KU LEUVEN

FACULTEIT SOCIALE WETENSCHAPPEN
MASTER OF SCIENCE IN DE
COMMUNICATIEWETENSCHAPPEN

Privacyvriendelijke fitness- en gezondheidstoepassingen in een big data-tijdperk

Promotor : Prof. Dr. K. SLEGERS
Verslaggever : Prof. Dr. D. DE GROOFF

MASTERPROEF
aangeboden tot het verkrijgen van de graad van Master of Science in de Communicatiewetenschappen
door **Evelien HERELIXKA**

academiejaar 2014-2015

Dankwoord

Eerst en vooral wil ik mijn respondenten bedanken, want zonder hun deelname kon deze masterproef niet tot stand komen. Ook dank aan professor Slegers en Bert Vandenberghe voor het vrijmaken van hun tijd en het geven van feedback. Tenslotte wil ik ook mijn vrienden en familie bedanken voor hun steun, aanmoediging en inspiratie.

Inhoudstafel

Inleiding

“Digitale metingen zullen ons op termijn wellicht gezonder maken, maar daar moeten we wel een prijs voor betalen: onze privacy.” Deze stelling uit Knack vat de essentie van deze masterproef samen (Peuteman & Pironet, 11.03.2015). Anno 2015 wordt er enorm veel data verzameld. Niet alleen online laten we informatie achter, maar ook onze smartphones slaan erg gedetailleerde informatie op. De opkomende quantified self-beweging levert nog zo’n bron van data op. Via allerlei apps en gadgets brengen de quantified selvers zichzelf in kaart: hun bloeddruk, locatie, eet- en slaappatroon en zelfs hun blootstelling aan de zon. Deze persoonlijke informatie levert natuurlijk tal van voordelen op (het kan een stimulans zijn om gezonder te leven, we kunnen inzichten uit de data destilleren,...), maar we lopen het gevaar dat we ervoor betalen met onze privacy omdat we toch heel persoonlijke gegevens vrijgeven.

Zeker in de context van de in populariteit stijgende fitness- en gezondheidstoepassingen is privacy van belang. Uit de data die zulke toepassingen verwerken is namelijk vaak gevoelige informatie af te leiden, zoals bepaalde ziektes en aandoeningen. Het gebruik van zulke toepassingen kan echter wel enorme voordelen opleveren. Indien zulke toepassingen op een grootschalige manier aangewend worden, zou het gebruik namelijk kunnen bijdragen tot een gezondere samenleving waar medische inzichten uit de data ontdekt kunnen worden en de gebruikers gemotiveerd worden tot een gezondere levensstijl. Als de gebruikers er echter niet op vertrouwen dat de apps goed met hun gegevens zullen omspringen, zal niemand van de toepassingen gebruik maken (Klasnja, Consolvo, Choudhury, Beckwith & Hightower, 2009; Prasad, Sorber, Stablein, Anthony & Kotz, 2012; Motti & Caine, 2014). Daarom is het van belang te peilen naar de privacybezorgdheden van gebruikers om ze vervolgens te kunnen oplossen, want om privacyvriendelijke apps te ontwikkelen moeten eerst de struikelblokken gekend zijn.

Daarom zal ik in deze masterproef enerzijds trachten te achterhalen hoe men staat tegenover het verzamelen en het gebruik van fitness- en gezondheidsdata: wat zijn de mogelijkheden en wat zijn de obstakels? In eerste instantie zal ik nagaan wat er in de literatuur beschouwd wordt als het grootste potentieel van fitness- en

gezondheidsapps en de big data die ze opleveren en wat eventuele keerzijden zijn. Dit zijn echter vaak opinies van academici, professionals en beleidsmakers. Daarom is het in tweede instantie ook belangrijk de eindgebruiker in het verhaal te betrekken. Er zal onderzocht worden hoe zij staan tegenover het verzamelen en gebruik van hun data. Want zijn ze überhaupt bezorgd om hun privacy wanneer ze zulke apps en toepassingen gebruiken? Indien dit het geval is, waar zijn ze dan bezorgd om en varieert deze bezorgdheid afhankelijk van bepaalde factoren? Anderzijds zal ik naast de opinies van academici, professionals, beleidsmakers en eindgebruikers ook op zoek gaan naar mogelijke oplossingen om de privacy van de gebruikers te waarborgen. We zullen op zoek gaan naar manieren om de privacybekommernissen in de toekomst te kunnen wegwerken.

Een belangrijk onderscheid waar aandacht aan moet worden besteed bij het bekijken van de onderzoeksresultaten van verschillende studies is het onderscheid tussen "natuurlijke" en "gedwongen" gebruikers. Laatstgenoemden gebruiken de fitness- en gezondheidsapps op vraag van onderzoekers voor de duur van een specifiek onderzoek, maar hun attitudes omtrent privacy kunnen mogelijks verschillen van de attitudes van natuurlijke gebruikers die zelf beslist hebben om zulke toepassingen te gebruiken. Naar de opvattingen van natuurlijke gebruikers is echter nog maar weinig onderzoek uitgevoerd. Zij verhouden zich ten eerste misschien anders ten opzichte van dataverzameling dan mensen die hier geen gebruik van maken. Ten tweede zijn ze door hun ervaring met fitness- en gezondheidstoepassingen mogelijks al in contact gekomen met bepaalde minpunten of privacyissues.

Daarom zal ik aan de hand van interviews bij natuurlijke gebruikers van fitness- en gezondheidstoepassingen proberen te achterhalen hoe zij zich verhouden ten opzichte van de verzameling en het gebruik van hun gezondheidsdata. Omdat het geen alledaags topic is, werden de deelnemers gevraagd op voorhand een opdrachtenbundel te maken omtrent dataverzameling in het algemeen. Aangezien naast hun opinie de gebruikers ook gevraagd werd hoe fitness- en gezondheidsapps in de toekomst meer vertrouwen zouden kunnen bieden, kreeg het onderzoek een generatieve toets om zo latente noden aan het licht te brengen.

Alvorens de methodologie en de resultaten van mijn onderzoek aan bod komen, zal eerst een overzicht van de literatuur gegeven worden. Hierin zullen eerst de concepten "big data" en "quantified self" verder toegelicht worden. Daaropvolgend komen de voor- en nadelen van het verzamelen en gebruiken van fitness- en gezondheidsdata aan bod door de ogen van de academici, professionals en beleidsmakers. Daarna worden de privacybezorgdheden vanuit het perspectief van de gebruiker besproken en wordt het onderscheid tussen "gedwongen" en "natuurlijke" gebruikers verder beargumenteerd. Vervolgens wordt besproken hoe de technologie het gebruik en de privacybezorgdheden beïnvloedt. Daarbij is het *privacy by design*-principe van belang. Tot slot komen mogelijke oplossingen voor privacyvriendelijke apps aan bod.

1. Literatuurstudie

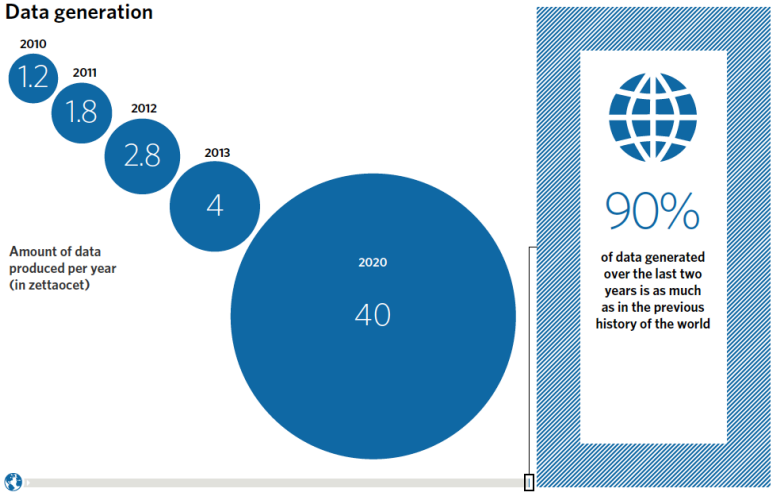
1.1 Big data

Tegenwoordig wordt er een enorme hoeveelheid informatie, zowel persoonlijke als feitelijke gegevens, verzameld via het internet en allerlei sensoren. Iemands contacten en relaties, zijn online aankopen, zijn locatie, zijn hartslag,... maar ook gedetailleerde informatie over de werking van machines en gegevens over het weer. Dit alles is mogelijk door de trend tot dataficatie, een term van Mayer-Schönberger en Cukier (2013). Dit houdt in dat we aan elk facet van het menselijk leven informatiewaarde hechten en het kwantificeren, zelfs aspecten zoals woorden, zithouding, de trillingen van een motor, interacties, locaties, gedachten en stemmingen. Allemaal zaken die vroeger ongrijpbaar waren.

