendheid gebeurt. Dit kan een groot risico zijn wanneer een ontwikkelaar kwade bedoelingen heeft met de verkregen gegevens. Een groot risico is de onwetendheid van de burger, de overheid en soms de app-ontwikkelaar zelf. Janneke Sloetjes deelde

in het interview een eigen ervaring met LinkedIn. LinkedIn heeft in haar app geen toestemming aan de gebruiker gevraagd om te synchroniseren met de kalender in de telefoon, maar zij deden dit wel. LinkedIn had een machtiging waar zij, als gebruiker, niks van af wist. Een aantal dagen later was er een groot datalek waarbij duizenden gegevens op straat kwamen te liggen. Ondanks dat zij zelf op de hoogte is van de gevaren van apps is het haar zelf ook overkomen. Burgers, overheden en bedrijven zijn zich wel steeds meer bewust van de gevaren van apps gezien de berichten in het nieuws. Overheden en bedrijven staan tegen overelkaar op het gebied van gegevensverzameling. Overheden staan in een tweestrijd, want zij hebben de plicht om de burger te beschermen en tegelijkertijd weten ze dat bedrijven geld moeten blijven verdienen, ook al gebeurt dit door middel van verkoop van persoonsgegevens. Grote multinationals zoals Google, Facebook en Microsoft hebben een charmeoffensief gestart tegen de overheid die in hun ogen (ook) verkeerd omgaat met de gegevens van burgers¹⁰¹. Dit is erg tegenstrijdig omdat juist deze bedrijven zelf meerdere malen zijn 'beschuldigd' van het verwerken van gegevens in strijd met de privacy. Bits of Freedom ziet wel oplossingen in het bestrijden van de risico's van apps vanuit de overheid, waaronder meer bewustwording naar de consument toe. Daarnaast moet er beter toezicht worden gehouden door bijvoorbeeld de OPTA of het Cbp. Bedrijven en app-ontwikkelaars moeten duidelijker zijn qua doelbinding, de consument moet op de hoogte gebracht worden welke gegevens er worden verzameld en wat er precies mee gebeurt. De overheid zelf kan de burger meer bewuster maken van de gevaren en tegelijkertijd moet de overheid er ook voor zorgen om zelf op een nette manier met persoonsgegevens om te gaan. Veel instanties van de overheid hebben vaak toegang tot gegevens waar zij niks mee te maken hebben. Kortom, het grote risico blijft de onwetendheid van alle partijen waar gegevens worden verwerkt, opgeslagen en wie toegang heeft tot gegevens. Daarnaast is het toezicht houden vanuit de overheid belangrijk op deze praktijken. Alleen het feit dat de overheid zelf 'faalt' maakt toezicht houden lastig en tegenstrijdig. Volgens Aramis Jean – Pierre wordt alles makkelijk geaccepteerd, apps zijn compleet ingespeeld op het gebruiksgemak. Hierdoor vergeten of negeren mensen de risico's die eraan kleven. Desondanks is er een snelle technologische ontwikkeling gaande en mensen zijn zich, dankzij de berichten in de media, bewust van de risico's. De wetgeving is ook bezig te veranderen (zie deelvraag 1.) de Europese Commissie is bezig om een nieuwe verordening in te voeren welke onze Wbp gaat vervangen. De verordening is strikter dan de Wbp en wordt volgens Aramis Jean – Pierre als het ware een "track en trace systeem". Als burgers moeten we eigenlijk gaan accepteren dat onze gegevens overal naar toegestuurd worden. Dit kunnen we door de snelle technologische ontwikkelingen niet meer tegenhouden. Door het track en trace systeem kunnen we in de toekomst wel bijhouden waar onze gegevens zich bevinden en wie daar inzicht in hebben. Aangezien een aantal lidstaten tegenwerken komt hopelijk deze verordening in mei 2016. Bedrijven willen zich ook blijven ontwikkelen op technisch gebied en moeten hierdoor onder andere goed hun beveiliging omtrent de verzamelde persoonsgegevens regelen. Ze lopen hierbij tegen de Wbp aan en hebben moeite om dit goed in hun systeem te implementeren. In de Wbp staan namelijk termen welke een ruimte interpretatie hebben zoals: "zorgvuldig". In de ogen van een organisatie staat het implementeren van de Wbp ook niet op de eerste plaats, omdat ze hierdoor tijd en geld moeten investeren in iets waar ze geen geld aan kunnen verdienen. Deze bovenstaande informatie komt uit de twee interviews. In de volgende deelvraag worden belangrijke punten meegenomen voor de analyse.

Deelvraag 4.2

Wat leert ons de vergelijking tussen de werkelijkheid volgens de experts en de theorie binnen dit onderzoek?

Deze deelvraag is compleet gewijd aan de analyse tussen de uitkomsten van de interviews in deelvraag 4.1 en de theorie welke in het onderzoek is behandeld. De theorie binnen dit onderzoek bestaat uit twee delen: een aantal onderzoeken (deelvraag 2.) en verschillende wet- en regelgeving

¹⁰¹ 'Global Government Surveillance Reform' www.reformgovernmentsurveillance.com

die toepassing heeft op de voorwaarden, handelen van apps en het beroepsgeheim. De verschillende toepasbare wet- en regelgeving is: Europese Richtlijnen, Boek 6 titel 5 afdeling 3 (algemene voorwaarden), Wbp, Tw., Advocatenwet, Gedragscode Advocaten en richtlijnen van de NCSC. In deze deelvraag worden de resultaten uit de onderzoeken en de wet- en regelgeving vergeleken met de werkelijkheid volgens de experts waarmee de interviews zijn gehouden.

Door de interviews met experts zijn er een aantal belangrijke punten naar voren gekomen welke als problemen en risico's in de praktijk kunnen worden aangemerkt. Volgens de experts:

- Is er een snelle technologische ontwikkeling gaande waardoor de wetgeving betreffende privacy moet worden aangepast;
- Moeten niet alleen app-bedrijven maar ook andere bedrijven maatregelen uit de Wbp implementeren in hun processen, dit wordt helaas niet altijd goed gedaan vanwege de moeite met o.a. de interpretatie;
- Is er onduidelijkheid naar de gebruikers toe vanuit de apps, welke gegevens worden verwerkt, waar ze worden opgeslagen en wat ermee gebeurt;
- Moeten apps duidelijker het doel voor de gegevenswerking toelichten (doelbinding);
- Zijn gratis apps niet gratis maar een doorgeefluik die gegevens naar bedrijven achter de apps sturen welke zij voor veelal commerciële doeleinden kunnen gebruiken;
- Zijn burgers op de hoogte van risico's maar weten ze niet precies welke risico's het zijn en mede door het gebruiksgemak van apps, wordt dit genegeerd;
- Heeft de overheid (Cbp of OPTA) als taak om meer toezicht houden hoe er met gegevensverwerking wordt omgegaan, zowel door bedrijven als de overheid zelf.

Uit zowel de onderzoeken als de interviews, is naar voren gekomen dat onwetendheid van de burger op het gebied van de installatievoorwaarden een grote rol speelt. Wat betreft de risico's die aan apps kleven op het gebied van privacy is de gebruiker wel op de hoogte van sommige risico's maar gezien het gebruiksgemak en enigszins goed vertrouwen, wordt dit genegeerd. De persoonsgegevens die apps verzamelen gaan volgens het onderzoek van Channel 4 de hele wereld over, hier is de wetgeving niet compleet op ingesteld. Er is een discrepantie tussen de wetgeving in Europa en daarbuiten. Europa en de VS hebben al een begin gemaakt met het Safe Harbor Principe, zodat gegevensverkeer tussen Europa en de VS op een goede manier wordt verwerkt die voldoet aan de Europese privacyrichtlijn. Volgens experts weten alleen bedrijven in de VS niet altijd of de gegevens naar de VS worden getransporteerd of naar andere servers over de wereld. Gegevens worden namelijk vaak verknipt en naar servers wereldwijd gestuurd. De uitkomsten van de experts en de onderzoeken uit deelvraag 2 hebben overeenkomsten. De onderzoekers zoals de artikel 29-werkgroep, het Cbp, Troy Hunt en Channel 4 waarschuwen dat apps privacyrisico's hebben en dat de doelbinding vaak niet wordt nageleefd, dit wordt ook bevestigd door de Janneke Sloetjes. Qua uitkomsten zitten de experts en de andere onderzoekers op een lijn. Er zit wel een verschil tussen de wetgeving en de werkelijkheid volgens de experts. In de werkelijkheid worden gegevens namelijk anders verwerkt dan wettelijk is toegestaan. In deelvraag 1. Subvraag c is door de onderzoeker zelf geconstateerd dat bepaalde handelingen van apps niet stroken met de Europese dan wel Nederlandse wet- en regelgeving. Dit is een directe toetsing van de feiten aan de wet. De experts geven zelf een brede context over de privacy van apps, ze toetsen het zelf niet concreet aan bepaalde wetgeving. Wel is gesteld dat bij de verwerking van persoonsgegevens er vaak geen doelbinding is (art. 7 Wbp), in tegenstelling wat de volgens de wet is voorgeschreven. Door de onderzoeker zelf is zoals eerder vermeld wel feitelijk getoetst in deelvraag 1 subvraag c.

4.2 Deelvraag 5.1 De advocatuur

Om de volgende deelvragen te kunnen beantwoorden zijn er interviews gehouden met medewerkers van twee kantoren in Groningen. Allereerst met mr. T.J.J. Bodewes, advocaat bij BoutOveres en ten tweede met G.J. Veldthuis, IT Manager bij TRIP Advocaten en notarissen. De uitwerkingen van de interviews zijn terug te lezen in bijlage 18 en 19.

Hoe wordt er binnen advocatenkantoren rekening gehouden met het gebruik van apps en de eventuele risico's?

Allereerst wil ik stellen dat ik mij er van bewust ben dat deze twee interviews een gering aantal bronnen is om een huidige situatie van de gehele advocatuur binnen Nederland vast te stellen. Bij het benaderen van vijf kantoren heb ik aangegeven met een advocaat te willen spreken. Twee kantoren hebben mijn verzoek geaccepteerd. Bij TRIP Advocaten is de IT manager naar voren geschoven aangezien de advocaten binnen TRIP weinig van smartphones en apps afweten (aldus TRIP). Dit statement bevestigt eigenlijk al mijn vermoedens dat er weinig kennis en bewustzijn is wat betreft apps, onder de advocaten zelf. Desondanks konden beide kantoren een goed beeld geven hoe er binnen middelgrote kantoren met smartphones wordt omgegaan. Daarnaast vonden ze beiden dat zij het meest van smartphones wisten binnen het kantoor. Hierdoor kan ik stellen dat ondanks dat ik maar met weinig kantoren contact heb gehad de resultaten indicatief zijn binnen de advocatuur.

Advocaten gaan over het algemeen op dezelfde manier met smartphones om zoals ieder ander, het is niet omdat zij advocaat zijn bij het downloaden van een app alle gebruiksvoorwaarden op de letter doornemen en uitpluizen. Binnen advocatenkantoren wordt er door de medewerkers veel gebruik gemaakt van smartphones. Bij BoutOveres schaft ieder zijn eigen telefoon aan en gebruikt deze zowel zakelijk als privé. Bij TRIP krijgt elke medewerker een iPhone en iPad van de zaak om zakelijk en privé te gebruiken.

Wat betreft het gebruik van apps gaan advocaten daar 'normaal' mee om. Binnen de kantoren is iedereen zich er van bewust dat het gebruik van apps risico's met zich mee kunnen brengen, maar wat deze risico's precies zijn is niet bekend bij de advocaten. Wel weten kantoren dat sommige apps e-mails of contactgegevens kunnen lezen en verwerken, maar wat ze vervolgens met deze gegevens doen is tevens niet duidelijk voor de kantoren.

Bij TRIP worden alle medewerkers voorzien van een iPhone en iPad, hiervoor heeft TRIP huisregels opgesteld hoe de medewerkers netjes met de devices om moeten gaan. Alle devices moeten zijn beveiligd met een toegangscode en centraal worden alle devices beveiligd door Mobile Iron. Wat betreft apps is TRIP (nog) niet actief bezig om bepaalde apps te verbieden voor medewerkers, de reden is vooral omdat zij het eerst wat aantrekkelijk willen maken voor iedereen om de luxe devices te gaan gebruiken voordat er meteen strenge regels worden opgelegd met betrekking tot het gebruik. Mochten er apps in de toekomst als risicovol worden bestempeld door TRIP, dan kan TRIP centraal met behulp van Mobile Iron regelen dat de apps worden geblokkeerd voor alle werknemers. Daarnaast kunnen alle werknemers toegang krijgen tot de servers van TRIP met alle dossiers door middel van een app die voor TRIP is ontwikkeld. De verbinding is hier wel extra beveiligd door middel van een SSL verbinding en een wachtwoord.

Vergelijking gegevens en vaststellen huidige situatie: Op basis van de interviews kan geconcludeerd worden dat het ene kantoor anders met smartphones om gaat dan het andere kantoor. Het is duidelijk uit de interviews dat er wel enig bewustzijn is met betrekking tot de risico's binnen de advocatuur. Wat de risico's precies zijn en wat er met verzamelde gegevens gebeurt is beide kantoren onduidelijk. TRIP probeert de risico's enigszins in te perken door de beveiliging op de devices 'maximaal' te regelen en huisregels op te stellen voor het gebruik. Desondanks kan er een kanttekening worden geplaatst bij de beveiliging van de app welke toegang tot de dossiers geeft. Een SSL verbinding zorgt ervoor dat 'niemand' van buiten in de verbinding kan komen. Wanneer een app

toegang heeft tot de keylog van de app kan deze alsnog bij de dossiers. Bij BoutOveres wordt er niets gedaan, terwijl 'bijna' iedereen daar ook een smartphone gebruikt. Bij BoutOvers wordt overigens niet alles over de smartphone gedaan, veel communicatie loopt via de vaste lijn en email op de PC. Beide kantoren vinden dat advocaten een eigen verantwoordelijkheid hebben om op een nette en betrouwbare manier met gegevens om te gaan. Mijn inziens hebben advocaten inderdaad hun eigen verantwoordelijkheid maar vanwege een gebrek aan kennis lopen ze onbewust toch risico's. De advocatuur moet proactief hun geheimhoudingsplicht bewaken en de kans op schending voorkomen.

Deelvraag 5.2

Welke relatie is er tussen het gebruik van apps door de kantoren en het beroepsgeheim van advocaten?

Bij beide kantoren zien advocaten het beroepsgeheim als een eigen verantwoordelijkheid in het ambt van een advocaat. Een advocaat moet zelf de afweging kunnen maken op wat voor manier hij met gegevens omgaat van cliënten. Advocaten ervaren nog geen problemen bij het uitoefenen van het beroepsgeheim in relatie tot het gebruik van apps. Ze zijn van mening dat wanneer apps toch aan informatie komen, deze op een nette manier verwerken en dat het voor een derde lastig is om aan die informatie te komen. Het is de kantoren ook nog niet bekend of er informatie is gelekt bij henzelf of andere kantoren. Het kan voorkomen dat de apps gegevens verwerken maar wanneer deze gegevens nergens opduiken is het "ook niet heel erg". Bij BoutOveres worden zaken met groot en vertrouwelijk belang vooral gecommuniceerd via de mail op de PC, face-to-face en de vaste lijn, mobiele telefoons worden dan enigszins vermeden. Bij TRIP proberen ze de gegevens zo goed mogelijk te beschermen door middel van een centraal beveiligingssysteem en huisregels.

In deze analyse worden tevens de uitkomsten uit deelvraag 5.1 meegenomen. Beide kantoren kunnen een goed beeld geven hoe er binnen het kantoor met smartphones wordt omgegaan. Daarnaast vonden beide medewerkers dat zij het meest van smartphones wisten binnen het kantoor. De keuze voor twee kantoren is gedaan om de huidige situatie vast te stellen en de hypothese te bevestigen. Beide kantoren vinden dat het beroepsgeheim een eigen verantwoordelijkheid van de advocaat is. Dit standpunt kan bevestigd worden door regel 6 sub 2 Gedragscode 1992 Advocaten (bijlage 16, regel 6); zie "naar zijn oordeel" en "goede beroepsuitoefening". Volgens de Gedragscode is een advocaat in staat om zelf zijn verantwoordelijkheid te nemen en te bepalen wanneer informatie (in overeenstemming met cliënt) wel of niet naar buiten kan treden. Wanneer er gegevens worden verzameld en naar derden worden verstuurd, zijn beide kantoren van mening dat dit op een nette manier gebeurt. Wanneer er wordt gekeken naar regel 6 Gedragscode 1992 Advocaten is een advocaat verplicht tot geheimhouding over alles wat met zijn cliënt te maken heeft. Gezien de onderzoeken in de theorie is het mogelijk dat er inmiddels via de toestellen van advocaten gegevens, zonder ondubbelzinnige toestemming, zijn verwerkt omtrent hun cliënt. De kantoren stellen dat zij er vanuit gaan dat deze gegevens veilig worden verwerkt en opgeslagen, alleen realiseren zij zich niet dat conform het beroepsgeheim het verwerken van gegevens zonder toestemming van de cliënt al in strijd is met het beroepsgeheim. Los van het feit dat de verwerking op een 'nette' manier gebeurt en er nog geen gegevens zijn gelekt.

In subvraag a. is onderzocht dat het installeren van een populaire app zoals Facebook meer risico's met zich meebrengt dan dat de gebruiker in eerste instantie denkt. De gebruiker wordt bij de installatie op de hoogte gebracht welke gegevens de app verzamelt. In de praktijk verzamelen en verspreiden de apps meer dan zij in de voorwaarden verklaren en beseffen de gebruikers niet wat de impact is van hun goedkeuren. Uit eerdere onderzoeken die zijn te lezen in deelvraag 2. is dit gebleken. In het onderzoek van Channel 4 kwam uitdrukkelijk naar voren dat apps zonder dat ze actief gebruikt worden informatie van en naar servers blijven versturen. Internetarchitect Troy Hunt heeft gewaarschuwd dat apps spyware met zich mee kunnen dragen die veel gegevens uit het toestel kunnen doorsturen. Daarnaast spelen internetcriminelen een rol als het gaat om het stelen of onderscheppen van gegevens.

De kantoren zijn alleen niet op de hoogte van deze risico's van apps. Dit brengt het gevaar met zich mee dat het beroepsgeheim kan worden geschonden zonder dat de advocaat daarvan op de hoogte is. Misschien heeft een derde partij in eerste instantie niet veel aan de persoonsgegevens van een cliënt. Dit argument wordt tevens door de kantoren gebruikt dit kan worden ontkracht door het feit dat een advocaat conform het beroepsgeheim nooit gegevens over de cliënt aan een derde mag verstrekken zonder zijn/haar toestemming. Gezien de uitkomsten van dit onderzoek in de vorige deelvragen kan gesteld worden dat dit gebeurt en in strijd is met het beroepsgeheim van de advocaat.

4.3 Deelvraag 6.1 De app-ontwikkelaars

Om deze deelvragen te kunnen beantwoorden zijn er interviews gehouden met twee medewerkers: Huibert Scholtens van Peperzaken en Alexander Postma van Appademic. De uitwerkingen van de interviews zijn terug te lezen in bijlage 20 en 21.

In hoeverre houden app-ontwikkelaars zich bezig met de privacy van vertrouwelijke informatie in in app bezig?

Allereerst wil ik stellen dat net als bij de experts en advocatenkantoren twee van de vier benaderde app-ontwikkelaars wouden meewerken aan dit onderzoek. De gegevens welke doormiddel van de interviews zijn verzameld vertonen veel overeenkomsten. De oorzaak hiervan is dat app-ontwikkelaars op veel fronten dezelfde werkzaamheden uitvoeren en alleen puur praktisch kijken naar de technische mogelijkheden en de wensen van de klant. Bijvoorbeeld het aanbieden van een app in een platform kan maar op één manier gebeuren. Hoe dat gebeurt wordt in deelvraag 6.2 verder uitgelegd. Het interviewen van twee app-ontwikkelaars is hierdoor voldoende geweest om de benodigde informatie voor dit onderzoek te verzamelen.

Bij het ontwikkelen van een app is het afhankelijk van de soort app die wordt gebouwd. De ene app is er alleen om informatie te geven aan de gebruiker terwijl de andere app zoals Facebook grote hoeveelheden data verzameld. Bij de eerste soort apps geeft de app-ontwikkelaar aan zich niet veel bezig te houden met privacy, maar bij de tweede soort apps wel.

Wat app-ontwikkelaars veel loggen zijn locatiegegevens die door een app worden verwerkt. Wanneer een gebruiker een jaar lang een app gebruikt die locatiegegevens verzameld kan de ontwikkelaar uittekenen waar die persoon zich het hele jaar door in Nederland heeft bevonden. De app-ontwikkelaar kan in een app een link bouwen waarmee de gebruiker via de app kan inloggen in Facebook, dan kan de app-ontwikkelaar alle gegevens verzamelen die de persoon op Facebook heeft staan. De app-ontwikkelaars krijgen vaak opdrachten van bedrijven om een app te bouwen, dan moet de ontwikkelaar zich houden aan de eisen die de opdrachtgever stelt. Het beheer van de app kan dan bij hen liggen of wordt later overgedragen aan het bedrijf zelf. Wanneer de ontwikkelaar de app beheert kan deze o.a. locatiegegevens, UDID etc. verzamelen. Het hangt er vanaf waarvoor de app in dat geval gemachtigd is.

Vergelijking gegevens en vaststellen huidige situatie: Beide ontwikkelaars geven aan zich te houden aan de privacy van vertrouwelijke informatie in de app. Ze weten dat er privacyrisico's kleven aan apps maar welke weten ze niet precies. Ze willen het ontwikkelen van een app volgens de wet doen, wanneer zij dit niet doen heeft dat voor henzelf consequenties zoals een slechte naam. Tegelijkertijd doen ze geen moeite om juridische kennis wat betreft apps op te doen. Ze geven beide aan dat de mogelijkheden bij het ontwikkelen van een app eindeloos zijn en wanneer iemand kwaad wil kan deze dat voor elkaar krijgen. Wanneer de interviews tussen de app-ontwikkelaars worden vergeleken valt het op dat er veel overeenkomsten in de uitkomsten zijn. Beide ontwikkelaars geven aan dat ze de privacy van het verwerken van gegevens belangrijk vinden.

De app-ontwikkelaars hopen gezien de manier waarop zij werken dat het ontwikkelen van een app op een veilige manier gebeurt. In hun perspectief hoeft er niet veel te veranderen, alleen dat er meer toezicht komt op het aanbieden van apps in bijvoorbeeld de Android Store. Het is relatief makkelijk om hier een app aan te bieden zonder dat deze volledig wordt gecontroleerd. Hier zouden ontwikkelaars met een 'slecht geweten' misbruik van kunnen maken en app-ontwikkelaars in het algemeen een slechte naam kunnen geven. App-ontwikkelaars hebben op het gebied van apps meer kennis dan advocaten. Zij zijn zich meer bewust van de risico's van apps en weten dat een app meer gegevens kan verzamelen dan wettelijk is toegestaan. De app – ontwikkelaars binnen het onderzoek geven aan te denken dat ze op een nette manier met de verkregen gegevens om te gaan en geen apps bouwen die gegevens verzamelen op een manier die in strijd is met de wet. Maar beiden hebben niet de juridische expertise in huis om daar een uitspraak over te kunnen doen, anders dan dat ze naar hun eigen morele standaard denken netjes te handelen.

Deelvraag 6.2

In hoeverre hebben app-ontwikkelaars invloed op de voorwaarden die platforms stellen wanneer zij een app willen aanbieden op het platform?

Een app-ontwikkelaar heeft geen invloed op de voorwaarden die platforms stellen. De voorwaarden staan van tevoren al vast en daar heeft de ontwikkelaar zich aan te houden. Er is wel een verschil in het aanbieden van apps bij verschillende platformen.

De app-ontwikkelaars bieden hun apps vrijwel altijd aan in de App Store en/of Google Play Store. Deze Stores hanteren jegens de ontwikkelaar verschillende voorwaarden en regels. Volgens de ontwikkelaars is Apple strenger in het controleren van apps dan Android.

De verschillen in het aanbieden zijn als volgt: wanneer een app klaar is wil de ontwikkelaar deze zo snel mogelijk op de markt brengen. Als de ontwikkelaar de app bij de App Store wil inschieten gaat Apple eerst de hele app doorlichten. Hiervoor gebruiken ze de source code die de ontwikkelaar beschikbaar moet stellen anders kan de app niet worden gecheckt. Apple hanteert veel voorwaarden waaraan de app moet voldoen. Zo zijn er voorwaarden omtrent: privacy, kinderen, pornografie, geweld, etc. Apple neemt een week de tijd om de app te controleren. Wanneer de app voldoet aan Apple haar voorwaarden, mag de app in de App Store worden gelanceerd. Als de app niet voldoet krijgt de ontwikkelaar deze terug met de opmerking wat er veranderd moet worden, na verbetering kan de ontwikkelaar de app alsnog aanbieden. Vanaf het moment dat de app naar Apple wordt gestuurd tot en met het moment van lancering kan door het controleren minimaal een week duren. Bij Android gaat het er 'makkelijker' aan toe. De app wordt bij het platform ingeschoten als deze klaar is en binnen een uur kan de app online staan en klaar om te downloaden. De app wordt door Android van tevoren niet compleet doorgelicht zoals bij Apple.

Vergelijking gegevens en vaststellen huidige situatie: Beide ontwikkelaars geven aan op dezelfde manier apps aan te bieden in de Store. Aangezien de Stores zelf regels hebben hoe een app moet worden aangeboden is dit voor iedereen gelijk. Beide partijen kunnen daarom ook geen invloed uitoefenen in het aanbieden van apps. Volgens Appademic wordt er automatisch wel gecontroleerd op een aantal zaken maar niet intensief. Als de app vervolgens wat langer in de Store staat en/of populairder wordt, gaat Android controleren. Mocht de app dan niet aan voorwaarden voldoen wordt deze uit de Store verwijderd. Het risico is wel dat in de tussentijd de app al gedownload kan zijn door gebruikers.

Deelvraag 6.3

Zijn er overeenkomsten en verschillen tussen het handelen van de app-ontwikkelaar in de praktijk en de resultaten uit de theorie?

In deze analyse worden de uitkomsten uit deelvraag 6.1 en 6.2 meegenomen. Er kan worden vastgesteld dat beide app-ontwikkelaars veel overeenkomsten hebben in zowel de manier van apps aanbieden als het ethische aspect op het gebied van privacy. In de theorie in deelvraag 1, subvraag 2 is in afbeelding 2 een weergave gegeven van het aanbieden van apps. De app-ontwikkelaars volgen beiden de verschillende manieren van aanbieden. Zoals eerder geconcludeerd is dit logisch aangezien zij zich hebben te houden aan de regels van de Stores. In de theorie is duidelijk naar voren gekomen dat apps meer gegevens verzamelen dan dat nodig is en wettelijk is toegestaan. Terwijl beide app-ontwikkelaars in de interviews aangeven dat zij netjes met de privacy van gebruikers omgaan en de app zo veilig mogelijk willen ontwikkelen. Hier ontstaat mijns inziens een breuk tussen de theorie en de uitkomsten van de interviews. In de theorie is op basis van onderzoek vastgesteld dat apps, behalve als de telefoon uit staat, gegevens verwerken. Veel apps zullen gegevens verwerken op een 'nette' manier en sommige gegevens zullen geen persoonsgegevens bevatten, maar technische aspecten van de app. Bij de interviews geven de ontwikkelaars aan netjes om te gaan met privacy en de app op een veilige manier te bouwen. Hoe kan het dan dat er toch veel ontwikkelde apps ondanks wat er in de wet staat zich er niet aan houden? Mogelijke antwoorden zijn: de interviews zijn gehouden met twee betrouwbare app-ontwikkelaars of de app-ontwikkelaars hebben in de interviews gezegd dat ze zich houden aan privacywetgeving, maar aan de achterkant worden er toch (bewust of onbewust) gegevens verwerkt. De verantwoordelijkheid ligt meestal niet bij de app-ontwikkelaar, aangezien zij meestal in opdracht een app ontwikkelen en het beheer van deze app later overdragen naar het bedrijf zelf. In dat geval is het bedrijf zelf verantwoordelijk voor de verwerking van de gegevens door de app. De ontwikkelaars geven ook aan dat de algemene voorwaarden door de bedrijven zelf worden opgesteld en zij daar geen invloed op kunnen uitoefenen. Wanneer zij zelf een app ontwikkelen moeten de gebruiksvoorwaarden voldoen aan de Wbp, hierdoor geven de gebruiksvoorwaarden de ontwikkelaars ook niet de mogelijkheid om bijvoorbeeld de geheimhoudingsplicht van de advocaten te schenden. Theoretisch gezien is het mogelijk dat apps veel gegevens verwerken die niet in overeenstemming zijn met de wet. Alleen de app-ontwikkelaars in de interviews geven aan dit niet te willen, aangezien hun naam wordt aangetast wanneer ze dit doen.

Deelvraag 7.1

Wat leert ons de vergelijking van de resultaten van elk van de drie onderzoeksobjecten?

Het antwoord op deze deelvraag bevat een overkoepelende analyse van de resultaten tussen alle drie de onderzoeksobjecten welke in dit onderzoek zijn gebruikt. Bij elk onderzoeksobject is een huidige situatie vastgesteld op basis van de uitkomsten van de interviews. Daarna zijn deze uitkomsten geanalyseerd met (een deel uit) de theorie. In de overkoepelende analyse worden alle drie de vastgestelde huidige situaties vergeleken zonder de daaropvolgende analyse. De reden is omdat elke analyse met een verschillend deel uit de theorie is vergeleken. De experts hebben aangegeven dat de kern van het probleem ligt in het feit dat er een grote onwetendheid is bij de burgers (en daarmee ook advocaten) op het gebied van de precieze gegevensverwerking door apps. Dit komt automatisch doordat apps vanuit hun kant niet goed de voorwaarden en risico's presenteren richting de gebruiker. Hierdoor is er sprake van een grote miscommunicatie tussen de gebruiker en de apps. Desondanks weten veel gebruikers dat er risico's aan apps kleven, maar welke precies is niet duidelijk. Nevenfactoren zijn de snelle technologische ontwikkeling en het (nu nog) onvoldoende toezicht houden door de overheid op het gebied van apps en gegevensverwerking. Ik zeg "nu nog" aangezien er in de toekomst nieuwe wetgeving aan komt op

dit gebied. Door deze snelle technologische ontwikkeling hebben veel bedrijven ook moeite om hun beveiliging up to date te houden en de maatregelen welke in de Wbp staan beschreven goed te implementeren. Deze uitkomsten kunnen worden bevestigd wanneer er wordt gekeken naar de huidige situatie bij de advocatenkantoren en app-ontwikkelaars. De advocaten weten dat er risico's zijn en dat er gegevens worden doorgestuurd naar de servers van apps, maar ze weten niet in hoe grote mate en of ze daarmee hun beroepsgeheim schenden. De app-ontwikkelaars hebben wel meer kennis van apps dan advocaten. Zij weten dat er risico's zijn bij apps, maar de precieze risico's weten ze zelf ook niet. Bij het bouwen van een app houden ze zich volgens henzelf aan de wetgeving wat betreft gegevensverwerking maar tegelijkertijd geven ze aan dat ze niet volledig op de hoogte zijn van de wetgeving, waaronder de Wbp. Desondanks vinden zij de privacy en veiligheid van verwerking van gegevens belangrijk. Ze krijgen immers een slechte naam wanneer er wordt gepubliceerd dat ze een gevaarlijke app hebben ontwikkeld. Maar zij doen niet anders dan als leek een inschatting maken wat redelijk is en hoe een privacyschending te voorkomen. Wanneer ik de uitkomsten van de experts vergelijk met de app-ontwikkelaars valt mij op dat wat Aramis Jean-Pierre vertelt over dat bedrijven moeite hebben met de interpretatie van de Wbp, klopt. App-ontwikkelaars geven aan dat het ontwikkelen van een app volgens de wetgeving gaat, maar wat de wetgeving precies inhoudt weten ze niet. Privacy en veiligheid van verwerking vinden ze belangrijk maar als ze niet weten hoe de wetgeving werkt kunnen ze ook niet inschatten of ze de privacy wel in acht nemen.

Samenvattend: de experts geven aan dat er risico's zijn bij het gebruik van apps (net als wat in de theorie wordt vermeld). De advocatenkantoren en app-ontwikkelaars bevestigen deze uitkomst door zelf te vertellen dat ze niet weten wat de precieze risico's zijn. De manier waarop advocaten met smartphones omgaan bevestigt dit, tevens met het feit dat zij gegevensverwerking door apps niet direct als schending van het beroepsgeheim zien.

Al met al blijkt, op basis van de theorie en praktijk, dat apps risico's met zich meebrengen. In het volgende hoofdstuk worden conclusies getrokken op basis van de resultaten uit alle hoofdstukken. Uit deze conclusies vloeien aanbevelingen voor Aecius uit.

Dit hoofdstuk vormt het slot van het onderzoeksrapport waar per hoofdstuk de conclusies worden besproken en de daaruit voortvloeiende aanbevelingen voor Aecius Juridisch Advies worden beschreven. De conclusies vloeien voort uit de bevindingen welke in dit onderzoek zijn gedaan en dragen bij aan de beantwoording van de centrale onderzoeksvraag: Welke conclusies zijn er af te leiden uit de in kaart gebrachte problemen en risico's van de (gebruiks)voorwaarden van apps en het handelen daarnaar, in relatie tot het beroepsgeheim van advocaten, blijkens het literatuuronderzoek en interviews?

5.1 Conclusies

Inleiding

Het onderzoek begint met een inleiding waarin verschillende punten van tevoren worden uitgezocht om een inschatting te kunnen maken of het onderzoek haalbaar is. De aanleiding van het onderzoek komt door een vraag vanuit Aecius. Deze vroeg zich af of er problemen zijn bij het gebruik van apps in relatie met de geheimhoudingsplicht van de advocatuur. Het is onduidelijk of advocaten bewust zijn van de problemen en risico's met betrekking tot apps volgens de gebruiksvoorwaarden in relatie tot het beroepsgeheim. Daarnaast is het geval dat mochten er problemen en risico's zijn met betrekking tot de gebruiksvoorwaarden van apps het nog onduidelijk is wat deze problemen en risico's zijn. Uit de formulering van dit probleem is een doelstelling ontstaan welke uit twee delen bestaat en uit het tweede gedeelte de centrale vraag voortvloeit. Om de centrale vraag te kunnen beantwoorden zijn er deelvragen opgesteld verdeeld in drie categorieën: theorie, empirische gedeelte en de analyse. Voordat deze doelstelling en centrale vraag kon worden opgesteld is er een onderzoekskader uitgewerkt. Het moet eerst duidelijk worden waarom dit onderzoek moet worden uitgevoerd. Binnen dit kader is uitgelegd wat de aanleiding is geweest voor dit onderzoek, in welke cyclus het onderzoek kan worden geplaatst, wat de relevantie van het onderzoek is, welke actoren een rol spelen, of er eerdere onderzoeken betreffende dit onderwerp zijn geweest en welke wet- en regelgeving een rol speelt.

Methodologische verantwoording

Het onderzoek gaat over een nieuw onderwerp waar weinig literatuur over te vinden is. Hierdoor is er gekozen voor de inductieve methode. Binnen dit onderzoek zijn er drie onderzoeksobjecten vastgesteld: experts, advocatenkantoren en app-ontwikkelaars, welke door middel van interviews (onderzoeksmethode) informatie verschaffen om de omvang van het probleem duidelijk te krijgen. De reden waarom er voor deze drie onderzoeksobjecten is gekozen, is omdat er op deze manier een beter beeld wordt gecreëerd, aangezien het onderwerp vanuit verschillende perspectieven wordt belicht. De experts zijn het "hoofdobject" binnen dit onderzoek aangezien zij de risico's duidelijk kunnen weergeven, de advocatenkantoren en app-ontwikkelaars zijn er om de huidige situatie vast te stellen. Om de verkregen informatie uiteindelijk te kunnen analyseren vindt er eerst een onderlinge vergelijking van de resultaten plaats met een daarop volgende analyse tussen de resultaten uit het theoretische gedeelte en het onderzoeksgedeelte.