Dit levert big data op. De term valt volgens Diebson (2012) voor het eerst midden jaren '90 in Silicon Valley door John Mashey. In de academische wereld is Diebson zelf de eerste die de term "big data" gebruikt op een congres over econometrie in 2000. Maar big data zorgt toch vooral in de private sector voor de nodige bedrijvigheid. In academische kring is er nog geen eensgezindheid over de betekenis van de term (Gandomi & Haider, 2015). Het is Laney die in een onderzoeksnota aan de META Group in 2001 voor het eerst spreekt

over de 3V's die big data kenmerken (Diebson, 2012). De 3V's staan voor volume *(volume)*, vlugheid (*velocity)* en variëteit *(variety)*.

De V van volume slaat op het feit dat de big data immens zijn. De mens genereert zoveel data dat de hoeveelheid tegenwoordig uitgedrukt moet worden in tera-, peta en zelfs zettabytes (Gandomi e.a., 2015). Maten waarbij we ons bijna niets meer kunnen voorstellen. De volgende illustratie probeert het toch iets bevattelijker te maken: op een terabyte kunnen 16 miljoen facebookfoto's gestockeerd worden. De Facebook-servers bevatten natuurlijk meer dan 16 miljoen foto's. Er wordt geschat dat er 260 miljard foto's bewaard worden. Hiervoor is een capaciteit van 20 petabytes beschikbaar (ibid.). Dit lijkt enorm, maar wat we als "big" categoriseren is relatief (ibid.). Wat vorig jaar als gigantisch werd bestempeld is dat vandaag al niet meer. Figuur 1 geeft weer hoe de hoeveelheid data bijna exponentieel toeneemt.



Figuur 1: toename van hoeveelheid data
Bron: European Voice, 2014, p.14.

Naast het volume worden big data verder gekenmerkt door vlugheid. Er wordt namelijk een stroom aan real-time informatie gegenereerd die ontzettend snel verandert (ibid.). Denk bijvoorbeeld aan GPS-data, clickstreams, bewakingscamera's, ...

De laatste V uit het 3V's-model staat voor variëteit. De data komen namelijk van verschillende bronnen en bestaan uit verschillende types: tekst, cijfers, foto's, audio en video en kunnen zowel gestructureerd als ongestructureerd zijn. Dit laatste is meestal het geval (ibid.). Denk maar aan de hierboven reeds vermelde clickstreams. Kortom, big data zijn heel groot, veranderen heel vlug en zijn heel verschillend. Het gevolg is dat traditionele dataverwerkings-programma's de big data niet (binnen een redelijke tijd) kunnen managen, verwerken en analyseren (Navetta, 2014; Gandomi e.a., 2015).

Aan het 3Vs-model wordt in het 4Vs-model nog het kenmerk "*value*" toegevoegd. Daarmee doelt men op de enorme waarde en hoeveelheid informatie die in de big data schuilgaan (Chen, Mao, Zhang, Leung, 2014). Van deze waarde zijn de gezondheidszorg en de geneeskunde zich bewust, onder andere om de kans op ziektes vroegtijdig te detecteren. McGregor en haar team bijvoorbeeld, destilleerden een patroon uit data die de monitoring van prematuren opleverde. De hartslag, de beweging van de borstkas, de bloeddruk, het zuurstofgehalte in het bloed en de ademhaling van een kindje worden verschillende keren per seconde geregistreerd. McGregor en haar collega's merkten dat het hartritme regelmatiger werd wanneer zich een infectie manifesteerde. Door dit inzicht kan reeds voor de symptomen de kop op steken al met een behandeling begonnen worden (Smolan & Erwitt, 2012).

Ook overheden en de belangrijkste economische industrieën zijn zich bewust van het potentieel van big data. Politiediensten maken bijvoorbeeld gebruik van data over eerdere misdaden om op basis daarvan af te leiden waar en wanneer een volgend misdrijf zal plaatsvinden (Cukier & Mayer-Schönberger, 2013). Gerechts-psychologen bepalen aan de hand van statistieken of een verdachte ook effectief een potentiële dader zou kunnen zijn. Zo blijkt uit de data bijvoorbeeld dat een verkrachter in 70% van de gevallen geen geweld gebruikt en zich eerder gedraagt als een gentleman. Wanneer een verkrachtingsslachtoffer dan beweert geschopt en geslagen te zijn, kan dit voor speurders een reden zijn om de verklaring te betwijfelen. Mogelijks is het slachtoffer hier op aandacht of wraak belust (Van der Meer, 13.03.2015).

Van het gebruik van big data in de private sector worden twee klassieke voorbeelden regelmatig aangehaald (Lane & Finsel, 2014). Target, een Amerikaanse winkelketen, analyseerde het koopgedrag van zijn klanten, legde zo interessante doelgroepen bloot en stuurde op basis daarvan gerichte advertenties uit. Zo kreeg een meisje verschillende promoties voor zwangerschaps- en babyproducten toegestuurd, waardoor haar vader ontdekte dat ze zwanger was. In het tweede voorbeeld analyseerde ook Walmart het koopgedrag van zijn consumenten. Daaruit bleek dat de verkoop van Pop-Tarts toenam in het orkaanseizoen. Op basis van dit inzicht besloot Walmart dan ook extra te voorzien in Pop-Tarts en zag zo zijn omzet stijgen.

Dit maakt tenslotte nog een laatste kenmerk van big data duidelijk: het belang van correlaties (Cukier & Mayer-Schönberger, 2013). Voor Walmart was het namelijk niet belangrijk te weten waarom de verkoop van Pop-Tarts toeneemt tijdens het orkaanseizoen, het kennen van het verband tussen beiden volstond om de omzet te zien stijgen. Verklaringen zijn vaak niet meer van tel, louter een correlatie volstaat in vele gevallen.

1.2 Quantified self als big data-bron

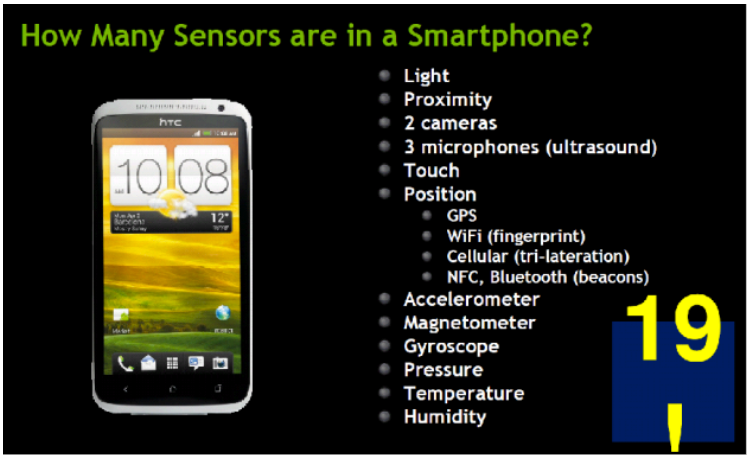
We kunnen dus stellen dat we aan het begin staan van het big data-tijdperk. “Data is de nieuwe olie”. Clive Humby stelt hiermee dat data beschouwd kunnen worden als een nieuwe belangrijke economische grondstof, zoals water en olie (Smolan & Erwitt, 2012). De quantified self-beweging is ook zo’n bron van big data. De data die het kwantificeren van het eigen lichaam opleveren, bieden tal van opportuniteiten, niet alleen voor de gebruiker maar ook voor de samenleving. Daar zal in de volgende paragraaf op worden in gegaan. In wat nu volgt, zal meer duiding gegeven worden bij het begrip “quantified self” en zullen de ontwikkelingen besproken worden die de groei van de quantified self-beweging hebben versneld.

De quantified self-beweging, naar een term van Wolf en Kelly (Bushhousen, 2014; Wolf, 2010), bestaat uit mensen die zichzelf via allerlei apps en gadgets zoals bijvoorbeeld Runkeeper of Fitbit kwantificeren of dataficeren, om het met de bovenvermelde term te benoemen. Verschillende aspecten van het lichaam zoals

bijvoorbeeld bloeddruk, aantal stappen, eet- en slaapgewoontes worden verzameld en opgeslagen. Quantified selvers brengen met andere woorden zichzelf in kaart. Tegenwoordig zijn er verschillende toepassingen op de markt die dit alles mogelijk maken. Fitbit en Jawbone UP zijn twee activiteitstrackers die als armband of clip gedragen kunnen worden. Ze registreren onder andere het aantal stappen, verbrande calorieën, slaappatroon,... Deze draagbare gadgets (ook wel wearables genoemd) worden gebruikt in combinatie met een app waarin de verzamelde data overzichtelijk weergegeven worden (Fitbit, 2015; Jawbone, 2015). Netatmo ontwikkelde recent een nieuw product dat kan toegevoegd worden aan de quantified self-familie: JUNE. Deze armband ziet er niet alleen uit als een sieraad, het meet de blootstelling aan de zon en geeft zo gepersonaliseerd advies (Netatmo, 2015). Runkeeper en de Calorieteënller van MyFitnessPal zijn twee populaire apps. Runkeeper registreert de snelheid, tijd, gelopen afstand en hartslag van de gebruiker, maar berekent daarnaast ook het aantal verbrande calorieën en het biedt audiobegeleiding aan (FitnessKeeper, 10.04.2015). MyFitnessPal (2015) biedt een software aan die het makkelijk maakt om bij te houden wat je eet en je calorieën te tellen. Dit is slechts een greep uit het grote aanbod aan gezondheidsapps. Apple lanceerde dan ook een platform, Gezondheid, dat de gebruiker in staat stelt om de metingen van verschillende fitness- en gezondheidsapps bijeen te brengen in één overzichtelijke app (Apple, 2015).