Theorie

Wet – en regelgeving

In de eerste deelvraag is het juridisch kader wat betreft de toepasselijke wet- en regelgeving omtrent apps uitgewerkt. Op zowel Europees als Nederlands niveau is wetgeving die betrekking heeft op apps. Op Europees niveau zijn richtlijnen van toepassing welke in deelvraag 1 zijn toegelicht. Op Nederlands niveau zijn er verschillende rechtsgebieden van toepassing op de voorwaarden en gegevensverwerking van apps. De terminologie welke de voorwaarden presenteren is niet eenduidig richting de gebruiker. Desondanks kunnen de installatie, dan wel gebruiksvoorwaarden juridisch gekwalificeerd worden als algemene voorwaarden. De drie belangrijkste wet – en regelgeving zijn:

De installatievoorwaarden van een app

Er zijn in het onderzoek de installatievoorwaarden van vijf apps op een Android toestel onderzocht: Facebook, Twitter, Whatsapp, Dropbox en Dirkzwager KennisBoek. Het werd al snel duidelijk dat alle apps ten minste toegang tot meerdere functies in het toestel wilden hebben. Van enkele machtigingen is logisch dat ze worden gevraagd, omdat deze de app nodig heeft om te kunnen functioneren. De meeste installatievoorwaarden voldoen in meer of mindere mate niet aan de Nederlandse Wbp gezien het missen van de motivering omtrent de noodzakelijkheid en doelbinding. Het aanbieden van een app loopt via platforms, hoofdzakelijk de App Store en de Google Play Store. Er kan geconcludeerd worden dat beide bedrijven verschillende manieren hanteren in het aanbieden van apps die voor elke ontwikkelaar hetzelfde zijn. De Google Play Store is minder streng dan de App Store. Een app kan daar meteen worden geplaatst en gedownload, waarna er installatievoorwaarden worden gepresenteerd. Bij de App Store wordt app van tevoren volledig doorgelicht. Wanneer deze voldoet aan de voorwaarden van Apple, wordt deze in de Store geplaatst. Bij Apple worden er bij installatie geen installatievoorwaarden gepresenteerd.

De gebruiksvoorwaarden van apps en de praktijk

Naast installatievoorwaarden bij Android hebben alle vijf de apps ook algemene voorwaarden, welke in het onderzoek gebruiksvoorwaarden worden genoemd. Deze voorwaarden zijn van toepassing tussen de gebruiker en de app wanneer de gebruiker de app heeft geïnstalleerd. In het onderzoek zijn per app alle gebruiksvoorwaarden langsgegaan en onderzocht wat de apps daadwerkelijk verzamelen en wat ze precies met de gegevens doen. Daarnaast is het opvallend dat de diensten verklaren dat zij de verzamelde gegevens gebruiken om de service richting hun gebruikers te verbeteren. In de praktijk zijn er bij alle vijf de apps andere conclusies door onderzoekers getrokken, welke zijn terug te lezen in de hoofdtypek¹⁰². Op basis van het onderzoek kan geconcludeerd worden dat de apps op basis van de verkregen Log Data (waar geen uitdrukkelijke toestemming voor wordt gevraagd) toch meer gegevens verzamelen dan de gebruiker door heeft. De diensten verklaren op basis van deze gegevens de service naar de gebruikers te kunnen verbeteren, maar dit is een erg breed argument, waaronder ook de plaatsing van advertenties kan vallen.

Installatievoorwaarden in strijd met Nederlandse wetgeving

In de hoofdtypek zijn de installatievoorwaarden getoetst aan de Nederlandse wetgeving. Inzake wetgeving betreffende algemene voorwaarden kan geconstateerd worden dat wanneer een beding uit de installatievoorwaarden wordt getoetst aan de open norm, deze als onredelijk bezwarend kan worden aangemerkt. Aangezien de verhouding tussen de maatschappelijke (machts)partijen niet gelijk is houdt de de app aanbieder in samenwerking met het platform geen rekening met de belangen van de wederpartij, wat de omschreven problemen in de hoofdtypek als gevolg heeft. Conform de toetsing aan de Wbp kan er geconcludeerd worden dat onderzochte installatievoorwaarden niet uitleggen wat het doel is van de toegang tot een functie in de telefoon en de daaruit te halen gegevens. Mijns inziens is de gegevensverwerking in veel gevallen niet noodzakelijk voor de uitvoering van de apps, Facebook heeft bijvoorbeeld niet altijd toegang tot de camera nodig om in zijn geheel te kunnen functioneren. Op basis van het onderzoek kan geconcludeerd worden dat de apps handelen in strijd met de Wbp, de aard van de gegevens wegen namelijk niet op tegen de noodzaak van de verwerking van de gegevens. Conform de Tw. kan er een kanttekening worden geplaatst bij het feit dat de gebruiker niet zijn gehele vrije wil kan uiten uitsluitend door het accepteren of niet accepteren van de installatievoorwaarden. Er kan bijvoorbeeld niet per machtiging worden ingesteld of de gebruiker wel of niet akkoord gaat.

¹⁰² zie deelvraag 1, subvraag b

Daarnaast wordt de gebruiker niet volledig geïnformeerd over de noodzakelijke inlichtingen voor goede oordeelsvorming.¹⁰³

De machtigingen worden summier beschreven waardoor er betwijfeld kan worden of de beschrijving bijdraagt aan de goede oordeelsvorming. Tevens wordt het vermelden van doeleinden nagelaten door de apps, dit kan geconcludeerd worden op basis van de eerdere resultaten uit het onderzoek. Tot slot kan gesteld worden dat een probleem van de voorwaarden van apps bij het niet motiveren van de doeleinden van de verwerking is. Naast de doelbinding, die veelal mist of onvolledig is, zijn ook andere bedingen in strijd met bepaalde artikelen van de Wbp en wetgeving betreffende algemene voorwaarden.

Problemen en risico's bij het gebruik van apps

Er zijn verscheidene onderzoeken geweest naar risico's bij het gebruik van apps. In de hoofdtekst zijn deze onderzoeken terug te lezen¹⁰⁴. De belangrijkste uitkomsten zijn dat apps in directe verbinding met het Operating System (OS) staan, hierdoor is het eenvoudig voor de app om data te verzamelen in tegenstelling tot een gewone internetbrowser. Beveiligingsexpert Troy Hunt heeft onderzocht dat veel iOS apps spyware met zich meedragen, deze spyware kan bijvoorbeeld het precieze gebruik van de telefoon of andere apps meten. Apple beweert dat zij alle apps voor het plaatsen in de App Store compleet doorlichten. Er kunnen vraagtekens worden gezet of alle apps in de App Store daardoor nog veilig zijn. Apps dragen privacygevoelige informatie over naar o.a. Flurry. Dit bedrijf analyseert de gegevens en verkoopt deze vervolgens door aan advertentiebedrijven. Daarnaast is geconstateerd dat wanneer een persoon ongeveer 30 apps op zijn telefoon heeft staan, er per 24 uur ongeveer 144.000 pakketjes met gegevens naar 315 servers over de hele wereld worden verstuurd. Er kan op basis van deze onderzoeken geconcludeerd worden dat apps in de praktijk enorme hoeveelheden persoonsgegevens verwerken zonder dat gebruikers dit weten en vaak hiervoor meestal niet of nauwelijks hun toestemming hebben verleend. Daarnaast weten gebruikers in het algemeen niet waarvoor hun gegevens worden gebruikt. Het blijkt dat de gegevensverzameling vooral als doel heeft om later te worden doorverkocht.

Het beroepsgeheim in combinatie met apps

Advocaten hebben een wettelijk beroepsgeheim waarbij schending strafbaar is¹⁰⁵. Een advocaat dient zich tevens in te schrijven bij de Orde van Advocaten en moet zich houden aan de eisen welke de Orde stelt. In de Gedragscode 1992 staat het beroepsgeheim voor de advocaat verder toegelicht. Uit de jurisprudentie in de hoofdtekst is gebleken dat advocaten het beroepsgeheim wel eens hebben geschonden, er is nog geen jurisprudentie of het op basis van apps wordt geschonden. De advocaat is verplicht tot geheimhouding¹⁰⁶. Tegenwoordig gebruiken veel advocaten smartphones als zakelijk communicatie middel. Daarnaast gaat steeds meer communicatie via e-mail en soms Whatsapp of SMS. De risico's van smartphones met apps zijn inmiddels duidelijk. Het is zeer waarschijnlijk dat persoonsgegevens van cliënten die over de smartphone worden gecommuniceerd in handen komt van derde partijen. Hiermee schendt de advocaat waarschijnlijk structureel zijn beroepsgeheim doordat zonder toestemming van de cliënt gegevens over hem worden verspreid naar derden.

Empirische gedeelte

De experts

Er zijn interviews gehouden met twee privacy experts waarin belangrijke informatie is vergaard voor de onderbouwing van dit onderzoek. De reden waarom er met twee experts is gesproken is al uitgelegd in deelvraag 4.1. In de hoofdtekst is in deelvraag 4.2 een opsomming gegeven van de belangrijke punten welke in de interviews met de experts naar voren komen. Op basis deze punten

¹⁰³ 'Onderzoek naar de verwerking van persoonsgegevens in het kader van de mobiele applicatie Whatsapp door Whatsapp Inc.' 28 januari 2013, www.cbppweb.nl pag. 30

¹⁰⁴ zie deelvraag 2

¹⁰⁵ artikel 272 Wetboek van Strafrecht

¹⁰⁶ Regel 6 Gedragscode 1992

kan geconcludeerd worden dat de snelle technologische ontwikkelingen ervoor zorgen dat de wetgeving betreffende privacy moet worden aangepast. Daarnaast zijn burgers op de hoogte van risico's alleen weten ze niet precies welke risico's er zijn en door het gebruiksgemak van apps negeren gebruikers deze risico's. Hierbij speelt de overheid ook een rol doordat zij niet genoeg toezichthouden op de gegevensverwerking door bedrijven. Tot slot functioneren apps als doorgeefluik zodat ze gegevens kunnen doorsturen naar bedrijven.

De advocatuur

Er zijn interviews gehouden met een advocaat en een IT Manager bij een advocatenkantoor. Er kan geconcludeerd worden dat advocaten zich niet bewust zijn van de omschreven risico's in de theorie en daarmee zonder dat ze het weten het beroepsgeheim schenden. Er kunnen namelijk cliëntgegevens in handen van derden komen zonder toestemming van de cliënt. De kantoren menen dat dit geen reëel gevaar is aangezien de derde partij, volgens henzelf, niets doet met de gegevens. Deze mening is overigens uitsluitend op een onderbuikgevoel gebaseerd. Een advocaat mag conform het beroepsgeheim nooit gegevens over de cliënt aan een derde verstrekken zonder diens toestemming. De mogelijkheid dat apps cliëntgegevens aan derden verstrekken is dus al voldoende om dit beroepsgeheim te schenden. Gezien de uitkomsten van dit onderzoek in de vorige deelvragen kan gesteld worden dat gegevensverwerking door apps in strijd is met het beroepsgeheim van de advocaat. Er is met een advocaat gesproken en een manager IT van een advocatenkantoor. Ik ben mij er van bewust dat deze twee interviews een gering aantal bronnen is, desondanks konden beiden een goed beeld geven hoe er binnen middelgrote kantoren met smartphones wordt omgegaan. Daarnaast vonden ze beiden dat zij het meest van smartphones wisten binnen het kantoor. Bij kleinere kantoren zal het besef vele malen kleiner zijn. Hierdoor kan ik stellen dat ondanks dat ik maar met weinig kantoren contact heb gehad toch een beeld kan schetsen hoe groot het besef is binnen de advocatuur.

De app-ontwikkelaars

Uit de interviews met de twee app-ontwikkelaars kan geconcludeerd worden dat men aangeeft zich te houden aan de privacy van vertrouwelijke informatie in de app. Ze weten evenwel niet precies welke privacyrisico's er kleven aan apps (net als de gewone burger), maar geven aan dat de technische mogelijkheden bij het ontwikkelen van een app eindeloos zijn. Wanneer iemand kwaad wil, is er altijd een weg. Er zijn veel overeenkomsten in de resultaten van beide gesprekken met de app-ontwikkelaars. De app-ontwikkelaars pleiten beiden voor veiligheid bij het ontwikkelen en in hun perspectief hoeft er niet veel te veranderen, alleen dat er meer toezicht komt op het aanbieden van apps in de Android Store. Op basis van de analyse tussen de theorie en de interviews kan mijns inziens worden geconcludeerd dat er een discrepantie is tussen beide resultaten. In de theorie zijn veel risico's blootgelegd en is gesteld dat apps in het algemeen risico's meedragen. Bij de interviews geven de ontwikkelaars aan netjes om te gaan met privacy en de app op een veilige manier te bouwen. Waarom zijn er dan toch veel apps strijdig met de wet? Mogelijke antwoorden zijn: de interviews zijn gehouden met twee betrouwbare app-ontwikkelaars of de app-ontwikkelaars hebben in de interviews gezegd dat ze zich houden aan privacywetgeving maar in de werkelijkheid worden er toch (bewust of onbewust) onrechtmatig gegevens verwerkt. Ook kan het zijn dat ontwikkelaars een ander beeld van privacy hebben, waarbij ze denken conform de wet te handelen, maar in feite de wet overtreden. De ontwikkelaars hebben namelijk zelf aangegeven geen kennis van het privacyrecht te hebben.

Eindconclusie

Al met al kan geconcludeerd worden dat apps problemen en risico's met zich meebrengen. Deze problemen en risico's zijn: het niet voldoen van de voorwaarden aan de wettelijke regels betreffende algemene voorwaarden, Wbp en Tw. Installatievoorwaarden schenden de open norm en verklaren niet het doel waarvoor de app de gegevens wil verzamelen. Daarnaast zijn veel gegevens die apps verzamelen niet noodzakelijk voor het functioneren van de apps. De verzamelde gegevens worden daarnaast gebruikt voor commerciële doeleinden. Net als gewone gebruikers is de advocatuur zich

niet bewust van de precieze risico's van apps. Het probleem en het risico hiervan is dat de advocaten automatisch het beroepsgeheim kunnen schenden wanneer zij apps op het toestel hebben staan, welke cliëntgegevens verwerken. De aanbevelingen die uit deze conclusie voortvloeien worden in 5.2 uitgelegd.

5.2 Aanbevelingen

De onderstaande aanbevelingen vloeien voort uit de getrokken conclusies en richten zich op het a-gedeelte van de geformuleerde doelstelling aan het begin van dit onderzoek. Het doel van dit onderzoek is: het doen van aanbevelingen aan Aecius Juridisch Advies, betreffende de relatie tussen het gebruik van apps conform de installatie- en gebruiksvoorwaarden en het handelen daarnaar door zowel de gebruiker als de app-ontwikkelaar en de mogelijke schending van beroepsgeheim binnen de advocatuur.

Op basis van de bovenstaande conclusies kunnen de volgende aanbevelingen aan Aecius Juridisch Advies worden gedaan:

- Binnen Aecius het zakelijke gebruik via de smartphone tot het minimum beperken, alsmede het downloaden van apps. Uit dit onderzoek is gebleken dat de vijf onderzochte apps bij cliëntgegevens kunnen komen, verzamelen en verwerken. Daarom raad ik het Aecius af deze apps op het toestel te installeren. Naast deze apps raad ik Aecius aan bij het downloaden van elke app de installatievoorwaarden door te nemen en te bedenken of de app daadwerkelijk nodig is.
- De bekendheid betreffende de risico's van apps is zeer gering en gezien de maatschappelijke relevantie is het belangrijk om deze bekendheid te vergoten. Dit Aecius kan doen door middel van:
 - Seminars en/of workshops geven aan de advocatuur, app-ontwikkelaars en het algemene publiek (bijvoorbeeld op de Hanze aan studenten). Vooral het bewustzijn binnen de advocatuur creëren is erg belangrijk aangezien advocaten nog niet realiseren wat de risico's voor hen inhouden.
 - Samenwerkingen aangaan met app-ontwikkelaars om op voorhand apps te laten voldoen aan wet- en regelgeving.
 - Een artikel schrijven over de risico's van installatie- en gebruiksvoorwaarden van apps en deze publiceren in de media; hierdoor wordt het bewustzijn van de risico's van apps vergroot en verspreid over een groter publiek.
 - Een kopie van dit verslag, dan wel een samenvatting, sturen naar het College Bescherming Persoonsgegevens zodat zij de grote apps als Twitter, Whatsapp, Facebook en Dropbox kunnen sommeren hun voorwaarden en praktijk (in Nederland) aan te passen.
 - Een landing page op de website van Aecius plaatsen met informatie over de risico's van apps.
- Binnen het onderzoek is de situatie binnen twee advocatenkantoren aan het licht gesteld. Mijn aanbeveling naar Aecius is om verder onderzoek te doen binnen meerdere advocatenkantoren naar apps en het bewustzijn van de risico's, om zo een nog breder beeld te krijgen. Uit de resultaten van de vorige twee interviews blijkt dat de advocatuur hier niet veel van af weet. Aecius zou met behulp van dit onderzoek daar gebruik van kunnen maken om kantoren beter te kunnen adviseren. Daarnaast kan er een verder onderzoek worden gedaan naar andere beroepsgroepen met beroepsgeheim en hoe zij met apps omgaan en of ze bewust zijn van de risico's.

Lijst van afkortingen en begrippen

Afkortingen

BW	-	Burgerlijk Wetboek
CBP	-	College Bescherming Persoonsgegevens
EVRM	-	Europees Verdrag van de Rechten van de Mens
GPS	-	Global Positioning System
iOS	-	Interactive Operating System
PC	-	Personal Computer
SMS	-	Short Message Service
Sr.	-	(Wetboek van) Strafrecht
USB	-	Universal Serial Bus
Wbp	-	Wet bescherming persoonsgegevens
Wet BIG	-	Wet op de beroepen in de individuele gezondheidszorg
ICT	-	Informatie- en communicatietechnologie

Begrippen

A

Account	: Term voor het hebben van toegang tot het internet, met het hebben van een gebruikersnaam en wachtwoord.
Android	: Is een (gratis) mobiel operating system (besturingssysteem).

B

Besturingssysteem	: Een pakket computerprogramma's dat ervoor zorgt dat je een computer/smartphone kan gebruiken.
Browser (type)	: Programma waarmee internet en documenten kunnen worden doorzocht (bijvoorbeeld Google Chrome en Safari).
Button	: Een knop of een grafische link afgebeeld op een scherm.

C

Chat	: Online interactieve communicatie, waarbij het mogelijk is een conversatie te voeren door middel van ingetypte teksten.
Cloud – dienst	: Een dienst waardoor gebruikers die erbij zijn aangesloten, persoonlijke data kan plaatsen. De data wordt opgeslagen in een zogehete 'cloud' dit zijn aan elkaar gekoppelde servers waarvan de gebruiker veelal niet weet waar ze bevinden.
Cookies	: Cookies zijn kleine pakketjes informatie die een webserver naar een browser stuurt met de bedoeling dat deze informatie bij het volgende bezoek weer terugkomt. Zo kunnen websites het internetgedrag van de gebruikers bijhouden.

D

Device	: Engelse woord voor "toestel of apparaat".
Disclaimer	: Algemene verklaring op een website waar de rechten en plichten beschreven staan van alle betrokken partijen. Ook kan de disclaimer een partij afwijzen van aansprakelijkheid.
Downloaden	: Digitale gegevens naar eigen apparaat halen vanaf een website of programma.

G

Gebruikersinterface : Manier waarop de gebruiker met het computersysteem communiceert, bijvoorbeeld het gebruik van de muis of hoe een scherm eruit ziet.

I

Implementatie : Invoering en ingebruikname van een nieuw systeem of beleid.

IP – adres : Een uniek identificatienummer van een computer welke is verbonden met het internet.

K

Keylog : Een programma of stuk hardware waarmee o.a. wachtwoorden kunnen worden achterhaald, die eerder zijn ingevoerd.

L

Liked : werkwoord is: “like”. Engelse term voor: “vind ik leuk”. Foto’s of berichten die op Facebook worden geplaatst kunnen gebruikers leuk vinden door op “vind ik leuk” of “like” te drukken.

Log Data : Een log houdt bij wat de leverancier wil dat het bijhoudt. Een log is het vaststellen van gebeurtenissen.

M

micro SD opslag : Is een geheugenkaart in een apparaat. Micro betekent dat het v voor kleine opslag is.

N

Netwerksockets : Manier van verbinden over een netwerk.

Netwerkkode : Code waarmee een netwerk is versleuteld.

O

Opt-in : Is een systeem waarvoor de gebruiker toestemming moet geven dat het systeem bijvoorbeeld commerciële berichten kan sturen.

Opt-out : Bijvoorbeeld bij het afmelden van een mailinglijst. Of het blijven ontvangen van reclamefolders tot dat de gebruiker aangeeft er geen gebruik van wenst te maken.

Operating System (OS) zie: besturingssysteem

P

Pad : Apparaat of programma dat wordt gemaakt om datapakketen te maken.

Privacy Policy : Engelse woord voor Privacy beleid

S

Screensavers : Is een programma die een zwart, animatie of afbeelding op het scherm weergeeft wanneer de gebruiker een bepaalde tijd de computer niet gebruikt.

SD opslag zie micro SD opslag

Smartphone : Mobiele telefoon met een groot aantal mogelijkheden die overeenkomt met dat van een computer.

Social Media : Online platformen waar de gebruikers zelf voor de inhoud zorgen.

Software : Programmatuur voor een computer

Spam : Het ongewenst ontvangen van elektronische informatie / reclame.

T

Tablet : Computer die enkel werkt met een touchscreen i.p.v. muis en of toetsenbord.

U

Uploaden : Bestanden van eigen computer overzetten naar andere computer door middel van een internetverbinding.

W

Widget Data : Een klein programmaatje dat als een soort van gadget werkt het geeft handige informatie of opzoekmogelijkheden.

Literatuur- en jurisprudentielijst

Juridische literatuur

Boeken

Bannier e.a. 2008

F.A.W. Bannier e.a. *Beroepsgeheim en verschoningsrecht*, Sdu Uitgevers: 2008.

Bruggeman 2006

E.M. Bruggeman, *Praktijkboek Koop/-aannemingsovereenkomst*, Instituut voor Bouwrecht: 2006.

Hesermans 2009

D.J. Hesermans, *Advocatenwet*, Deventer: Kluwer 2009.

Kranenborg en Verhey 2011

H.R. Kranenborg en L.F.M. Verhey, *Wet bescherming persoonsgegevens in Europees Perspectief*, Deventer: Kluwer 2011, p. 11 en 12

Strikwerda 2000

L. Strikwerda, *Inleiding tot het Nederlandse Internationaal Privaatrecht*, Deventer: Kluwer 2000.

Wessels 2007

B. Wessels, *Contracten maken*, Deventer: Kluwer 2007.

Niet – juridische literatuur

Boeken

Saunders, Lewis en Thornhill 2008

M. Saunders, P. Lewis en A. Thornhill, *Methoden en technieken van onderzoek*, Amsterdam: Pearson Education Benelux 2008, p. 31 en 35

Artikelen uit tijdschriften, publicaties en presentaties

Cbp 2013

College bescherming persoonsgegevens, 'Gebruik persoonsgegevens door app alleen toegestaan met toestemming gebruiker' *Cbp* maart 2013

Ter inzage via: www.cbpweb.nl/Pages/pb_20130314-wp29-opinie-mobiele-apps.aspx

Cbp 2013

College bescherming persoonsgegevens, 'Overtredingen WhatsApp deels beeindigd na onderzoek CBP en Canadese privacytoezichthouder' *Cbp* januari 2013

Ter inzage via: www.cbpweb.nl/Pages/pb_20130128-whatsapp.aspx

Engelfriet 2013

A.Engelfriet, 'Wanneer is een wet nu optioneel?' *iusmentis* 2013

Ter inzage via: blog.iusmentis.com/2013/07/19/wanneer-is-een-wet-nu-optioneel/

Van Der Heide 2011

M. van der Heide, 'Tweentwintig klachten na inzage gegevens op Facebook' *Bits of Freedom* 2011

Ter inzage via: <https://www.bof.nl/2011/10/27/tweentwintig-klachten-na-inzage-gegevens-op-facebook/>

Van Hoek 2011

C. van Hoek, 'Facebook gebruikt updates en 'likes' voor reclame' *NU.nl* 2011

Ter inzage via: www.nu.nl/internet/2622369/facebook-gebruikt-updates-en-likes-reclame.html

Niamat 2011

R. Niamat, 'Safe Harbor – een korte opfris cursus (column)' *ISPam.nl* 2011

Ter inzage via: www.ispam.nl/archives/21019/safe-harbor-een-korte-opfris-cursus-column/

Redactie Computerworld.nl

Redactie Computerworld.nl, 'Hoe veilig zijn smartphone apps?' *Computerworld* 2011

Ter inzage via: www.computerworld.nl/beveiliging/74852-hoe-veilig-zijn-je-smartphone-apps/pagina-4

Redactie Security.nl

Redactie Security.nl, 'Wat weten Facebook en Google over je?' *Security.nl* 2011

Ter inzage via: www.security.nl/posting/34667/

Remie 2012

M. Remie, '50 MB aan tweets, adressen en al je nummers. Dit is wat Twitter van je weet' *NRC* 2012

Ter inzage via: www.nrc.nl/nieuws/2012/04/18/50-mb-aan-tweets-adressen-en-al-je-nummers-dit-is-wat-twitter-van-je-weet/

Repairing

Repairing.nl, 'Vrijwel elke iPhone besmet met spyware' Repairing

Ter inzage via: www.repairing.nl/vrijwel-elke-iphone-besmet-met-spyware/

Soghoian 2011

C. Soghoian, 'How Dropbox sacrifices user privacy for cost savings' *slight paranoia* 2011

Ter inzage via: www.paranoia.dubfire.net/2011/04/how-dropbox-sacrifices-user-privacy-for.html

White 2013

G. White, 'Secret lives of phones: how yours contacts 315 servers a day' *Channel 4* 2013

Ter inzage via: www.channel4.com/news/phone-mobile-data-24-hours-apps-security-secret

Zaal 2011

R. Zaal, 'Dropbox in de knoop met privacy' *AutomatiseringGids* 2011

Ter inzage via: www.automatiseringgids.nl/nieuws/2011/20/dropbox-in-de-knoop-met-privacy

Berichten uit kranten en andere media**Televisie-uitzending**

'Radar' TROS Nederland 2, 18 november 2013

Rapporten, scripties en niet uitgegeven teksten**Artikel 29 Data Protection Working Party**

Opinion 02/2013 on apps on smart devices (Opinie), 00461/13/EN, WP 202

College bescherming persoonsgegevens 2013

Onderzoek naar de verwerking van persoonsgegevens in het kader van de mobiele applicatie whatsapp door WhatsApp Inc. (Rapport definitieve bevindingen), Z2011-00987

Jurisprudentie

HR 23 mei 1921, NJ 1921, 564 (*Elektriciteitsarrest*)
HR 13 mei 1966, NJ 1967, 3 (*Alnati arrest*)
HR 1 maart 1986, NJ 1986, 173 (*Notaris Maas arrest*)
HR 5 april 2006, LJN: 2006, 248
HR 31 januari 2013, LJN: BQ6575
HR 14 mei 2013, LJN: BZ9943

Raad van Discipline, 's – Hertogenbosch H258 – 2010, YA1772

Wet – en regelgeving

Europese verdragen en richtlijnen

Artikel 8 Europees Verdrag van de Rechten van de Mens
Verdrag van Straatsburg

Richtlijn 95/46/EG is een richtlijn van het Europees Parlement en de Raad van 24 oktober 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)

Richtlijn 2000/31/EG is een richtlijn van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt (Richtlijn inzake elektronische handel) (*PbEG* 2000, L 178)

Richtlijn 2002/19/EG is een richtlijn van het Europees Parlement en de Raad van 7 maart 2002 inzake de toegang tot en interconnectie van elektronische-communicatienetwerken en bijbehorende faciliteiten (Toegangsrichtlijn) (*PbEG* 2002, L 108)

Richtlijn 2002/20/EG is een richtlijn van het Europees Parlement en de Raad van 7 maart 2002 betreffende de machtiging voor elektronische – communicatienetwerken en – diensten (Machtigingsrichtlijn) (*PbEG* 2002, L 108)

Richtlijn 2002/21/EG is een richtlijn van het Europees Parlement en de Raad van 7 maart 2002 inzake een gemeenschappelijke regelgevingskader voor elektronische-communicatienetwerken en diensten (Kaderrichtlijn) (*PbEG* 2002, L 108)

Richtlijn 2002/22/EG is een richtlijn van het Europees Parlement en de Raad van 7 maart 2002 inzake de universele dienst en gebruikersrechten met betrekking tot elektronische-communicatienetwerken en diensten (Universeledienstrichtlijn) (*PgEG* 2002, L 108)

Richtlijn 2002/58/EG is een richtlijn van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (*PbEG* 2002, L 201)

Nederlandse wetgeving

Burgerlijk Wetboek
Dienst van de informatiemaatschappij
Strafrecht
Telecommunicatiewet
Wet bescherming Persoonsgegevens

Nederlandse regelgeving

Beveiligingsrichtlijnen voor mobiele apparaten en ICT – beveiligingsrichtlijnen voor webapplicaties door Nationaal Cyber Security Center (NCSC)

Gedragscode Centrale Controle Verordeningen van de Nederlandse Orde van Advocaten en lokale Orden van Advocaten (Gedragscode 1992)

Parlementaire stukken

Voorstel voor een verordening betreffende de bescherming van individuen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, versie behandelfase Eerste Kamer, januari 2014

Wijziging Wet bescherming persoonsgegevens (meldplicht datalekken), *Kamerstukken II* 2013/14, 33 662

Internet

Websites

De onderstaande websites zijn in de periode van 13 september 2013 t/m 15 januari 2014 bezocht en gebruikt

College bescherming persoonsgegevens

www.cbpweb.nl

<http://www.mijnprivacy.nl/Vraag/Apps/Paginas/Apps.aspx>

Dirkzwager

www.kennisboek.nl

Dropbox

www.dropbox.com

<https://www.dropbox.com/privacy#terms>

Encyclo – online encyclopedie

<http://www.encyclo.nl/zoek.php?woord=beroepsgeheim>

EUR-Lex

eur-lex.europa.eu

Europese Unie

europa.eu/index_nl.htm

Facebook

<http://investor.fb.com/results.cfm>

<https://www.facebook.com/policies/>

<https://www.facebook.com/legal/terms>

<https://www.facebook.com/about/privacy>

Ius mentis

<http://www.iusmentis.com/contracten/algemenevoorwaarden/>

KPN

www.kpn.nl

Marketingfacts

<http://www.marketingfacts.nl/berichten/social-media-in-nederland-twitter-en-facebook-het-meest-actief-gebruikt>

<http://www.marketingfacts.nl/berichten/social-media-cijfers-augustus-2013-overzicht>

Nederlandse Orde van Advocaten

<https://www.advocatenorde.nl/advocaten/juridische-databank/wetenregelgeving/list/hoofdstuk>

NCSC

www.ncsc.nl

PCMag

<http://www.pcmag.com/article2/0,2817,2401625,00.asp>

Reform Government Surveillance

www.reformgovernmentsurveillance.com

Techcrunch

<http://techcrunch.com/2013/07/09/dropbox-dbx-conference/>

TelecomNieuwsNet

www.telecomnieuwsnet.wordpress.com/2013/08/29/mobiele-apps-hebben-vaak-nog-vaag-privacy-beleid/

Tweakers

www.tweakers.net/nieuws/89824/gfk-nederland-telt-5-komma-6-miljoen-tabletgebruikers.html

Webwereld – ICT nieuws

<http://webwereld.nl/e-commerce/57155-facebook-betaalt-miljoenen-voor-privacy-misstap>

<http://webwereld.nl/beveiliging/79104-microsoft-en-google-starten-rechtszaak-over-dataverzoeken>

Wikipedia

www.nl.wikipedia.org/wiki/Beroepsgeheim

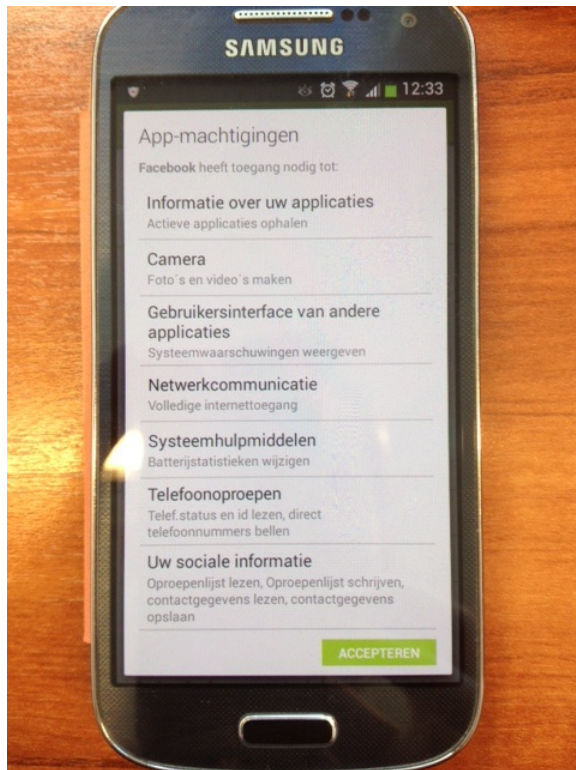
ZDNet

<http://www.zdnet.nl/nieuws/151048/google-gmail-gebruikers-hoeven-niet-te-rekenen-op-privacy-update-/>

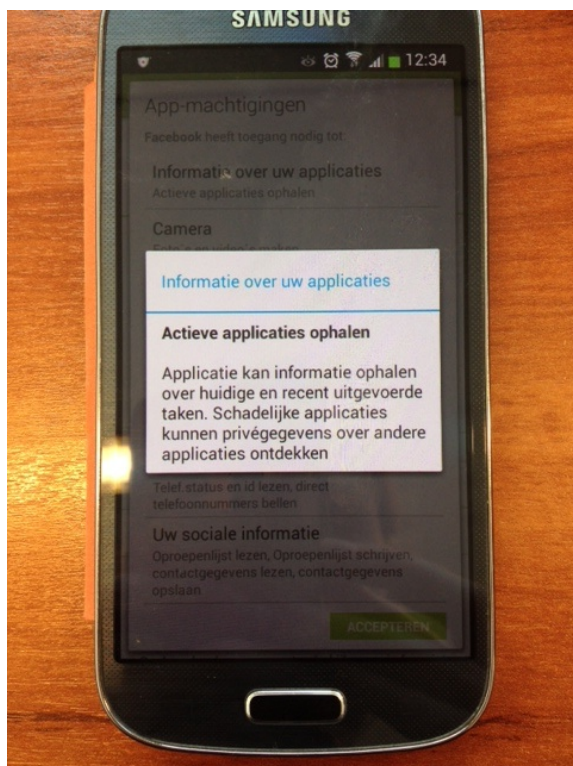
Bijlagen

Bijlage 1.

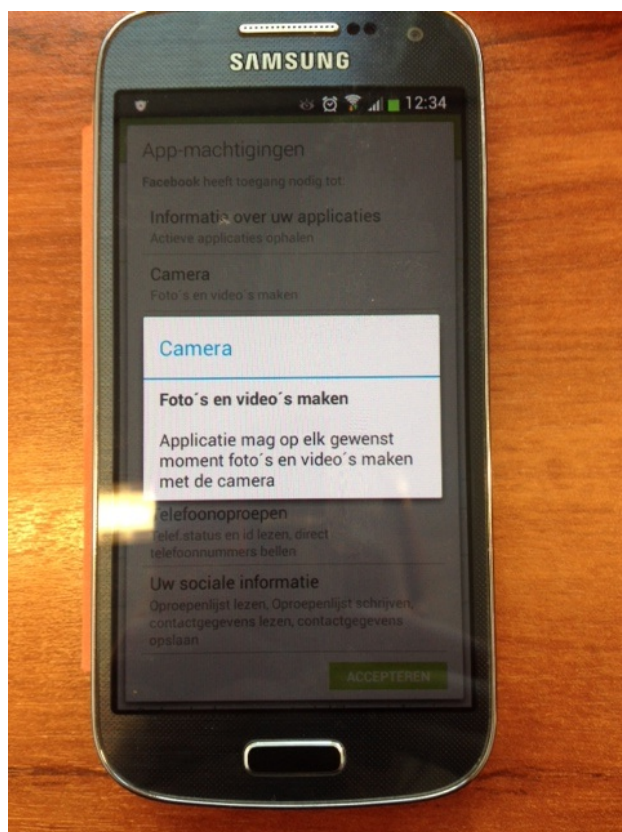
Foto's app-machtigingen Facebook. Samsung Galaxy SIII mini.



Afbeelding 1.



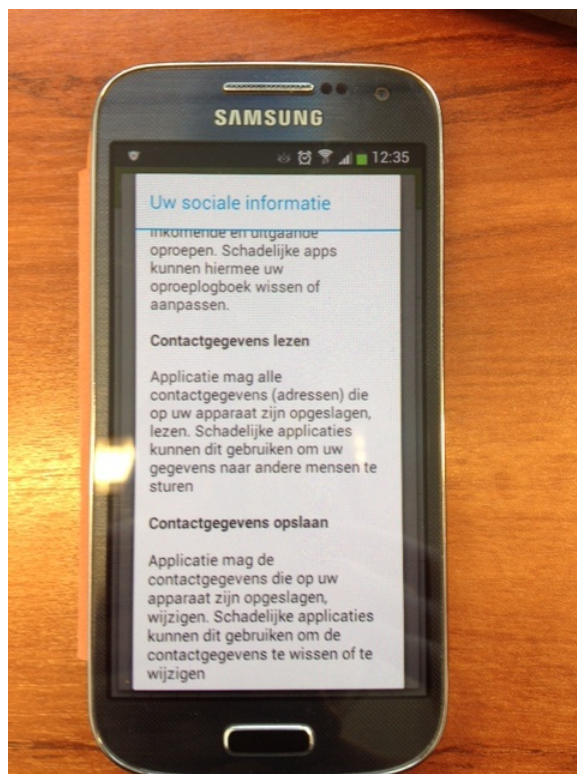
Afbeelding 2.



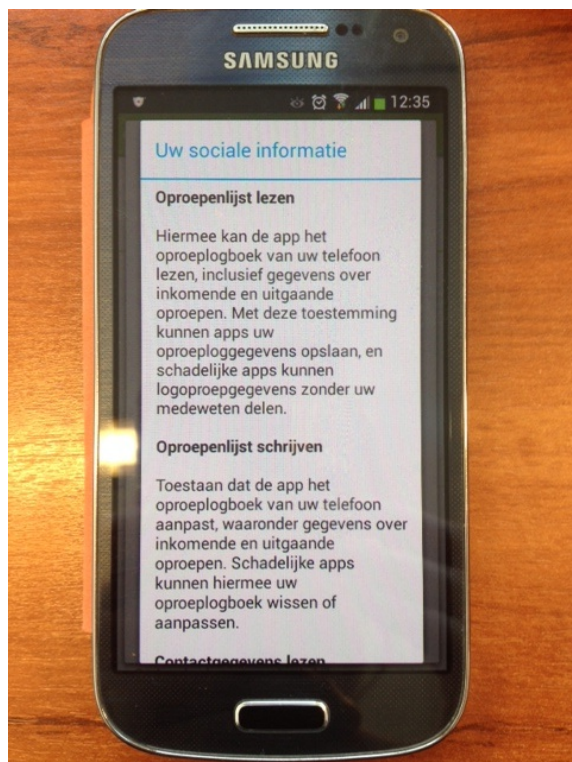
Afbeelding 3.



Afbeelding 4.



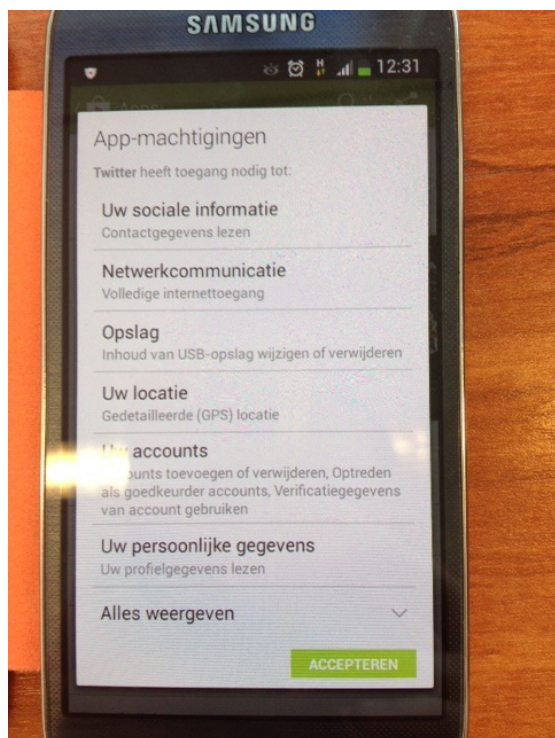
Afbeelding 5.



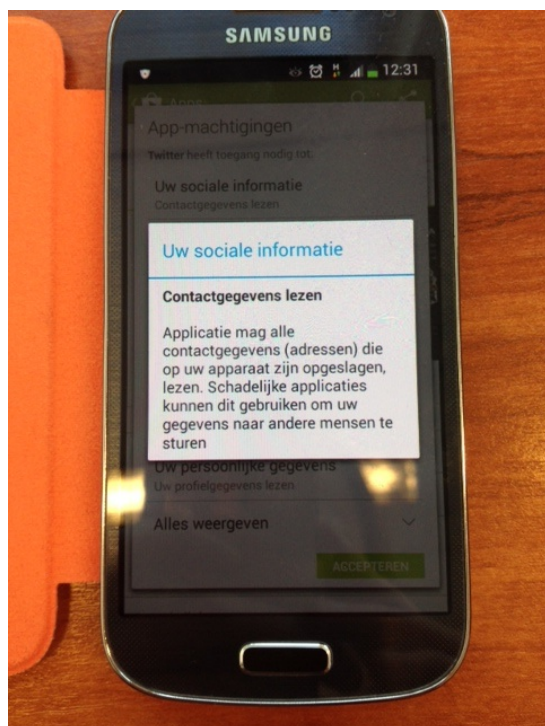
Afbeelding 6.

Bijlage 2.

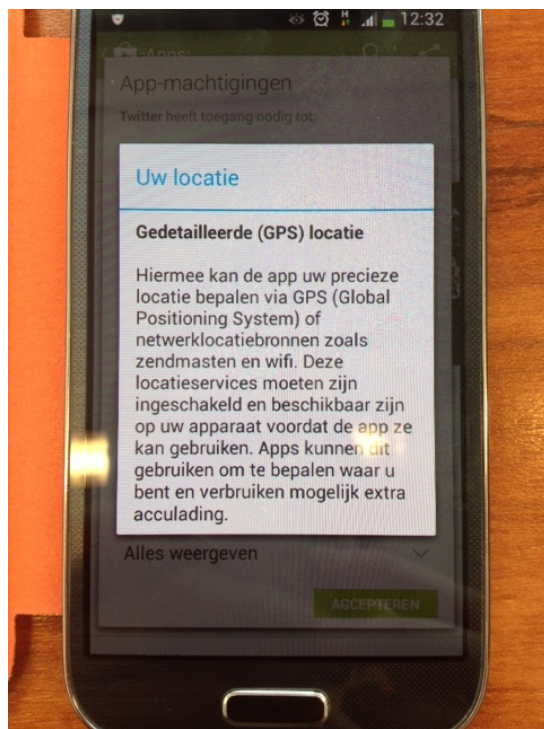
Foto's app-machtigingen Twitter. Samsung Galaxy SIII mini.



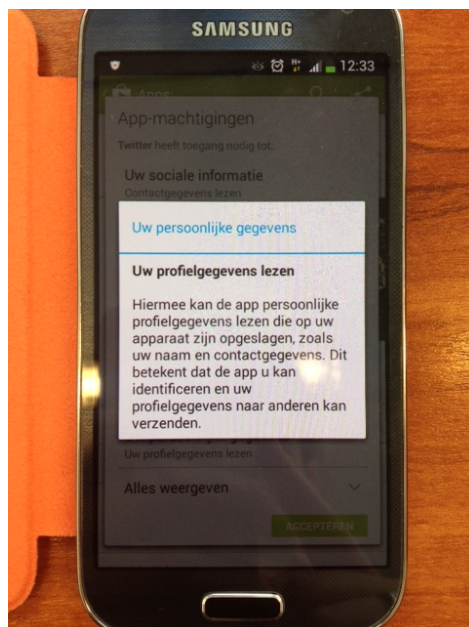
Afbeelding 7.



Afbeelding 8.



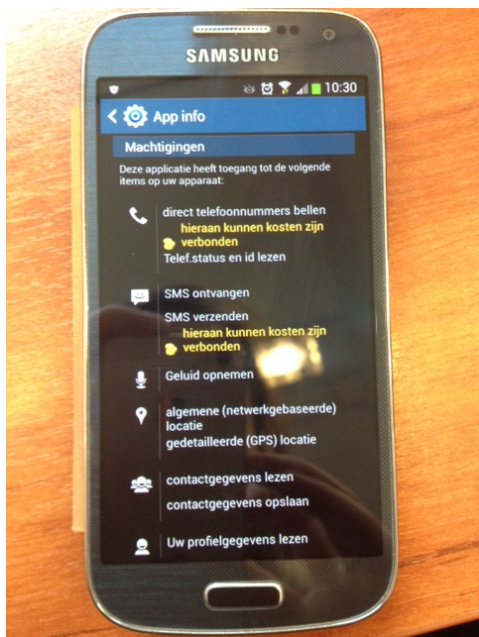
Afbeelding 9.



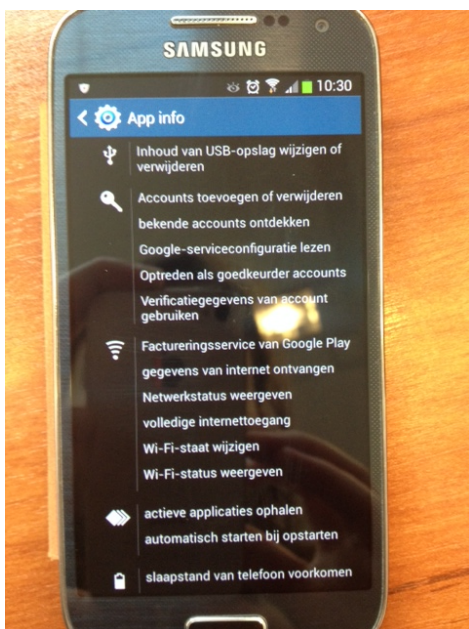
Afbeelding 10.

Bijlage 3.

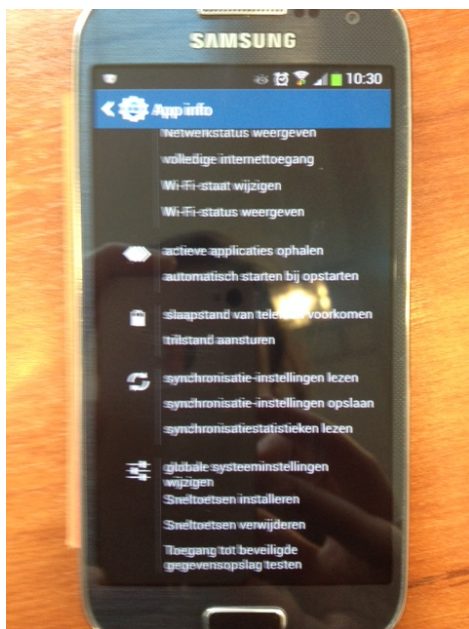
Foto's App – machtigingen Whatsapp Samsung Galaxy SIII mini



Afbeelding 11



Afbeelding 12



Afbeelding 13



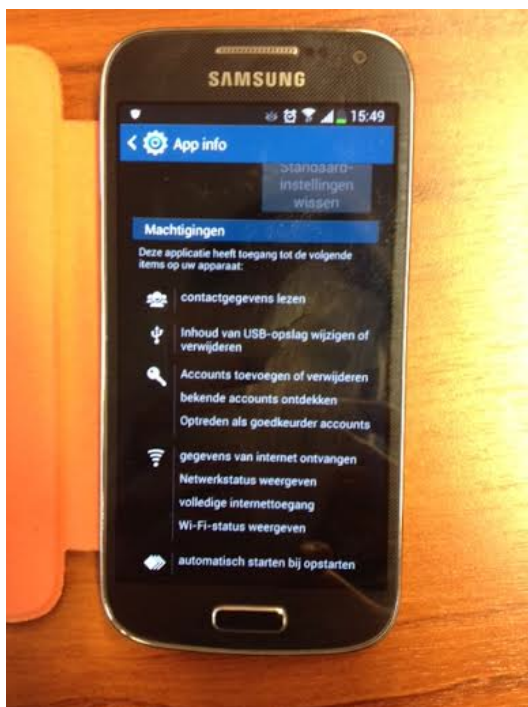
Afbeelding 14



Afbeelding 15. Schermafbeelding van Iphone 4S

Bijlage 4.

Foto app machtigeningen Dropbox Samsung Galaxy SIII mini



Afbeelding 16.

Bijlage 5.

Foto's app-machtigeningen KennisBoekapp Dirk Zwager, Iphone 4S

A screenshot of the 'Dirkzwager KennisBoek' app's registration screen on an iPhone 4S. The status bar at the top shows 'vodafone NL', '3G', the time '11:37', and '81%' battery. The app's title bar is red with a back arrow and the text 'Dirkzwager KennisBoek'. Below the title bar, the word 'Registreer' is centered. The registration form consists of five text input fields: 'Gebruikersnaam', 'Email Adres', 'Naam', 'Wachtwoord', and 'Wachtwoord (controle)'. Below these fields, there is a section titled 'Voorkeuren ontvangen digitale nieuwsbrief' (Preferences for receiving digital newsletter) with four buttons: 'Geen' (selected), 'Per dag', 'Per week', and 'Per maand'. At the bottom of the form, the word 'Optioneel' is displayed.

Afbeelding 17.

••••• Vodafone NL 3G 11:34 82%

Dirkzwager KennisBoek

Optioneel

Bedrijfsnaam

Functie

Op het gebruik van deze app is een disclaimer van toepassing. Het gebruik van deze app brengt voorts verwerkingen van persoonsgegevens met zich mee.

Lees hierover meer in de disclaimer en privacystatement

Registreer

Ik heb al een account

Afbeelding 18.

••••• Vodafone NL 3G 10:32 93%

Facebook

Dirkzwager Kennisboek ontvangt de volgende gegevens: jouw openbaar profiel, vriendenlijst en e-mailadres.

?

Annuleren OK

Afbeelding 19.

••••• Vodafone NL 3G 10:32 93%

accounts.google.com

Google

Log in met uw Google-account



E-mailadres

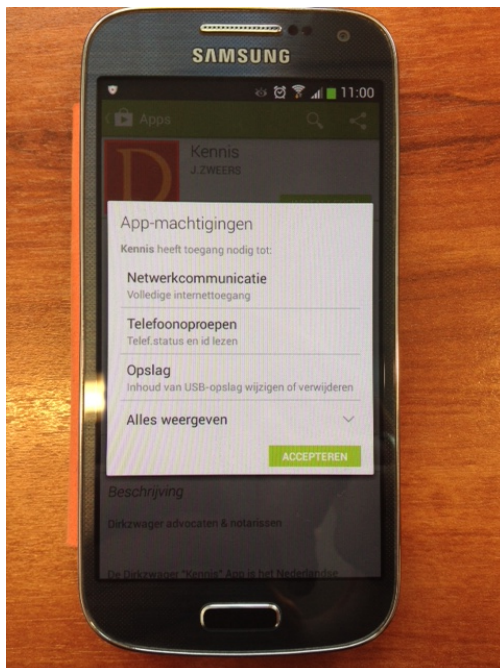
Wachtwoord

Inloggen

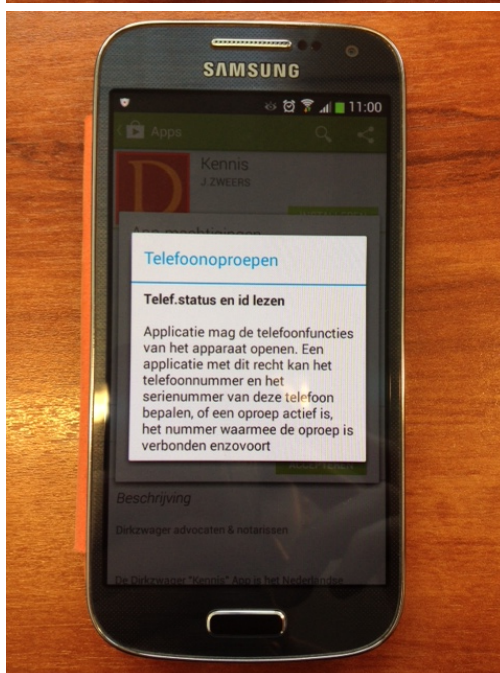
Heeft u hulp nodig?

Afbeelding 20.

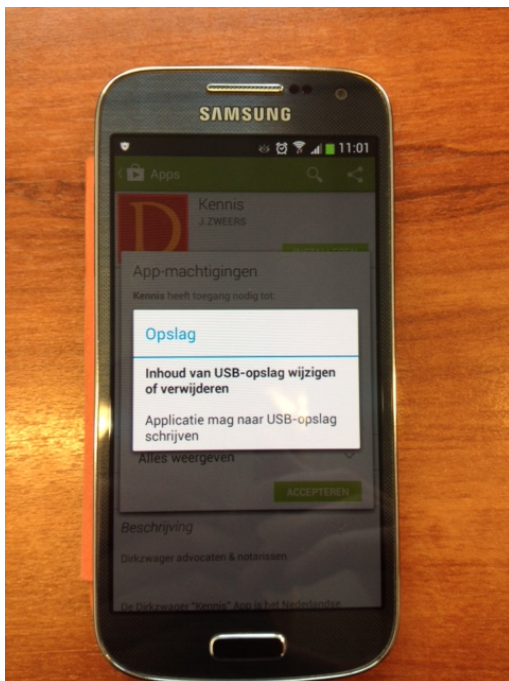
Afbeeldingen 21,22,23 zijn foto's van een Samsung Galaxy SIII mini



Afbeelding 21.



Afbeelding 22.



Afbeelding 23.

De blauwgedrukte tekst in de volgende bijlagen verwijst naar het desbetreffende stuk uit de tekst.

Bijlage 6.

Verklaring van rechten en verantwoordelijkheden Facebook

Bron: www.facebook.com zoek op: Gebruiksvoorwaarden

Deze overeenkomst is oorspronkelijk opgesteld in het Engels (VS). Voor zover een eventuele vertaalde versie van deze overeenkomst tegenstrijdig is met de Engelse versie, is de Engelse versie bindend. In artikel 17 staan wijzigingen aan de algemene voorwaarden voor gebruikers buiten de Verenigde Staten.

Laatst gewijzigd: 11.12.12. **Verklaring van rechten en verantwoordelijkheden** Deze Verklaring van rechten en verantwoordelijkheden ("Verklaring," "Voorwaarden" of "VRV") is afgeleid van de [Facebook-principes](#) en is van toepassing op onze relatie met gebruikers en anderen die interactie voeren met Facebook. Wanneer je Facebook gebruikt of opent, verklaar je akkoord te gaan met deze Verklaring, die regelmatig wordt bijgewerkt in overeenstemming met de bepalingen in onderstaand artikel 14. Onder aan dit document staan informatiebronnen over de manier waarop Facebook werkt.

Privacy We vinden je privacy erg belangrijk. We hebben een [Beleid inzake gegevensgebruik](#) opgesteld dat belangrijke bepalingen bevat over hoe je Facebook kunt gebruiken om items te delen met anderen en hoe we jouw inhoud en informatie verzamelen en kunnen gebruiken. We raden je aan het Beleid inzake gegevensgebruik te lezen en op basis hiervan beslissingen te nemen.

Inhoud en informatie delen Je bent zelf eigenaar van alle inhoud en informatie die je plaatst op Facebook en in je privacy- en app-instellingen kun je bepalen hoe dit wordt gedeeld. Verder gelden de volgende bepalingen:

Voor inhoud waarop intellectuele-eigendomsrechten rusten, zoals foto's en video (IE-inhoud), geef je

ons nadrukkelijk de volgende toestemming, afhankelijk van je privacy- en app-instellingen: je verleent ons een niet-exclusieve, overdraagbare, royaltyvrije, wereldwijde licentie om alle IE-inhoud te gebruiken die je plaatst op Facebook of in verband met Facebook (IE-licentie). Deze IE-licentie eindigt wanneer je jouw IE-inhoud of je account verwijderd, tenzij je jouw inhoud hebt gedeeld met anderen en zij de inhoud niet hebben verwijderd.

Wanneer je IE-inhoud verwijderd, wordt deze verwijderd op een manier die vergelijkbaar is met het legen van de prullenbak op een computer. Je begrijpt dat verwijderde inhoud echter gedurende een redelijke tijd mogelijk aanwezig blijft in back-ups (maar niet beschikbaar is voor anderen).

Wanneer je een toepassing gebruikt, kan het zijn dat de toepassing je toestemming vraagt voor toegang tot je inhoud en informatie alsook de inhoud en informatie die anderen met je hebben gedeeld. We vereisen van toepassingen dat deze je privacy respecteren en je acceptatie van die toepassing is bepalend voor de manier waarop de toepassing je inhoud en informatie kan gebruiken, opslaan en overdragen. (Voor meer informatie over het platform lees je ons [Beleid inzake gegevensgebruik](#) en de [Platformpagina](#).)

Wanneer je inhoud of informatie publiceert met de instelling Openbaar, betekent dit dat je iedereen, inclusief mensen buiten Facebook, toestemming geeft om die informatie te bekijken en te gebruiken en deze aan jou te koppelen (d.w.z. je naam en profielfoto).

We stellen het altijd op prijs als je feedback of andere suggesties over Facebook geeft, maar je moet begrijpen dat we deze kunnen gebruiken zonder enige verplichting om je hiervoor te belonen (net zoals jij geen verplichting hebt om deze aan te bieden).

Veiligheid We doen ons best om Facebook veilig te houden, maar kunnen dit niet garanderen. We hebben je hulp nodig om Facebook veilig te houden. Daarom moet je je houden aan de volgende regels:

Je plaatst geen niet-geautoriseerde commerciële berichten (zoals spam) op Facebook.

Je verzamelt geen inhoud of informatie van gebruikers en gebruikt Facebook niet op andere manieren via geautomatiseerde middelen (zoals harvesting bots, robots, spiders of scrapers) zonder onze voorafgaande toestemming.

Je houdt je op Facebook niet bezig met illegale marketing op meerdere niveaus zoals piramideconstructies.

Je uploadt geen virussen of andere schadelijke code.

Je vraagt mensen niet om hun aanmeldingsgegevens en je meldt je niet aan op een account van iemand anders.

Je zult geen gebruikers pesten, intimideren of lastig vallen.

Je plaatst geen inhoud die: haatdragend, bedreigend of pornografisch is; die aanzet tot geweld; of die naaktbeelden of nodeloos geweld bevat.

Je ontwikkelt en beheert geen toepassingen van derde partijen met inhoud op het gebied van alcohol, dating of andere 18+-inhoud (waaronder advertenties) zonder passende leeftijdsbeperkingen toe te passen.

Je houdt je aan onze [Promotierichtlijnen](#) en alle geldende wetten wanneer je een prijsvraag, giveaway of loterij ("promotie") publiceert op Facebook.

Je gebruikt Facebook niet voor onwettige, misleidende, kwaadaardige of discriminerende activiteiten.

Je doet niets waardoor de correcte werking of weergave van Facebook verstoord, overbelast of onmogelijk kan worden, zoals een Denial of Service-aanval of verstoring van paginaweergave of andere Facebook-functionaliteiten.

Je faciliteert of stimuleert geen schending van deze Verklaring of onze beleidsregels.

Registratie en accountbeveiliging Facebook-gebruikers verstrekken hun echte namen en gegevens en we hebben je hulp nodig om dit zo te houden. Hier volgen enkele regels waaraan je je moet

houden met betrekking tot registratie en beveiliging van je account:

Je verstrekt geen valse persoonlijke gegevens op Facebook en maakt zonder toestemming geen account voor iemand anders.

Je maakt niet meer dan één persoonlijke account.

Als we je account deactiveren, maak je geen ander account zonder onze toestemming.

Je gebruikt je persoonlijke tijdlijn niet voor eigen commercieel gewin en gebruikt een Facebook-pagina voor die doeleinden.

Je gebruikt Facebook niet als je jonger bent dan 13 jaar.

Je gebruikt Facebook niet als je bent veroordeeld voor een zedenmisdrijf.

Je houdt je contactgegevens correct en actueel.

Je deelt je wachtwoord niet met anderen (en ontwikkelaars delen hun geheime sleutel niet), je verleent niemand toegang tot je account en je doet niets wat de beveiliging van je account kan schaden.

Je draagt je account (waaronder pagina's of toepassingen die je beheert) niet over aan iemand anders zonder dat je onze schriftelijke toestemming hebt.

Als je een gebruikersnaam of vergelijkbare identificatie selecteert voor je account of pagina, behouden wij ons het recht voor om deze te verwijderen of terug te vorderen indien wij menen dat deze ongepast is (bijvoorbeeld wanneer een eigenaar van een handelsmerk klaagt over een gebruikersnaam die weinig lijkt op de werkelijke naam van een gebruiker).

De rechten van anderen beschermen We respecteren de rechten van anderen en verwachten dat jij dit ook doet.

Je plaatst geen inhoud of onderneemt geen actie op Facebook waarmee de rechten van iemand anders worden geschonden of overtreden, of waarmee de wet op een andere wijze wordt overtreden.

We kunnen inhoud en informatie die je op Facebook plaatst verwijderen indien we vinden dat hiermee deze Verklaring of onze beleidsregels worden geschonden.

We bieden je tools waarmee je jouw intellectuele-eigendomsrechten kunt beschermen. Zie voor meer informatie onze pagina [Schending van intellectuele-eigendomsrechten rapporteren](#).

Als we je inhoud hebben verwijderd wegens inbreuk op de auteursrechten van iemand anders en je denkt dat dit onterecht is, kun je bezwaar maken.

Als je herhaaldelijk inbreuk maakt op de intellectuele-eigendomsrechten van anderen, zullen we je account indien terecht uitschakelen.

Je maakt geen gebruik van onze auteursrechten of handelsmerken (waaronder Facebook, het Facebook-logo, het F-logo, FB, Face, Porren, Book en Prikbord) of andere soortgelijke verwarrende merken, behalve wanneer dit uitdrukkelijk is toegestaan in onze Richtlijnen voor gebruik van merken of wanneer je schriftelijke toestemming van ons hebt.

Als je informatie verzamelt van gebruikers, moet je: hun toestemming krijgen, duidelijk maken dat jij (en niet Facebook) degene bent die de informatie verzamelt en een privacybeleid publiceren waarin wordt uitgelegd welke informatie je verzamelt en hoe je deze gebruikt.

Je plaatst geen identiteitsdocumenten of gevoelige financiële informatie van anderen op Facebook.

Je tagt geen gebruikers en stuurt geen uitnodigingen via e-mail aan personen die geen Facebook gebruiken, zonder hun toestemming. Facebook biedt functies voor sociale rapporten waarmee gebruikers feedback kunnen geven over taggen.

Mobiele en andere apparaten We bieden onze mobiele services momenteel gratis aan, maar houd er rekening mee dat de normale tarieven van je telecomaandbieder (zoals voor sms) gewoon van toepassing zijn.

Wanneer het nummer van je mobiele telefoon wijzigt of wordt gedeactiveerd, werk je binnen 48 uur je accountgegevens op Facebook bij om ervoor te zorgen dat je berichten niet worden verzonden naar de persoon die je oude nummer krijgt.

Jij geeft toestemming en alle noodzakelijke rechten die nodig zijn om gebruikers in staat te stellen hun apparaten te synchroniseren (met behulp van een toepassing) met gegevens die zichtbaar over hun zijn op Facebook.

Betalingen Als je een betaling doet op Facebook of Facebook-tegoedpunten gebruikt, ga je akkoord met onze [Betelingsvoorwaarden](#).

Speciale bepalingen voor sociale plug-ins Als je onze sociale plug-ins, zoals de knoppen Delen of Vind ik leuk op je website plaatst, gelden voor jou de volgende aanvullende voorwaarden: We geven je toestemming om de sociale plug-ins van Facebook te gebruiken zodat gebruikers links of inhoud van je website op Facebook kunnen plaatsen. Je geeft ons toestemming om dergelijke links en inhoud te gebruiken op Facebook en om anderen dergelijke links en inhoud te laten gebruiken op Facebook. Je plaatst geen sociale plug-in op een pagina die inhoud bevat die deze Verklaring zou schenden als deze op Facebook zou zijn geplaatst.

Speciale bepalingen voor ontwikkelaars/beheerders van toepassingen en websites Als je ontwikkelaar of beheerder bent van een platformtoepassing of -website, gelden voor jou de volgende aanvullende voorwaarden:

Je bent verantwoordelijk voor je toepassing, de inhoud en al je gebruik van het platform. Dit betekent onder andere dat je ervoor moet zorgen dat je toepassing of je gebruik van het platform voldoet aan onze [Beleidsregels van het Facebook-platform](#) en onze [Advertentierichtlijnen](#).

Voor je toegang tot en gebruik van gegevens die je ontvangt van Facebook, gelden de volgende beperkingen:

Je vraagt alleen gegevens die je nodig hebt voor je toepassing.

Je hebt een privacybeleid waarin gebruikers wordt uitgelegd welke gebruikersgegevens je gaat gebruiken en hoe je deze gegevens gebruikt, weergeeft, deelt of overdraagt. Daarnaast plaats je de URL van je privacybeleid in de [Ontwikkelaarstoepassing](#).

Je zult geen gebruikersgegevens gebruiken, weergeven, delen of overdragen op een manier die niet overeenkomt met je privacybeleid.

Je verwijdert alle gegevens die je van ons ontvangt over een gebruiker indien de gebruiker je dit vraagt en je biedt gebruikers een manier om een dergelijk verzoek in te dienen.

Je gebruikt gegevens die je van ons ontvangt over een gebruiker niet in advertenties.

Je zult gegevens die je van ons ontvangt niet direct of indirect overdragen naar (of gebruiken in verband met) een reclamenetwerk, reclame-uitwisseling, een gegevenshandelaar of een andere reclamegerelateerde toolset, zelfs niet als een gebruiker toestemming geeft voor een dergelijke overdracht of gebruik.

Je verkoopt geen gebruikersgegevens. Als je wordt overgenomen door of fuseert met een derde partij, kun je de gebruikersgegevens blijven gebruiken in je toepassing, maar je kunt gebruikersgegevens niet buiten je toepassing gebruiken.

We kunnen van je eisen dat je gebruikersgegevens verwijdert indien je deze gebruikt op een manier die volgens ons niet overeenkomt met de verwachtingen van gebruikers.

We kunnen je toegang tot gegevens beperken.

Je houdt je aan alle andere beperkingen in onze [Beleidsregels van het Facebook-platform](#).

Je geeft ons geen informatie die je zelfstandig hebt verzameld van een gebruiker of de inhoud van een gebruiker zonder de toestemming van die gebruiker.

Je maakt het voor gebruikers makkelijk om je toepassing te verwijderen of om de verbinding hiermee

te verbreken.

Je maakt het voor gebruikers makkelijk om contact met je op te nemen. We kunnen je e-mailadres doorgeven aan gebruikers of anderen die beweren dat je hun rechten hebt geschonden of overtreden.

Je biedt klantenondersteuning voor je toepassing.

Je toont op www.facebook.com geen advertenties van derde partijen of velden voor het zoeken op internet.

We verlenen je alle rechten die je nodig hebt om de code, API's, gegevens en tools te gebruiken die je van ons ontvangt.

Je zult geen code, API's of tools verkopen, overdragen of in sublicentie verlenen aan anderen.

Je zult aan anderen je relatie met Facebook niet anders voorstellen dan deze in werkelijkheid is.

Je mag de logo's gebruiken die we beschikbaar stellen aan ontwikkelaars en je mag een persbericht of andere publieke verklaring uitgeven zolang je je houdt aan onze [Beleidsregels van het Facebook-platform](#).

We kunnen een persbericht uitgeven waarin we onze relatie met jou beschrijven.

Je houdt je aan alle geldende wetten. Je zult met name het volgende doen (indien van toepassing):

Een beleid hebben voor het verwijderen van inhoud waarmee de rechten van anderen worden geschonden en voor het beëindigen van je service voor herhaaldelijke overtreders. Dit beleid moet voldoen aan de bepalingen van de Digital Millennium Copyright Act (Amerikaanse wet voor bescherming van auteursrechten).

De Video Privacy Protection Act naleven (VPPA, Amerikaanse wet voor bescherming van privacy inzake videogegevens) en de benodigde toestemming vragen aan gebruikers zodat gebruikersgegevens waarop de VPPA van toepassing is mogen worden gedeeld op Facebook. Je verklaart dat het doorgeven van gegevens aan ons niet incidenteel is voor je normale bedrijfsvoering.

We garanderen niet dat het platform altijd gratis zal zijn.

Je verleent ons alle rechten die nodig zijn om je toepassing te laten werken met Facebook, waaronder het recht om inhoud en informatie die je aan ons verstrekt te gebruiken in streams, tijdlijnen en andere actie verhalen.

Je verleent ons het recht om een link te maken naar je toepassing of deze in een frame te gebruiken, en om inhoud, waaronder advertenties, rond je toepassing te plaatsen.

We kunnen je toepassing, inhoud en gegevens analyseren voor elk willekeurig doel, waaronder commerciële doeleinden (zoals voor het bepalen van de doelgroep voor advertenties en het indexeren van inhoud voor zoekopdrachten).

We kunnen je toepassing controleren om te kijken of deze veilig is voor gebruikers.

We kunnen toepassingen maken die vergelijkbare functies en services bieden of die anderszins concurreren met je toepassing.

Over advertenties en andere commerciële inhoud die worden geboden of verbeterd door Facebook

Ons doel is advertenties en commerciële inhoud te leveren die waardevol zijn voor onze gebruikers en adverteerders. Om ons hierbij te helpen, ga je akkoord met het volgende:

Je kunt je [privacyinstellingen](#) gebruiken om beperkingen in te stellen voor hoe je naam en profielfoto kunnen worden geassocieerd met commerciële, gesponsorde of verwante inhoud (zoals een merk dat je leuk vindt) die door ons wordt weergegeven of verbeterd. Je geeft ons toestemming om je naam en profielfoto te gebruiken in verband met die inhoud, in overeenstemming met de beperkingen die je erop zet.

We geven je inhoud of informatie niet zonder jouw toestemming aan adverteerders.

Je begrijpt dat we betaalde services en communicatie mogelijk niet altijd als zodanig herkennen.

Speciale bepalingen voor adverteerders Je kunt je advertenties richten op je gewenste doelgroep door advertenties te kopen op Facebook of ons uitgeversnetwerk. De volgende aanvullende voorwaarden gelden als je een order plaatst via onze online advertentieportal.

Wanneer je een order plaatst, geef je op welk type advertentie je wilt kopen, hoeveel je wilt uitgeven en hoeveel je biedt. Als we je order accepteren, plaatsen we jouw advertenties als er ruimte beschikbaar is. Wanneer we je advertentie plaatsen, doen we ons best om de advertenties te tonen aan de doelgroep die je hebt opgegeven. We kunnen echter niet in elk geval garanderen dat je advertentie de beoogde doelgroep bereikt.

We kunnen de criteria voor de doelgroep die je opgeeft verruimen wanneer we denken dat hiermee de effectiviteit van je advertentiecampagne wordt verbeterd.

Je betaalt voor je orders in overeenstemming met onze [Betalingvoorwaarden](#). Het bedrag dat je verschuldigd bent, wordt berekend op basis van onze volgmechanismen.

Je advertenties voldoen aan onze [Advertentierichtlijnen](#).

We bepalen de grootte, plaatsing en positionering van je advertenties.

We bieden geen garanties voor de reacties op je advertenties, zoals het aantal keer dat er op een advertentie wordt geklikt.