De groei van de quantified self-beweging en toename in gezondheidstoepassingen werd versneld door vier factoren, zo stelt Wolf (Bushhousen, 2014; Wolf, 06.2010). Ten eerste zien we vandaag overal de verspreiding van mobiele apparaten. De iMinds Digimeter 2014 (Vanhaelewyn, Pauwels, Maes & De Marez, 2014) brengt, op basis van een vragenlijst bij een representatieve steekproef van 2028 Vlamingen, de adoptie van onder andere gsm, smartphone en tablet goed in kaart en biedt steun voor de eerste stelling van Wolf. Een meerderheid gebruikt inderdaad al mobiele apparaten: 57,3% van de Vlamingen heeft een smartphone. Het smartphone-gebruik overtreft daarmee voor het eerst het gebruik van de traditionele gsm (52,7%). Ook tablets worden al door een meerderheid van de Vlaamse bevolking gebruikt (55,8%). Ten tweede, zo stelt Wolf, zijn sensoren zoals een accelerometer of GPS-

sensor beter en kleiner geworden. Daardoor kunnen we ze dus makkelijker in onze mobiele apparaten integreren. Tegenwoordig zitten er tot 19 verschillende sensoren in een smartphone (zie figuur 2).



Figuur 2: aantal sensoren in een smartphone
Bron: Entelechyasia, 2012.

Ten derde is het dankzij nieuwe ontwikkelingen zoals cloud computing en de toename in de opslagcapaciteit van chips gemakkelijker en goedkoper om alle verzamelde data te bewaren (Dehaene & Reynaert, 2014). Ook de dataverwerking verbetert sterk door de evolutie van allerlei nieuwe analysetools (Gandomi e.a., 2015). Ten slotte dragen ook de sociale media bij aan de groei van de quantified self-beweging. Zij maken het namelijk mogelijk en normaal om ons hele leven met elkaar te delen en elkaar aan te moedigen.

1.3 Het potentieel van big data uit fitness- en gezondheidstoepassingen

Tot dusver zou het stilaan moeten beginnen duidelijk worden dat er potentieel schuilt in de big data die gezondheidstoepassingen opleveren. Ook beleidsmakers zijn zich daar bewust van. De Europese Unie gelooft in het gebruik van mobiele toepassingen want door verschillende sociaal-maatschappelijke veranderingen zoals de vergrijzing en de verwachte toename in obesitas zal de gezondheidszorg onder druk komen te staan (Europese Commissie, 2014). De data die gezondheidsapps en wearables opleveren, kunnen een belangrijke rol spelen in de ontwikkeling naar een meer efficiënte en kwaliteitsvolle gezondheidszorg en zouden op de volgende drie niveaus verlichting kunnen bieden:

- op het niveau van het individu,
- op het niveau van de arts-patiënt-relatie,
- op het niveau van de samenleving.

1.3.1 Op het niveau van het individu

Het zien van gedetailleerde persoonlijke gezondheidsinformatie zou de gebruiker kunnen motiveren (Waltz, 2012). Als hij in een grafiek gevisualiseerd ziet hoeveel hij is afgevallen en hoe zijn conditie er op vooruitgaat zou dit een enorme stimulans kunnen zijn om verder te gaan met deze gezonde levensstijl (ibid.; Zuckerman & Gal-Oz, 2014; Nakajima & Lehdonvirta, 2013). Hij kan zich meer bewust worden van zijn slechte gewoontes zoals roken, overmatige consumptie van alcohol en ongezonde voeding en op die manier gestimuleerd worden (Fraser, Kwon & Neuer, 2011). Het is echter nog onduidelijk of het zien van zijn data ook effectief een gedragsverandering teweegbrengt, zo stelt Kvedar (Waltz, 2012). Hij stelt namelijk dat amper tien procent van de populatie alleen op basis van het zien van zijn data, zijn gedrag ook daadwerkelijk zal veranderen. De andere 90% heeft een additionele motivator nodig zoals een coach of een spelelement (ibid.).

Twee studies toonden aan dat indien een spelelement toegevoegd wordt aan een activiteitstracker, men bepaalde gebruikers

effectief kan aanzetten om meer te bewegen. *Fish'n Steps* verbindt een stappenteller met een virtuele vis (Lin, Mamykina, Lindtner, Delajoux & Strub, 2006). Die vis zit in een aquarium met andere vissen, die op hun beurt weer andere gebruikers representeren. Indien er meer gestapt wordt zal de vis gelukkiger zijn, meer bewegen en groeien. Zes weken lang testten 19 deelnemers de toepassing uit. Veertien deelnemers ervaarden een positieve verandering: ze zetten meer stappen of stonden positiever ten opzichte van bewegen. Enkelen negeerden echter de display wanneer hun vis er slecht aan toe was. Voor hen werkte de virtuele vis dus niet als een stimulans. Het tweede onderzoek liet drie vriendengroepen, in totaal dertien vrouwen, twee weken *Houston* gebruiken (Consolvo, Klasnja, McDonald, Avrahami, Froehlich, LeGrand, Libby, Mosher & Landay, 2008). *Houston* is ook een stappenteller. Hier werden de gebruikers beloond met een sterretje bij hun vooropgestelde aantal stappen wanneer ze dit doel effectief behaalden. Na een periode van twee weken waren de deelnemers zich meer bewust van hun hoeveelheid beweging en werden ze ook effectief gemotiveerd door de simpele beloningen, namelijk de sterretjes naast hun behaalde doelen (ibid.).

Ook zouden apps patiënten kunnen aanmoedigen hun medicatie nauwgezet in te nemen. Zo zijn er apps op de markt die de gebruiker helpen zijn medicatie nauwgezet in te nemen (MediSafe, 2015; EarthFlare, 2014). Er zijn eveneens verschillende applicaties beschikbaar die jonge vergeetachtige vrouwen helpen bij het innemen van hun anticonceptiepil (Baviux, 2015; Ben Basha, 2015).

Onderzoek toont echter aan dat het gebruik van zulke toepassingen niet wordt volgehouden eens het nieuwe er af is. De Consumer Health Information Corporation (2011) nam een online survey af bij 395 smartphongebruikers. Daaruit bleek dat 26% van de apps amper één keer gebruikt worden. Van de mensen die aangeven hun apps effectief te gebruiken, haakt toch ook 74% af na het tiende gebruik. Ook Becker en collega's (2013) stelden vast dat het appgebruik niet langdurig wordt volgehouden. Ze ontwikkelden een gratis app voor patiënten om hun medicatiegebruik op te volgen zodat de inname correct en op een regelmatige basis gebeurde. De onderzoekers brachten vervolgens het gebruik van de app in kaart. Hij werd door 11688 mensen gedownload. Na een maand gebruikte

amper nog een kwart van de gebruikers de app, na een jaar was dit nog maar 1 procent. Ook in het onderzoek van Lin e.a. (2006) met de virtuele vis, daalde het enthousiasme van de deelnemers na de eerste twee weken.

We kunnen dus besluiten dat fitness- en gezondheids-toepassingen de gebruiker er toe kunnen aanzetten een gezondere levensstijl aan te houden, zeker indien er een spelelement aan gekoppeld wordt. Het gebruik van een specifieke app wordt echter wel niet altijd lang volgehouden.

1.3.2 Op het niveau van de arts-patiënt-relatie

Naast het stimuleren van de gebruiker, laten verschillende mobiele toepassingen patiënten toe om zelf hun gezondheidstoestand op te volgen. Verschillende activiteitstrackers zoals Fitbit en Jawbone leveren gedetailleerde informatie over de calorie-inname, de mate van activiteit en het slaapgedrag van de gebruiker (Fitbit, 2015; Jawbone, 2015). Ook zijn er verschillende apps op de markt die de hartslag van de gebruiker kunnen meten zonder externe hardware door gebruik te maken van de camera van de smartphone (Runtastic, 2015; Azumio Inc., 2015). Zo kunnen veranderingen in de gezondheidstoestand eventueel zichtbaar worden.