We hebben geen invloed op de manier waarop er op de advertenties wordt geklikt. We hebben systemen die proberen bepaalde klikactiviteiten te detecteren en te filteren, maar we zijn niet verantwoordelijk voor klikfraude, technologische problemen of andere mogelijk ongeldige klikactiviteiten die mogelijk van invloed zijn op de kosten van lopende advertenties.

Je kunt je order op elk moment annuleren via onze online portal, maar het kan tot 24 uur duren voordat lopende advertenties worden gestopt. Je moet wel betalen voor alle lopende advertenties.

Onze licentie om je advertentie uit te voeren, eindigt wanneer we je order hebben voltooid. Je begrijpt dat als gebruikers interactie hebben gevoerd met je advertentie, dat je advertentie dan aanwezig blijft totdat de gebruikers deze verwijderen.

We kunnen je advertentie en gerelateerde inhoud en informatie gebruiken voor marketing- of promotiedoeleinden.

Zonder onze schriftelijke toestemming breng je geen persbericht uit en doe je geen publieke verklaringen over je relatie met Facebook.

We kunnen een advertentie weigeren of verwijderen, ongeacht de reden.

Als je advertenties plaatst namens iemand anders, moet je toestemming hebben om deze advertenties te plaatsen en gelden de volgende bepalingen:

Je garandeert dat je de juridische bevoegdheid hebt om de adverteerder te binden aan deze Verklaring.

Je gaat ermee akkoord dat als de adverteerder die je vertegenwoordigt deze Verklaring schendt, we jou verantwoordelijk kunnen houden voor die schending.

Speciale bepalingen voor pagina's Als je een Facebook-pagina maakt of beheert, of een promotie of aanbieding publiceert op je pagina, dan ga je akkoord met onze [richtlijnen voor Facebook-pagina's](#).

Speciale bepalingen voor software Als je software downloadt, zoals een stand-alone softwareproduct of een invoegtoepassing voor een browser, ga je ermee akkoord dat de software zo nu en dan upgrades, updates en extra functies van ons downloadt met verbeteringen en verdere ontwikkelingen van de software.

Je gaat ermee akkoord de broncode niet aan te passen, er geen afgeleide producten mee te maken, te decompileren of op andere wijze van ons te verkrijgen, tenzij je nadrukkelijke toestemming hebt om dit te doen volgens een open source-licentie of we je nadrukkelijke, geschreven toestemming daarvoor hebben gegeven.

Wijzigingen

Tenzij we een wijziging doorvoeren om juridische of bestuurlijke redenen, of om een incorrecte tekst te corrigeren, krijg je zeven (7) dagen vooraf kennisgeving (bijvoorbeeld doordat we de wijziging publiceren op de pagina [Facebook Site Governance](#)) en heb je de mogelijkheid te reageren op de

wijzigingen in de Verklaring. Je kunt ook naar onze pagina [Facebook Site Governance](#) gaan en de pagina leuk vinden om updates te krijgen over wijzigingen in de Verklaring.

Als we wijzigingen aanbrengen aan beleidsregels waarnaar in deze Verklaring wordt verwezen of die hierin zijn opgenomen, kunnen we een kennisgeving plaatsen op de pagina Site Governance. Wanneer je na de wijzigingen aan onze voorwaarden Facebook blijft gebruiken, verklaar je akkoord te gaan met de gewijzigde voorwaarden.

Beëindiging Als je de letter of geest van deze Verklaring schendt of op andere wijze een risico of mogelijke juridische blootstelling voor ons creëert, kunnen we je toegang tot Facebook geheel of gedeeltelijk stopzetten. We zullen je hierover via e-mail informeren of wanneer je de volgende keer probeert je account te openen. Je kunt je account op elk moment verwijderen of deactiveren. In alle dergelijke gevallen vervalt de geldigheid van deze Verklaring, maar blijven de volgende artikelen van kracht: 2.2, 2.4, 3-5, 8.2, 9.1-9.3, 9.9, 9.10, 9.13, 9.15, 9.18, 10.3, 11.2, 11.5, 11.6, 11.9, 11.12, 11.13 en 15-19.

Geschillen Je zult eventuele claims, juridische procedures of geschillen (claims) die je met ons hebt, voortvloeiend uit of met betrekking tot deze Verklaring of Facebook, uitsluitend oplossen in een rechtbank in het district Santa Clara (VS). Deze Verklaring en eventuele claims tussen jou en ons zijn onderworpen aan de wetten van de Amerikaanse staat Californië, ongeacht eventuele bepalingen inzake conflicten of wetten. Je gaat ermee akkoord je te onderwerpen aan de persoonlijke rechtspraak van de rechtbanken in Santa Clara, Californië, voor het procederen van dergelijke claims.

Indien iemand een claim tegen ons indient met betrekking tot jouw acties, inhoud of informatie op Facebook, zul je ons schadeloos stellen tegen alle schade, verliezen en kosten die gerelateerd zijn aan een dergelijke claim (inclusief redelijke juridische vergoedingen en kosten). Hoewel we regels bieden voor het gedrag van gebruikers, controleren of sturen we de acties van gebruikers op Facebook niet en zijn we niet verantwoordelijk voor de inhoud of informatie die gebruikers overdragen of delen op Facebook. We zijn niet verantwoordelijk voor eventuele aanstootgevende, ongepaste, obscene, illegale of op andere wijze afkeurenswaardige inhoud of informatie die je mogelijk op Facebook vindt. We zijn niet verantwoordelijk voor het online of offline gedrag van Facebook-gebruikers.

WE PROBEREN FACEBOOK ONLINE, FOUTVRIJ EN VEILIG TE HOUDEN, MAAR JE GEBRUIKT HET OP EIGEN RISICO. WE BIEDEN FACEBOOK ZOALS HET WORDT GEBODEN (AS IS), ZONDER EXPLICIETE OF IMPLICIETE GARANTIES, WAARONDER, MAAR NIET BEPERKT TOT, IMPLICIETE GARANTIES VAN VERHANDELBAARHEID, GESCHIKTHEID VOOR EEN BEPAALD DOEL EN NIET-NALEIVING. WE GARANDEREN NIET DAT FACEBOOK ALTIJD VEILIG, BEVEILIGD OF FOUTVRIJ ZAL ZIJN OF DAT FACEBOOK ALTIJD ZAL WERKEN ZONDER STORINGEN, VERTRAGINGEN OF ONREGELMATIGHEDEN. FACEBOOK IS NIET VERANTWOORDELIJK VOOR DE ACTIES, INHOUD, INFORMATIE OF GEGEVENS VAN DERDE PARTIJEN EN JE VRIJWAART ONS, ONZE DIRECTEUREN, MANAGERS, MEDEWERKERS EN AGENTEN VAN EVENTUELE CLAIMS EN SCHADE, BEKEND EN ONBEKEND, DIE VOORTVLOEIEN UIT OF VERBAND HOUDEN MET EVENTUELE CLAIMS DIE JE TEGEN DERGELIJKE PARTIJEN HEBT. ALS JE INWONER BENT VAN CALIFORNIË, DOE JE AFSTAND VAN ARTIKEL 1542 VAN HET BURGERLIJK WETBOEK, WAARIN STAAT: EEN ALGEMENE RELEASE IS NIET GELDIG OP CLAIMS DIE DE SCHULDEISER NIET KENT OF VERMOEDT TE BESTAAN TEN GUNSTE VAN HEM/HAAR OP HET MOMENT VAN UITROLLEN VAN DE RELEASE, WELKE ALS HIJ/ZIJ DEZE HAD GEWETEN AANZIENLIJK VAN INVLOED ZOUDEN ZIJN GEWEEST OP ZIJN/HAAR VEREFFENING MET DE SCHULDENAAR. WE ZIJN JEGENS JOU NIET AANSPRAKELIJK VOOR EVENTUELE WINSTDERIVING OF ANDERE GEVOLGSCHADE, SPECIALE, INDIRECTE OF INCIDENTELE SCHADE DIE VOORTVLOEIT UIT OF VERBAND HOUDT MET DEZE VERKLARING OF MET FACEBOOK, ZELFS NIET ALS WE ZIJN GEÏNFORMEERD OVER DE MOGELIJKHEID VAN DERGELIJKE SCHADE. ONZE TOTALE AANSPRAKELIJKHEID DIE VOORTVLOEIT UIT DEZE VERKLARING OF VAN FACEBOOK ZAL NIET HOGER ZIJN DAN HONDERD AMERIKAANSE DOLLAR (USD

100,00) OF HET BEDRAG DAT JE ONS IN DE AFGELOPEN 12 MAANDEN HEBT BETAALD. KRACHTENS BEPAALDE GELDENDE WETTEN IS HET NIET TOEGESTAAN DE AANSPRAKELIJKHEID OF INCIDENTELE SCHADE OF GEVOLGSCHADE TE BEPERKEN OF AF TE WIJZEN, WAARDOOR BOVENSTAANDE BEPERKING OF AFWIJZING MOGELIJK NIET OP JOU VAN TOEPASSING IS. IN DERGELIJKE GEVALLEN IS DE AANSPRAKELIJKHEID VAN FACEBOOK BEPERKT VOOR ZOVER MAXIMAAL MOGELIJK IS VOLGENS DE GELDENDE WET.

Speciale bepalingen voor gebruikers buiten de Verenigde Staten Wij streven ernaar een algemene community te creëren met consistente regels voor iedereen, maar wij willen ook plaatselijke wetten respecteren. De volgende bepalingen gelden voor gebruikers en niet-gebruikers die interactie voeren met Facebook buiten de Verenigde Staten:

Je gaat ermee akkoord dat je persoonlijke gegevens worden overgedragen naar en verwerkt in de Verenigde Staten.

Als je je bevindt in een land waartegen de Verenigde Staten een embargo heeft uitgesproken of als jij of je organisatie staat vermeld op de lijst "Specially Designated Nationals" van het Amerikaanse ministerie van Financiën, mag je je op Facebook niet bezighouden met commerciële activiteiten (zoals advertenties of betalingen) of een platformtoepassing of -website beheren. (Op genoemde lijst staan personen en organisaties waarmee Amerikaanse burgers en ingezetenen van de Verenigde Staten geen zaken mogen doen.)

Bepaalde specifieke voorwaarden die alleen gelden voor Duitse gebruikers zijn [hier](#) beschikbaar.

Definities

Met "Facebook" bedoelen we de functies en services die we beschikbaar stellen, waaronder via (a) onze website op www.facebook.com en andere websites van het Facebook-merk of via co-branding (waaronder subdomeinen, internationale versies, widgets en mobiele versies); (b) ons platform; (c) sociale plug-ins zoals de knop Vind ik leuk, de knop Delen en ander vergelijkbaar aanbod; en (d) andere media, software (zoals een werkbalk), apparaten of netwerken die nu bestaan of later worden ontwikkeld.

Met "Platform" bedoelen we een set API's en services (zoals inhoud) waarmee anderen, waaronder toepassingontwikkelaars en websitebeheerders gegevens kunnen ophalen van Facebook of gegevens aan ons kunnen verstrekken.

Met "informatie" bedoelen we feiten en andere gegevens over jou, waaronder acties door gebruikers en niet-gebruikers die interactie voeren met Facebook.

Met "inhoud" bedoelen we alles wat jij of andere gebruikers plaatsen op Facebook en niet onder de definitie van informatie valt.

Met "gegevens", "gebruikersgegevens" of "gegevens van de gebruiker" bedoelen we alle gegevens, waaronder de inhoud of informatie van een gebruiker die jij of een derde partij kan ophalen van Facebook of aan Facebook kan verstrekken via het platform.

Met "plaatsen" bedoelen we posten op Facebook of op andere wijze beschikbaar stellen door Facebook te gebruiken.

Met "gebruiken" bedoelen we gebruiken, kopiëren, openbaar publiceren of weergeven, distribueren, wijzigen, vertalen en afgeleide producten maken van.

Met "actieve geregistreerde gebruiker" bedoelen we een gebruiker die zich in de afgelopen 30 dagen minimaal eenmaal heeft aangemeld bij Facebook.

Met "toepassing" bedoelen we elke toepassing of website die het platform gebruikt, evenals alle andere dingen die gegevens van ons ontvangen of hebben ontvangen. Als je het platform niet meer gebruikt maar niet alle gegevens van ons hebt verwijderd, geldt de term toepassing totdat je alle gegevens hebt verwijderd.

Overig Als je ingezetene bent van of je voornaamste zakelijke vestigingsplaats hebt in de VS of Canada, is deze Verklaring een overeenkomst tussen jou en Facebook, Inc. Als dit niet het geval is, is deze Verklaring een overeenkomst tussen jou en Facebook Ireland Limited. Verwijzingen naar "ons", "wij" en "onze" zijn verwijzingen naar Facebook, Inc. of Facebook Ireland Limited, afhankelijk van de situatie.

Deze Verklaring vormt de hele overeenkomst tussen de partijen met betrekking tot Facebook en geldt boven eventuele eerdere overeenkomsten.

Indien een deel van deze Verklaring niet-afdwingbaar blijkt te zijn, blijft het resterende deel volledig van kracht en geldig.

Als we iets uit deze Verklaring niet afdwingen, kan dit niet worden beschouwd als toestemming. Een eventuele wijziging of verklaring van afstand van deze Verklaring moet schriftelijk worden gedaan en door ons worden ondertekend.

Je draagt geen rechten of verplichtingen onder deze Verklaring over aan iemand anders zonder dat je onze toestemming hebt.

Al onze rechten en verplichtingen onder deze Verklaring kunnen we vrij toewijzen in het geval van een fusie, overname of verkoop van activa, krachtens de wet of anderszins.

Niets in deze Verklaring zal ons ervan weerhouden om ons aan de wet te houden.

Met deze Verklaring worden geen rechten van derde partijen verleend.

We behouden ons alle rechten voor die niet nadrukkelijk aan jou zijn verleend.

Bij het gebruiken of openen van Facebook houd je je aan alle geldende wetten.

Je kunt ook de volgende documenten bekijken voor meer informatie over je gebruik van Facebook:

- [Beleid inzake gegevensgebruik](#): het Beleid inzake gegevensgebruik bevat informatie om je uit te leggen hoe we informatie verzamelen en gebruiken.
- [Betalingsvoorwaarden](#): deze aanvullende voorwaarden gelden voor alle betalingen die op of via Facebook worden gedaan.
- [Platformpagina](#): op deze pagina wordt uitgelegd wat er gebeurt wanneer je een toepassing van een derde partij toevoegt of Facebook Connect gebruikt. Je leest hier ook hoe zij je gegevens kunnen gebruiken.
- [Beleidsregels van het Facebook-platform](#): in deze richtlijnen staan de beleidsregels die gelden voor toepassingen, waaronder Connect-sites.
- [Advertentierichtlijnen](#): in deze richtlijnen staan de beleidsregels die gelden voor advertenties die geplaatst zijn op Facebook.
- [Promotierichtlijnen](#): in deze richtlijnen staan de beleidsregels die voor jou gelden als je op Facebook prijsvragen, loterijen en andere typen promoties aanbiedt.
- [Brand Permissions Center](#): in deze richtlijnen staan de beleidsregels die gelden voor het gebruik van Facebook-handelsmerken, -logo's en -screenshots.
- [Schending van intellectueel-eigendomsrechten rapporteren](#)
- [Richtlijnen voor Facebook-pagina's](#): deze richtlijnen gelden voor je gebruik van Facebook-pagina's.
- [Richtlijnen voor de community](#): in deze richtlijnen staan onze verwachtingen betreffende de inhoud die je op Facebook plaatst en je activiteiten op Facebook.

Om de Verklaring van de rechten en verantwoordelijkheden te openen in een andere taal, wijzig je de taalinstelling voor je Facebook-sessie door op de taalink te klikken. Deze link bevindt zich op de meeste pagina's in de linkerbovenhoek. Als de Verklaring niet beschikbaar is in de taal die je hebt geselecteerd, wordt standaard de Engelse versie weergegeven.

Bijlage 7.

Beleid inzake gegevens gebruik

Bron: www.facebook.com zoek op: privacybeleid

Informatie die we over jou ontvangen

We krijgen verschillende soorten informatie over jou, waaronder:

Je gegevens

Jouw gegevens is de informatie die verplicht is wanneer je je registreert als lid van de site en de gegevens die je zelf deelt.

1.1 Registratiegegevens Wanneer je je aanmeldt voor Facebook, wordt je gevraagd informatie zoals je naam, e-mailadres, verjaardag en geslacht op te geven. In bepaalde gevallen kun je wellicht ook andere gegevens registreren, zoals je telefoonnummer.

1.2 Gegevens die je zelf deelt Je gegevens omvatten ook de gegevens die je zelf op Facebook deelt, zoals wanneer je een statusupdate plaatst, een foto uploadt of reageert op het verslag van een vriend.

Dit omvat ook de gegevens die jij zelf openbaar maakt wanneer je iets doet, zoals wanneer je een vriend toevoegt, een pagina of website leuk vindt, een plaats aan je verslag toevoegt, onze importeerfunctie gebruikt of wanneer je aangeeft dat je een relatie hebt.

Je naam, profielfoto, omslagfoto's, geslacht, netwerken, gebruikersnaam en gebruikers-ID worden behandeld zoals alle andere gegevens die je openbaar maakt. Meer informatie.

Met je verjaardag kunnen we er bijvoorbeeld voor zorgen dat je inhoud en advertenties te zien krijgt die geschikt zijn voor iemand van jouw leeftijd.

2. Informatie over jou die anderen delen

We ontvangen informatie over jou van je vrienden en anderen, zoals wanneer ze je contactgegevens uploaden, een foto met jou erop plaatsen, je taggen in een foto of statusupdate of bij een locatie, of je toevoegen aan een groep.

Wanneer mensen Facebook gebruiken, kunnen ze informatie over jou en anderen die ze hebben opslaan en delen, zoals wanneer ze hun uitnodigingen en contacten uploaden en beheren.

3. Andere informatie die we over jou hebben ontvangen

We ontvangen ook andere soorten informatie over jou:

3.1 We ontvangen gegevens over je wanneer je iets doet met Facebook, zoals wanneer je iemands tijdlijn bekijkt, een bericht stuurt of ontvangt, zoekt naar een vriend of pagina, een advertentie bekijkt of erop klikt of op een andere manier met dingen interactie hebt, een Facebook Mobile-app gebruikt of wanneer je Facebook-tegoedpunten koopt of andere aankopen doet via Facebook.

3.2 Als je inhoud zoals foto's of video's op Facebook plaatst, kunnen we extra gegevens die hiermee te maken hebben ontvangen (of metagegevens), zoals de tijd, de datum en de plaats waar je de foto of video hebt gemaakt.

3.3 We ontvangen gegevens van de computer, mobiele telefoon of ander apparaat waarmee je een bezoek brengt aan Facebook, ook wanneer meerdere gebruikers zich via hetzelfde apparaat aanmelden. Dit kan bijvoorbeeld je IP-adres zijn en andere informatie over factoren zoals je internet-service, je locatie, het type browser dat je gebruikt (inclusief identificatie) of de pagina's die je bezoekt. We kunnen je GPS-locatie of andere gegevens verkrijgen zodat we je kunnen vertellen of een van je vrienden in de buurt is.

We ontvangen gegevens wanneer je een game, toepassing of website opent die gebruikmaakt van het Facebook-platform of wanneer je naar een website gaat met een Facebook-functie (zoals een sociale plug-in), soms via cookies. Dit kan de datum en de tijd zijn waarop je de site opent, het webadres (de URL), technische informatie over het IP-adres, de browser en het besturingssysteem dat je gebruikt en, als je bent aangemeld op Facebook, je gebruikers-ID.

Soms krijgen we gegevens van onze dochterbedrijven of onze advertentiepartners, klanten en andere externe partijen die ons (of hen) helpen advertenties weer te geven, online-activiteiten te

begrijpen en Facebook in zijn algemeenheid te verbeteren. Als een adverteerder ons bijvoorbeeld informatie over je geeft (zoals hoe je op een advertentie op Facebook of een andere site reageert), dan kunnen we de effectiviteit van die advertenties meten en de kwaliteit van de advertenties verbeteren.

3.6 We stellen ook gegevens samen uit de informatie die we al over jou en je vrienden hebben. Zo kunnen we bijvoorbeeld gegevens over jou op een rijtje zetten om te bepalen welke vrienden we in je nieuwsoverzicht laten zien of om tags voor te stellen voor de foto's die je plaatst. We kunnen je huidige woonplaats samenvoegen met GPS- en andere locatiegegevens die we over je hebben om jou en je vrienden bijvoorbeeld te laten weten welke evenementen er in de buurt worden gehouden [of welke aanbiedingen er zijn waar je wellicht in bent geïnteresseerd. We kunnen ook gegevens over jou gebruiken om je advertenties te laten zien die relevanter voor je kunnen zijn.](#)

Wanneer we je GPS-locatie ontvangen, combineren we deze met andere locatiegegevens die we over je hebben (zoals je huidige woonplaats). Maar we bewaren ze alleen tot ze niet langer nuttig zijn om je services te bieden, zoals het bewaren van je meest recente GPS-coördinaten om je relevante meldingen te sturen.

We geven onze advertentiepartners of klanten pas gegevens nadat we je naam of andere elementen die je persoonlijk zouden kunnen identificeren, hebben verwijderd of wanneer we de gegevens zodanig hebben gecombineerd met de gegevens van anderen dat ze niet meer in verband kunnen worden gebracht met jou.

Openbare gegevens

Wanneer we de term 'openbare gegevens' gebruiken (soms ook wel 'delen met iedereen'), dan bedoelen we daar de gegevens mee die jij openbaar maakt, en de gegevens die altijd openbaar zijn.

4. Gegevens die je openbaar maakt

Als je ervoor kiest je gegevens openbaar te maken, dan is dat precies wat het zegt: iedereen, inclusief mensen die niet op Facebook zitten, kan je gegevens zien.

Als je ervoor kiest je gegevens openbaar te maken, betekent dat ook dat deze gegevens:

- met jou kunnen worden geassocieerd (bijvoorbeeld je naam, profielfoto's, omslagfoto's, Facebook-tijdslijn, gebruikers-ID enzovoort.), zelfs buiten Facebook;
- kunnen worden weergegeven wanneer iemand een zoekopdracht uitvoert op Facebook of via een openbare zoekmachine;
- toegankelijk zijn voor de met Facebook geïntegreerde games, toepassingen en websites die jij en je vrienden gebruiken, en
- toegankelijk zijn voor iedereen die onze API's zoals onze [Graph API](#) gebruikt.

Soms kun je geen publiek selecteren als je iets plaatst (zoals wanneer je op het prikbord van een pagina schrijft of reageert op een nieuwsartikel dat gebruikmaakt van onze reactieplug-in). Dit komt doordat sommige soorten verslagen altijd openbaar zijn. Als algemene regel geldt dat je ervan uit moet gaan dat als je geen [deelpictogram](#) ziet, de informatie openbaar zal zijn.

Wanneer anderen informatie over jou delen, kunnen ze deze ook openbaar maken.

5. Gegevens die altijd openbaar zijn

De onderstaande soorten gegevens zijn altijd openbaar en worden behandeld zoals alle andere gegevens die je zelf openbaar maakt.

- **Naam** Dit helpt je vrienden en familie om jou te vinden. Als je je echte naam liever niet deelt, kun je je account altijd [verwijderen](#).
- **Profielfoto's en omslagfoto's** Dit helpt je vrienden en familie om zeker te weten dat jij het bent. Als je deze foto's liever niet openbaar maakt, kun je ze altijd verwijderen. De vorige foto blijft openbaar zichtbaar in je profielfoto- of omslagfotoalbum staan wanneer je een nieuwe profielfoto of albumfoto toevoegt tenzij je de foto verwijdert.
- **Netwerk** Hiermee kun je zien met wie je gegevens deelt voordat je 'Vrienden en netwerken' instelt als aangepast publiek. Als je je netwerk liever niet openbaar maakt, kun je [het netwerk verlaten](#).
- **Geslacht** Hiermee kunnen we op de juiste wijze aan je refereren.

- **Gebruikersnaam en gebruikers-ID** Hiermee kun je een aangepaste link geven naar je tijdlijn of pagina, e-mail ontvangen op je Facebook-e-mailadres en help je het Facebook-platform mogelijk te maken. [Meer informatie](#).

Gebruikersnamen en gebruikers-ID's

Je Facebook-URL, of gebruikersnaam, is een unieke link naar je tijdlijn die je aan mensen kunt geven of op een externe website kunt plaatsen. Gebruikersnamen staan in de URL van je tijdlijn. We gebruiken je gebruikers-ID ook om je Facebook-account te identificeren.

Als iemand je gebruikersnaam of gebruikers-ID heeft, kunnen ze de informatie gebruiken om gegevens over jou op te zoeken via de website facebook.com. Als iemand bijvoorbeeld jouw gebruikersnaam heeft, kan hij/zij facebook.com/gebruikersnaam invoeren in een browser en jouw openbare gegevens bekijken plus alles waarvoor jij de privacyinstelling Openbaar hebt ingesteld. Zo kan iemand met je gebruikersnaam of gebruikers-ID ook informatie over jou zien via onze API's, zoals onze [Graph API](#). Ze kunnen je openbare gegevens zien plus je leeftijdscategorie, taal en land.

Als je niet wilt dat je gegevens toegankelijk zijn voor platformtoepassingen, kun je alle [platformtoepassingen uitschakelen via je privacyinstellingen](#). Als je het [platform](#) uitschakelt, betekent dat ook dat je geen gebruik meer kunt maken van games of andere toepassingen totdat je het platform weer inschakelt. Ga voor meer informatie over de gegevens die apps ontvangen wanneer je ze gebruikt naar [Andere websites en toepassingen](#).

Als je gegevens wilt zien die via onze Graph API beschikbaar is, typ je gewoon <https://graph.facebook.com/> in je browser.

Je Facebook-e-mailadres omvat je openbare gebruikersnaam, zoals in dit voorbeeld: gebruikersnaam@facebook.com. Alle deelnemers aan een gesprek kunnen een antwoord sturen naar dit adres.

6. Hoe gebruiken we de informatie die we ontvangen?

We gebruiken de gegevens die we over jou ontvangen voor de services en functies die we leveren aan jou en andere gebruikers zoals je vrienden, onze partners, de adverteerders die advertenties op de site kopen en de ontwikkelaars die de games, toepassingen en websites die je gebruikt. We gebruiken de gegevens die we over jou ontvangen bijvoorbeeld niet alleen om mensen te helpen de dingen die jij doet en deelt te zoeken en te zien, maar ook:

- om Facebook-producten, -services en -integraties veilig te houden;
- om de rechten of het eigendom van Facebook en anderen te beschermen;
- om je locatiefuncties en services te bieden zoals jou en je vrienden op de hoogte te stellen dat er een evenement in de buurt plaatsvindt;
- om de effectiviteit van de advertenties die jij en anderen zien, te meten of er meer inzicht in te krijgen, zoals het weergeven van advertenties die voor jou relevantie hebben;
- om voorstellen te doen aan jou en andere gebruikers op Facebook, zoals: dat je vrienden de importeerfunctie voor contactpersonen kunnen gebruiken omdat jij ook via deze weg vrienden hebt gevonden, of dat een andere gebruiker jou als vriend toevoegt omdat die gebruiker hetzelfde e-mailadres heeft geïmporteerd als jij, of dat je vriend je in een foto met jou erop tagt die hij of zij heeft geüpload en
- voor interne bewerkingen, zoals probleemoplossing, gegevensanalyse, tests, onderzoek en verbetering van service.

Door ons deze toestemming te geven, geef je ons niet alleen de mogelijkheid om Facebook aan te bieden zoals het nu is, maar laat je ons ook innovatieve functies en services ontwikkelen die op nieuwe manieren gebruikmaken van de informatie die we over jou ontvangen.

Je blijft de eigenaar van al je gegevens, zelfs al geef je ons toestemming de gegevens die we van je hebben te gebruiken. Jouw vertrouwen is belangrijk voor ons en daarom delen we gegevens over jou niet met anderen tenzij we:

- je toestemming daarvoor hebben;
- je hiervan op de hoogte hebben gesteld door je bijvoorbeeld te informeren via dit beleid; of
- je naam of andere informatie die jou persoonlijk zou kunnen identificeren eruit hebben verwijderd.

Uiteraard bepalen zij voor informatie over jou die anderen delen, hoe deze wordt gedeeld. We slaan gegevens op zolang dat nodig is om producten en services aan jou en anderen te kunnen aanbieden, inclusief degenen die hierboven worden beschreven. Gegevens die normaliter worden geassocieerd met je account, worden bewaard tot je account wordt verwijderd. Voor bepaalde categorieën gegevens, kunnen we je ook meer informatie geven over specifiek beleid voor gegevensretentie.

We kunnen je vriend voorstellen om jou in een foto te taggen door de foto's van je vriend te vergelijken met de informatie die we hebben verzameld uit de foto's waarin je bent getagd. Hierdoor kunnen we deze suggesties doen. Jij bepaalt of we andere gebruikers voorstellen je te taggen in een foto. Dit doe je met behulp van de opties bij Instellingen voor tags. Meer informatie.

Je account verwijderen en deactiveren

Als je je account niet meer wilt gebruiken, kun je het deactiveren of verwijderen.

Deactiveren

Wanneer je je account deactiveert, zet je je account als het ware in de wacht. Andere gebruikers kunnen je tijdelijk niet meer zien, maar we verwijderen geen informatie die in je account is opgeslagen. Een account deactiveren is hetzelfde als ons vertellen geen informatie te verwijderen omdat je je account wellicht in de toekomst weer wilt activeren. Je kunt je account deactiveren op de pagina [Accountinstellingen](#).

Als je account is gedeactiveerd, kunnen je vrienden je nog steeds in hun vriendenlijst zien staan.

Verwijderen

Wanneer je account verwijderd, wordt het account permanent verwijderd van Facebook. Het duurt ongeveer een maand om een account te verwijderen, maar sommige gegevens kunnen tot maximaal negentig dagen bewaard blijven in back-ups en logboeken. Verwijder je account alleen als je er écht zeker van bent dat je het nooit meer wilt activeren. Je kunt je account [hier](#) verwijderen. [Meer informatie](#).

Bepaalde gegevens zijn noodzakelijk om je services te kunnen bieden, dus we verwijderen deze gegevens pas als je je account hebt verwijderd. Sommige dingen die je doet op Facebook worden niet opgeslagen in je account, zoals wanneer je een bericht plaatst in een groep of iemand een bericht stuurt (zelfs nadat je je account hebt verwijderd, kan je vriend nog steeds een bericht hebben dat je hebt verstuurd). Die informatie blijft bestaan nadat je je account hebt verwijderd.

Bijlage 8.

Terms of Service Twitter

Bron: www.twitter.com

These Terms of Service ("**Terms**") govern your access to and use of the services, including our various websites, SMS, APIs, email notifications, applications, buttons, and widgets, (the "**Services**" or "**Twitter**"), and any information, text, graphics, photos or other materials uploaded, downloaded or appearing on the Services (collectively referred to as "**Content**"). Your access to and use of the Services are conditioned on your acceptance of and compliance with these Terms. By accessing or using the Services you agree to be bound by these Terms.

1. Basic Terms

You are responsible for your use of the Services, for any Content you post to the Services, and for any consequences thereof. The Content you submit, post, or display will be able to be viewed by other users of the Services and through third party services and websites (go to the [account settings](#) page to control who sees your Content). You should only provide Content that you are comfortable sharing with others under these Terms.

What you say on Twitter may be viewed all around the world instantly. You are what you Tweet!

You may use the Services only if you can form a binding contract with Twitter and are not a person barred from receiving services under the laws of the United States or other applicable jurisdiction. If you are accepting these Terms and using the Services on behalf of a company, organization, government, or other legal entity, you represent and warrant that you are authorized to do so. You may use the Services only in compliance with these Terms and all applicable local, state, national, and international laws, rules and regulations.

The Services that Twitter provides are always evolving and the form and nature of the Services that Twitter provides may change from time to time without prior notice to you. In addition, Twitter may stop (permanently or temporarily) providing the Services (or any features within the Services) to you or to users generally and may not be able to provide you with prior notice. We also retain the right to create limits on use and storage at our sole discretion at any time without prior notice to you.

The Services may include advertisements, which may be targeted to the Content or information on the Services, queries made through the Services, or other information. The types and extent of advertising by Twitter on the Services are subject to change. In consideration for Twitter granting you access to and use of the Services, you agree that Twitter and its third party providers and partners may place such advertising on the Services or in connection with the display of Content or information from the Services whether submitted by you or others.

2. Privacy

Any information that you provide to Twitter is subject to our Privacy Policy, which governs our collection and use of your information. **You understand that through your use of the Services you consent to the collection and use (as set forth in the Privacy Policy) of this information, including the transfer of this information to the United States and/or other countries for storage, processing and use by Twitter.** As part of providing you the Services, we may need to provide you with certain communications, such as service announcements and administrative messages. These communications are considered part of the Services and your Twitter account, which you may not be able to opt-out from receiving.

Tip You can opt-out of most communications from Twitter including our newsletter, new follower emails, etc. Please see the Notifications tab of Settings for more.

3. Passwords

You are responsible for safeguarding the password that you use to access the Services and for any activities or actions under your password. We encourage you to use "strong" passwords (passwords that use a combination of upper and lower case letters, numbers and symbols) with your account. Twitter cannot and will not be liable for any loss or damage arising from your failure to comply with the above.

4. Content on the Services

All Content, whether publicly posted or privately transmitted, is the sole responsibility of the person who originated such Content. We may not monitor or control the Content posted via the Services and, we cannot take responsibility for such Content. Any use or reliance on any Content or materials posted via the Services or obtained by you through the Services is at your own risk.

We do not endorse, support, represent or guarantee the completeness, truthfulness, accuracy, or reliability of any Content or communications posted via the Services or endorse any opinions expressed via the Services. You understand that by using the Services, you may be exposed to Content that might be offensive, harmful, inaccurate or otherwise inappropriate, or in some cases, postings that have been mislabeled or are otherwise deceptive. Under no circumstances will Twitter be liable in any way for any Content, including, but not limited to, any errors or omissions in any Content, or any loss or damage of any kind incurred as a result of the use of any Content posted, emailed, transmitted or otherwise made available via the Services or broadcast elsewhere.

5. Your Rights

You retain your rights to any Content you submit, post or display on or through the Services. By submitting, posting or displaying Content on or through the Services, you grant us a worldwide, non-exclusive, royalty-free license (with the right to sublicense) to use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute such Content in any and all media or distribution methods (now known or later developed).

Tip This license is you authorizing us to make your Tweets available to the rest of the world and to let others do the same.

You agree that this license includes the right for Twitter to provide, promote, and improve the Services and to make Content submitted to or through the Services available to other companies, organizations or individuals who partner with Twitter for the syndication, broadcast, distribution or publication of such Content on other media and services, subject to our terms and conditions for such Content use.

Twitter has an evolving set of [rules](#) for how ecosystem partners can interact with your Content. These rules exist to enable an open ecosystem with your rights in mind. But what's yours is yours – you own your Content (and your photos are part of that Content).

Such additional uses by Twitter, or other companies, organizations or individuals who partner with Twitter, may be made with no compensation paid to you with respect to the Content that you submit, post, transmit or otherwise make available through the Services.

We may modify or adapt your Content in order to transmit, display or distribute it over computer networks and in various media and/or make changes to your Content as are necessary to conform and adapt that Content to any requirements or limitations of any networks, devices, services or media.

You are responsible for your use of the Services, for any Content you provide, and for any consequences thereof, including the use of your Content by other users and our third party partners. You understand that your Content may be syndicated, broadcast, distributed, or published by our partners and if you do not have the right to submit Content for such use, it may subject you to liability. Twitter will not be responsible or liable for any use of your Content by Twitter in accordance with these Terms. You represent and warrant that you have all the rights, power and authority necessary to grant the rights granted herein to any Content that you submit.

6. Your License To Use the Services

Twitter gives you a personal, worldwide, royalty-free, non-assignable and non-exclusive license to use the software that is provided to you by Twitter as part of the Services. This license is for the sole purpose of enabling you to use and enjoy the benefit of the Services as provided by Twitter, in the manner permitted by these Terms.

7. Twitter Rights

All right, title, and interest in and to the Services (excluding Content provided by users) are and will remain the exclusive property of Twitter and its licensors. The Services are protected by copyright, trademark, and other laws of both the United States and foreign countries. Nothing in the Terms gives you a right to use the Twitter name or any of the Twitter trademarks, logos, domain names, and other distinctive brand features. Any feedback, comments, or suggestions you may provide regarding Twitter, or the Services is entirely voluntary and we will be free to use such feedback, comments or suggestions as we see fit and without any obligation to you.