Onderzoekers ontwikkelden de app *"bant"* (ondertussen ook verkrijgbaar in de Apple Store) die het patiënten makkelijk maakt om via een bluetooth-glucosemeter hun glucoselevel te monitoren. Ze koppelden er naast het gebruik van sociale media ook een spelelement aan dat de gebruikers aanspoorde om hun suikergehalte vaker te meten. Na een pilootstudie van drie maanden bij zestien deelnemers tussen 12 en 16 jaar, bleek dat het gemiddeld aantal keer dat de patiënten een meting uitvoerden was toegenomen met 49,6%. Veertien van de 16 deelnemers gaven bovendien aan dat ze de app verder zouden gebruiken (Cafazzo, Casselman, Katzman, Palmert, 2012, p. S77-S78).

Carrera en Dalton (2014) halen bewijs aan waaruit blijkt dat door zelfmonitoring bij chronisch zieken er ook minder nodeloos contact opgenomen moet worden met de arts. Het is niet alleen gemakkelijker en comfortabeler voor de patiënt om thuis zijn

gezondheidstoestand op te volgen, de tijd die daarenboven vrijkomt voor de dokter kan gespendeerd worden aan de patiënten die de arts het meest nodig hebben, zo stellen Steinhubl en collega's (2013).

De data die door fitness- en gezondheidstoepassingen gegenereerd worden, leveren een enorm vermogen aan gedetailleerde informatie op over de gezondheidstoestand en het gedrag van de gebruiker. De informatie die stappentellers en activiteitstrackers verzamelen is vaak van een hoge kwaliteit aangezien het op regelmatige tijdstippen automatisch wordt verzameld zonder vertekening door zelfrapportage (Markowetz, Blaszkiewicz, Montag, Switala & Schlaepfer, 2014). Hoewel dit natuurlijk niet altijd het geval is, want er zijn verschillende toepassingen te bedenken waarbij de gebruiker de data wel zelf invoert, zoals bijvoorbeeld een calorieënteller. De gedetailleerde informatie die de mobiele gezondheidsapplicaties genereren, zouden de arts een holistisch beeld van zijn patiënt kunnen opleveren. Op basis hiervan is hij dan in staat een goed gefundeerde diagnose te stellen en kan hij ook een behandeling op maat van zijn patiënt voorschrijven (Europese Commissie, 2014, p.5 ; Fraser e.a., 2012, p.3). Uit een survey van Research Now (2015) bij 1000 app-gebruikers en 500 professionals uit de gezondheidssector blijkt dat 86% van de professionals gelooft dat de data uit gezondheidsapps hen meer informatie over hun patiënten zullen bezorgen en 50% gelooft ook echt dat ze op basis van die gedetailleerde informatie de efficiëntie van de zorgverlening kunnen verhogen.

We kunnen dus stellen dat de arts-patiënt-relatie verlicht wordt door het gebruik van fitness- en gezondheidstoepassingen. De patiënt kan ten eerste zijn eigen gezondheidstoestand opvolgen zonder contact met de arts, wat niet alleen comfortabeler is voor hem, maar ook efficiënter voor de arts. De data bieden de arts ten tweede bijkomende gedetailleerde informatie over zijn patiënt.

1.3.3 Op het niveau van de samenleving

Niet alleen kan het gebruik van fitness- en gezondheidstoepassingen in de gezondheidszorg tijdbesparender zijn voor de arts en comfortabeler voor de patiënt, studies suggereren dat het ook

kostenbesparender kan zijn voor de hele samenleving. Een kosteneffectiviteitsanalyse van het gebruik van de CardioManager-app door Spanjaarden uit Castile en Leon met hartfalen, maakte duidelijk dat het gebruik van de app de regio tot 9000€ per patiënt zou kunnen besparen. Hiervoor werd eerst de huidige kost geschat van de zorg van patiënten met hartfalen in de regio. Dit gebeurde op basis van cijfers van het Spaanse Ministerie van Volksgezondheid. Vervolgens werd ook berekend wat de kost van de zorg zou zijn als de CardioManager-app geïntroduceerd zou worden (Martín, Martínez-Pérez, de la Torre-Díez & López-Coronado, 2014). Ook een analyse van PwC in 2013 toont aan dat het gebruik van mobiele toepassingen in de gezondheidszorg de Europese kosten in deze sector met 99 miljard euro kan terugdringen (PwC, 2013).

Daarenboven zou de enorme hoeveelheid data die de mobiele applicaties voortbrengen in onderzoek nieuwe inzichten kunnen opleveren. Ziektes zouden vroegtijdig opgespoord kunnen worden en symptomen zouden blootgelegd kunnen worden. Op die manier kunnen we preventief handelen (Europese Commissie, 2014; Markowitz, Blaszkiewicz, Montag, Switala & Schlaepfer, 2013). De volgende toepassingen maken duidelijk dat er inderdaad nuttige inzichten uit de data naar boven kunnen komen. Uit een analyse van de data over de bedbezetting in Deense ziekenhuizen, bleek dat een hoge bedbezettingsgraad samenhing met een toename van 9% in de mortaliteitscijfers in vergelijking met de ziekenhuizen met een lage bezettingsgraad. Deze bevindingen maken de problematiek van de overbezetting duidelijk en zetten aan hier oplossingen voor te bedenken. Dankzij het analyseren van de bedbezettingscijfers werd dus duidelijk dat overbezetting mee aan de basis ligt van hogere sterftecijfers en dat hier oplossingen voor moeten gevonden worden zodat men de mortaliteit kan terugdringen (Madsen, Ladelund en Linneberg, 2014). Ook uit een studie waarin de hartslagsignalen van 764 patiënten werden geanalyseerd bleek dat het mogelijk is om patiënten met een verhoogd risico op sterfte te identificeren (Syed, Scirica, Mohanavelu, Sung, Michelson, Cannon, Stone, Stultz & Guttag, 2009). Zo kunnen de patiënten met een verhoogd risico vroeger geholpen worden. Verder is ook het voorbeeld dat hierboven aangehaald werd over het vroegtijdig detecteren van infecties bij prematuren een goede illustratie van de inzichten die de analyse van

gezondheidsdata kunnen opleveren.

Apple speelt met zijn recente lancering van ResearchKit goed in op het idee om inzichten de destilleren uit de grote hoeveelheid fitness- en gezondheidsdata (Apple, 2015). ResearchKit is een open source software die onderzoekers in staat stelt apps te creëren die gebruik maken van de data verzameld door de iPhone en Gezondheid-app van de potentiële deelnemers. Er werd onder andere al een app ontwikkeld die data verzamelt over astmapatiënten: hun astmasymptomen, het gebruik van hun inhalator, hun aantal stappen,... (Icahn School of Medicine, 2015). De ResearchKit stelt mensen dus in staat bij te dragen aan de vooruitgang van de gezondheidszorg.

Naast een motivatie voor de gebruiker en een verlichting van de arts-patiënt-relatie, kunnen fitness- en gezondheidstoepassingen dus ook op het niveau van de samenleving voordelen opleveren. Niet alleen kan de adoptie ervan de kosten in de gezondheidszorg terugdringen, uit de data kunnen daarenboven interessante inzichten naar voren komen zodat we preventief actie kunnen ondernemen.

1.4 De keerzijde van big data uit fitness- en gezondheidstoepassingen

De voordelen die de data uit fitness- en gezondheidstoepassingen opleveren, moeten natuurlijk afgewogen worden tegen mogelijke nadelen en problemen. Zo kan ten eerste de interpretatie van de gegevens moeilijk zijn, zowel voor de gebruiker als de arts die er daarenboven ook wat weigerachtig tegenover staat. Verder is er maar een beperkt publiek dat gebruik maakt van de verschillende fitness- en gezondheidstoepassingen. Ten slotte kan de privacy in het gedrang komen bij de verzameling van gezondheidsgerelateerde persoonlijke gegevens.

1.4.1 Gebruik van de gegevens

Susan Etlinger (2014) en Cukier en Mayer-Schönberger (2013) beklemtonen dat we kritisch moeten omgaan met big data. Het is de

mens die er info uit destilleert. Het zijn niet de data die betekenis creëeren, maar het zijn wij die betekenis geven aan de data. Er moet plaats blijven voor een menselijke blik, intuïtie en creativiteit zodat we ons leven niet op een machinematige manier leiden en alle beslissingen overlaten aan computers. Bedenk wat er kan gebeuren als we het aanwerven van personeel of het toekennen van een hypotheek volledig aan een algoritme overlaten. Elke situatie is anders en er mag niet alleen door een computer over beslist worden. De beslissing zou minstens bekrachtigd moeten worden door een expert (Mayer-Schönberger & Cukier, 2013). De data zijn een hulpmiddel op basis waarvan de mens beslissingen kan maken (Cukier e.a., 2013). We moeten de data goed aanwenden. Daarvoor is het belangrijk het kritisch en probleemoplossend denken te stimuleren (Etlinger, 2014). Dit geldt ook specifiek voor de medische context. Aaron Carroll, een professor in de pediatrie verbonden aan de Indiana University, benadrukt in een van de video's op zijn Youtube-kanaal *Healthcare Triage* dat de arts absoluut noodzakelijk blijft (Carroll, 2014). We zullen het stellen van diagnoses nooit volledig aan de technologie overlaten, de interpretatie van de mens blijft nodig.

Maar het is voor de arts en de patiënt vaak niet eenvoudig om de big data te interpreteren. Ze zijn immers niet opgeleid om met zo'n informatie om te gaan. Om aan dit probleem tegemoet te komen, zouden artsen (en patiënten) gebruik kunnen maken van visuele analytische tools zodat ze makkelijker beslissingen kunnen nemen op basis van de verzamelde data (Ola & Sedig, 2014). Visuele analytische tools stellen de gebruiker in staat de data op een toegankelijke manier te benaderen door ze visueel voor te stellen (ibid.). Denk aan grafieken, puntenwolken of taart- en staafdiagrammen (ibid.). Computers maken deze representaties daarenboven interactief zodat de gebruiker kan zien wat er verandert als hij bepaalde factoren wijzigt of toevoegt (ibid.).

Dehzad en collega's (2014) peilden naar de factoren die de adoptie van mobiele toepassingen in de gezondheidszorg mogelijk hinderen. Daarvoor namen ze een online survey af bij zowel artsen, ontwikkelaars als beleidsmakers. Vervolgens interviewden ze nog negen van de deelnemers om een beter begrip te krijgen van de barrières en om de mogelijke opportuniteiten te bespreken. Daaruit

bleek dat dokters nieuwe technologieën zoals apps en andere toepassingen moeilijk kunnen incorporeren in hun werkomgeving. De technologieën zijn nog niet voldoende aan aangepast aan de werkomgeving van de arts. Een andere nog belangrijkere hindernis die daar mee samenhangt is de conservatieve aard van de gezondheidssector. Artsen stellen het persoonlijk contact met de patiënt centraal en zijn terughoudend ten aanzien van nieuwe technologieën.

Tot slot hebben volgens Carroll (2014), in tegenstelling met het voordeel van een hollistischer beeld dat in paragraaf 1.3.2 beschreven werd, artsen geen nood aan zoveel gedetailleerde data. Dit leidt alleen maar tot een onnodige overload. Hoewel 86% van de artsen wel gelooft dat de data uit mobiele fitness- en gezondheidstoepassingen hen meer informatie over de patiënt zullen opleveren, staan ze er momenteel toch nog wat weigerachtig tegenover. Momenteel gebruikt amper 16% van de artsen een smartphone-technologie in interactie met hun patiënten, maar 46% gelooft wel dat ze mobiele gezondheids-toepassingen in de komende vijf jaar zullen introduceren (Research Now, 2015). Dit onderzoek spreekt zich echter alleen uit over het gebruik van smartphone-technologieën. Mogelijks ligt het gebruik dus hoger als we ook andere technologieën in rekening zouden brengen.

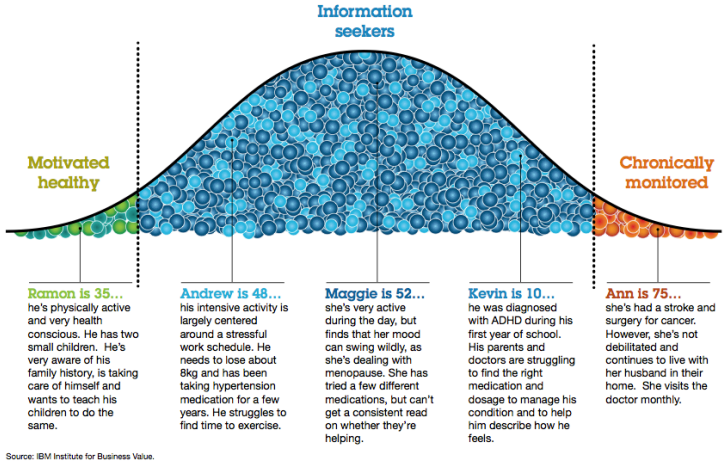
We kunnen dus besluiten dat het voor de arts (en de patiënt) niet altijd eenvoudig is om de data te interpreteren, hoewel dit noodzakelijk is. Daarnaast staat de gezondheidssector momenteel nog weigerachtig tegenover de nieuwe ontwikkelingen.

1.4.2 Beperkt publiek

In een rapport van IBM stellen de auteurs dat de gebruikers van gezondheidstoepassingen momenteel veelal bestaan uit twee groepen. Het zijn ofwel chronisch zieken die de technologie moeten gebruiken, vaak voorgeschreven door een arts. Ofwel zijn het gebruikers die erg geïnteresseerd zijn in technologie, fitness en gezondheid en die bereid zijn om wat geld te betalen en tijd te investeren in de nieuwste gadgets (Fraser e.a., 2011). We zien een soortgelijke verdeling opduiken in een rapport van research2guidance

op basis van een online survey bij meer dan 2000 app-ontwikkelaars. Hieruit blijkt dat het grootste deel van de gezondheidsapps ontwikkeld wordt met het oog op enerzijds chronisch zieken (31%) en anderzijds de fitness-geïnteresseerden (28%). Daarnaast worden apps gericht op artsen (14%), ziekenhuizen (7%), tijdelijk zieken (8%) en anderen (8%) (research2guidance, 2014).
IBM gelooft echter dat deze twee groepen (de fitness-geïnteresseerden en de chronisch zieken) niet de volledige samenleving behelzen. Zij stellen dan ook voor om zich als ontwikkelaar van gezondheidstoepassingen naast de chronisch zieken en de gezonde mensen die uit een sterke interesse gebruik maken van zulke toepassingen, ook te richten op "de informatiezoekers" (Fraser e.a., 2011). Ze omschrijven dit segment als een grote technologisch nog onvoldoende uitgeruste groep die op zoek is naar een manier om controle te krijgen over zijn ongezonde levensstijl of bepaalde niet-levensbedreigende aandoening (ibid.). Figuur 3 schematiseert dit idee: een grote groep informatiezoekers naast de chronisch zieken en de fitness-geïnteresseerden.

Carroll betoogt dat ook ouderen en armen mogelijks uit de boot vallen door de voor hen moeilijk te hanteren technologie en de vaak hoge kostprijs van fitness- en gezondheids-toepassingen (Carroll, 2014). Deze groepen zouden toch allemaal aangeboord moeten worden, wil de samenleving en meer specifiek de gezondheidszorg ten volle genieten van de voordelen die het gebruik van de gezondheidsdata opleveren, zoals hierboven uiteengezet.



Figuur 3: de populatie gebruikers van fitness- en gezondheids-toepassingen volgens IBM
Bron: Fraser, Kwon & Neuer, 2011, p.3.

1.4.3 Privacy

Een mogelijke reden waarom het grote publiek achterblijft met de adoptie van fitness- en gezondheidstoepassingen, heeft misschien te maken met privacyissues. Het recht op privacy is namelijk een belangrijke universele waarde die in het gedrang komt wanneer in het big data-tijdperk massale hoeveelheden persoonlijke data verzameld worden (Cukier & Mayer-Schönberger, 2013). Indien de gebruikers er niet zeker van kunnen zijn dat hun privacy gewaarborgd zal worden, zullen zij geen vertrouwen hebben in de gezondheids-toepassingen en ze zodus niet gebruiken (Klasnja e.a., 2009; Prasad e.a., 2012; Motti e.a., 2014).

Voor ik verder toelicht hoe (de bescherming van) de privacy nu juist in het gedrang komt in de big data-context, is het vooreerst belangrijk een gemeenschappelijk begrip te hebben van de term privacy. Het lijkt voor velen een vaag en moeilijk te definiëren begrip. Zo stelde rechter Biggs in 1956 dat *"een hooiberg na de doortocht van een orkaan nog beter in vorm is dan de conceptuele*

structuur van het begrip privacy" (Vedder, 25.02.2015). Maar de betekenis van privacy die de rechters Warren en Brandeis al in 1890 neerschreven, blijft ook vandaag nog overeind. Onder privacy verstonden de rechters het volgende (ibid.): *"Het recht van individuen om beschermd te worden tegen niet door hen gevraagde kennisneming en verspreiding van informatie over hun privéleven (zowel gevoelens, gedachten, emoties als handelingen inclusief relaties, geschriften en uitlatingen) in het bijzonder via publicaties."* De gegevensbescherming van gezondheidsdata, waar het in deze masterproef eigenlijk om gaat, valt dus ook onder deze definitie, daar die gegevens ook beschouwd kunnen worden als informatie over het privéleven. Het is echter belangrijk te benadrukken dat gegevensbescherming slechts een dimensie is van privacy (ibid.).