8. Restrictions on Content and Use of the Services

Please review the [Twitter Rules](#) (which are part of these Terms) to better understand what is prohibited on the Service. We reserve the right at all times (but will not have an obligation) to remove or refuse to distribute any Content on the Services, to suspend or terminate users, and to reclaim usernames without liability to you. We also reserve the right to access, read, preserve, and disclose any information as we reasonably believe is necessary to (i) satisfy any applicable law,

regulation, legal process or governmental request, (ii) enforce the Terms, including investigation of potential violations hereof, (iii) detect, prevent, or otherwise address fraud, security or technical issues, (iv) respond to user support requests, or (v) protect the rights, property or safety of Twitter, its users and the public.

Twitter does not disclose personally identifying information to third parties except in accordance with our [Privacy Policy](#).

Except as permitted through the Services, these Terms, or the terms provided on [dev.twitter.com](#), you have to use the [Twitter API](#) if you want to reproduce, modify, create derivative works, distribute, sell, transfer, publicly display, publicly perform, transmit, or otherwise use the Content or Services.

We encourage and permit broad re-use of Content. The Twitter API exists to enable this.

You may not do any of the following while accessing or using the Services: (i) access, tamper with, or use non-public areas of the Services, Twitter's computer systems, or the technical delivery systems of Twitter's providers; (ii) probe, scan, or test the vulnerability of any system or network or breach or circumvent any security or authentication measures; (iii) access or search or attempt to access or search the Services by any means (automated or otherwise) other than through our currently available, published interfaces that are provided by Twitter (and only pursuant to those terms and conditions), unless you have been specifically allowed to do so in a separate agreement with Twitter (NOTE: crawling the Services is permissible if done in accordance with the provisions of the robots.txt file, however, scraping the Services without the prior consent of Twitter is expressly prohibited); (iv) forge any TCP/IP packet header or any part of the header information in any email or posting, or in any way use the Services to send altered, deceptive or false source-identifying information; or (v) interfere with, or disrupt, (or attempt to do so), the access of any user, host or network, including, without limitation, sending a virus, overloading, flooding, spamming, mail-bombing the Services, or by scripting the creation of Content in such a manner as to interfere with or create an undue burden on the Services.

9. Copyright Policy

Twitter respects the intellectual property rights of others and expects users of the Services to do the same. We will respond to notices of alleged copyright infringement that comply with applicable law and are properly provided to us. If you believe that your Content has been copied in a way that constitutes copyright infringement, please provide us with the following information: (i) a physical or electronic signature of the copyright owner or a person authorized to act on their behalf; (ii) identification of the copyrighted work claimed to have been infringed; (iii) identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit us to locate the material; (iv) your contact information, including your address, telephone number, and an email address; (v) a statement by you that you have a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law; and (vi) a statement that the information in the notification is accurate, and, under penalty of perjury, that you are authorized to act on behalf of the copyright owner.

We reserve the right to remove Content alleged to be infringing without prior notice, at our sole discretion, and without liability to you. In appropriate circumstances, Twitter will also terminate a user's account if the user is determined to be a repeat infringer. Our designated copyright agent for notice of alleged copyright infringement appearing on the Services is:

Twitter, Inc.

Attn: Copyright Agent

1355 Market Street, Suite 900

San Francisco, CA 94103

Reports: <https://support.twitter.com/forms/dmca>

Email: copyright@twitter.com

10. Ending These Terms

The Terms will continue to apply until terminated by either you or Twitter as follows.

You may end your legal agreement with Twitter at any time for any reason by [deactivating](#) your accounts and discontinuing your use of the Services. You do not need to specifically inform Twitter when you stop using the Services. If you stop using the Services without deactivating your accounts, your accounts may be deactivated due to prolonged inactivity under our [Inactive Account Policy](#).

We may suspend or terminate your accounts or cease providing you with all or part of the Services at any time for any reason, including, but not limited to, if we reasonably believe: (i) you have violated these Terms or the [Twitter Rules](#), (ii) you create risk or possible legal exposure for us; or (iii) our provision of the Services to you is no longer commercially viable. We will make reasonable efforts to notify you by the email address associated with your account or the next time you attempt to access your account.

In all such cases, the Terms shall terminate, including, without limitation, your license to use the Services, except that the following sections shall continue to apply: 4, 5, 7, 8, 10, 11, and 12.

Nothing in this section shall affect Twitter's rights to change, limit or stop the provision of the Services without prior notice, as provided above in section 1.

11. Disclaimers and Limitations of Liability

Please read this section carefully since it limits the liability of Twitter and its parents, subsidiaries, affiliates, related companies, officers, directors, employees, agents, representatives, partners, and licensors (collectively, the "Twitter Entities"). Each of the subsections below only applies up to the maximum extent permitted under applicable law. Some jurisdictions do not allow the disclaimer of implied warranties or the limitation of liability in contracts, and as a result the contents of this section may not apply to you. Nothing in this section is intended to limit any rights you may have which may not be lawfully limited.

A. The Services are Available "AS-IS"

Your access to and use of the Services or any Content are at your own risk. You understand and agree that the Services are provided to you on an "AS IS" and "AS AVAILABLE" basis. Without limiting the foregoing, to the maximum extent permitted under applicable law, THE TWITTER ENTITIES DISCLAIM ALL WARRANTIES AND CONDITIONS, WHETHER EXPRESS OR IMPLIED, OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

The Twitter Entities make no warranty and disclaim all responsibility and liability for: (i) the completeness, accuracy, availability, timeliness, security or reliability of the Services or any Content; (ii) any harm to your computer system, loss of data, or other harm that results from your access to or use of the Services or any Content; (iii) the deletion of, or the failure to store or to transmit, any Content and other communications maintained by the Services; and (iv) whether the Services will meet your requirements or be available on an uninterrupted, secure, or error-free basis. No advice or information, whether oral or written, obtained from the Twitter Entities or through the Services, will create any warranty not expressly made herein.

B. Links

The Services may contain links to third-party websites or resources. You acknowledge and agree that the Twitter Entities are not responsible or liable for: (i) the availability or accuracy of such websites or resources; or (ii) the content, products, or services on or available from such websites or resources. Links to such websites or resources do not imply any endorsement by the Twitter Entities of such websites or resources or the content, products, or services available from such websites or resources. You acknowledge sole responsibility for and assume all risk arising from your use of any such websites or resources.

C. Limitation of Liability

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE TWITTER ENTITIES SHALL NOT BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR PUNITIVE DAMAGES, OR ANY LOSS OF PROFITS OR REVENUES, WHETHER INCURRED DIRECTLY OR INDIRECTLY, OR ANY LOSS OF DATA, USE, GOOD-WILL, OR OTHER INTANGIBLE LOSSES, RESULTING FROM (i) YOUR ACCESS TO OR USE OF OR INABILITY TO ACCESS OR USE THE SERVICES; (ii) ANY CONDUCT OR CONTENT OF ANY THIRD PARTY ON THE SERVICES, INCLUDING WITHOUT LIMITATION, ANY DEFAMATORY, OFFENSIVE

OR ILLEGAL CONDUCT OF OTHER USERS OR THIRD PARTIES; (iii) ANY CONTENT OBTAINED FROM THE SERVICES; OR (iv) UNAUTHORIZED ACCESS, USE OR ALTERATION OF YOUR TRANSMISSIONS OR CONTENT.

IN NO EVENT SHALL THE AGGREGATE LIABILITY OF THE TWITTER ENTITIES EXCEED THE GREATER OF ONE HUNDRED U.S. DOLLARS (U.S. \$100.00) OR THE AMOUNT YOU PAID TWITTER, IF ANY, IN THE PAST SIX MONTHS FOR THE SERVICES GIVING RISE TO THE CLAIM.

THE LIMITATIONS OF THIS SUBSECTION SHALL APPLY TO ANY THEORY OF LIABILITY, WHETHER BASED ON WARRANTY, CONTRACT, STATUTE, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE, AND WHETHER OR NOT THE TWITTER ENTITIES HAVE BEEN INFORMED OF THE POSSIBILITY OF ANY SUCH DAMAGE, AND EVEN IF A REMEDY SET FORTH HEREIN IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE.

12. General Terms

A. Waiver and Severability

The failure of Twitter to enforce any right or provision of these Terms will not be deemed a waiver of such right or provision. In the event that any provision of these Terms is held to be invalid or unenforceable, then that provision will be limited or eliminated to the minimum extent necessary, and the remaining provisions of these Terms will remain in full force and effect.

B. Controlling Law and Jurisdiction

These Terms and any action related thereto will be governed by the laws of the State of California without regard to or application of its conflict of law provisions or your state or country of residence. All claims, legal proceedings or litigation arising in connection with the Services will be brought solely in the federal or state courts located in San Francisco County, California, United States, and you consent to the jurisdiction of and venue in such courts and waive any objection as to inconvenient forum.

If you are a federal, state, or local government entity in the United States using the Services in your official capacity and legally unable to accept the controlling law, jurisdiction or venue clauses above, then those clauses do not apply to you. For such U.S. federal government entities, these Terms and any action related thereto will be governed by the laws of the United States of America (without reference to conflict of laws) and, in the absence of federal law and to the extent permitted under federal law, the laws of the State of California (excluding choice of law).

C. Entire Agreement

These Terms, the [Twitter Rules](#) and our [Privacy Policy](#) are the entire and exclusive agreement between Twitter and you regarding the Services (excluding any services for which you have a separate agreement with Twitter that is explicitly in addition or in place of these Terms), and these Terms supersede and replace any prior agreements between Twitter and you regarding the Services. Other than members of the group of companies of which Twitter, Inc. is the parent, no other person or company will be third party beneficiaries to the Terms.

We may revise these Terms from time to time, the most current version will always be at twitter.com/tos. If the revision, in our sole discretion, is material we will notify you via an @Twitter update or e-mail to the email associated with your account. By continuing to access or use the Services after those revisions become effective, you agree to be bound by the revised Terms.

These Services are operated and provided by Twitter Inc., 1355 Market Street, Suite 900, San Francisco, CA 94103. If you have any questions about these Terms, please [contact us](#).

Effective: June 25, 2012

Bijlage 9.

Privacy Policy Twitter

Bron: www.twitter.com

1. Twitter instantly connects people everywhere to what's most meaningful to them. Any registered user can send a Tweet, which is a message of 140 characters or less that is public by default and can include other content like photos, videos, and links to other websites.

What you say on Twitter may be viewed all around the world instantly

This Privacy Policy describes how and when Twitter collects, uses and shares your information when you use our Services. Twitter receives your information through our various websites, SMS, APIs, email notifications, applications, buttons, widgets, and ads (the "**Services**" or "**Twitter**") and from our partners and other third parties. For example, you send us information when you use Twitter from our website, post or receive Tweets via SMS, or access Twitter from an application such as Twitter for Mac, Twitter for Android or TweetDeck. When using any of our Services you consent to the collection, transfer, manipulation, storage, disclosure and other uses of your information as described in this Privacy Policy. Irrespective of which country you reside in or supply information from, you authorize Twitter to use your information in the United States and any other country where Twitter operates.

If you have any questions or comments about this Privacy Policy, please contact us at privacy@twitter.com or [here](#).

Information Collection and Use

We collect and use your information below to provide our Services and to measure and improve them over time.

2. Information Collected Upon Registration: When you create or reconfigure a Twitter account, you provide some personal information, **such as your name, username, password, and email address**. Some of this information, for example, your name and username, is listed publicly on our Services, including on your profile page and in search results. Some Services, such as search, public user profiles and viewing lists, do not require registration.

3. Additional Information: You may provide us with **profile information to make public, such as a short biography, your location, your website, or a picture. You may provide information to customize your account, such as a cell phone number for the delivery of SMS messages.** We may use your contact information to send you information about our Services or to market to you. You may use your account settings to unsubscribe from notifications from Twitter. You may also unsubscribe by following the instructions contained within the notification or the instructions on our website. **We may use your contact information to help others find your Twitter account, including through third-party services and client applications.** Your privacy settings control whether others can find you by your email address or cell phone number. **You may choose to upload your address book so that we can help you find Twitter users you know. We may later suggest people to follow on Twitter based on your imported address book contacts, which you can delete from Twitter at any time.** If you email us, we may keep your message, email address and contact information to respond to your request. If you connect your Twitter account to your account on another service in order to cross-post between Twitter and that service, the other service may send us your registration or profile information on that service and other information that you authorize. This information enables cross-posting, helps us improve the Services, and is deleted from Twitter within a few weeks of your disconnecting from Twitter your account on the other service. Learn more [here](#). Providing the additional information described in this section is entirely optional.

4. Tweets, Following, Lists and other Public Information: Our Services are primarily designed to help you share information with the world. Most of the information you provide us is information you are asking us to make public. This includes not only the messages you Tweet and the metadata provided with Tweets, such as when you Tweeted, but also the lists you create, the people you follow, the Tweets you mark as favorites or Retweet, and many other bits of information that result from your use of the Services. Our default is almost always to make the information you provide public for as long as you do not delete it from Twitter, but we generally give you settings to make the information **more private if you want**. Your public information is broadly and instantly disseminated. For instance, your public user profile information and public Tweets may be searchable by search engines and are immediately delivered via SMS and our [APIs](#) to a wide range of users and services, with one example being the United States Library of Congress, which archives Tweets for historical purposes. When you

share information or content like photos, videos, and links via the Services, you should think carefully about what you are making public.

5. Location Information: You may choose to publish your location in your Tweets and in your Twitter profile. You may also tell us your location when you set your trend location on Twitter.com or enable your computer or mobile device to send us location information. You can set your Tweet location preferences in your [account settings](#) and learn more about this feature [here](#). Learn how to set your mobile location preferences [here](#). We may use and store information about your location to provide features of our Services, such as Tweeting with your location, and to improve and customize the Services, for example, with more relevant content like local trends, stories, ads, and suggestions for people to follow.

6. Links: Twitter may keep track of how you interact with links across our Services, including our email notifications, third-party services, and client applications, by redirecting clicks or through other means. We do this to help improve our Services, to provide more relevant advertising, and to be able to share aggregate click statistics such as how many times a particular link was clicked on.

7. Cookies: Like many websites, we use cookies and similar technologies to collect additional website usage data and to improve our Services, but we do not require cookies for many parts of our Services such as searching and looking at public user profiles or lists. A cookie is a small data file that is transferred to your computer's hard disk. Twitter may use both session cookies and persistent cookies to better understand how you interact with our Services, to monitor aggregate usage by our users and web traffic routing on our Services, and to customize and improve our Services. Most Internet browsers automatically accept cookies. You can instruct your browser, by changing its settings, to stop accepting cookies or to prompt you before accepting a cookie from the websites you visit. However, some Services may not function properly if you disable cookies. Learn more about how we use cookies and similar technologies [here](#).

8. Log Data: Our servers automatically record information ("**Log Data**") created by your use of the Services. **Log Data may include information such as your IP address, browser type, operating system, the referring web page, pages visited, location, your mobile carrier, device and application IDs, search terms, and cookie information. We receive Log Data when you interact with our Services, for example, when you visit our websites, sign into our Services, interact with our email notifications, use your Twitter account to authenticate to a third-party website or application, or visit a third-party website that includes a Twitter button or widget. Twitter uses Log Data to provide our Services and to measure, customize, and improve them.** If not already done earlier, for example, as provided below for Widget Data, we will either delete Log Data or remove any common account identifiers, such as your username, full IP address, or email address, after **18 months**.

9. Widget Data: We may tailor content for you based on your visits to third-party websites that integrate Twitter buttons or widgets. When these websites first load our buttons or widgets for display, we receive Log Data, including the web page you visited and a cookie that identifies your browser ("**Widget Data**"). After a maximum of 10 days, we start the process of deleting or aggregating Widget Data, which is usually instantaneous but in some cases may take up to a week. While we have the Widget Data, we may use it to tailor content for you, such as suggestions for people to follow on Twitter. Tailored content is stored with only your browser cookie ID and is separated from other Widget Data such as page-visit information. This feature is optional and not yet available to all users. If you want, you can suspend it or turn it off, which removes from your browser the unique cookie that enables the feature. Learn more about the feature [here](#). For Tweets, Log Data, and other information that we receive from interactions with Twitter buttons or widgets, please see the other sections of this Privacy Policy.

10. Third-Parties: Twitter uses a variety of third-party services to help provide our Services, such as hosting our various blogs and wikis, and to help us understand the use of our Services, such as Google Analytics. These third-party service providers may collect information sent by your browser as part of a web page request, such as cookies or your IP address. Third-party ad partners may share information with us, like a browser cookie ID or cryptographic hash of a common account identifier (such as an email address), to help us measure ad quality and tailor ads. For example, this allows us to display ads about things you may have already shown interest in. If you prefer, you can turn off

tailored ads in your [privacy settings](#) so that your account is not matched to information shared by ad partners for tailoring ads. Learn more about this setting and your additional Do Not Track browser option [here](#).

Information Sharing and Disclosure

We do not disclose your private personal information except in the limited circumstances described here.

11. Your Consent: We may share or disclose your information at your direction, such as when you authorize a third-party web client or application to access your Twitter account.

12. Service Providers: We engage service providers to perform functions and provide services to us in the United States and abroad. We may share your private personal information with such service providers subject to confidentiality obligations consistent with this Privacy Policy, and on the condition that the third parties use your private personal data only on our behalf and pursuant to our instructions.

13. Law and Harm: Notwithstanding anything to the contrary in this Policy, we may preserve or disclose your information if we believe that it is reasonably necessary to comply with a law, regulation or legal request; to protect the safety of any person; to address fraud, security or technical issues; or to protect Twitter's rights or property. However, nothing in this Privacy Policy is intended to limit any legal defenses or objections that you may have to a third party's, including a government's, request to disclose your information.

14. Business Transfers: In the event that Twitter is involved in a bankruptcy, merger, acquisition, reorganization or sale of assets, your information may be sold or transferred as part of that transaction. The promises in this Privacy Policy will apply to your information as transferred to the new entity.

15. Non-Private or Non-Personal Information: We may share or disclose your non-private, aggregated or otherwise non-personal information, such as your public user profile information, public Tweets, the people you follow or that follow you, or the number of users who clicked on a particular link (even if only one did).

Modifying Your Personal Information

If you are a registered user of our Services, we provide you with tools and [account settings](#) to access or modify the personal information you provided to us and associated with your account.

You can also permanently delete your Twitter account. If you follow the instructions [here](#), your account will be deactivated and then deleted. When your account is deactivated, it is not viewable on Twitter.com. For up to 30 days after deactivation it is still possible to restore your account if it was accidentally or wrongfully deactivated. After 30 days, we begin the process of deleting your account from our systems, which can take up to a week.

16. Our Policy Towards Children

Our Services are not directed to persons under 13. If you become aware that your child has provided us with personal information without your consent, please contact us at privacy@twitter.com. We do not knowingly collect personal information from children under 13. If we become aware that a child under 13 has provided us with personal information, we take steps to remove such information and terminate the child's account. You can find additional resources for parents and teens [here](#).

17. EU Safe Harbor Framework

[Twitter complies with the U.S.-E.U. and U.S.-Swiss Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement. To learn more about the Safe Harbor program, and to view our certification, please visit the U.S. Department of Commerce website.](#)

Changes to this Policy

We may revise this Privacy Policy from time to time. The most current version of the policy will govern our use of your information and will always be at <https://twitter.com/privacy>. If we make a change to this policy that, in our sole discretion, is material, we will notify you via an @Twitter update or email to the email address associated with your account. By continuing to access or use the Services after those changes become effective, you agree to be bound by the revised Privacy

Policy.

Effective: October 21, 2013

Bijlage 10.

Terms of Service Whatsapp

Bron: www.whatsapp.com

1. Your Acceptance

This is an agreement between WhatsApp Inc., a California corporation ("WhatsApp"), the owner and operator of www.whatsapp.com (the "WhatsApp Site"), the WhatsApp software, including WhatsApp Messenger (collectively, including all content provided by WhatsApp through WhatsApp Messenger and the WhatsApp Site, the "WhatsApp Service", or the "Service"), and you ("you" or "You"), a user of the Service. BY USING THE SERVICE, YOU ACKNOWLEDGE AND AGREE TO THESE TERMS OF SERVICE, AND WHATSAPP'S PRIVACY POLICY, WHICH CAN BE FOUND AT <http://www.whatsapp.com/legal/#Privacy>, AND WHICH ARE INCORPORATED HEREIN BY REFERENCE. If you choose to not agree with any of these terms, you may not use the Service.

2. WhatsApp Service

These Terms of Service apply to all users of the WhatsApp Service. Information provided by our users through the WhatsApp Service may contain links to third party websites that are not owned or controlled by WhatsApp. WhatsApp has no control over, and assumes no responsibility for, the content, privacy policies, or practices of any third party websites. In addition, WhatsApp will not and cannot censor or edit the content of any third-party site. By using the Service, you expressly acknowledge and agree that WhatsApp shall not be responsible for any damages, claims or other liability arising from or related to your use of any third-party website.

3. WhatsApp Access

A. Subject to your compliance with these Terms of Service, WhatsApp hereby grants you permission to use the Service, provided that: (i) your use of the Service as permitted is solely for your personal use, and you are not permitted to resell or charge others for use of or access to the Service, or in any other manner inconsistent with these Terms of Service; (ii) you will not duplicate, transfer, give access to, copy or distribute any part of the Service in any medium without WhatsApp's prior written authorization; (iii) you will not attempt to reverse engineer, alter or modify any part of the Service; and (iv) you will otherwise comply with the terms and conditions of these Terms of Service and Privacy Policy.

B. In order to access and use the features of the Service, you acknowledge and agree that you will have to provide WhatsApp with your mobile phone number. You expressly acknowledge and agree that in order to provide the Service, WhatsApp may periodically access your contact list and/or address book on your mobile device to find and keep track of mobile phone numbers of other users of the Service. When providing your mobile phone number, you must provide accurate and complete information. You hereby give your express consent to WhatsApp to access your contact list and/or address book for mobile phone numbers in order to provide and use the Service. We do not collect names, addresses or email addresses, just mobile phone numbers. You are solely responsible for the status messages that you submit and that are displayed for your mobile phone number on the WhatsApp Service. You must notify WhatsApp immediately of any breach of security or unauthorized use of your mobile phone. Although WhatsApp will not be liable for your losses caused by any unauthorized use of your account, you may be liable for the losses of WhatsApp or others due to such unauthorized use.

C. You agree not to use or launch any automated system, including without limitation, "robots," "spiders," "offline readers," etc. or "load testers" such as wget, apache bench, mswebstress, httload, blitz, Xcode Automator, Android Monkey, etc., that accesses the Service in a manner that sends more request messages to the WhatsApp servers in a given period of time than a human can reasonably produce in the same period by using a WhatsApp application, and you are forbidden from ripping the content unless specifically allowed. Notwithstanding the foregoing, WhatsApp grants the operators of public search engines permission to use spiders to copy materials from the website for the sole purpose of creating publicly available searchable indices of the materials, but not caches or archives of such materials. WhatsApp reserves the right to revoke these exceptions either generally or in specific cases. While we don't disallow the use of sniffers such as Ethereal, tcpdump or HTTPWatch in general, we do disallow any efforts to reverse-engineer our system, our protocols, or explore outside the boundaries of the normal requests made by WhatsApp clients. We have to disallow using request modification tools such as fiddler or whisker, or the like or any other such tools activities that are meant to explore or harm, penetrate or test the site. You must secure our permission before you measure, test, health check or otherwise monitor any network equipment, servers or assets hosted on our domain. You agree not to collect or harvest any personally identifiable information, including phone number, from the Service, nor to use the communication systems provided by the Service for any commercial solicitation or spam purposes. You agree not to spam, or solicit for commercial purposes, any users of the Service.

4. Intellectual Property Rights

The design of the WhatsApp Service along with WhatsApp created text, scripts, graphics, interactive features and the like, except Status Submissions (as defined below), and the trademarks, service marks and logos contained therein ("Marks"), are owned by or licensed to WhatsApp, subject to copyright and other intellectual property rights under United States and foreign laws and international conventions. The Service is provided to you AS IS for your information and personal use only. WhatsApp reserves all rights not expressly granted in and to the Service. You agree to not engage in the use, copying, or distribution of any of the Service other than expressly permitted herein, including any use, copying, or distribution of Status Submissions of third parties obtained through the Service for any commercial purposes.

5. User Status Submissions

A. The WhatsApp Service allows WhatsApp users to submit status text, profile photos and other communications submitted by you, as well as the automatic submission of your "last seen" status (collectively, the "Status Submissions"). These Status Submissions may be hosted, shared, and/or published as part of the WhatsApp Service, and may be visible to other users of the Service who have your mobile phone number in their mobile phone and which you have not expressly blocked. For clarity, direct messages, location data and photos or files that you send directly to other WhatsApp users will only be viewable by those WhatsApp user(s) or group(s) you directly send such information; but Status Submissions may be globally viewed by WhatsApp users that have your mobile phone number on their smartphone, unless the user is blocked by you. Currently, we have no method of providing different levels of visibility of your Status Submissions among users that have your mobile phone number – you acknowledge and agree that any Status Submissions may be globally viewed by users that have your mobile phone number, so don't submit or post status messages or profile photos that you don't want to be seen globally. A good rule of thumb is if you don't want the whole world to know something or see something, don't submit it as a Status Submission to the Service. The submission of your 'last seen' status is done on an automatic basis. As clarified in the following section, you retain your ownership rights in your Status Submissions. You understand that whether or not such Status Submissions are published, WhatsApp does not guarantee any confidentiality with respect to any submissions.

B. You shall be solely responsible for your own Status Submissions and the consequences of posting or publishing them. Because WhatsApp is only acting as a repository of data, user submitted statuses

do not necessarily represent the views or opinions of WhatsApp, and WhatsApp makes no guarantees as to the validity, accuracy or legal status of any status. In connection with Status Submissions, you affirm, represent, and/or warrant that: (i) you own or have the necessary licenses, rights, consents, and permissions to use and authorize WhatsApp to use all patent, trademark, trade secret, copyright or other proprietary rights in and to any and all Status Submissions to enable inclusion and use of the Status Submissions in the manner contemplated by the Service and these

Terms of Service; and (ii) you have the written consent, release, and/or permission of each and every identifiable individual person in the Status Submission to use the name or likeness of each and every such identifiable individual person to enable inclusion and use of the Status Submissions in the manner contemplated by the Service and these Terms of Service. To be clear: you retain all of your ownership rights in your Status Submissions, but you have to have the rights in the first place. However, by submitting the Status Submissions to WhatsApp, you hereby grant WhatsApp a worldwide, non-exclusive, royalty-free, sublicenseable and transferable license to use, reproduce, distribute, prepare derivative works of, display, and perform the Status Submissions in connection with the WhatsApp Service and WhatsApp's (and its successor's) business, including without limitation for promoting and redistributing part or all of the WhatsApp Service (and derivative works thereof) in any media formats and through any media channels. You also hereby grant each subscriber to your status on the WhatsApp Service a non-exclusive license to access your Status Submissions through the Service. The foregoing license granted by you terminates once you remove or delete a Status Submission from the WhatsApp Service.

C. In connection with Status Submissions, you further agree that you will not: (i) submit material that is copyrighted, protected by trade secret or otherwise subject to third party proprietary rights, including privacy and publicity rights, unless you are the owner of such rights or have permission from their rightful owner to post the material and to grant WhatsApp all of the license rights granted herein; (ii) publish falsehoods or misrepresentations that could damage WhatsApp or any third party; (iii) submit material that is unlawful, obscene, defamatory, libelous, threatening, harassing, hateful, racially or ethnically offensive, or encourages conduct that would be considered a criminal offense, give rise to civil liability, violate any law, or is otherwise inappropriate; (iv) post advertisements or solicitations of business; (v) impersonate another person; (vi) send or store material containing software viruses, worms, Trojan horses or other harmful computer code, files, scripts, agents or programs; (vii) interfere with or disrupt the integrity or performance of the Service or the data contained therein; or (viii) attempt to gain unauthorized access to the Service or its related systems or networks.

D. Adult content must be identified as such. WhatsApp does not endorse any Status Submission or any opinion, recommendation, or advice expressed therein, and WhatsApp expressly disclaims any and all liability in connection with Status Submissions. WhatsApp does not permit copyright infringing activities and infringement of intellectual property rights via its Service, and WhatsApp will remove all content and Status Submissions if properly notified that such content or Status Submission infringes on another's intellectual property rights. To file a copyright infringement notification, please send a written communication that includes substantially the following (see Section 512(c)(3) of the Digital Millennium Copyright Act): (i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed; (ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works; (iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material, including the mobile phone number of the WhatsApp user allegedly infringing the copyrighted work; (iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted; (v) A statement that the complaining party has a good faith belief that use of the

material in the manner complained of is not authorized by the copyright owner, its agent, or the law; and (vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed. Such takedown notices may be emailed to support at whatsapp.com. WhatsApp reserves the right to remove content and Status Submissions without prior notice. WhatsApp may also terminate a user's access to the Service, if they are determined to be a repeat infringer, or for any or no reason, including being annoying. A repeat infringer is a User who has been notified of infringing activity more than once and/or has had a Status Submission removed from the Service more than twice. An annoying person is anyone who is (capriciously or not) determined to be annoying by authorized WhatsApp employees, agents, subagents, superagents or superheros. WhatsApp also reserves the right to decide whether content or a Status Submission is appropriate and complies with these Terms of Service for violations other than copyright infringement and violations of intellectual property law, such as, but not limited to excessive length or limited interest. WhatsApp may remove such Status Submissions and/or terminate a User's access for uploading such material in violation of these Terms of Service at any time, without prior notice and at its sole discretion.

E. You understand that when using the WhatsApp Service you will be exposed to Status Submissions from a variety of sources, and that WhatsApp is not responsible for the accuracy, usefulness, safety, or intellectual property rights of or relating to such Status Submissions, and that such Status Submissions are not the responsibility of WhatsApp. You further understand and acknowledge that you may be exposed to Status Submissions that are inaccurate, offensive, indecent, or objectionable, and you agree to waive, and hereby do waive, any legal or equitable rights or remedies you have or may have against WhatsApp with respect thereto, and agree to indemnify and hold WhatsApp, its officers, directors, employees, agents, affiliates, and/or licensors, harmless to the fullest extent allowed by law regarding all matters related to your use of the WhatsApp Service.

F. WhatsApp permits you to link to materials on the Service for personal purposes only. WhatsApp reserves the right to discontinue any aspect of the WhatsApp Service at any time.

6. Warranty Disclaimer

YOU AGREE THAT YOUR USE OF THE WHATSAPP SERVICE SHALL BE AT YOUR SOLE RISK. TO THE FULLEST EXTENT PERMITTED BY LAW, WHATSAPP, ITS OFFICERS, DIRECTORS, EMPLOYEES, AND AGENTS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, IN CONNECTION WITH THE SERVICE AND YOUR USE THEREOF. WHATSAPP MAKES NO WARRANTIES OR REPRESENTATIONS ABOUT THE ACCURACY OR COMPLETENESS OF THIS SERVICE'S CONTENT AND ASSUMES NO LIABILITY OR RESPONSIBILITY FOR ANY (I) ERRORS, MISTAKES, OR INACCURACIES OF CONTENT, (II) PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM YOUR ACCESS TO AND USE OF OUR SERVICE, (III) ANY UNAUTHORIZED ACCESS TO OR USE OF OUR SERVERS AND/OR ANY AND ALL PERSONAL INFORMATION AND/OR FINANCIAL INFORMATION STORED THEREIN, (IV) ANY INTERRUPTION OR CESSATION OF TRANSMISSION TO OR FROM OUR SERVICE, (V) ANY BUGS, VIRUSES, TROJAN HORSES, OR THE LIKE WHICH MAY BE TRANSMITTED TO OR THROUGH OUR SERVICE THROUGH THE ACTIONS OF ANY THIRD PARTY, AND/OR (VI) ANY ERRORS OR OMISSIONS IN ANY CONTENT OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT POSTED, EMAILED, TRANSMITTED, OR OTHERWISE MADE AVAILABLE VIA THE WHATSAPP SERVICE. WHATSAPP DOES NOT WARRANT, ENDORSE, GUARANTEE, OR ASSUME RESPONSIBILITY FOR ANY PRODUCT OR SERVICE ADVERTISED OR OFFERED BY A THIRD PARTY THROUGH THE WHATSAPP SERVICE OR ANY HYPERLINKED WEBSITE OR FEATURED IN ANY USER STATUS SUBMISSION OR OTHER ADVERTISING, AND WHATSAPP WILL NOT BE A PARTY TO OR IN ANY WAY BE RESPONSIBLE FOR MONITORING ANY TRANSACTION BETWEEN YOU AND THIRD-PARTY PROVIDERS OF PRODUCTS OR SERVICES. AS WITH THE PURCHASE OF A PRODUCT OR SERVICE THROUGH ANY MEDIUM OR IN ANY ENVIRONMENT, YOU SHOULD USE YOUR BEST JUDGMENT AND EXERCISE CAUTION WHERE APPROPRIATE. AND AGAIN, USE THIS JUST FOR FUN.

7. Limitation of Liability

IN NO EVENT SHALL WHATSAPP, ITS OFFICERS, DIRECTORS, EMPLOYEES, OR AGENTS, BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES WHATSOEVER RESULTING FROM ANY (I) ERRORS, MISTAKES, OR INACCURACIES OF CONTENT, (II) PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM YOUR ACCESS TO AND USE OF OUR SERVICE, (III) ANY UNAUTHORIZED ACCESS TO OR USE OF OUR SECURE SERVERS AND/OR ANY AND ALL PERSONAL INFORMATION AND/OR FINANCIAL INFORMATION STORED THEREIN, (IV) ANY INTERRUPTION OR CESSATION OF TRANSMISSION TO OR FROM OUR SERVERS, (V) ANY BUGS, VIRUSES, TROJAN HORSES, OR THE LIKE, WHICH MAY BE TRANSMITTED TO OR THROUGH OUR SERVICE BY ANY THIRD PARTY, (VI) ANY ERRORS OR OMISSIONS IN ANY CONTENT OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF YOUR USE OF ANY CONTENT POSTED, EMAILED, TRANSMITTED, OR OTHERWISE MADE AVAILABLE VIA THE WHATSAPP CLIENT, WHETHER BASED ON WARRANTY, CONTRACT, TORT, OR ANY OTHER LEGAL THEORY, AND WHETHER OR NOT THE COMPANY IS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND/OR (VII) THE DISCLOSURE OF INFORMATION PURSUANT TO THESE TERMS OF SERVICE OR PRIVACY POLICY. THE FOREGOING LIMITATION OF LIABILITY SHALL APPLY TO THE FULLEST EXTENT PERMITTED BY LAW IN THE APPLICABLE JURISDICTION.

YOU SPECIFICALLY ACKNOWLEDGE THAT WHATSAPP SHALL NOT BE LIABLE FOR USER SUBMISSIONS OR THE DEFAMATORY, OFFENSIVE, OR ILLEGAL CONDUCT OF ANY THIRD PARTY AND THAT THE RISK OF HARM OR DAMAGE FROM THE FOREGOING RESTS ENTIRELY WITH YOU.

The Service is controlled and offered by WhatsApp from its facilities in the United States of America. WhatsApp makes no representations that the WhatsApp Service is appropriate or available for use in other locations. Those who access or use the WhatsApp Service from other jurisdictions do so at their own volition and are responsible for compliance with local law.

8. Indemnity

You agree to defend, indemnify and hold harmless WhatsApp, its parent corporation, officers, directors, employees and agents, from and against any and all claims, damages, obligations, losses, liabilities, costs or debt, and expenses (including but not limited to attorney's fees) arising from: (i) your use of and access to the WhatsApp Service; (ii) your violation of any term of these Terms of Service; (iii) your violation of any third party right, including without limitation any copyright, property, or privacy right; or (iv) any claim that one of your Status Submissions caused damage to a third party. This defense and indemnification obligation will survive these Terms of Service and your use of the WhatsApp Service. We don't support or encourage illegal consumption of alcohol or tobacco, so there.