In het big data-tijdperk komt de privacy mogelijk in het gedrang want naast de enorme hoeveelheid onpersoonlijke data zoals de sensorgegevens van machines, wordt ook ontzettend veel persoonlijke data verzameld (Mayer-Schönberger e.a., 2013). De drie basisstrategieën ter bescherming van de privacy worden in het big data-tijdperk namelijk uitgehold, zo stellen Mayer-Schönberger en Cukier (ibid.). Ten eerste is het *notice and consent*-principe moeilijk vol te houden in de context van big data. Het *notice and consent*-principe houdt in dat de gebruiker op de hoogte wordt gebracht van enkele voorwaarden, rechten en plichten en het gebruik dat er van zijn persoonlijke data gemaakt zal worden. Op basis van deze informatie verklaart hij zich vervolgens al dan niet akkoord. Maar in een big data-context kan de betrokkene moeilijk op voorhand op de hoogte worden gebracht van het gebruik en het doel van de verzameling van zijn gegevens. Big data-analisten stuiten namelijk pas tijdens de verwerking op inzichten en verdere toepassingen (ibid.; Bertels, 11.03.2015). De tweede strategie is eigenlijk de negatieve tegenhanger van de eerste strategie: namelijk het weigeren gebruik te laten maken van je gegevens. Ondanks het weigeren om gegevens prijs te geven, is er nog steeds informatie over de gebruiker af te leiden, zo stellen Mayer-Schönberger en Cukier (ibid.). Wat we leren over die gebruiker is namelijk dat hij die informatie niet wilt vrijgeven en dat hij dus mogelijks iets wilt verbergen. Ten derde kunnen we volgens Mayer-Schönberger en Cukier (ibid.) ook niet meer volledig steunen op de anonimisering van gegevens. Doordat

het mogelijk is om verschillende datasets aan elkaar te koppelen, kunnen anonieme gegevens toch herleid worden naar individuele personen. Er zijn verschillende voorbeelden bekend waarbij een bedrijf, zoals bijvoorbeeld Netflix, zijn database geanonimiseerd beschikbaar stelde om er in wedstrijdverband interessante inzichten uit te laten halen. In het geval van Netflix wonnen diegenen die het aanbevelingssysteem konden verbeteren de Netflix-prijs. Maar door in dit geval de geanonimiseerde Netflix-database samen te brengen met de publiek beschikbare database van IMDB, waren onderzoekers in staat Netflix-klanten te identificeren. Als de onderzoekers wisten welke minder populaire films de klant had beoordeeld op IMDB en daarenboven wisten op welke datum hij die beoordeling had gepost, konden ze in 99% van de gevallen zijn identiteit achterhalen.

Ondanks het feit dat het in de context van big data moeilijker wordt om de privacy te beschermen is het wel een universeel en fundamenteel recht dat absoluut gewaarborgd moet worden. Het kan voor sommigen enerzijds een intrinsieke waarde hebben (Vedder, 25.02.2015). Zij willen geen inmenging van anderen in hun privéleven en willen bepaalde informatie gewoon voor zich houden. Anderzijds is het recht op privacy ook vaak instrumenteel om andere rechten te waarborgen (ibid.). Zo wil een individu bijvoorbeeld zijn reputatie of status beschermen of eventuele fysieke, materiële of financiële schade vermijden (ibid.). Hij kan namelijk te maken krijgen met geweld omwille van zijn overtuiging. Er kan ingebroken worden omdat zijn welstand bekend raakte. Zijn verzekeraar kan hem een duurdere (of goedkopere) premie aanrekenen op basis van de data over zijn rijgedrag (Golia & O'Donnell, 2011).

Privacy is daarnaast ook instrumenteel om de vrijheid en de autonomie van de burger te waarborgen opdat een democratische rechtstaat kan bestaan (Vedder, 25.02.2015). Velen geloven echter dat privacy niet nodig is als ze niks verkeerd doen of niks te verbergen hebben (Greenwald, 2014). Dat privacy aan de basis ligt van de vrijheid en de autonomie van de burger, valt intuïtief al te begrijpen (ibid.). Zonder de blik van anderen zijn we veel vrijer: we kunnen vrijuit praten, durven luidop meezingen en dansen, maken onze eigen keuzes. Wanneer we weten dat anderen ons gadeslaan, doen we ons best te conformeren aan de heersende normen (ibid.). Greenwald stelt dan ook dat de privacy geschonden is als we bekeken

worden, ook al wordt het toezicht ten goede aangewend (ibid.). Dat de vrijheid en autonomie die privacy ons schenkt aan de basis ligt van de democratie maakt Greenwald (ibid.) duidelijk met de volgende denkpiste. Wanneer iemand er ideologieën of opvattingen op nahoudt die indruisen tegen het heersende gedachtegoed, zou een overheid die hier weet van heeft, die persoon monddood kunnen maken. Op die manier kan er geen kritiek geleverd worden op de regering. Dit druist echter in tegen de principes van de democratie en maakt zo duidelijk dat privacy daarvoor noodzakelijk is.

Greenwald heeft het over massasurveillance naar aanleiding van de onthullingen van Snowden over de NSA, maar ook in de context van gezondheidsdata is privacy belangrijk (Martínez-Pérez, De La Torre-Díez & López-Coronado, 2015). Deze persoonlijke informatie kan in verkeerde handen onaangenaame gevolgen hebben. Ze kunnen, zoals hierboven al werd aanghaald, door een verzekeraar gebruikt worden om zijn klanten een duurdere premie aan te rekenen. Daarnaast zouden ook overheden op basis van de fitness- en gezondheidsdata bepaalde discriminerende maatregelen kunnen treffen.

Tot dusver kwamen de voor- en nadelen van het gebruik van fitness- en gezondheidstoepassingen aan bod op basis van wat er in de literatuur beschreven wordt. Er is geloof in het potentieel van het gebruik van zulke toepassingen, maar er moeten nog enkele hindernissen overwonnen worden, waaronder vooral de bescherming van de privacy. Daarom zal in wat volgt ingezoomd worden op de privacybezorgdheden van de eindgebruiker die we moeten kennen alvorens we een oplossing kunnen aanreiken.

1.5 Privacybezorgdheden bij gebruikers van gezondheidstoepassingen

Verschillende onderzoeken trachtten de privacybezorgdheden die optreden bij het gebruik van gezondheidsapplicaties en –toepassingen te achterhalen. Als zij namelijk die bezorgdheden kunnen wegnemen en de privacy van de gebruiker kunnen garanderen, zal er een groter vertrouwen zijn in de gezondheidstoepassingen, met als gevolg een grotere utilisatie bij het brede publiek (Klasnja e.a., 2009; Prasad e.a.,

2012; Motti e.a., 2014). Zo zijn we op weg naar een gezondere samenleving en een verlichting van de gezondheidszorg, die onder druk staat door ondere andere de vergrijzing en obesitas.

In wat volgt zal ik de privacybezorgdheden bespreken die naar voor komen uit onder andere focusgroepen, gebruikersonderzoek met personen die gezondheidstoepassingen gebruikten op vraag van de onderzoekers en een inhoudsanalyse van reacties van "natuurlijke" gebruikers. Hieruit blijkt dat de privacybezorgdheden variëren afhankelijk van tal van factoren. Vooreerst hangen de bezorgdheden af van het type verzamelde informatie, ten tweede zijn er drie voorwaarden voor de dataverzameling die de privacy-bekommernissen beïnvloeden en tot slot speelt ook de ontvanger en het gebruik dat hij van de data zal maken een rol.

1.5.1 Privacybezorgdheden afhankelijk van sensor en data

Klasnja e.a. (2009) lieten 24 deelnemers drie maanden lang hun activiteiten bijhouden. Ofwel droegen ze een wearable die automatisch detecteerde of ze wandelden, liepen, fietsten, ... waarbij ze handmatig in hun gsm de overige activiteiten (zoals zwemmen) bijhielden. Ofwel hielden ze alles manueel bij in een dagboek in hun gsm. Het is belangrijk op te merken dat de deelnemers voor het onderzoek niet uit zichzelf bezig waren met gezondheidsapplicaties. Na drie maanden vond een interview plaats waarbij hen eerst werd uitgelegd hoe de gezondheidstoepassing precies werkte. Er werd namelijk toegelicht hoe de toepassing hun activiteiten kon afleiden uit de data en hoe het een onderscheid kon maken tussen zitten, wandelen en lopen. Daarna werd gepeild naar hun bezorgdheden over de dataverzameling en de opslag op hun toestel en een bijbehorende website. Tot slot stelden de onderzoekers nog enkele verbeteringen voor waaronder het toevoegen van extra sensoren, namelijk GPS en audio, waardoor er meer activiteiten gedetecteerd zouden kunnen worden.

Uit de resultaten komt duidelijk naar voor dat de bezorgdheden afhankelijk zijn van de sensor en de data die ermee verzameld worden. Zo waren de deelnemers niet ongerust over de accelerometer en de barometer omdat ze de informatie die zo verzameld wordt niet

als gevoelig beschouwen. De meningen omtrent de GPS-data liepen meer uiteen. Deze data werden namelijk wel als gevoelig gecategoriseerd. Sommigen maakten zich zorgen omdat deze data in de handen van een crimineel hun fysieke veiligheid zouden kunnen bedreigen, anderen vonden het simpelweg griezelig en voelden zich bekeken. Over het gebruik van de audiosensor om zo extra activiteiten te detecteren, maakten alle deelnemers zich zorgen. Zij zouden zich voortdurend in de gaten gehouden voelen. De deelnemers vonden het aanvaardbaarder indien alleen de nodige frequenties opgenomen zouden worden zodat niet woordelijk zou worden geregistreerd wat ze zeiden. Op basis van deze gefilterde audio zou dan het type activiteit afgeleid kunnen worden, maar de meesten bleven het te intrusief vinden.

De gevoeligheid van de data heeft ook te maken met de context van de dataverzameling. Indien de data bijvoorbeeld verzameld werden in een confidentiële setting of wanneer de gebruiker zich in een kwetsbare positie bevindt, waren de deelnemers bezorgder om hun privacy: bijvoorbeeld op een consultatie bij een arts of psycholoog of indien de gebruiker een relatie heeft met een controlerende partner (Klasnja, 2009).

Raij, Kumar, Ghosh en Srivastava (2011) gingen in hun onderzoek nog een stap verder. Zij peilden niet naar de bezorgdheden over de verzameling van schijnbaar onschuldige gegevens verzameld door bijvoorbeeld een accelerometer en een barometer, maar naar de bezorgdheden omtrent de inferenties die op basis van die onschuldige data gemaakt kunnen worden. Zo kunnen bijvoorbeeld iemands ademhalings- en locatiegegevens gecombineerd worden met publieke kaarten en cijfers over milieuvervuiling. Zo kan onthuld worden wat de mate is van blootstelling aan luchtvervuiling. Raij e.a. onderzochten echter de bezorgdheden met betrekking tot de volgende gedragingen en contexten: sporten, pendelen, de mate van stress, conversaties en de plaatsen waar hij zich begeeft. Deze informatie kon dus afgeleid worden uit de combinatie van schijnbaar onschuldige gegevens.

Via flyers en van mond tot mond rekruteerden de onderzoekers 66 studenten die wilden meewerken. Zij werden in twee groepen verdeeld. De eerste groep droeg eerst drie dagen de AutoSense-sensor. Deze wearable registreert fysiologische data waaronder de

hartactiviteit, ademhaling, versnelling, temperatuur en huidgeleiding van de gebruiker. Op basis van deze data kan de AutoSense inferenties maken over het gedrag en de psychologische toestand van de gebruiker. Na deze periode van drie dagen vulden ze een privacysurvey in die peilde naar hun bezorgheden omtrent het vrijgeven van de bovenvermelde gedragingen en contexten. Hoe bezorgd zijn de respondenten wat betreft het registreren van informatie over hun sportactiviteit, de plaatsen waar ze vaak komen, hun conversaties, pendelgedrag en stressniveau? Na het invullen van de survey kregen ze voor het eerst grafieken te zien die afgeleid waren van hun verzamelde data: hun periodes van stress en conversatie etc. Daarna vulden ze tot slot voor een tweede maal de privacysurvey in. De tweede groep vulde de privacysurvey eenmaal in, zonder een periode van dataverzameling met de AutoSense en dus ook zonder de daaropvolgende sessie waar de persoonlijke grafieken getoond werden. De opsplitsing in de twee groepen gebeurde om na te gaan of een persoonlijke betrokkenheid de privacybezorgdheden beïnvloedt. Waren de privacybezorgdheden volgens de survey groter voor de groep die zelf de AutoSense gebruikten en vervolgens geconfronteerd werd met wat hij had vrijgegeven, dan de groep die geen data verzamelde en er zodus ook niet mee geconfronteerd kon worden? Dit was inderdaad het geval, maar daar zal ik in een verdere paragraaf uitgebreider op terugkomen.

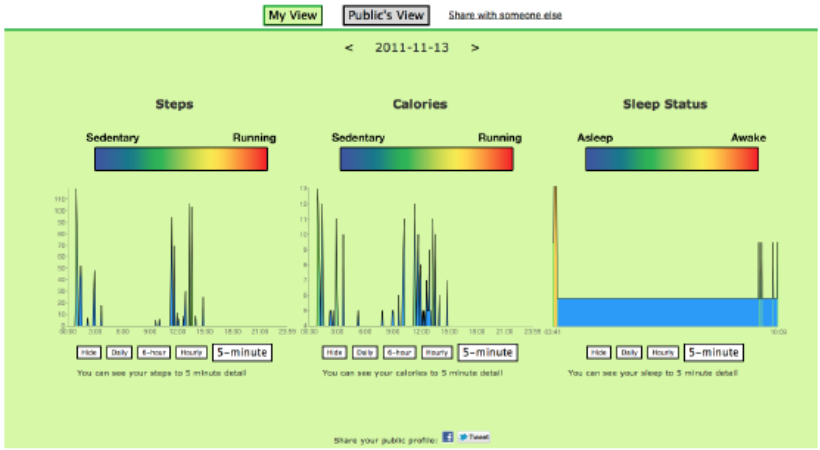
Voor de groep die zelf betrokken was bij de dataverzameling waren de bezorgdheden die via de survey gemeten werden het grootst voor conversaties (2,1 op een vijfpuntenschaal met 1 niet bezorgd en 5 heel bezorgd), pendelen (2,4) en stresslevel (2,6). De respondenten zijn dus een beetje bezorgd hierover. Uit de analyse van het open veld uit de survey blijkt dat deze hogere mate van bezorgdheid over het stressniveau voortvloeit uit een angst dat persoonlijke gedachten ontmanteld zouden worden door de verzameling van gegevens over het stresslevel. De psychologische toestand, waaronder we dus ook hun stressniveau verstaan, is namelijk standaard privé aangezien het niet observeerbaar is met het blote oog. Over het sporten en de plaatsen waar ze zich begeven was deze groep minder bezorgd (respectievelijk 1,5 en 1,7 op een vijfpuntenschaal). De groep die de survey eenmaal invulde, scoorde voor de vijf types informatie (sporten, plaatsen, conversatie, pendelen en stresslevel) steeds tussen

1 en 1,4 op een vijfpuntenschaal. Deze groep was dus eerder niet bezorgd. Zij gebruikten zelf de AutoSense niet en hadden slechts een beperkte mate van bezorgdheid. Dit maakt duidelijk dat indien er sprake is van een persoonlijke betrokkenheid, zoals bij de eerste groep die zelf data verzamelde, de privacybezorgdheden groter zijn. Hier zal, zoals reeds vermeld werd, verder dieper op worden in gegaan.

1.5.2 Privacybezorgdheden afhankelijk van drie voorwaarden

De privacybezorgdheden van de gebruikers hangen niet enkel af van het type sensor en de verzamelde data, maar zijn ook afhankelijk van enkele voorwaarden. Ten eerste speelt de mate van *abstractie* een belangrijke rol. Zo maakten de deelnemers in het onderzoek van Klasnja e.a. (2009), waarbij de deelnemers drie maanden hun activiteit registreerden en vervolgens geïnterviewd werden, zich minder zorgen om de gefilterde audio-data dan over de ruwe audio-data omdat de gefilterde audio-data als minder persoonlijk beschouwd werd. Ook Raij e.a. (2011) merkten op dat de bezorgdheden die gemeten werden aan de hand van een survey die ook hierboven al vermeld werd, toenamen indien er extra contextfactoren werden toegevoegd aan de verzamelde data zoals de precieze locatie, de duur of een exacte tijdsaanduiding. Dit maakt de gedragingen namelijk minder abstract. Er valt veel meer informatie uit af te leiden. Als we bijvoorbeeld niet alleen weten dat iemand sport, maar ook waar, wanneer en hoelang, weten we al veel meer. De deelnemers waren het meest verontrust wanneer de fysieke locatie in combinatie met de exacte tijd toegevoegd werd aan hun gedragingen en activiteiten. Dat de mate van abstractie een rol speelt zien we tenslotte ook opduiken bij Prasad, Sorber, Stablein, Anthony en Kotz (2012) waar de precisie van de data die de gebruikers prijs gaven een rol speelde bij de mate van bezorgdheid. De onderzoekers vroegen een steekproef bestaande uit 21 studenten, twaalf werknemers en acht gepensioneerden om vijf dagen een Fitbit te dragen en de verzamelde data online te uploaden. Aan de hand van een interface konden ze hun data bekijken en konden ze precies zien wat de persoon met wie ze hun informatie deelden zou waarnemen

(zie figuur 4 en 5). Zo konden ze goed beslissen met wie en hoe ze hun data wilden delen. Hiervoor werd eerst gevraagd dat de deelnemers familieleden en vrienden zouden selecteren naar wie de informatie verzonden zou worden. Daarnaast kregen ze ook verzoeken van derde partijen zoals academische instellingen en de overheid. Tot slot had iedere deelnemer ook een openbaar profiel. Aan de hand van de instellingen voor het delen die de gebruiker koos (verbergen, dagoverzicht delen, 6-uuroverzicht delen, uuroverzicht delen, 5-minutenoverzicht delen), stelden de onderzoekers een *sharing score* op (respectievelijk 0,1,2,3,4). Indien de gebruiker bezorgd was om zijn privacy, omdat zoals uit de interviews die erna plaats vonden, bleek dat hij bijvoorbeeld zijn data niet met zijn moeder wilde delen of omdat de informatie te persoonlijk was zoals bijvoorbeeld een vooropgesteld doel, nam de *sharing score* af. De deelnemers probeerden met andere woorden hun privacybezorgdheden dus deels te neutraliseren door de data op een minder precieze manier vrij te geven. Figuur 4 geeft de data weer zoals de gebruiker die te zien kreeg. Hij geeft ze echter op een minder precieze manier aan zijn moeder door, zoals figuur 5 illustreert. Naast de kwantitatieve *sharing scores* die zo verzameld werden, vonden er ook na de vijf dagen waarin de deelnemers de Fitbit droegen nog interviews plaats die deze stelling bevestigden. Uit de interviews bleek namelijk dat de gebruikers meer of minder wilden delen afhankelijk van wie de ontvanger was van de data. Zo stelde iemand dat hij zijn calorieën met een vijf-minuten-precisie wel wilde delen met iemand die zwaarder was, maar niet met vrienden die meer sportten dan hij.