9. Ability to Accept Terms of Service

You affirm that you are either more than 16 years of age, or an emancipated minor, or possess legal parental or guardian consent, and are fully able and competent to enter into the terms, conditions, obligations, affirmations, representations, and warranties set forth in these Terms of Service, and to abide by and comply with these Terms of Service. In any case, you affirm that you are at least 16 years old as the WhatsApp Service is not intended for children under 16. If you are under 16 years of age, you are not permitted to use the WhatsApp Service. You further represent and warrant that you are not located in a country that is subject to a U.S. Government embargo, or that has been designated by the U.S. Government as a "terrorist-supporting" country, and that you are not listed on any U.S. Government list of prohibited or restricted parties. WhatsApp is the developer of the Service, with an address at 3561 Homestead Road, #416, Santa Clara, CA 95010-5161, info at whatsapp.com.

10. Assignment

These Terms of Service, and any rights and licenses granted hereunder, may not be transferred or assigned by you, but may be assigned by WhatsApp without restriction.

11. General

You agree that: (i) the WhatsApp Service shall be deemed solely based in California; (ii) the WhatsApp Service shall be deemed a passive server that does not give rise to personal jurisdiction over WhatsApp, either specific or general, in jurisdictions other than California; and (iii) that you agree to subject to the jurisdiction of California in the event of any legal dispute. These Terms of Service shall be governed by the internal substantive laws of the State of California, without respect to its conflict of laws principles. Any claim or dispute between you and WhatsApp that arises in whole or in part from the WhatsApp Service shall be decided exclusively by a court of competent jurisdiction located in Santa Clara County, California. These Terms of Service, together with the Privacy Policy at <http://www.whatsapp.com/legal/#Privacy> and any other legal notices published by WhatsApp, including, but not limited to an end user license agreement, shall constitute the entire agreement between you and WhatsApp concerning the WhatsApp Service. If any provision of these Terms of Service is deemed invalid by a court of competent jurisdiction, the invalidity of such provision shall not affect the validity of the remaining provisions of these Terms of Service, which shall remain in full force and effect. No waiver of any term of this these Terms of Service shall be deemed a further or continuing waiver of such term or any other term, and WhatsApp's failure to assert any right or provision under these Terms of Service shall not constitute a waiver of such right or provision. WhatsApp reserves the right to amend or modify these Terms of Service at any time, and it is your responsibility to review these Terms of Service for any changes. If you do not agree to the revised Terms, your only recourse is to discontinue the use of the WhatsApp Service. Your continued use of the WhatsApp Service following any amendment of these Terms of Service will signify your assent to and acceptance of its revised terms. YOU AND WHATSAPP AGREE THAT ANY CAUSE OF ACTION ARISING OUT OF OR RELATED TO THE WHATSAPP SERVICE MUST COMMENCE WITHIN ONE (1) YEAR AFTER THE CAUSE OF ACTION ACCRUES. OTHERWISE, SUCH CAUSE OF ACTION IS PERMANENTLY BARRED.

Privacy Notice

WhatsApp Inc. ("WhatsApp") recognizes that its customers, visitors and users, want to know what's up with privacy. WhatsApp provides this Privacy Policy to help you make an informed decision about whether to use or continue using the WhatsApp Site, WhatsApp Software and/or the WhatsApp Service. If you do not agree to our practices, please do not use the WhatsApp Site, WhatsApp Software, or WhatsApp Service. This Privacy Policy is incorporated into and is subject to the WhatsApp Terms of Service. Your use of the WhatsApp Site, WhatsApp Software and the WhatsApp Service and any personal information you provide on the WhatsApp Site or WhatsApp Service remains subject to the terms of this Privacy Policy and our Terms of Service.

Please note that any Status Submissions or other content posted at the direction or discretion of users of the WhatsApp Service becomes published content and is not considered personally identifiable information subject to this Privacy Policy.

1. What Does This Privacy Policy Cover?

This Privacy Policy is part of WhatsApp's Terms of Service and covers the treatment of user information, including personally identifying information, obtained by WhatsApp, including information obtained when you access the WhatsApp's Site, use the WhatsApp Service or any other software provided by WhatsApp.

This Privacy Policy does not apply to the practices of companies that WhatsApp does not own or control, or to individuals whom WhatsApp does not employ or manage, including any of the third parties to which WhatsApp may disclose user information as set forth in this Privacy Policy.

2. The Information WhatsApp Collects

WhatsApp may obtain the following types of information from or concerning you or your mobile phone device, which may include information that can be used to identify you as specified below (“Personally Identifying Information”):

3. User Provided Information: You provide certain Personally Identifiable Information, such as your mobile phone number, push notification name (if applicable), billing information (if applicable) and mobile device information to WhatsApp when choosing to participate in various uses of the WhatsApp Service, such as registering as a user, updating your status or requesting status for your contacts. **In order to provide the WhatsApp Service, WhatsApp will periodically access your address book or contact list on your mobile phone to locate the mobile phone numbers of other WhatsApp users (“in-network” numbers), or otherwise categorize other mobile phone numbers as “out-network” numbers, which are stored as one-way irreversibly hashed values.**

4. Cookies Information: When you visit the WhatsApp Site, we may send one or more cookies - a small text file containing a string of alphanumeric characters - to your computer that uniquely identifies your browser. WhatsApp uses both session cookies and persistent cookies. A persistent cookie remains after you close your browser. Persistent cookies may be used by your browser on subsequent visits to the site. Persistent cookies can be removed by following your web browser help file directions. A session cookie is temporary and disappears after you close your browser. You can reset your web browser to refuse all cookies or to indicate when a cookie is being sent. However, the WhatsApp Site may not function properly if the ability to accept cookies is disabled.

5. Log File Information: When you use the WhatsApp Site, our servers automatically record certain information that your web browser sends whenever you visit any website. These server logs may include information such as your web request, Internet Protocol ("IP") address, browser type, browser language, referring / exit pages and URLs, platform type, number of clicks, domain names, landing pages, pages viewed and the order of those pages, the amount of time spent on particular pages, the date and time of your request, one or more cookies that may uniquely identify your browser, your phone number, phone number you are requesting the status of and various status information. When you use the WhatsApp Service, our servers log certain general information that our application sends whenever a message is sent or received, or if you update or request any status information, including time and date stamps and the mobile phone numbers the messages were sent from and to.

6. The Information WhatsApp Does Not Collect

WhatsApp does not collect names, emails, addresses or other contact information from its users' mobile address book or contact lists other than mobile phone numbers—the WhatsApp mobile application will associate whatever name the WhatsApp user has assigned to the mobile telephone number in his/her mobile address book or contact list — and this occurs dynamically on the mobile device itself and not on WhatsApp's servers and is not transmitted to WhatsApp. This means that if you have your friend's mobile phone number associated with the name “Shakespeare” in your mobile address book, that's the name that will appear for that mobile phone number in your WhatsApp contact list. We do not collect location data, but users may voluntarily share their location with other users via the WhatsApp Service.

The contents of messages that have been delivered by the WhatsApp Service are not copied, kept or archived by WhatsApp in the normal course of business. The WhatsApp Service is meant to be a SMS replacement, using data service through a user's phone (either via cell network or wifi). Users type their messages, which are sent via data service to our servers, and routed to the intended recipient (who must also be a WhatsApp user), if that recipient is online. If the recipient is not online, the undelivered message is held in WhatsApp's server until it can be delivered. If the message is undelivered for thirty (30) days, the undelivered message is deleted from our servers. Once a message has been delivered, it no longer resides on our servers. The contents of any delivered messages are not kept or retained by WhatsApp — the only records of the content of any delivered messages reside directly on the sender's and recipient's mobile devices (and which may be deleted at the user's option). Notwithstanding the above, WhatsApp may retain date and time stamp information associated with successfully delivered messages and the mobile phone numbers involved in the messages, as well as any other information which WhatsApp is legally compelled to collect. Files that are sent through the WhatsApp Service will reside on our servers after delivery for a short period of time, but are deleted and stripped of any identifiable information within a short period of time in accordance with our general retention policies.

7. The Way WhatsApp Uses Information

If you submit Personally Identifiable Information to us through the WhatsApp Site, or WhatsApp Service, [then we use your personal information to operate, maintain, and provide to you the features and functionality of the WhatsApp Site and WhatsApp Service](#). In particular, your mobile phone number is essential to your use of the WhatsApp Service and will be retained. Any billing information that may be collected from you will be deleted thirty (30) days after the termination of your account with WhatsApp. Any Personally Identifiable Information or status content that you voluntarily disclose on the WhatsApp Service becomes publicly available and may be collected and used by other users of the WhatsApp Service (unless such user is blocked by you). Your name (as it is saved in other user's mobile phone address book or contact list) may be displayed to other users when you update your status messages through the WhatsApp Service and other users may contact you through the WhatsApp Service. [We do not use your mobile phone number or other Personally Identifiable Information to send commercial or marketing messages without your consent or except as part of a specific program or feature for which you will have the ability to opt-in or opt-out. We may, however, use your mobile phone number \(or email address, if provided\) without further consent for non-marketing or administrative purposes \(such as notifying you of major WhatsApp Site or WhatsApp Service changes or for customer service purposes\)](#). We may use both your Personally Identifiable Information and certain non-personally-identifiable information (such as anonymous user usage data, cookies, IP addresses, browser type, clickstream data, etc.) to improve the quality and design of the WhatsApp Site and WhatsApp Service and to create new features, promotions, functionality, and services by storing, tracking, and analyzing user preferences and trends. Hopefully we improve the WhatsApp Site and Service and don't make it suck worse. We may use cookies and log file information to: (a) remember information so that you will not have to re-enter it during your visit or the next time you use the WhatsApp Service or WhatsApp Site; (b) provide custom, personalized content and information; (c) monitor individual and aggregate metrics such as total number of visitors, pages viewed, etc.; and (d) track your entries, submissions, views and such.

8. When WhatsApp Discloses Information

Other users of the WhatsApp Service may see your Status Submissions in a way that is consistent with the use of the WhatsApp Service. For example, a status of "Can't talk, please SMS instead" set by phone number +1 (408) 555-1212 will be available to every user of the WhatsApp Service who has that mobile phone number in their mobile phone's address book or contact list. In other words: If another user has your mobile phone number stored in their mobile phone address book or contact list, they will be able see your status information unless you have chosen to block such user. "Last Seen" information is available and displayed to each user who has your mobile phone number in their mobile phone address book or contact book (and which you have not blocked), and reflects the

last approximate time the WhatsApp mobile application has been used or brought to the foreground on your mobile phone. “Last Seen” information is reported to WhatsApp when a user brings the mobile application to the foreground. We do not sell or share your Personally Identifiable Information (such as mobile phone number) with other third-party companies for their commercial or marketing use without your consent or except as part of a specific program or feature for which you will have the ability to opt-in or opt-out. [We may share your Personally Identifiable Information with third party service providers to the extent that it is reasonably necessary to perform, improve or maintain the WhatsApp Service.](#) We may share non-personally-identifiable information (such as anonymous User usage data, referring / exit pages and URLs, platform types, asset views, number of clicks, etc.) with interested third-parties to assist them in understanding the usage patterns for certain content, services, advertisements, promotions, and/or functionality on the WhatsApp Site. We may collect and release Personally Identifiable Information and/or non-personally-identifiable information if required to do so by law, or in the good-faith belief that such action is necessary to comply with state and federal laws (such as U.S. Copyright Law), international law or respond to a court order, subpoena, or search warrant or equivalent, or where in our reasonable belief, an individual’s physical safety may be at risk or threatened. WhatsApp also reserves the right to disclose Personally Identifiable Information and/or non-personally-identifiable information that WhatsApp believes, in good faith, is appropriate or necessary to enforce our Terms of Service, take precautions against liability, to investigate and defend itself against any third-party claims or allegations, to assist government enforcement agencies, to protect the security or integrity of the WhatsApp Site or our servers, and to protect the rights, property, or personal safety of WhatsApp, our users or others.

9. Your Choices

You may, of course, decline to submit Personally Identifiable Information through the WhatsApp Site or the WhatsApp Service, in which case WhatsApp may not be able to provide certain services to you. If you do not agree with our Privacy Policy or Terms of Service, please delete your account, uninstall the WhatsApp mobile application and discontinue use of the WhatsApp Service; your continued usage of the WhatsApp Service will signify your assent to and acceptance of our Privacy Policy and Terms of Service. To protect your privacy and security, we take reasonable steps (such as SMS authentication in certain cases) to verify your identity before registering your mobile phone number and granting you access to the WhatsApp Service. Please contact WhatsApp via email to support at support@whatsapp.com or available web forms with any questions or comments about this Privacy Policy, your personal information, your consent, or your opt-in or opt-out choices.

10. Third-party Advertisers, Links to Other Sites

We are [not fans of advertising](#). WhatsApp is currently ad-free and we hope to keep it that way forever. We have no intention to introduce advertisement into the product, but if we ever do, will update this section.

11. Our Commitment To Data Security

WhatsApp uses commercially reasonable physical, managerial, and technical safeguards to preserve the integrity and security of your personal information. We cannot, however, ensure or warrant the security of any information you transmit to WhatsApp and you do so at your own risk. Using unsecured wifi or other unprotected networks to submit messages through the WhatsApp Service is never recommended. Once we receive your transmission of information, WhatsApp makes commercially reasonable efforts to ensure the security of our systems. However, please note that this is not a guarantee that such information may not be accessed, disclosed, altered, or destroyed by breach of any of our physical, technical, or managerial safeguards. If WhatsApp learns of a security systems breach, then we may attempt to notify you electronically so that you can take appropriate protective steps. WhatsApp may post a notice on the WhatsApp Site or through the WhatsApp Service if a security breach occurs.

12. Our Commitment To Childrens' Privacy

Protecting the privacy of young children is especially important. For that reason, WhatsApp does not knowingly collect or maintain Personally Identifiable Information or non-personally-identifiable information on the WhatsApp Site or WhatsApp Service from persons under 16 years of age, and no part of the WhatsApp Service is directed to or intended to be used by persons under 16. If you are under 16 years of age, then please do not use the WhatsApp Service or access the WhatsApp Site at any time or in any manner. If WhatsApp learns that Personally Identifiable Information of persons under 16 years of age has been collected on the WhatsApp Site or WhatsApp Service, then WhatsApp may deactivate the account and/or make the status submissions inaccessible. And always, think of the children!

13. Special Note to International Users

The WhatsApp Site and Service are hosted in the United States and are intended for and directed to users in the United States. If you are a user accessing the WhatsApp Site and Service from the European Union, Asia, or any other region with laws or regulations governing personal data collection, use, and disclosure, that differ from United States laws, please be advised that through your continued use of the WhatsApp Site and Service, which are governed by California law, this Privacy Policy, and our Terms of Service, you are transferring your personal information to the United States and you expressly consent to that transfer and consent to be governed by California law for these purposes.

In the Event of Merger, Sale, or Bankruptcy

In the event that WhatsApp is acquired by or merged with a third party entity, we reserve the right to transfer or assign the information we have collected from our users as part of such merger, acquisition, sale, or other change of control. In the (hopefully) unlikely event of our bankruptcy, insolvency, reorganization, receivership, or assignment for the benefit of creditors, or the application of laws or equitable principles affecting creditors' rights generally, we may not be able to control how your personal information is treated, transferred, or used.

Changes and updates to this Privacy Notice

This Privacy Policy may be revised periodically and this will be reflected by the "effective date" below. Please revisit this page to stay aware of any changes. Your continued use of the WhatsApp Site and WhatsApp Service constitutes your agreement to this Privacy Policy and any amendments

Date Last Modified: This Privacy Notice was last modified July 7th, 2012

Bijlage 11.

Gebruiksvoorwaarden Dropbox

Bron: www.dropbox.com

Last Modified: March 26, 2012

Thank you for using Dropbox! These terms of service (the "**Terms**") govern your access to and use of Dropbox ("**we**" or "**our**") websites and services (the "**Services**"), so please carefully read them before using the Services.

1. **By using the Services you agree to be bound by these Terms.** If you are using the Services on behalf of an organization, you are agreeing to these Terms for that organization and promising that you have the authority to bind that organization to these terms. In that case, "you" and "your" will refer to that organization.

You may use the Services only in compliance with these Terms. You may use the Services only if you have the power to form a contract with Dropbox and are not barred under any applicable laws from doing so. The Services may continue to change over time as we refine and add more features. We may stop, suspend, or modify the Services at any time without prior notice to you. We may also remove any content from our Services at our discretion.

2. Your Stuff & Your Privacy

By using our Services you provide us with information, files, and folders that you submit to Dropbox (together, “your stuff”). You retain full ownership to your stuff. We don’t claim any ownership to any of it. These Terms do not grant us any rights to your stuff or intellectual property except for the limited rights that are needed to run the Services, as explained below.

We may need your permission to do things you ask us to do with your stuff, for example, hosting your files, or sharing them at your direction. This includes product features visible to you, for example, image thumbnails or document previews. It also includes design choices we make to technically administer our Services, for example, how we redundantly backup data to keep it safe. You give us the permissions we need to do those things solely to provide the Services. This permission also extends to trusted third parties we work with to provide the Services, for example Amazon, which provides our storage space (again, only to provide the Services).

To be clear, aside from the rare exceptions we identify in our [Privacy Policy](#), no matter how the Services change, we won’t share your content with others, including law enforcement, for any purpose unless you direct us to. How we collect and use your information generally is also explained in our [Privacy Policy](#).

You are solely responsible for your conduct, the content of your files and folders, and your communications with others while using the Services. For example, it’s your responsibility to ensure that you have the rights or permission needed to comply with these Terms.

We may choose to review public content for compliance with our community guidelines, but you acknowledge that Dropbox has no obligation to monitor any information on the Services. We are not responsible for the accuracy, completeness, appropriateness, or legality of files, user posts, or any other information you may be able to access using the Services.

Sharing Your Stuff

The Services provide features that allow you to share your stuff with others or to make it public. There are many things that users may do with that stuff (for example, copy it, modify it, re-share it). Please consider carefully what you choose to share or make public. Dropbox has no responsibility for that activity.

Your Responsibilities

Files and other content in the Services may be protected by intellectual property rights of others. Please do not copy, upload, download, or share files unless you have the right to do so. You, not Dropbox, will be fully responsible and liable for what you copy, share, upload, download or otherwise use while using the Services. You must not upload spyware or any other malicious software to the Service.

You, and not Dropbox, are responsible for maintaining and protecting all of your stuff. Dropbox will not be liable for any loss or corruption of your stuff, or for any costs or expenses associated with backing up or restoring any of your stuff. If your contact information, or other information related to your account, changes, you must notify us promptly and keep your information current. The Services are not intended for use by you if you are under 13 years of age. By agreeing to these Terms, you are representing to us that you are over 13.

Account Security

You are responsible for safeguarding the password that you use to access the Services and you agree not to disclose your password to any third party. You are responsible for any activity using your account, whether or not you authorized that activity. You should immediately notify Dropbox of any unauthorized use of your account. You acknowledge that if you wish to protect your transmission of data or files to Dropbox, it is your responsibility to use a secure encrypted connection to communicate with the Services.

Software and Updates

Some use of our Service requires you to download a client software package (“Software”). Dropbox hereby grants you a limited, nonexclusive, nontransferable, revocable license to use the Software, solely to access the Services. Your license to use the Software is automatically revoked if you violate these Terms in a manner that implicates our intellectual property rights. We hereby reserve all rights not expressly granted in these Terms. You must not reverse engineer or decompile the Software, nor attempt to do so, nor assist anyone else to do so. Our Services may update the Software on your device automatically when a new version is available. Our pause syncing feature pauses syncing of your files, but may not cease all data transfer, so you should exit the desktop client if you’d like to stop data transfer.

Dropbox Property and Feedback

These terms do not grant you any right, title, or interest in the Services, Software, or the content in the Services. While we appreciate it when users send us feedback, please be aware that we may use any feedback, comments, or suggestions you send us or post in our forums without any obligation to you. The Software and other technology we use to provide the Services are protected by copyright, trademark, and other laws of both the United States and foreign countries. These Terms do not grant you any rights to use the Dropbox trademarks, logos, domain names, or other brand features.

Acceptable Use Policy

You will not, and will not attempt to, misuse the Services, and will use the Services only in a manner consistent with the Dropbox [Acceptable Use Policy](#).

Copyright

Dropbox respects others’ intellectual property and asks that you do too. We will respond to notices of alleged copyright infringement if they comply with the law and are properly provided to us. Such notices should be reported using our [DMCA Process](#). We reserve the right to delete or disable content alleged to be infringing and to terminate repeat infringers. Our designated agent for notice of alleged copyright infringement on the Services is:

Copyright Agent Dropbox, Inc. 185 Berry St. Ste. 400 San Francisco, CA
94107 copyright@dropbox.com

Other Content

The Services may contain links to third-party websites or resources. Dropbox does not endorse and is not responsible or liable for their availability, accuracy, the related content, products, or services. You are solely responsible for your use of any such websites or resources. Also, if we provide you with any software under an open source license, there may be provisions in those licenses that expressly conflict with these Terms, in which case the open source provisions will apply.

Termination

Though we’d much rather you stay, you can stop using our Services any time. We reserve the right to suspend or end the Services at any time, with or without cause, and with or without notice. For example, we may suspend or terminate your use if you are not complying with these Terms, or use

the Services in any way that would cause us legal liability or disrupt others' use of the Services. If we suspend or terminate your use, we will try to let you know in advance and help you retrieve data, though there may be some cases (for example, repeatedly or flagrantly violating these Terms, a court order, or danger to other users) where we may suspend immediately.

Dropbox is Available "AS-IS"

Though we want to provide a great service, there are certain things about the service we can't promise. For example, THE SERVICES AND SOFTWARE ARE PROVIDED "AS IS", AT YOUR OWN RISK, WITHOUT EXPRESS OR IMPLIED WARRANTY OR CONDITION OF ANY KIND. WE ALSO DISCLAIM ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. (We are not shouting- it's just that these disclaimers are really important, so we want to highlight them). Dropbox will have no responsibility for any harm to your computer system, loss or corruption of data, or other harm that results from your access to or use of the Services or Software. Some states do not allow the types of disclaimers in this paragraph, so they may not apply to you.

Limitation of Liability

TO THE FULLEST EXTENT PERMITTED BY LAW, IN NO EVENT WILL DROPBOX, ITS AFFILIATES, OFFICERS, EMPLOYEES, AGENTS, SUPPLIERS OR LICENSORS BE LIABLE FOR (A) ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, EXEMPLARY OR CONSEQUENTIAL (INCLUDING LOSS OF USE, DATA, BUSINESS, OR PROFITS) DAMAGES, REGARDLESS OF LEGAL THEORY, WHETHER OR NOT DROPBOX HAS BEEN WARNED OF THE POSSIBILITY OF SUCH DAMAGES, AND EVEN IF A REMEDY FAILS OF ITS ESSENTIAL PURPOSE; (B) AGGREGATE LIABILITY FOR ALL CLAIMS RELATING TO THE SERVICES MORE THAN THE GREATER OF \$20 OR THE AMOUNTS PAID BY YOU TO DROPBOX FOR THE PAST THREE MONTHS OF THE SERVICES IN QUESTION. Some states do not allow the types of limitations in this paragraph, so they may not apply to you.

Modifications

We may revise these Terms from time to time and the most current version will always be posted on our website. If a revision, in our sole discretion, is material we will notify you (for example via email to the email address associated with your account). Other changes may be posted to our blog or terms page, so please check those pages regularly. By continuing to access or use the Services after revisions become effective, you agree to be bound by the revised Terms. If you do not agree to the new terms, please stop using the Services.

Miscellaneous Legal Terms

THESE TERMS AND THE USE OF THE SERVICES AND SOFTWARE WILL BE GOVERNED BY CALIFORNIA LAW EXCEPT FOR ITS CONFLICTS OF LAWS PRINCIPLES. ALL CLAIMS ARISING OUT OF OR RELATING TO THESE TERMS OR THE SERVICES OR SOFTWARE MUST BE LITIGATED EXCLUSIVELY IN THE FEDERAL OR STATE COURTS OF SAN FRANCISCO COUNTY, CALIFORNIA, AND BOTH PARTIES CONSENT TO VENUE AND PERSONAL JURISDICTION THERE. These Terms constitute the entire and exclusive agreement between you and Dropbox with respect to the Services, and supersede and replace any other agreements, terms and conditions applicable to the Services. These Terms create no third party beneficiary rights. Dropbox's failure to enforce a provision is not a waiver of its right to do so later. If a provision is found unenforceable the remaining provisions of the Agreement will remain in full effect and an enforceable term will be substituted reflecting our intent as closely as possible. You may not assign any of your rights in these Terms, and any such attempt is void, but Dropbox may assign its rights to any of its affiliates or subsidiaries, or to any successor in interest of any business associated with the Services. Dropbox and you are not legal partners or agents; instead, our relationship is that of independent contractors.

Bijlage 12.

Privacybeleid Dropbox

Bron: www.dropbox.com

Last Modified: April 10, 2013

This Privacy Policy provides our policies and procedures for collecting, using, and disclosing your information. Users can access the Dropbox service (the “**Service**”) through our website www.dropbox.com, applications on Devices, through APIs, and through third-parties. A “**Device**” is any computer used to access the Dropbox Service, including without limitation a desktop, laptop, mobile phone, tablet, or other consumer electronic device. This Privacy Policy governs your access of the Dropbox Service, regardless of how you access it, and by using our Services you consent to the collection, transfer, processing, storage, disclosure and other uses described in this Privacy Policy. All of the different forms of data, content, and information described below are collectively referred to as “information.”

1. The Information We Collect And Store

We may collect and store the following information when running the Dropbox Service:

Information You Provide. When you register an account, we collect some personal information, such as your name, phone number, credit card or other billing information, email address and home and business postal addresses. You may also ask us to import your contacts by giving us access to your third party services (for example, your email account) or to use your social networking information if you give us access to your account on social network connection services. When you invite others to join Dropbox by using our referral page, we send them a one-time email for that referral. You may also provide us with your contacts’ email addresses when sharing folders or files with them. We may also receive Personal Information (for example, your email address) through other users, for example if they have tried to share something with you or tried to refer Dropbox to you.

Files. We collect and store the files you upload, download, or access with the Dropbox Service (“**Files**”). If you add a file to your Dropbox that has been previously uploaded by you or another user, we may associate all or a portion of the previous file with your account rather than storing a duplicate.

Log Data. When you use the Service, we automatically record information from your Device, its software, and your activity using the Services. This may include the Device’s Internet Protocol (“IP”) address, browser type, the web page visited before you came to our website, information you search for on our website, locale preferences, identification numbers associated with your Devices, your mobile carrier, date and time stamps associated with transactions, system configuration information, metadata concerning your Files, and other interactions with the Service.

Cookies. We also use “cookies” to collect information and improve our Services. A cookie is a small data file that we transfer to your Device. We may use “persistent cookies” to save your registration ID and login password for future logins to the Service. We may use “session ID cookies” to enable certain features of the Service, to better understand how you interact with the Service and to monitor aggregate usage and web traffic routing on the Service. You can instruct your browser, by changing its options, to stop accepting cookies or to prompt you before accepting a cookie from the websites you visit. If you do not accept cookies, however, you may not be able to use all aspects of the Service.

2. How We Use Personal Information

Personal Information. In the course of using the Service, we may collect personal information that

can be used to contact or identify you (“**Personal Information**”). **Personal Information is or may be used: (i) to provide and improve our Service, (ii) to administer your use of the Service, (iii) to better understand your needs and interests, (iv) to personalize and improve your experience, and (v) to provide or offer software updates and product announcements.** If you no longer wish to receive communications from us, please follow the “unsubscribe” instructions provided in any of those communications, or update your account settings information.

Geo-Location Information. Some Devices allow applications to access real-time location-based information (for example, GPS). Our mobile apps do not collect such information from your mobile device at any time while you download or use our mobile apps as of the date this policy went into effect, but may do so in the future with your consent to improve our Services. **Some photos and videos you place in Dropbox may contain recorded location information. We may use this information to optimize your experience.** If you do not wish to share files embedded with your geo-location information with us, please do not upload them. If you don’t want to store location data in your photos or videos, please consult the documentation for your camera to turn off that feature. Also, some of the information we collect from a Device, for example IP address, can sometimes be used to approximate a Device’s location.

Analytics. We also collect some information (ourselves or using third party services) using logging and cookies, such as IP address, which can sometimes be correlated with Personal Information. We use this information for the above purposes and to monitor and analyze use of the Service, for the Service’s technical administration, to increase our Service’s functionality and user-friendliness, and to verify users have the authorization needed for the Service to process their requests. **As of the date this policy went into effect, we use Google Analytics. To learn more about the privacy policy of Google Analytics, click here, and to learn how to opt out of that service click here.**

3. Information Sharing and Disclosure

Your Use. We will display your Personal Information in your profile page and elsewhere on the Service according to the preferences you set in your account. Any information you choose to provide should reflect how much you want others to know about you. Please consider carefully what information you disclose in your profile page and your desired level of anonymity. You can review and revise your profile information at any time. We do not sell your personal information to third parties. We may also share or disclose your information with your consent, for example if you use a third party application to access your account (see below). Through certain features of the Service, you may also have the ability to make some of your information public. Public information may be broadly and quickly disseminated.

Service Providers, Business Partners and Others. We may use certain trusted third party companies and individuals to help us provide, analyze, and improve the Service (including but not limited to data storage, maintenance services, database management, web analytics, payment processing, and improvement of the Service’s features). These third parties may have access to your information only for purposes of performing these tasks on our behalf and under obligations similar to those in this Privacy Policy. As of the date this policy went into effect, we use Amazon’s S3 storage service to store some of your information (for example, your Files). You can find more information on Amazon's data security from the [S3 site](#) or, read more about [how Dropbox and Amazon securely store data](#).

Third-Party Applications. We may share your information with a third party application with your consent, for example when you choose to access our Services through such an application. We are not responsible for what those parties do with your information, so you should make sure you trust the application and that it has a privacy policy acceptable to you.

Compliance with Laws and Law Enforcement Requests; Protection of Dropbox's Rights. We may disclose to parties outside Dropbox files stored in your Dropbox and information about you that we collect when we have a good faith belief that disclosure is reasonably necessary to (a) comply with a law, regulation or compulsory legal request; (b) protect the safety of any person from death or

serious bodily injury; (c) prevent fraud or abuse of Dropbox or its users; or (d) to protect Dropbox's property rights. If we provide your Dropbox files to a law enforcement agency as set forth above, we will remove Dropbox's encryption from the files before providing them to law enforcement. However, Dropbox will not be able to decrypt any files that you encrypted prior to storing them on Dropbox.

Business Transfers. If we are involved in a merger, acquisition, or sale of all or a portion of our assets, your information may be transferred as part of that transaction, but we will notify you (for example, via email and/or a prominent notice on our website) of any change in control or use of your Personal Information or Files, or if either become subject to a different Privacy Policy. We will also notify you of choices you may have regarding the information.

Non-private or Non-Personal Information. We may disclose your non-private, aggregated, or otherwise non-personal information, such as usage statistics of our Service.

4. Changing or Deleting Your Information

If you are a registered user, you may review, update, correct or delete the Personal Information provided in your registration or account profile by changing your "account settings." If your personally identifiable information changes, or if you no longer desire our service, you may update or delete it by making the change on your [account settings](#). In some cases we may retain copies of your information if required by law. For questions about your Personal Information on our Service, please contact privacy@dropbox.com. We will respond to your inquiry within 30 days.

5. Data Retention

We will retain your information for as long as your account is active or as needed to provide you services. If you wish to cancel your account or request that we no longer use your information to provide you services, you may delete your account [here](#). We may retain and use your information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements. Consistent with these requirements, we will try to delete your information quickly upon request. Please note, however, that there might be latency in deleting information from our servers and backed-up versions might exist after deletion. In addition, we do not delete from our servers files that you have in common with other users.

6. Dropbox for Business Users

If you have a Dropbox for Business account, your Administrator may be able to:

- access information in and about your Dropbox for Business account;
- disclose, restrict, or access information that you have provided or that is made available to you when using your Dropbox for Business account; and
- control how your Dropbox for Business account may be accessed or deleted.

Please refer to your organization's policies if you have questions about your Administrator's rights.

7. Dropbox Community

Our Service offers publicly accessible community services such as blogs, forums, and wikis. You should be aware that any information you provide in these areas may be read, collected, and used by others who access them. Your posts may remain even after you cancel your account. For questions about your Personal Information on our Service, please contact privacy@dropbox.com.

Our Site includes links to other Web sites whose privacy practices may differ from those of Dropbox. If you submit personal information to any of those sites, your information is governed by their privacy statements. We encourage you to carefully read the privacy statement of any Web site you visit.

8. Security

The security of your information is important to us. When you enter sensitive information (such as a credit card number) on our order forms, we encrypt the transmission of that information using secure socket layer technology (SSL).

We follow generally accepted standards to protect the information submitted to us, both during transmission and once we receive it. No method of electronic transmission or storage is 100% secure, however. Therefore, we cannot guarantee its absolute security. If you have any questions about security on our website, you can view our [Security Overview Page](#) or contact us at security@dropbox.com.

9. Our Policy Toward Children

Our Services are not directed to persons under 13. We do not knowingly collect personally identifiable information from children under 13. If a parent or guardian becomes aware that his or her child has provided us with Personal Information without their consent, he or she should contact us at privacy@dropbox.com. If we become aware that a child under 13 has provided us with Personal Information, we will take steps to delete such information from our files.

10. Safe Harbor

Dropbox has received TRUSTe's Privacy Seal signifying that this privacy statement and our practices have been reviewed by TRUSTe for compliance with TRUSTe's program requirements including transparency, accountability and choice regarding the collection and use of your personal information. The TRUSTe program does not cover information that may be collected through downloadable software.

Dropbox complies with the U.S. – E.U. Safe Harbor Framework and the U.S. – Swiss Safe Harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal data from European Union member countries and Switzerland. Dropbox has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement. To learn more about the Safe Harbor program, and to view Dropbox's certification, please visit <http://export.gov/safeharbor>.

If you have questions regarding this statement, you should first contact us at privacy@dropbox.com. If you do not receive acknowledgement of your inquiry or your inquiry has not been satisfactorily addressed, you should then contact TRUSTe at http://www.truste.org/consumers/watchdog_complaint.php, by fax at 415-520-3420, or by mail to TRUSTe Safe Harbor Compliance Dept., click for mailing address. The TRUSTe dispute resolution process is only available in English.

11. Contacting Us

If you have any questions about this Privacy Policy, please contact us at privacy@dropbox.com or at 185 Berry Street, 4th floor, San Francisco, CA 94107.

12. Changes to our Privacy Policy

This Privacy Policy may change from time to time. If we make a change to this privacy policy that we believe materially reduces your rights, we will provide you with notice (for example, by email). And we may provide notice of changes in other circumstances as well. By continuing to use the Service after those changes become effective, you agree to be bound by the revised Privacy Policy.

Bijlage 13.

Disclaimer en privacybeleid KennisBoek (Dirkzwager)

Bron: www.dirkzwager.nl

Toepassingsbereik

Deze disclaimer en dit privacy statement zijn van toepassing op (het gebruik van) alle externe (reclame-)uitingen van Dirkzwager advocaten & notarissen N.V. ("Dirkzwager"), waaronder de uitingen via de door Dirkzwager geëxploiteerde websites hierna gezamenlijk of afzonderlijk aangeduid als de "Website"), de door Dirkzwager verstuurd elektronische nieuwsbrieven (hierna aangeduid als de "Nieuwsbrief"); de door Dirkzwager geëxploiteerde applicatie ten behoeve van mobiele telefoons (hierna: aangeduid als de "App"); het relatiemagazine Samenspraak (hierna aangeduid als "Samenspraak") Hierna gezamenlijk te noemen: de "Dirkzwager Uitingen".

DISCLAIMER

Via de Dirkzwager Uitingen wordt algemene informatie verstrekt over Dirkzwager en/of juridische of andere onderwerpen. Voor zover de Dirkzwager Uitingen juridische onderwerpen betreffen is niet beoogd om juridisch advies te verlenen voor concrete situaties. De betreffende informatie wordt door ons met zorg samengesteld, doch voor de juistheid en volledigheid daarvan kan niet worden ingestaan. Dirkzwager aanvaardt geen enkele aansprakelijkheid voor de onjuistheid en onvolledigheid van de aangeboden informatie. Verwijzingen via de Dirkzwager Uitingen naar sites en andere externe bronnen die niet door ons worden onderhouden zijn louter ter informatie voor de bezoeker opgenomen. Hoewel Dirkzwager uiterst selectief is ten aanzien van de externe bronnen waarnaar verwezen wordt, kunnen wij niet instaan voor de inhoud en het functioneren daarvan, noch voor de kwaliteit van eventuele producten en/of diensten die daarop worden aangeboden. Het is de ontvanger/gebruiker van de betreffende Dirkzwager Uitingen niet toegestaan deze te vermenigvuldigen, te distribueren, te verspreiden of tegen vergoeding beschikbaar te stellen aan derden, zonder uitdrukkelijke, schriftelijke toestemming van Dirkzwager.

PRIVACY STATEMENT

1. Algemeen De Dirkzwager Uitingen zijn eigendom van en worden beheerd door Dirkzwager. Dirkzwager respecteert uw privacy en draagt er zorg voor dat de persoonlijke informatie die u eventueel aan ons verstrekt, vertrouwelijk en in overeenstemming met de Wet Bescherming Persoonsgegevens wordt behandeld.

2. Verwerking van persoonsgegevens Als persoonsgegevens gelden gegevens die kunnen worden gebruikt om uw identiteit te achterhalen. Dirkzwager maakt daarbij onderscheid tussen (1) persoonsgegevens die u actief aan ons verstrekt en (2) persoonsgegevens die – om technische redenen – automatisch aan ons worden doorgegeven. Onder persoonsgegevens die u actief aan ons verstrekt zijn onder meer begrepen de naam, contactgegevens, voorkeuren en andere gegevens die u aan ons heeft verstrekt (bijvoorbeeld tijdens een registratieprocedure of tijdens het contact met een advocaat of notaris). Daarnaast geldt dat bij het bezoeken van de Website en het gebruik van de App automatisch enkele technische gegevens door uw apparatuur aan onze computers worden verstrekt, zoals het door u gebruikte IP-adres, het besturingssysteem, de gebruikte internet browser en (in sommige gevallen) de laatste internetpagina die u heeft bezocht.

3. Doeleinden verwerking De persoonsgegevens die Dirkzwager in het kader van de Dirkzwager Uitingen verwerkt, worden uitsluitend gebruikt voor de volgende doeleinden voor het verrichten van de aangeboden diensten (zoals het middels de App toezenden van informatie conform uw voorkeuren, het publiceren van door u gegeven en ter publicatie aangeboden commentaren en reacties, etc.)

om met u in contact te kunnen treden;
om u te informeren over nieuwe producten en/of aanbiedingen van Dirkzwager (al dan niet toegespitst op de door u kenbaar gemaakte interessegebieden);
het analyseren en verbeteren van dienstverlening van Dirkzwager (waaronder begrepen het meten en analyseren van statistische gegevens omtrent het gebruik van de Dirkzwager Uitingen);
het verrichten van marktonderzoek ten behoeve van Dirkzwager

4. Het anderszins verwerken van uw persoonsgegevens geschiedt alleen voor zover u Dirkzwager daarvoor ondubbelzinnig toestemming heeft verleend. Die toestemming kan blijken uit het enkele feit dat u per e-mail of anderszins een vraag aan Dirkzwager stelt.

5. De Nieuwsbrief De Nieuwsbrief wordt toegezonden aan alle abonnees van de Nieuwsbrief. Het abonneebestand bestaat uit twee groepen: (1) personen die zich via de Website hebben aangemeld en (2) bestaande klanten van Dirkzwager. Aanmelding via de Website geschiedt door middel van een zogenaamd double opt-in proces, dat wil zeggen dat u alleen als abonnee genoteerd wordt wanneer u na aanmelding via de Website de instructies opvolgt die u vervolgens per e-mail worden toegezonden. Hierdoor wordt zeker gesteld dat alleen degene die beschikt over de betreffende mailbox zich kan abonneren op de Nieuwsbrief. Het is daarnaast mogelijk dat u als bestaande relatie van Dirkzwager op verzoek van een jurist of andere medewerker van Dirkzwager aan het abonneebestand bent toegevoegd. U ontvangt hierover in dat geval een bericht. Het betreffende bericht bevat een hyperlink waarmee u zich met één klik weer kunt afmelden indien u geen interesse heeft in de Nieuwsbrief. Daarnaast treft u onderaan iedere nieuwsbrief een hyperlink aan waarmee u zich eenvoudig kunt uitschrijven als abonnee van de Nieuwsbrief.

6. Gebruik van Google Analytics op de Website en in de App De Website maakt gebruik van Google Analytics, een webanalyse-service die wordt aangeboden door Google Inc. ("Google"). Google Analytics maakt gebruik van "cookies" (tekstbestandjes die op Uw computer worden geplaatst) om de website te helpen analyseren hoe gebruikers de site gebruiken. De door het cookie gegenereerde informatie over Uw gebruik van de website (met inbegrip van Uw IP-adres) wordt overgebracht naar en door Google opgeslagen op servers in de Verenigde Staten. Google gebruikt deze informatie om bij te houden hoe u de website gebruikt, rapporten over de website-activiteit op te stellen voor website-exploitanten en andere diensten aan te bieden met betrekking tot website-activiteit en internetgebruik. Google mag deze informatie aan derden verschaffen indien Google hiertoe wettelijk wordt verplicht, of voor zover deze derden de informatie namens Google verwerken. Google zal Uw IP-adres niet combineren met andere gegevens waarover Google beschikt. U kunt het gebruik van cookies weigeren door in Uw browser de daarvoor geëigende instellingen te kiezen. Wij wijzen u er echter op dat u in dat geval wellicht niet alle mogelijkheden van deze website kunt benutten. Wanneer u niet wilt dat uw websitebezoek wordt gemeten door Google Analytics, dan kunt u via <http://tools.google.com/dlpage/gaoptout?hl=nl> eenvoudig een tool downloaden waarmee Google Analytics wordt geblokkeerd. Door gebruik te maken van de Website geeft u toestemming voor het verwerken van de informatie door Google op de wijze en voor de doeleinden zoals hiervoor omschreven.

7. De App In de App wordt, net als op de Website, algemene informatie verstrekt over onder meer enkele juridische onderwerpen. De App biedt echter enkele aanvullende functionaliteiten ten opzichte van de Website. Voor het gebruik van deze extra functionaliteit dient u zich eenmalig te registreren. De persoonsgegevens die u bij registratie opgeeft worden verwerkt overeenkomstig de doeleinden zoals beschreven in paragraaf 3 van dit Privacy Statement. Na registratie kunt u in de App:

informatie eenvoudig filteren aan de hand van uw eigen voorkeuren, zodat u alleen informatie ontvangt over de onderwerpen die uw interesse hebben;
reageren op de informatie die wordt aangeboden in de App en deze reactie delen met andere gebruikers van de App;
informatie die in de App wordt aangeboden eenvoudig delen met derden;

8. De instellingen/voorkeuren die u in de App maakt worden opgeslagen op onze server. Deze gegevens kunnen op ieder moment door u worden gewijzigd in de App. Door de App te gebruiken geeft u toestemming voor deze verwerking van gegevens. Eventuele reacties/commentaren die u via de App verzendt, worden opgeslagen op de computers van Dirkzwager. Voor de andere verwerkingen van persoonsgegevens die het gebruik van de App met zich meebrengt (zoals statistische gegevens over gebruik), wordt verwezen naar hetgeen hiervoor in paragraaf 2 en 3 van dit Privacy Statement reeds is opgemerkt.

9. Wijzigingen Deze Privacy Statement kan worden gewijzigd. Deze wijzigingen worden bekendgemaakt in de Dirkzwager Uitingen. Dirkzwager kan uw persoonsgegevens verwerken voor nieuwe doeleinden die nog niet staan vermeld in deze Privacy Statement. In dat geval zullen wij contact met u opnemen alvorens uw gegevens te gebruiken voor deze nieuwe doeleinden, om u op de hoogte te stellen van de wijzigingen aan ons reglement voor de bescherming van persoonlijke gegevens en om u de kans te bieden gebruik van uw gegevens voor die doeleinden te weigeren.

Vragen en recht op inzage en correctie Indien u vragen heeft over de verwerking van uw persoonsgegevens door Dirkzwager, of indien u inzage wenst in, dan wel wijziging wenst van uw persoonsgegevens, neem dan contact op met de afdeling marketing en communicatie, bereikbaar op telefoonnummer 026 – 353 83 26 of e-mailadres info@dirkzwager.nl

Bijlage 14.

Privacy Policy Flurry

Bron: www.flurry.com

Last Updated: October 21, 2013

1. OVERVIEW

Flurry, Inc. takes the privacy of our customers ("Customer" or "you" or "your") and their end users ("End Users") seriously. We recognize that privacy is an important issue, so we design and operate our services with the protection of your privacy in mind. This privacy policy ("Policy") explains how your personal information and information regarding your End Users is collected, used, and disclosed by Flurry, Inc. and its subsidiaries, and any parent and affiliated companies ("Flurry", "us" or "we") with respect to the services referred to in this Policy. This Policy applies to the websites provided by Flurry (collectively the "Sites") and the Flurry services outlined below (collectively, "Flurry Services"). This Policy does not apply to websites, applications or services that display or link to different privacy statements.

2. HOW WE COLLECT AND USE INFORMATION

2.1 Using Flurry services: When you use Flurry Services, we may request information, including your first and last name, an email address and password, and your cell phone number to create your Customer account. We use such information to manage your account and to provide you with access to the Flurry Services. We may also use the information to notify you of updates to the Flurry Services and provide you with access to special promotions.

2.2 Via Email: We place email links on the Sites to allow you to contact us directly. The information you provide, which may include personal information, is used to respond directly to your questions or comments. We may also file your comments to improve the Sites and Flurry Services, or review and discard the information.

2.3 Via Flurry Analytics: Flurry Analytics provides information to you about how your End Users use their mobile applications as well as how applications are performing across different handsets. Flurry obtains this information as a result of data being sent to our servers from our software "agent" if embedded by you in an End User's mobile application. The data collected by the agent may include: agent version, platform, SDK version, timestamp, API key (identifier for application), application version, device identifier, iOS Identifier for Advertising, iOS Identifier for Vendors, Media Access Control (MAC) address, International Mobile Equipment Identity (IMEI), Model, manufacture and OS

version of device, session start/stop time, device uptime, locale (specific location where a given language is spoken), mobile network code/mobile country code, time zone, network status (WiFi, etc.), memory, disk, CPU and battery usage information. We hash iOS device identifiers, MAC address and IMEI; however, we do not hash platform device identifiers such as the iOS Identifier for Advertising, ANDROID_ID and the BB_PIN. Hashing involves the transformation of these identifiers into a value or key that represents the original identifier. The device identifiers (if applicable), IMEI (if applicable), MAC address (if applicable), and platform are hashed to a Flurry ID. Flurry may use any combination of the data collected by the software agent to identify an End User's device. If you use the restricted version of Flurry Analytics in an application, our agent collects the same information as described above, but it restricts the use of the device identifiers to provide analytics only for that application. An application using this restricted version will not be able to use benchmark data, Personas, or age and gender estimations provided under the complete version of Flurry Analytics. In addition, your analytics information will not include any latitude and longitude data at any level from your End Users. If our mobile web software agent is embedded by you in your mobile web application, we may use persistent cookies in conjunction with our software agent to collect the same information as described above, with the exception of any device identifier, iOS Identifier for Advertising, iOS Identifier for Vendors, Media Access Control (MAC) address, and IMEI. In addition, Flurry may collect the following data if you select the option for Flurry to collect and provide such data to Flurry: User ID (for your service), latitude and longitude, gender, age, events, errors, and page views. However, if you are using the restricted version of Flurry Analytics, you may not select this option to collect and provide to Flurry any personal information (including, but not limited to, latitude and longitude). Finally, we see the IP address, device type, locale and timezone of the user through the HTTP request. Flurry uses this data to enable demographic and customer-created segment advertising targeting, create reports for you to analyze your End Users and to create reports and/or metrics against which you can compare your user base. In addition, unless you are using the restricted version of Flurry Analytics, we may provide you with the option of exporting raw Flurry data to your servers such as timestamp, platform, event, and user ID. You can also record errors that occur in your applications and receive an export of data containing the error information.

Flurry Analytics Reports: Your End User data collected via Flurry Analytics is presented to you to analyze your applications. In addition, unless you are using the restricted version of Flurry Analytics, aggregated and anonymous benchmark data that includes your End User data and all other Customers' End User data is provided as well. However, you (as well as other Customers) may opt-out of having End User data included in the benchmark data. End User data from applications using the restricted version of Flurry Analytics will not be included in the benchmark data and will have no access to benchmark data from the Flurry dataset.

Via Flurry User Acquisition Analytics: Flurry User Acquisition Analytics allows you to segment the clicks and installs of your applications and in-app events by the traffic acquisition sources, such as third-party ad networks, email campaigns, mobile web campaigns or any other traffic source that can support third-party URLs. In order to use Flurry User Acquisition Analytics, you must use the complete feature set version of Flurry Analytics. Flurry will use the End User's IP addresses, HTTP headers and device identifiers through this service to help you keep track of clicks, installs, and in-app events. Flurry may receive End User data from your advertising partners and transfer back such End User data to your advertising partners in connection with Flurry User Acquisition Analytics.

Via Flurry AppCircle: Flurry AppCircle is an ad network that uses Flurry Analytics in combination with a recommendation engine to create suggestions about applications or other products and services that may be of interest to particular End Users. We provide the device identifiers of the End Users who download applications or access services based on these recommendations to the applicable publisher. We also provide the timestamp of when the End User clicked on the ad and downloaded the application and may provide city level information regarding the End User's location. The device identifier, timestamp and location information may be collected by Flurry or received directly from third party real-time bidding exchange partners. You can retrieve recommendations created for a particular End User by passing the device identifier of the End User to the Flurry servers. If you participate in AppCircle Rewards, you can determine how many rewarded application installations or rewarded video clip views an End User has completed. You can pass the device identifier to Flurry

and get back a list of times of the application installations or the video clip views. You may also get a list of device identifiers of all of your End Users who have completed an AppCircle rewards installation or rewards video clip view. We may provide reports to advertisers that include (i) the device identifiers of End Users that clicked on an ad, installed the application or viewed the video clip, (ii) the name of the publishing application associated with the click, installation or view and (iii) the time at which the click, installation or viewing of the video clip occurred. You may run a re-engagement campaign to try and engage End Users who have not used an application within a specific time frame. Flurry will internally identify End Users by their Flurry ID who have the application installed, but have not used the application within the specified time frame. Flurry may then show them an advertisement for such application. GetBanner is part of Flurry AppCircle and allows you to format a single Flurry AppCircle ad as a clickable HTML banner. This allows Customers who do not embed the Flurry SDK in their applications to make use of Flurry AppCircle ads manually. The data we collect in connection with GetBanner includes your API Access Code, the API key (identifier for application), End User device identifier, platform, landscape, banner orientation, reward message, end user IP address, theme identifier, and custom parameters. You must pass this data to us in the parameters of the application. We do not collect the data ourselves from the End User's device. Flurry's InstallNotify API (application programming interface) allows advertisers who do not use Flurry's SDK to acquire users through the AppCircle network, and to confirm that those users converted through Flurry. For each install, advertisers send Flurry a single API call that may contain the iOS UDID, Android_ID, a hash of the MAC address, or a hash of the IMEI. These identifiers are used to determine if the install was driven through Flurry's network. An advertiser may request a list of the identifiers of devices, install timestamps, and source (e.g., AppCircle) to confirm that they were converted via the Flurry network. Flurry's Get Recommendations API allows publishers who do not use Flurry's SDK to host Flurry ad units and monetize through an API feed. Publishers make a request to the Flurry GetRecommendations API with a call that may contain the iOS UDID, Android_ID, a hash of the MAC address, or a hash of the IMEI. These identifiers are used to determine the set of ads that will be returned to the publisher.

Via Flurry Real-Time Bidding Marketplace & Exchange Partners The Flurry Real-Time Bidding Marketplace ("Flurry RTB Service") is an automated real-time auction service that enables media buyers to bid on and purchase inventory from publishers for the placement of advertisements, whether for themselves or on behalf of third party advertisers. The Flurry RTB Service enables media buyers to deliver ads through the Flurry RTB Service by responding to ad requests delivered through Flurry's real-time bidding application programming interface. If you have received consent from your End Users, you may submit ad requests which may include device identifiers (including iOS Identifier for Advertising, iOS UDID, Android_ID, MAC address or IMEI), age ranges, gender, device type, OS, language, Personas, latitude and longitude, and customer key values for the purpose of selling your inventory through the Flurry RTB Marketplace. Such data may be used by media buyers to optimize their bids on impressions and focus their advertising purchases, and for retargeting ads to End Users.

Via Flurry AppSpot: Flurry AppSpot is an advertising service that allows a publisher to sell advertising space to advertisers in order to place such advertisements within their applications, including advertisements served by Flurry AppCircle. Flurry AppSpot must be used in conjunction with Flurry Analytics and may be used with Flurry AppCircle. Age ranges, gender, device type, OS, language, analytics segments created by you, Personas (as described below) and custom key values can be used by you to provide focused advertising to End Users. For example, you can create campaigns to run on your applications focusing on segments created by you within Flurry Analytics. Key values allow you to pass a specific key value pair to AppSpot as part of the ad request and then focus direct-sold campaigns or network campaigns to those values. An advertiser may request a list of the device identifiers of End Users, install timestamps, and the names of the publisher applications associated with clicks, completed views or installs.

Via Flurry AppCloud: Flurry AppCloud is a collection of mobile application development services for use in building and improving mobile applications. Data provided through the Flurry AppCloud service will be stored on servers at Cloudant. Through the Flurry AppCloud service, Flurry will provide metrics on a number of items, such as how push notifications affect End User use of your application. In addition, Flurry AppCloud will allow you to access some of the Flurry Analytics metrics through the

AppCloud service. Such metrics may include Personas, Customer created-segments and other anonymous application usage characteristics of the End User.

Personas: Personas are groups of End Users that share a similar interest. Flurry uses aggregated data provided by Flurry Analytics across multiple applications to build Personas. Based on an End User's application usage (session length, creation or interaction with an application event, or frequency), End Users may be classified into one or more Personas. Flurry categorizes its Customer's applications under the Personas. If an End User uses a number of applications categorized under a Persona, e.g., travel applications under a Business Traveler Persona, Flurry may place that End User within the Business Traveler Persona. Advertisers can offer ads using this Persona. In addition, Flurry Analytics will show you metrics on the different Personas. For example, you can see what percentage of your End Users are Avid Travelers and Sports Fanatics and the actual number of End Users that are in a Persona for each of your applications.

Customer Use of Data: Flurry is not responsible for any use by Customers of any data about their End Users. End Users should review the Customers' policies to understand their use of End User data.

Consents: You are responsible for obtaining all applicable End User consents to Flurry's collection and use of the End User information.

3. OTHER USES OF PERSONAL INFORMATION

Flurry may also use personal information collected from you for the following general purposes: (1) to fulfill your requests for Flurry Services; (2) to improve our Sites and Flurry Services; (3) to contact you to resolve problems; (4) to send you information about Flurry Services including confirmations, invoices, technical notices, updates, security alerts, and support and administrative messages; (5) to communicate with you about products and services offered by Flurry and our selected partners; (6) to conduct research; and (7) to make the Sites easier to use by reducing the need for you to enter information.

4. COOKIES AND WEB BEACONS

Cookies In order to provide you with personalized service, Flurry uses "cookies" to keep and occasionally track information about your visits to the Sites. A cookie is a small text file that is stored on a user's computer or mobile device for record-keeping purposes. We use both session ID cookies and persistent cookies on the Sites. We use session cookies to make it easier for you to navigate the Sites. A session ID cookie expires when you close your browser. A persistent cookie remains on your hard drive or mobile device for an extended period of time. When using the Site, we set a persistent cookie to store your password if you choose "auto login", so you don't have to enter it more than once. We also store your display resolution and whether JavaScript is enabled in your browser to enhance the experience on the Sites. Most Web browsers (including mobile Web browsers) are set to accept first party cookies by default. However, some Web browsers (including mobile Web browsers) are set to not accept third party cookies by default. You can typically remove or reject cookies by following directions provided in your Internet browser's help file or in the "Settings" of your mobile device. However, removing cookies may not allow you to take full advantage of all features on the Sites. In the case of our mobile web software agent, Flurry uses persistent cookies in conjunction with the software agent to collect the information as described in this policy and to provide our Flurry Analytics and advertising services. Flurry also uses persistent cookies to effect Flurry's mobile Web application opt-out by an End User as described below. Removing or rejecting cookies via the "Settings" on your browser may affect an End User's mobile Web application opt-out as described below.

Web Beacons We may collect information using Web beacons. Web beacons or "gifs", are electronic images that may be used on our Site, in our Services, or in our emails. We use Web beacons to deliver cookies, count visits and to tell if an email has been opened and acted upon.

5. THIRD PARTY TOOLS/ANALYTICS ON SITES

The Sites may also contain third party tracking tools from third party service providers, which may enable these third parties to analyze our Customers' information. While these third parties may have access to your personal information in connection with the performance of services for Flurry, they will not be permitted to use such information for any purpose other than providing their services.

6. END USER OPT-OUT OF FLURRY SERVICES

For Mobile Native Applications Your End Users of your mobile native applications can opt out of

Flurry Analytics tracking and personalized ads/recommendations from Flurry by clicking [here](#). You must include this link in your privacy policy and/or describe Flurry's opt-out to your End Users in such a manner that they can easily find it. Your End Users can type in the device identifier and/or MAC address and select their phone type. If an End User opts out of Flurry Analytics tracking for mobile native applications, Flurry will stop tracking data for the device identified by the provided MAC address and/or device identifier going forward. The Flurry Analytics tracking of that End User's device will stop across all mobile native applications within the Flurry network. In addition, Flurry will stop providing personalized recommendations to the device identifier and/or MAC address across all native application publishers within the Flurry network.

For Mobile Web Applications Your End Users of your mobile Web applications can opt out of Flurry Analytics tracking and personalized ads/recommendations. Because a Web-based application utilizing the Flurry Analytics software agent accessed via a mobile Web browser requires the use of persistent cookies instead of device identifiers, your End Users of your mobile Web application must (a) ensure that their mobile Web browser permits the use of third party cookies, and (b) opt out of Flurry's mobile Web software agent by clicking [here](#). If you use this mobile Web software agent, you must include this link in your privacy policy and/or describe Flurry's mobile Web opt-out to your End Users in such a manner that they can easily find it. If an End User opts out of Flurry Analytics tracking for mobile Web applications, Flurry will stop tracking data for the mobile Web browser in which the End User opted out going forward. The Flurry Analytics tracking of that End User's mobile Web browser will stop across all mobile Web applications within the Flurry network. In addition, Flurry will stop providing personalized recommendations to the mobile Web browser across all mobile Web application publishers within the Flurry network. This opt-out mechanism is effected by Flurry placing a persistent third party cookie on the End User's mobile Web browser. If your End User removes existing cookies on a particular browser, and continues to use your mobile Web application containing Flurry Analytics, the cookie that enabled the opt-out will be deleted and tracking by Flurry Analytics will resume until the End User opts out of Flurry's Mobile Web tracking again by following the instructions above.

The opt-outs described here are specific to Flurry activities and do not affect the activities of other ad networks or analytics providers that you use. An End User's opt-out of Flurry tracking in a native application is separate from an opt-out of Flurry tracking in a mobile Web application. Also, if an End User enables third party cookies on a mobile Web browser, parties other than Flurry may also place cookies for their tracking or advertising purposes.

7. HOW WE DISCLOSE OR SHARE INFORMATION WITH OTHERS

Except as described in this policy, Flurry does not rent, sell, or share personally identifiable information collected on the Sites or through the Flurry Services with other people or nonaffiliated companies unless we have your consent, or under the following circumstances:

with third party vendors, consultants and other service providers who work for us and need access to your information to do that work;

to comply with laws or to respond to lawful requests and legal process;

to protect the rights and property of Flurry, our agents, customers, users, and others including to enforce our agreements, policies and terms of use;

in an emergency to protect the personal safety of Flurry, its customers, or any person;

in connection with or during negotiation of any merger, sale of company assets, financing or acquisition of all or a portion of our business to another company.

We may also share aggregated or anonymized information in a form that does not directly identify you or your End Users with any third parties.

8. UPDATING YOUR INFORMATION AND CONTACT PREFERENCES

We provide you the mechanism to review and update your information through the Sites. If you wish to review or update your information, please visit www.flurry.com and login using the user name and password you created. Next, please select "your profile," which can be found in the upper right corner of the screen. You have the ability to opt-out of receiving email communications from Flurry via your preference settings on your profile page. In addition, you can opt-out of receiving promotional emails from us by following the instructions in those emails. If you opt-out, we may still send you non-promotional emails, such as emails about your account or our ongoing business

relations.

Under California law, California residents who have an established business relationship with us may choose to opt-out of the disclosure of personal information about them to third parties for such third parties' direct marketing purposes. As detailed above, our policy is not to disclose personal information collected online to a third party for direct marketing purposes without your approval. If you choose to opt- out at any time after granting approval, email privacy@flurry.com.

9. HOW WE PROTECT YOUR PERSONAL INFORMATION

Flurry uses reasonable efforts to help protect your personal information against unauthorized access and unauthorized alteration, disclosure or destruction. However, we cannot guarantee that your personal information will be absolutely protected. For example, your personal information may be affected by actions outside of our control, such as computer "hacking" and physical theft. You acknowledge that you provide your personal information at your own risk.

10. OUR POLICY REGARDING CHILDREN

We do not knowingly collect or solicit personal information from anyone under the age of 13 or knowingly allow such persons to register on the Sites or for the Flurry Services. If you are under 13, please do not attempt to register or send any information about yourself to us, including your name, address, telephone number, or email address. No one under the age of 13 may provide any personal information to us. In the event that we learn that we have collected personal information from a child under age 13 we will delete that information as quickly as possible. If you believe that we might have any information from or about a child under the age of 13, please contact us at privacy@flurry.com.

Our Customers may not use the Flurry Services in connection with any application labeled or described as a "Kids" or "Children" application and may not use the Flurry Services a) in connection with any application, advertisement or service directed towards children or b) to collect any personal information from children.

Notwithstanding the foregoing, you may use the restricted version of Flurry Analytics in connection with an application labeled or described as a "Kids" or "Children" application or in connection with an application or service directed towards children.

11. INTERNATIONAL TRANSFER

We may, in the process of providing services to you, transfer information that we collect about you or your End Users, including personal information, to affiliated entities, or to other third parties across borders and from your country or jurisdiction to other countries or jurisdictions around the world. If you or your End Users are located in the European Union or other regions with laws governing data collection and use that may differ from U.S. law, please note that you are transferring information and permitting the transfer of information, including personal information, to a country and jurisdiction that does not have the same data protection laws as your jurisdiction, and you consent to the transfer of information to the U.S. and the use and disclosure of information about you and your End Users, including personal information, as described in this Privacy Policy.

12. CHANGES TO THIS PRIVACY POLICY

We may change this Privacy Policy at any time. We will post all changes to this Privacy Policy on this page and will indicate at the top of the page the modified policy's effective date.

13. CONTACT US

If you have any questions or suggestions regarding this Privacy Policy, please contact us at privacy@flurry.com.

Flurry, Inc., 360 3rd St. Ste. 750, San Francisco, CA 94107

Bijlage 15.

Gedragcode 1992 Advocaten

Regel 6 (regel 9 en 10 oud)

1. De advocaat is verplicht tot geheimhouding; hij dient te zwijgen over bijzonderheden van door hem behandelde zaken, de persoon van zijn cliënt en de aard en omvang van diens belangen.

2. Indien een juiste uitvoering van de hem opgedragen taak naar zijn oordeel een gebruik maken van zijn verkregen kennis naar buiten eist, staat dat de advocaat vrij, voor zover de cliënt daartegen geen bezwaar heeft en voor zover dit in overeenstemming is met een goede beroepsuitoefening.
3. De advocaat legt zijn medewerkers en personeel de inachtneming van een gelijke geheimhouding op.
4. De geheimhoudingsplicht duurt voort na de beëindiging van de relatie met de cliënt.
5. Indien de advocaat aan een wederpartij vertrouwelijkheid heeft toegezegd of deze vertrouwelijkheid voortvloeit uit de aard van zijn relatie met een derde, zal de advocaat deze vertrouwelijkheid ook jegens zijn cliënt in acht nemen.

Toelichting op regel 6 (regel 9 en 10 oud)

De bij de wet geregelde zwijgplicht en het wettelijke verschoningsrecht van de advocaat strekken zich alleen uit tot datgene wat de cliënt de advocaat heeft toevertrouwd, daaronder begrepen hetgeen hem ter kennis kwam tijdens (schikkings)onderhandelingen. Dat wordt slechts anders als is komen vast te staan dat die onderhandelingen tot overeenstemming hebben geleid. Alleen in dat geval is er geen zwijgplicht.

Met het oog op een goede beroepsuitoefening is het gewenst dat de geheimhoudingsplicht van de advocaat zich verder uitstrekt. In het eerste lid van het nieuwe artikel staat de algemene norm van het beroepsgeheim, d.w.z. de geheimhoudingsplicht in enge zin en 'geroddel'. Het gaat om alle kennis omtrent zijn cliënt, hoe ook verkregen: van de cliënt, van derden, vertrouwelijk of niet. De behandeling van een zaak eist natuurlijk veelvuldig, dat de advocaat zijn kennis omtrent de cliënt wel naar buiten brengt. In het tweede lid is geformuleerd dat de advocaat dit mag doen, voor zover de cliënt daartegen geen bezwaar heeft. Cliënten ontslaan advocaten zo nu en dan van hun geheimhoudingsplicht. De advocaat behoudt niettemin een eigen verantwoordelijkheid. Dit wordt in het tweede lid tot uitdrukking gebracht in het begrip goede beroepsuitoefening. Er is geen aanleiding de advocaat te verplichten mededelingen van derden te verzwijgen tegenover zijn cliënt, ook niet wanneer het gaat om mededelingen over zijn cliënt. Dit is alleen anders als de vertrouwelijkheid rechtstreeks voortvloeit uit de aard van de relatie van de advocaat met een derde, bijvoorbeeld een andere cliënt, of als de advocaat vertrouwelijkheid heeft toegezegd. De advocaat doet er in het algemeen niet verstandig aan dergelijke toezeggingen te doen.

Bijlage 16.

Uitwerking interview met: Janneke Sloetjes, Bits of Freedom

Donderdag 12 december 2013

1. Gebruikt u zelf een smartphone met apps? (Ja, wat voor smartphone, hoeveel apps ongeveer? Welke apps gebruikt u het meest? – Nee, waarom niet? (misschien een iPad?))

Nee → verder naar vraag 4.

Ja, een iPhone 4S, ik gebruik nog geen 40 apps. Wanneer ik een app download let ik op de voorwaarden.

2. Leest u bij het installeren van een app de gebruiksvoorwaarden van de Store en de app zelf? (Waarom wel/niet?)

Ja, in principe wel. Stel zelf de vraag hoeveel data de app gebruikt en of de app deze data echt nodig heeft.

Van de Apple Store heb ik de voorwaarden eens gelezen.

3. Heeft u een app wel eens niet geïnstalleerd omdat, u de gebruiksvoorwaarden heeft gelezen?

Ja, ik heb Viber niet geïnstalleerd en sommige apps gebruik ik beperkt. Shazam gebruik ik bijvoorbeeld niet vanwege de voorwaarden.

4. Waarom vraag Android bij het installeren van de app wel machtigingen en Apple niet? Heeft Apple automatisch toegang tot dezelfde gegevens als bij Android?

Voor de toegang tot de smartphone maakt het niet uit of er machtigingen worden gevraagd, al weet ik het technisch gezien niet precies. Op de twee verschillende platformen is er geen verschil tussen het doorgeven van informatie. Zo geven ze beide identificeerbare nummers (UDID) door. Apple doet ook een strengere check van te voren, bij Android doen ze dat niet. Desondanks weet je het niet precies wat er aan de achterkant gebeurt en wat apps in detail doorgeven en verwerken.

Bij Apple is de gebruiker statistisch iets beter af qua veiligheid.

5. Wat zijn volgens u de grootste risico's van apps?

Apps die veel persoonlijke gegevens verzamelen, foto's en contactenlijsten opslaan op de servers. Wat er dan vervolgens gebeurt met deze gegevens en wie er toegang tot hebben is nog de vraag.

Bijvoorbeeld bij LinkedIn, vorig jaar was er een data lek. Bij consumenten die de LinkedIn hadden gedownload werd automatisch de kalender van de smartphone gekoppeld aan de app, zonder toestemming. Zo konden afspraken die werden gemaakt via LinkedIn meteen in de agenda worden gezet en LinkedIn kon kijken of de persoon beschikbaar was.

Hier hoefden gebruikers geen toestemming voor te geven. Twee dagen later was er een enorm lek bij LinkedIn waar van duizenden gebruikers gegevens waren gestolen.

Daarnaast speelt ook de onwetendheid van mensen een rol en de onveilige opslag van de servers. Tot slot de vraag: welke overheden kunnen erbij? En in welke mate?

5a. Wat vindt u ervan hoe apps met gegevens van gebruikers omgaan?

De meeste apps zijn best netjes, veel app-ontwikkelaars houden zich aan de regels. Toch zijn er ook veel ontwikkelaars die "vanaf de zolderkamer" opereren en kwaad willen en/of kunnen.

Sommige apps zijn dubieus, schort aan informatie vanuit app ontwikkelaar. De app vraagt bijvoorbeeld wel toegang maar geen uitleg waarom de app deze gegevens nodig heeft.

Google handelt in strijd met Cbp, want zij maken in de nieuwe voorwaarden niet duidelijk waarom ze gegevens nodig hebben en wat zij er mee doen. Ze trekken daarnaast het begrip 'om onze services en diensten te verbeteren' erg breed.

De onwetende consument heeft vaak ook geen idee wat er mee gebeurt.

6. Wat is de oorzaak dat apps gegevens verzamelen?

Nodig om te kunnen functioneren, Whatsapp moet toegang hebben tot deel van contacten om mensen te kunnen bereiken. Veel dingen zijn ook handig, mensen willen ook een bepaalde functionaliteit toevoegen aan telefoon dus daarom moeten apps wel toegang hebben tot een aantal zaken.

Veel apps verzamelen ook dingen die niet nodig zijn. Flashlight verzamelt bijvoorbeeld: locatiegegevens, camera op ieder moment toegang tot foto's en video's. De doelbinding is dan weg.

7. Wat is / zijn eventuele oplossing(en) voor de risico's van apps?

Beter toezicht op de app markt. → door Cbp en/of OPTA

App-ontwikkelaars zitten over de hele wereld o.a. in Europa en Amerika, kan probleem zijn qua wetgeving wanneer het buiten de EU is.

Meer duidelijkheid over doelbinding, wat verzamelen en wat niet, vragen om toestemming en niet zoals dat nu bij cookies gebeurt. Specifieker en duidelijker.

Niet elke app checken, hogere pakkans, boetebeleid.

8. Wat vindt u van de ontwikkelingen die op het moment spelen omtrent apps en gegevensverwerking?

Goed, over de hele linie is er meer aandacht gekomen voor privacy ook ten opzichte van de overheid.

Privacy en gegevensverwerking kan breder worden getrokken dan alleen op het gebied van apps.

Sociale dienst van de gemeente kan bijvoorbeeld ook in gegevens kijken betreffende huur terwijl zij daar in eerste instantie niks mee te maken hebben. Zo geldt het ook voor meerdere instanties zoals

de politie. Er moet meer bewustwording van de consument komen maar dit kan alleen slagen als er meer informatie komt en strengere eisen vanuit de overheid.
Bedrijven blijven achter in informatieverplichting de wil is er niet om te verbeteren of te veranderen.

8a. Gaat hier een verandering in komen of gaat dit de komende jaren op dezelfde voet verder? (Zo ja, wat voor veranderingen?)

Het is een spannende tijd nu. In Brussel wordt er besloten over nieuwe Wbp in Europa. Wetgever heeft in 2012 een voorstel gedaan, politieke partijen zijn wat aan het afzwakken omdat, bedrijven moeten geld blijven verdienen door o.a. het verzamelen van gegevens.

Er is op dit moment (en het kan nog versterkt worden) een tweestrijd tussen politiek en bedrijfsleven. Grote bedrijven zoals Apple, Google en Facebook hebben een actie gestart tegen de manier waarop overheid de overheid gegevens verzamelt.

(www.reformgovernmentsurveillance.com)

Dit is als het ware een charmeoffensief naar de gebruikers toe, zelf doen zij het namelijk net zo goed. Daarnaast verdienen de bedrijven geld aan de gegevens van gebruikers, dus zijn hebben er een groot belang in.

Dit zal misschien nog een gevecht worden tussen de overheid en de bedrijven. Tegelijkertijd moet de overheid ook zelf haar best blijven doen want, zij verzamelen ook allerlei gegevens van burgers en hebben soms toegang tot zaken waar zij ook niet in mogen kijken.

Qua de gegevensverwerking hebben we met z'n alleen geen idee meer waar alles is opgeslagen. Sommige apps weten soms ook niet waar gegevens staan, omdat veel gegevens worden verknipt en her en der worden verwerkt en opgeslagen.

9. Hoe vindt u dat de 'gewone' burger met apps omgaat? Hoe staat de maatschappij op dit moment tegenover privacy?

Wij doen niet veel onderzoeken naar wat de burger in de algemene zin vindt van privacy. Denk wel dat mensen in de algemene zin beseffen dat zij soms onbedoeld sporen achterlaten.

Rondom onthullingen rond de NSA en wantrouwen ontstaat naar overheden en bedrijven.

De Belastingdienst wou leaserijders volgen bij parkeren → mensen zijn hiertegen.

Het is goed dat mensen zich afvragen dat mensen zich afvragen wat mag en niet mag. Overheden terugroepen of het mag.

10. Heeft u zelf eens een nare ervaring gehad met het gebruik van apps?

Ja met LinkedIn, hoe komen gegevens uit mijn kalender in de app terecht? Daar had ik geen toestemming voor gegeven en heb dit toen meteen uitgezet.

Bijlage 17.

Uitwerking interview met: Aramis Jean Pierre, Privacy Officer DUO

Datum: 10 januari 2014

1. Waarom heeft DUO een privacyofficer in dienst genomen en wat houdt deze functie in?

Mijn functie bij DUO is niet privacy officer maar functionaris voor de gegevensbescherming. Deze functie houdt in dat ik toezicht hou op de vereisten van de Wbp binnen DUO. De functie van Functionaris voor de gegevensbescherming bij DUO is bij wet vastgesteld, er zijn 2 functionarissen binnen onderwijs waarvan 1 binnen DUO. Een functionaris wordt geacht onafhankelijk op te treden binnen de organisatie.

Een privacy officer implementeert maatregelen en is een adviseur voor de eerste lijn.

Bij wet is (4 keer) vastgesteld dat DUO een toezichthouder moet hebben. Het staat 1x in de kaderwetgeving (WOT: Wet op het onderwijstoezicht) en in drie specifieke wetten betreffende: voortijdig schoolverlaten, diplomaregister en inburgeringwetgeving. Waarom bij deze wetten?

Omdat deze bestanden bijzondere persoonsgegevens bevatten (ras, politieke voorkeur, geaardheid,

geloof of van zodanig grote omvang zijn dat eventuele inbreuk op de gegevens kan leiden tot grote impact op de levenssfeer van betrokkenen).

1a. Omdat bedrijven/overheden een privacy officer in dienst hebben betekent dit dat er meer waarde wordt gehecht aan privacy door de overheid of dat er meer gevaren zijn op het gebied van privacy?

Veel organisaties hebben een privacy officer in dienst wiens functie vergelijkbaar is met een functionaris gegevensbescherming. Deze hebben echter niet de wettelijke bevoegdheden en beschermingsmaatregelen op basis van de Wbp

“Gevaren” kan beter geformuleerd worden als “risico’s”. DUO verwerkt veel persoonsgegevens van studenten. Dit brengt automatisch risico’s met zich mee. Elke student/scholier heeft een Onderwijsnummer (OWN), dit omdat minderjarige allochtone studenten geen BSN hebben en het verplicht is om iedere minderjarige in Nederland onderwijs te bieden. Hiermee kunnen ze zich inschrijven voor een studie.

Daarnaast is DUO heel goed in het verwerken van heel veel persoonsgegevens hierdoor is in nog 3 specifieke wetten (zie vraag 1.) opgenomen dat een toezichthouder moet worden aangesteld. Een risico is dat bijvoorbeeld buitenlandse studenten uit China willen studeren in Nederland. Vanuit de Chinese overheid wordt het niet gewaardeerd dat een student politicologie gaat studeren. Daarom schrijven deze studenten zich in als kunstgeschiedenis student en een maand later switchen ze naar politicologie zonder dat het gemeld wordt naar China, uit bescherming van de student. Wanneer er wordt gekeken naar de bijzondere persoonsgegevens (geloof, politieke voorkeur etc.) moeten deze gegevens over de hele linie gelijkwaardig en goed beschermd worden. Je weet nooit in wat voor politiek klimaat Nederland terecht kan komen. Een oud voorbeeld is de Tweede Wereldoorlog, alle joden stonden in Amsterdam netjes geregistreerd met de gevolgen van dien. Algemeen moet worden gesteld dat een organisatie die grote hoeveelheden persoonsgegevens verwerkt moet zorg dragen voor een goede bescherming van persoonsgegevens. Als overheid zijn we dit verplicht aan de burger en onze opdrachtgever(s). In tegenstelling tot het verleden brengt de verwerking van persoonsgegevens tegenwoordig andere risico’s met zich mee doordat digitalisering andere mogelijkheden tot inbreuk mogelijk maakt. Persoonsgegevens zijn gewild bij derden omdat er een financieel gewin mee kan worden behaald. Om te voorkomen dat derden onrechtmatig in het bezit komen van deze gegevens is het noodzaak om zowel technische als organisatorische maatregelen te treffen ter bescherming van de persoonsgegevens.

2. Waar lopen instanties het meeste tegen aan wanneer zij de privacy van haar gebruikers/klanten willen beschermen? (Wat voor risico’s, moeite met wetgeving?)

Deze vraag is gesteld in de richting van “moeite met wetgeving”.

Wbp is een kaderwet, het zijn algemene regels. De termen: “zorgvuldig” en “doelbinding” is erg subjectief om te implementeren omdat, elke persoon daar een andere interpretatie aan kan geven.

3. Kent u voorbeelden waarbij bedrijven of instanties zich niet aan de Wbp hielden wat betreft het beschermen van de persoonsgegevens/privacy van hun klanten/gebruikers. (Zo ja, welke voorbeelden?)

Ja, maar mag geen namen noemen. In zijn algemeenheid loopt elke organisatie tegen dit probleem aan. Wij als DUO hebben dit ook gehad. Een aantal jaar geleden is MijnDUO een tijdje open geweest. Dit betekend dat wanneer een student naar MijnDUO website ging hij/zij de inloggegevens van de vorige bezoeker kon zien. Dit was een fout in de programmatuur en is direct hersteld. Alle mogelijke geraadpleegde inloggegevens hebben wij toen gedurende een bepaalde periode gelogd en gevolgd om te controleren of er niks raars gebeurde met die gegevens.

Meestal zijn het “foutjes” die bedrijven onbewust maken.

Daarnaast gaan de technische ontwikkelingen sneller dan maatregelen, en de technische ontwikkelingen moeten ook technisch goed beveiligd kunnen worden en blijven.

Als toezichthouder moet ik bedenken wat de meest vergaande gevolgen kunnen zijn en daarna de gevolgen terug brengen naar redelijke paden. Wat bijvoorbeeld nu heel vergaand kan zijn kan over een jaar al als alledag worden bestempeld.

4. Vindt u dat de manier van verwerken van persoonsgegevens volgens de Wbp een goede manier is of kunnen er zaken verbeterd worden? (zo ja, welke zaken?)

Wbp is een kapstok en wij mogen blij zijn dat we deze wet hebben. Wbp is van dwingend recht maar met een ruimte interpretatie.

Volgens Aramis Jean Pierre zal de privacywet wijzigen in de toekomst. Het strikt beschermen van gegevens wordt door de techniek ingehaald. Er komt meer transparantiewetgeving: verspreiding van de gegevens kan niet worden tegengehouden maar waar onze gegevens zijn en wie het gebruikt kunnen we later wel traceren. (Track en Trace systeem). Dit is opgenomen in nieuwe EG-verordening, welke volgens planning dit jaar mei in werking zou treden, maar wegens tegenstrijd van lidstaten wordt het hopelijk mei 2016.

De privacyverordening wordt nu aangehaald als: Algemene Verordening Gegevensbescherming (AVG).

5. Ondanks dat de Wbp van dwingend recht is en duidelijk is geformuleerd zijn er toch bedrijven/overheden die er tegen aan lopen (bijv. Gebruikersnamen, rekeningnummers komen op straat te liggen etc.) Hoe kan dit?

In vraag 3 is deze vraag al grotendeels behandeld. Toch speelt de moedwilligheid van organisaties een rol. De Wbp schrijft maatregelen voor maar soms zijn organisaties niet bereid of zien de noodzaak er niet van in om te investeren in het goed implementeren van de Wbp in hun processen. In hun ogen is dat namelijk niet belangrijk.

6. Loopt u tijdens uw werkzaamheden tegen zaken aan waarbij de privacy van burgers gevaar loopt? (zo ja, welke zaken?)

Ja, anders zou ik hier niet zitten. Er zijn altijd risico's. Een voorbeeld is dat studenten telefonisch het afhaaladres van hun OV-chipkaart konden krijgen met behulp van hun correspondentienummer. Familie van een weggelopen Turks meisje had haar correspondentienummer achterhaald en kwamen, door te bellen, erachter waar zij haar OV kon ophalen. Familieleden hebben twee weken lang gepost bij het afhaaladres en uiteindelijk hebben ze haar gevonden en meegenomen naar Turkije. Het betrof hier om een geautomatiseerd informatiesysteem waarbij de klant d.m.v. het invoeren van het correspondentienummer, via de computer het afhaaladres van de OV-kaart kon achterhalen.

7. Wat vindt u van de ontwikkelingen die op het moment spelen omtrent gegevensverwerking van burgers door overheden/bedrijven? (En als u er bekend mee bent, met apps)

Snelle ontwikkeling. Er is een bewustwording gaande wanneer je kijkt wat er in de media wordt gepubliceerd en in het nieuws. De Europese Commissie heeft onderzoek gedaan naar de privacy bij lidstaten, dit is voor de lidstaten een extra incentive om hun wetgeving betreffende privacy op orde te krijgen.

De Nederlandse overheid is bezig met het voorstel meldplicht datalekken. Wanneer een bedrijf een datalek heeft moet deze conform een bepaalde procedure dit oplossen en melden bij het CBP wanneer dit niet gebeurt krijgen ze een boete per incident.

U gaf aan dat u geen expert bent op het gebied van apps, desondanks wil ik u toch een aantal vragen stellen m.b.t. apps:

8. Gebruikt u zelf een smartphone met apps? (Ja, wat voor smartphone, hoeveel apps ongeveer? Welke apps gebruikt u het meest? – Nee, waarom niet?)

Ja, een Blackberry (zonder apps) en een Samsung S1 voor prive gebruik. Alleen op de Samsung heb ik 2 apps (Google Maps en Whatsapp). De locatievoorzieningen heb ik uit staan. Het was een bewuste keuze om mijn Android te gebruiken aangezien ik daar geen bijzondere vertrouwelijke gegevens verwerk.

9. Leest u bij het installeren van een app de gebruiksvoorwaarden van de Store en de app zelf? (Waarom wel/niet?)

Ja, ik lees het helemaal door. Dit gezien de functie die ik heb.

Ik gebruik heel weinig apps en bewust heb ik ervoor gekozen om geen Facebook en Twitter te gebruiken. Ik wil zo veel mogelijk grip houden op de gegevens die eventueel over mij op internet wordt verspreid.

10. Denkt u dat apps privacyrisico's met zich mee brengen? (Zo ja, welke risico's?)

Ja, ik denk vooral de gratis apps en spelletjes apps. Gratis apps zijn namelijk geen gratis apps, gegevens die deze apps verzamelen worden namelijk voor andere doeleinden gebruikt. Vooral om geld te verdienen aan de gegevens. Daarnaast kan het zo zijn dat 9 van de 10 apps op je telefoon veilig zijn maar dat net 1 gratis spelletjes app als doorgeef luik werkt door gegevens uit de andere apps te verwerken en door te sturen naar bedrijven.

10a. Wat vindt u ervan hoe apps met gegevens van gebruikers omgaan?

In zijn algemeenheid weinig over te zeggen. Het zijn niet de apps die met gegevens van de gebruikers omgaan maar de bedrijven achter de apps. De apps functioneren vooral als doorgeefluik voor de gegevens.

11. Gaat er een verandering komen over hoe er met privacy wordt omgegaan of gaat dit de komende jaren op dezelfde voet verder? (Zo ja, wat voor veranderingen?)

Ja er gaat een verandering komen: de wetgeving verandert en er komt een grotere bewustwording onder de burgers doormiddel van de media.

12. Hoe vindt u dat de 'gewone' burger met apps omgaat? Hoe staat de maatschappij op dit moment tegenover privacy?

Alles wordt geaccepteerd, apps hebben vooral gebruiksgemak. Ik denk wanneer de digitale effecten fysiek zichtbaar worden gemaakt dat dan heel veel mensen schrikken van wat er gebeurt met hun gegevens.

Bijlage 18.

Uitwerking interview met: mr. T.J.J. Bodewes, advocaat BoutOveres

Datum: 27 november 2013

1. Gebruikt u zelf een smartphone met apps? (Ja, welke, hoeveel apps ongeveer? Welke apps gebruikt u het meest? – Nee, waarom gebruikt u geen smartphone?)

Ja, ik gebruik een HTC Desire Z, ongeveer drie jaar oud met Android Software. De meeste apps die worden gebruikt zijn: de NS app voor treintijden, Whatsapp en een aantal spelletjes. Bij elkaar zijn het ongeveer 5 gedownloade apps. Ik vind een aantal zaken belangrijk aan een smartphone dat is: GPS, communicatie en af en toe documenten te kunnen openen.

2. Wordt er binnen dit kantoor veel gebruik gemaakt van smartphones? (Gebruikt men het zowel zakelijk als prive?)

Vrijwel iedereen gebruikt een smartphone, zowel privé als zakelijk. Collega's gebruiken ook een smartphone voor zowel privé als zakelijk. Voor zover ik weet worden er geen smartphones van de zaak verstrekt aan werknemers en schaft iedereen zijn eigen telefoon aan.

3. Heeft uw kantoor een beleid betreffende smartphones en het gebruik daarvan?

Er is binnen het kantoor geen expliciet beleid betreffende smartphones en het gebruik ervan. Ik ga bewust met mijn smartphone om en doe er niet alles mee. Bij zaken met een groot belang (vertrouwelijke zaken) zal er over het algemeen minder snel communicatie met de smartphone plaatsvinden.

Op het kantoor gebruikt het merendeel van de werknemers een Samsung met Android software, een enkeling maakt gebruik van een iPhone.

Het kantoor heeft ook een Twitter account, deze wordt door 1 persoon beheerd voor zover ik weet wordt het alleen beheerd via de computer en niet via de smartphone.

4. Op wat voor manieren communiceert u met uw cliënten?

Per email, telefonisch over de vaste lijn, face-to-face. Soms bel ik ook cliënten met mijn smartphone, ik sla dan niet de telefoonnummers op in het toestel. Van maar een paar cliënten heb ik het telefoonnummer opgeslagen in mijn adresboek. Met cliënten Whatsapp ik niet en sporadisch heb ik een keer wat over de SMS verstuurd naar een paar cliënten.

Ik e-mail nu nog niet via mijn smartphone ook is mijn zakelijke account er niet op aangesloten, wel mijn Hotmail account en soms stuur ik zakelijke e-mails door naar mijn Hotmail account. Een aantal collega's hebben wel het zakelijke email account gekoppeld aan de smartphone. Ik denk er over na om het zelf ook te gaan doen in de toekomst, alleen ben ik me wel bewust dat e-mails kunnen worden onderschept. Bij voorkeur gebruik ik de vaste lijn op kantoor.

5. In hoeverre denkt u dat apps een risico vormen voor de privacy van u en uw cliënten?

Ik merkte het op toen ik Whatsapp installeerde er veel app machtigingen werden gevraagd. Ik ben mij er wel van bewust dat bepaalde gegevens worden verwerkt door een app, zoals telefoonboek of e-mails. Ik vraag mij af en toe wel af of apps gesprekken kunnen opnemen of dat ze e-mails en berichten verwerken. Ik denk dat er wel een gevaar zit in wat er met gegevens gebeurt en wie er mee kijkt. Maar in eerste instantie ga ik er vanuit dat apps de verkregen gegevens op een nette manier behandelen.

6. Hoe ziet u het beroepsgeheim?

Het beroepsgeheim en de vertrouwelijkheid van de cliënt heb ik hoog in het vaandel staan, met name de relatie advocaat – cliënt. Vooral bij zaken met een groot en vertrouwelijk belang ben ik extra voorzichtig wanneer het gaat om gegevensoverdracht en verstrekking. Daarnaast ben ik van mening dat advocaten zelf moeten letten op wat 'vertrouwelijke informatie' is en op welke manier hierover wordt gecommuniceerd. Zo vind ik dat een adres van een persoon vrij makkelijk te traceren is en dat het een gegeven is dat een persoon ook snel zou geven in het algemeen. Communicatie zal dan misschien eerder via bijvoorbeeld Whatsapp kunnen plaatsvinden. Bij meer vertrouwelijke informatie zal communicatie minder snel via Whatsapp verlopen.

7. Weten jullie welke voorwaarden aan apps zijn verbonden? Leest u de gebruiksvoorwaarden wanneer u een app installeert? Heeft u wel eens een app niet geïnstalleerd omdat u de gebruiksvoorwaarden heeft gelezen?

Nee, het is in mijn opinie vooral gemakzucht om de voorwaarden te accepteren omdat het er erg veel zijn en het tijd kost om ze allemaal door te lezen. Daarnaast ga ik er van uit dat apps vertrouwelijk met verkregen gegevens omgaan en deze niet zomaar aan derden verstrekken of dat derden er gemakkelijk aan kunnen komen. Bij Whatsapp had ik bij het installeren wel enige twijfel toen de app-machtigingen naar voren kwamen vooral omdat, Whatsapp ook toegang heeft tot het telefoonboek. Maar het is een afweging die je maakt bij het downloaden want, als je niet akkoord gaat kun je het ook niet gebruiken dus, "vooruit maar".

8. In hoeverre bent u op de hoogte van de ontwikkelingen omtrent apps en gegevensverzameling?

Niet zozeer op de hoogte van gegevensverwerking van apps. Wel ben ik geïnteresseerd in het ICT Recht. Binnen het kantoor is er geen persoon die zich bezig houdt met apps en gegevensverzameling daarvan. Wel vind ik het een interessant onderwerp en wanneer een leuk artikel voorbij komt dan lees ik deze door.

9. Heeft u zelf eens een nare ervaring gehad met het gebruik van apps?

Nee dat niet.

Bijlage 19.

Uitwerking interview met: G.J. Veldthuis, Manager IT TRIP Advocaten

Datum: 3 december 2013

1. Gebruikt u zelf een smartphone met apps? (Ja, welke, hoeveel apps ongeveer? Welke apps gebruikt u het meest? – Nee, waarom gebruikt u geen smartphone?)

Ja, een iPhone 4 en een iPad. Alle medewerkers van TRIP hebben een iPhone en iPad van de zaak. Het doel is dat deze drie jaar mee kunnen gaan. Op dit moment variëren de versies binnen het kantoor van zowel een iPhone 4 tot en met iPhone 5.

De apps die ik zelf gebruik zijn Mail en Twitter, Dropbox voor privé. Medewerkers binnen dit kantoor gebruiken ook Facebook, Dirkwager en Whatsapp op hun devices. Weet niet precies welke apps medewerkers nog meer gebruiken.

2. Wordt er binnen dit kantoor veel gebruik gemaakt van smartphones?

Ja, zie vraag 1. Daarnaast maken medewerkers ook gebruik van een app die toegang geeft tot de gehele server van TRIP met betrekking tot de dossiers. De devices die de medewerkers krijgen worden zowel prive als zakelijk gebruikt.

3. Heeft uw kantoor een beleid betreffende smartphones en het gebruik daarvan?

Ja, voorheen had het kantoor een ICT reglement alleen dit was toegespitst op het gebruik van de PC. Met name hoe er veilig met internet en mail kon worden omgegaan. Sinds de zomer is het uitgebreid met een huisregels betreffende het datagebruik op de iPhones en iPads. Daarin staat ook hoe er met gegevens moet worden omgegaan en wanneer er informatie wordt uitgewisseld bijvoorbeeld op USB sticks. Ze proberen de risico's zoveel mogelijk in te perken en iedereen bewust te maken van de gevoeligheid van informatie.

Alle iPhones en iPads zijn daarnaast allemaal beveiligd via Mobile Iron, dit programma kan ook apps op een zwarte lijst zetten wanneer apps risicovol zijn (dit wordt nog niet gebruikt). Alle devices kunnen op deze manier makkelijk tegelijk worden beveiligd met hetzelfde programma. De devices mogen ook niet worden geïllegaliseerd. Daarnaast moeten alle devices zijn beveiligd met een wachtwoord/toegangscade.

4. Op wat voor manieren communiceert u met uw cliënten?

In dit kantoor wordt er vooral gebruik gemaakt van Email en telefoon. De iPhones en iPad van de zaak worden veelvuldig gebruikt door de medewerkers om telefoontjes te plegen en snel e-mails te lezen.

5. Denkt u dat apps een risico vormen voor de privacy van u en uw cliënten?

Er is wel een risico, bij IT proberen ze het zo goed mogelijk in te kaderen door beveiligingsmaatregelen te treffen. Advocaten vinden het over het algemeen makkelijk en verdiepen zich niet al te veel in de stof. Wanneer IT ziet dat iets niet verantwoord is proberen ze er wat aan te doen.

6. Hoe ziet u het beroepsgeheim?

Zelf geen advocaat, maar kent de lijnen van het beroepsgeheim. Vindt dat als er informatie lekt maar komt nergens anders boven water dan is er in eerste instantie nog niks aan de hand. Het wordt pas 'gevaarlijk' wanneer de gelekte informatie daadwerkelijk bovenkomt. Tot dusver is het nog niet gebeurd.

7. Weten jullie welke voorwaarden aan apps zijn verbonden? Leest u de gebruiksvoorwaarden wanneer u een app installeert? Heeft u wel eens een app niet geïnstalleerd omdat u de gebruiksvoorwaarden heeft gelezen.

Het is de eigen verantwoordelijkheid van de advocaten om zo goed mogelijk met hun devices en apps om te gaan. Zoals eerder gezegd zijn advocaten wel makkelijk in het downloaden van apps en

toevallig omdat, ze advocaat zijn hoeft nog niet te betekenen dat ze alle gebruiksvoorwaarden telkens doornemen.

8. In hoeverre bent u op de hoogte van de ontwikkelingen omtrent apps en gegevensverzameling?

Probeer het zo goed mogelijk bij te houden. Geregeld contact met de leverancier van de beveiligingssoftware om bij te praten over de ontwikkelingen op beveiligingsgebied. Email is privacygevoelig maar, advocaten (en niet alleen bij TRIP) doen veel over de mail omdat, het gemakkelijk werkt.

9. Heeft u zelf eens een nare ervaring gehad met het gebruik van apps?

Niet eigen ervaring, wel eens een stuk gelezen in het Financieel Dagblad waarbij een aantal Economen niet de Facebook app hadden gedownload vanwege het feit dat ze veel data kunnen ophalen.

Bijlage 20.

Uitwerking interview met: Huibert Scholters, Peperzaken

Datum: 9 december 2013

1. Gebruikt u zelf een smartphone met apps? (Ja, welke, hoeveel apps ongeveer? Welke apps gebruikt u het meest? – Nee, waarom gebruikt u geen smartphone?)

Ja op kantoor gebruikt iedereen een smartphone. Zelf gebruik ik een iPhone. De reden waarom er op kantoor veel smartphones zijn is om de apps te testen op verschillende toestellen met verschillende software van Apple tot Blackberry. Ik gebruik weinig apps ongeveer 4 terwijl ik ongeveer 100 tot 150 apps op mijn toestel heb staan.

2. Hoeveel apps ontwikkelt uw bedrijf ongeveer per maand?

Ongeveer 3 a 4 apps per maand. In 2008 is Peperzaken gestart omdat, de iPhone in dat jaar in Nederland werd gelanceerd. Toen is door Peperzaken de NU.nl app ontwikkeld. Rond 2008 waren er zo'n 20.000 iPhone gebruikers en 19.800 NU.nl downloads.

Een app ontwikkelen is een tijdrovend proces wat niet in een dag klaar is, daarom worden er ongeveer 3 a 4 apps per maand ontwikkeld.

We richten ons voornamelijk op de B2E (Business to Employee) en B2B (Business tot Business). Een aantal apps zoals Fit for Free en Nu.nl zijn op consumenten gericht.

3. Worden de door jullie ontwikkelde apps aangeboden via de iTunes Store of Google Play Store of via een andere manier?

Beide, voor consumenten in de App Store en Google Play Store. Er is ook een Enterprise Store dat is een afgeschermd Store voor bijvoorbeeld de NaM of Shell, daarin worden apps aangeboden specifiek voor de werknemers.

4. Zit er een verschil in het aanbieden van apps bij de iTunes Store of bij de Google Play Store? (Hebben jullie invloed op de voorwaarden van de platformen?)

Bij het bouwen van de app zit er al een verschil in software. Bij iOS wordt een net ontwikkelde app aangeboden aan Apple dan gaat Apple in een week checken of de app voldoet aan haar voorwaarden. Bijvoorbeeld op het gebied van privacy, content, locatievoorzieningen etc. Bij goedkeuring wordt de app in de Store aangeboden. Wanneer de app wordt afgekeurd moet de ontwikkelaar de app verbeteren en opnieuw aanbieden, waarbij er opnieuw gecheckt gaat worden door Apple. Zelf hebben wij dit nog niet meegemaakt.

Apple krijgt van de app de complete source code zodat ze de gehele app kunnen doorlichten.

Bij Android zijn ze makkelijker, wanneer een app in de Google Store wordt ingeschoten staat het er een uur later in de Store en kan voor de consument meteen het downloaden beginnen. Nadat de app in de Store staat gaat Android pas checken aan voorwaarden, wanneer de app wordt afgekeurd

wordt deze uit de Store gehaald. Het risico is wel dat de app in de tussentijd een aantal keer gedownload kan zijn.

Bij het aanbieden van een app zien wij de app als een product die wordt aangeboden in een winkel tot en met het aanschafmoment. Daarna verandert het in een dienst die op de gebruiker wordt afgestemd.

5. Worden er regels opgelegd bij het ontwikkelen van apps? Zo ja, welke regels? Zo nee, waarom niet?

Ja, iOS heeft guidelines waaraan de app-ontwikkelaars moeten voldoen en bij Android weet ik niet. Regels die worden opgelegd hebben betrekking op privacy, functioneren etc.

6. Waarom vraagt Android bij installeren wel een app- machtiging en Apple niet? Heeft Apple hierdoor automatisch toegang tot dezelfde zaken in de iPhone als Android op een Samsung?

Bij iOS wordt voor het aanbieden van de app al veel getackeld daarnaast krijgt de app expliciet toestemming wanneer deze toegang wil tot bepaalde zaken in de telefoon.

Apple heeft alleen toegang wanneer de gebruiker er expliciet mee akkoord gaat.

Het is enigszins scheef dat Android al goedkeuring vraagt voordat de consument eerst de app heeft gebruikt.

Qua machtigingen vraagt bijvoorbeeld Facebook toegang tot de camera. Dit wil niet zeggen dat Facebook zonder toestemming foto's kan maken maar dat zij toegang hebben tot de Camera rol.

Wat wel gevaarlijker is, is toegang tot de microfoon die sommige apps vragen bijvoorbeeld de Sleep Talk Recorder app. Deze app activeert automatisch de microfoon van het toestel wanneer deze stemgeluiden hoort. Het is technisch mogelijk dat andere apps dat ook kunnen doen.

Wat betreft de app machtiging: "opslag" is er niet veel om zorgen over te maken. De app haalt namelijk geen gegevens uit de opslag weg omdat, de persoonlijke opslag is versleuteld. De app gebruikt de opslag om standaard elementen uit de app op te slaan. Bijvoorbeeld bij de Nu.nl app is de layout hetzelfde, alleen de newsfeed wordt continue ververs. De layout wordt opgeslagen in de opslag zodat de app sneller laadt en opstart.

7. Kunnen apps theoretisch gezien een grote inbreuk maken in de software van een smartphone? (Kan een app inbreken op een telefoon en allemaal gegevens 'stelen?')

In de theorie kan ontzettend veel, bijv. Facebook en LinkedIn zouden inbreuk kunnen maken op persoonsgegevens. In de praktijk breken apps niet in het complete toestel in.

App-ontwikkelaars kunnen locatiegegevens loggen, zo kan er gekeken worden welke route iemand een heel jaar lang door Nederland heeft afgelegd. App-ontwikkelaar zelf doet niks met deze log gegevens.

8. Welke gegevens worden in de praktijk verwerkt door de meeste apps?

Locatievoorzieningen, dit kan doormiddel van GPS of driepuntsmeting.

GPS is vrij accuraat, tot op 5 meter. Driepuntsmeting gebeurt wanneer de app weet wat het IP adres is, wifi-netwerk of het netwerk waar de gebruiker op zit aangesloten (bijv. KPN). Dit is minder accuraat ongeveer 50 meter tot 150 meter. Het wordt meer accuraat wanneer de persoon zich beweegt, dan kan er worden gekeken welke kant deze persoon opgaat.

Veel apps vragen ook het UDID (Unique Device Identifier Number), dit is als het ware het Burger Service nummer van het toestel. Dit nummer kan een app niet automatisch koppelen aan een persoon, dat kan alleen als ook het e-mailadres en naam etc. wordt verstrekt.

9. Bent u zich bewust van de wetgeving omtrent software en gegevensverwerking?

Nee, de meeste zaken sturen wij door naar een jurist. De telecom markt is ook ontzettend veranderlijk en er zijn veel technologische ontwikkelingen. De algemene voorwaarden die apps hebben worden ook door de organisaties zelf opgesteld en niet door de app ontwikkelaar.

10. *Bent u zich bewust van de privacyrisico's van apps of hebben apps volgens u geen privacyrisico's?*
Ja, de mogelijkheden zijn eindeloos wanneer iemand kwaad wil doen. De persoon overtreedt de wet wanneer deze expres een app ontwikkeld waar privacy risico's aan kleven.
Zo is het bijvoorbeeld ook met het stelen van een auto, er staan tientallen auto's op de parkeerplaats die je op verschillende manieren kan stelen, maar wanneer je dit doet overtreedt je de wet en de pakkans is aanwezig.
Het is wel zo dat wij niet weten hoe bedrijven aan de achterkant met de informatie omgaan die zij verkrijgen via de app.

Qua veiligheid denk ik dat iOS wel veiliger is dan Android gebaseerd op wat hierboven staat (expliciet vragen, mogelijkheid tot weigeren van een machtiging).

Bijlage 21.

Uitwerking interview met: Alexander Postma, Appademic

Datum: 9 december 2013

1. *Gebruikt u zelf een smartphone met apps? (Ja, welke, hoeveel apps ongeveer? Welke apps gebruikt u het meest? – Nee, waarom gebruikt u geen smartphone?)*

Ja, een iPhone 5S het meest gebruik ik Whatsapp, Nu.nl, Facebook en Instagram. Alle collega's gebruiken een smartphone en de verdeling is ongeveer 50/50 tussen iPhone en Android.

2. *Hoeveel apps ontwikkeld uw bedrijf ongeveer per maand?*

Wij zijn net anderhalf jaar bezig en ontwikkelen ongeveer 1 app per maand. Het ontwikkelen kost veel tijd. Bekende apps die wij hebben ontwikkeld zijn Cigarette, 112Groningen en Modelscout.

3. *Worden de door jullie ontwikkelde apps aangeboden via de iTunes Store of Google Play Store of via een andere manier?*

Alleen bij App Store en Android Store.

4. *Zit er een verschil in het aanbieden van apps bij de iTunes Store of bij de Google Play Store? (Hebben jullie invloed op de voorwaarden van de platformen?)*

We hebben geen invloed en er zit een verschil wat betreft het aanbieden van app op beide platformen. Bij Android staat het binnen 1 uur in de Store na het inschieten van de app. Wanneer een app wordt ingeschoten wordt er door Google wel automatisch getest maar achteraf gebeurt dit door mensen.

Bij Apple wordt er eerst gecheckt of de app aan voorwaarden voldoet. Onze Cigarette app is bijvoorbeeld na de eerste keer teruggestuurd omdat, er een locatielimiet op zat en deze heb ik eruit gehaald en bij de tweede keer aanbieden kwam de app wel door de check.

Wat mij betreft is Android fijner bij het aanbieden van een app. Wanneer een app eindelijk klaar is ben je natuurlijk blij en het geeft dan meteen een goed gevoel om jouw app online te zien staan. Bij Apple duurt het eerst minimaal een week en dan zakt het gevoel ook wat weg.

5. *Worden er regels opgelegd bij het ontwikkelen van apps? Zo ja, welke regels? Zo nee, waarom niet?*

Ja, door Apple en Google worden bij betaalde apps afgesproken dat er een 30/70 verdeling is wat betreft de opbrengsten.

Apple is strenger wat betreft de regels bij het ontwikkelen van de apps, zo worden de apps ook eerst door hun gecheckt en er mogen geen apps worden ontwikkeld die zijn aangesloten bij Bitcoin.

De Cigarette app heb ik zelf ontwikkeld hierdoor krijgen wij gegevens van gebruikers op onze servers binnen. Zo kan ik zien wat de locatie is van gebruikers die de app hebben gedownload en gebruikers.

Daarbij wordt het soort toestel gekoppeld bijvoorbeeld Android of Apple (niet het ID nummer). Wij slaan deze gegevens op, op onze servers om later te kunnen gebruiken of voor pushmeldingen. Ik kan ook in de app bouwen dat deze linkt met Facebook, dan kan ik wel allerlei persoonsgegevens achterhalen van gebruikers.

6. Waarom vraagt Android bij installeren wel een machtiging en Apple niet? Heeft Apple automatisch een machtiging bij het downloaden?

Dit zou te maken kunnen hebben met het gebruiksgemak van de software. Apple wil niet dat consumenten eerst allemaal zaken moeten doorlezen maar dat zij meteen de app kunnen gebruiken. Daarom checken zij een app uitvoerig voordat deze wordt aangeboden in een Store. Android gaat er wat makkelijker mee om, daar kan een app meteen worden geplaatst en gedownload en achteraf wordt pas gecheckt of het veilig is.

7. Kunnen apps theoretisch gezien een grote inbreuk maken in de software van een smartphone? (Kan een app inbreken op een telefoon en allemaal gegevens 'stelen?')

Bij iOS weet ik niet. Bij Android kan wel vooral wanneer gebruikers niet updaten dan verouderd de software snel. Ook kan er op Android een virusscanner worden gedownload terwijl dit bij Apple niet nodig is, dat zegt ook wat over de veiligheid.

8. Welke gegevens worden in de praktijk verwerkt door de meeste apps?

Locatie, dit wordt meestal opgeslagen.

UDID's worden ook vaak verwerkt. Wanneer een gebruiker een app koppelt met Facebook krijgt deze app meteen ook alle Facebook gegevens en toegang tot vriendenlijsten en foto's.

9. Bent u zich bewust van de wetgeving omtrent software en gegevensverwerking?

Ja, is bekend met het CBP.

10. Bent u zich bewust van de privacyrisico's van apps of hebben apps volgens u geen privacyrisico's?

Wel van de risico's maar weet niet welke privacy risico's precies.

Zelf denk ik wel dat Apple veiliger is dan Android, in een Android app kunnen virussen worden ingebouwd en snel worden verspreid wanneer de app na het inschieten nog niet gecontroleerd is.

Bijlage 22.
Schematische weergave onderzoeksmodel