Figuur 4: interface die de verzamelde data weergeeft zoals de gebruiker die te zien kreeg
Bron: Prasad, Sorber, Stablein, Anthony & Kotz, 2012, p.120.

Figuur 5: interface die de gebruiker toont hoe zijn moeder de data te zien zal kreeg
Bron: Prasad, Sorber, Stablein, Anthony & Kotz, 2012, p.120.

Niet alleen een grotere mate van abstractie kan de bezorgdheden temperen. Ook indien de gegevens alleen opgeslagen zouden worden voor *zolang als nodig* is om de werking van de toepassing te garanderen, is men sneller bereid zijn locatie- en audiodata vrij te geven. Dat blijkt het onderzoek van Klasnja e.a. (2009) dat hierboven al aan bod kwam, waarbij de deelnemers geïnterviewd werden na een periode van drie maanden waarin ze hun activiteit registreerden.

Tenslotte verwondert het niet dat ook de mogelijkheid tot identificatie, met andere woorden de mate van *anonimiteit*, een invloed heeft op de privacybezorgdheden. Dit hangt ook enigszins af van de persoon met wie de data gedeeld zullen worden, maar daar handelt de volgende paragraaf verder over. De survey van Raij e.a. (2011) toont aan dat de bezorgdheid verdubbelt indien de identiteit van de gebruiker zou worden toegevoegd aan de data over zijn dagelijkse activiteiten en deze vervolgens met het publiek worden gedeeld. In geval de data met identiteit echter enkel gedeeld zouden worden met Raij's onderzoeksteam, namen de bezorgdheden niet significant toe. Ook uit de interviews van Prasad e.a. (2012) blijkt dat de perceptie van anonimiteit die de gebruikers hebben, hun bereidheid tot delen beïnvloedt. Zo hadden enkele deelnemers het gevoel dat hun informatie zonder hun naam toch niet aan hen gelinkt zou kunnen worden. Bijgevolg hadden ze geen moeite met het doorgeven van hun informatie aan derden.

1.5.3 Privacybezorgdheden afhankelijk van gebruik

Tot slot variëren de privacybezorgdheden naast het soort verzamelde data en de drie voorwaarden ook naargelang het gebruik dat van de data gemaakt kan worden, zowel door de gebruiker zelf als door derden. Daarmee samenhangend zijn de privacybezorgdheden ook afhankelijk van de ontvanger van de data, daar elke ontvanger een specifiek gebruik voor ogen heeft. Onderzoekers zullen de data willen gebruiken voor onderzoek, private bedrijven zullen de data willen gebruiken om winst te maken.

Wanneer de gebruikers gevraagd werd naar wat het vrijgeven van hun persoonlijke data hen zou opleveren, maakten ze daarbij een kosten-batenanalyse waarbij ze het voordeel van de toepassing

afwogen tegen het nadeel die het gebruik ervan zou opleveren (Klasnja, 2009). Bij het gebruik van Runkeeper bijvoorbeeld, doet de gebruiker enerzijds enigermate afstand van zijn privacy door het vrijgeven van locatiegegevens, maar het gebruik van de app levert hem anderzijds wel de mogelijkheid op om looproutes te plannen.

Uit de survey van Raij (2011) komt naar voor dat mensen enigszins bezorgd zijn over hun privacy indien data over hun dagelijkse activiteiten bekend zouden worden gemaakt aan het grote publiek. Die mate van bezorgdheid was groter dan wanneer de data enkel zouden gedeeld worden met het onderzoeksteam, andere onderzoekers of andere deelnemers. Zoals hierboven al aangehaald, hangt de mate van anonimiteit nauw samen met de ontvanger van de data: indien hun identiteit namelijk wordt toegevoegd bij de vrijgave aan het grote publiek, verdubbelden de bezorgdheden. De kwantitatieve resultaten van de gebruikersstudie van Prasad sluiten hier bij aan en geven weer dat de deelnemers respectievelijk het makkelijkst hun gezondheidsdata delen met hun familie, vrienden, derde partijen en als laatst pas met het grote publiek (Prasad e.a., 2009).

Het kwalitatieve luik van Prasads (2012) onderzoek maakt duidelijk dat de privacybezorgdheden heel erg afhankelijk zijn van de relatie die de gebruiker heeft met de persoon waarmee de data gedeeld worden. De onderzoekers vroegen de deelnemers, zoals hierboven al uiteengezet, om gedurende vijf dagen gebruik te maken van een Fitbit. Naast de kwantitatieve gegevens die zo verzameld werden, vonden er ook interviews plaats. Hieruit bleek dat het niet voor iedereen zo is dat hij liever zijn data deelt met zijn familie dan met derde partijen. Dit is voor iedereen verschillend en er schuilen ook diverse motieven achter. Sommigen willen hun persoonlijke informatie wel met onpersoonlijke derde partijen delen, maar niet met hun familie en vrienden uit vrees hen ongerust te maken of anders bekeken te worden. Daartegenover waren er ook gebruikers die wel bereid waren hun informatie te delen met familie en vrienden, maar niet met onbekende derde partijen omdat zij de derde partijen niet kenden en geen connectie met hen hadden. Anderen tenslotte, wilden aan iedereen, inclusief onderzoekers, hun data vrijgeven behalve aan particuliere bedrijven. In deze zin hangt de ontvanger

van de data dus concreet samen met het gebruik dat er van zal gemaakt worden en beïnvloedt het op die manier de bezorgdheid.

Tot dusver kan men tot het besluit komen dat de privacybezorgdheden afhankelijk zijn van een veelheid aan factoren. Zo speelt ten eerste het type informatie dat verzameld wordt een belangrijke rol. Het aantal stappen vindt men doorgaans minder privé dan iemands locatie. Daarnaast zijn er drie belangrijke voorwaarden die beïnvloeden hoe bezorgd men is over zijn privacy: indien er een hoge mate van abstractie is, de data maar voor zolang als nodig bijgehouden worden of indien de identiteit niet aan de data gekoppeld wordt, zijn de privacybezorgdheden beperkter. Tot slot variëren de bezorgdheden afhankelijk van de persoon met wie de data gedeeld worden en het gebruik dat er respectievelijk van gemaakt zal worden.

We kunnen dus besluiten dat het privacybegrip heel relatief en contextafhankelijk is. Dit sluit aan bij het contextuele integriteitsmodel van Helen Nissenbaum (zoals kort uitgelegd door Shklovski e.a., 2014, pp.3-4). Nissenbaum stelt dat de informatie die we vrijgeven in de ene situatie geen bedreiging vormt voor onze privacy, maar wanneer we diezelfde informatie in een andere situatie zouden delen, kan hij anders gepercipieerd worden. Zo kan het gebeuren dat iemand bijvoorbeeld wel gevoelige informatie wil delen via zijn gezondheidsapp, maar niet via *Candy Crush*.

1.5.4 Afhankelijk van betrokkenheid gebruiker

Naast het type data, het gebruik dat er van de data zal worden gemaakt en de drie voorwaarden die hierboven aan bod kwamen, is er mogelijks een belangrijke methodologische factor die de onderzoeksresultaten met betrekking tot de privacybezorgdheden beïnvloedt, namelijk het feit of de deelnemers in de context van het onderzoek persoonlijk betrokken waren bij de verzameling van gezondheidsdata. Als mensen een survey moeten invullen over hoe bezorgd ze zijn over het vrijgeven van gezondheids- en locatiegegevens, zonder zelf de toepassing te gebruiken en hun persoonlijke informatie weergegeven te zien, zijn zij minder bezorgd dan wanneer ze zelf zo'n toepassing gebruiken en met hun eigen vrijgegeven data geconfronteerd worden. Tot deze conclusie kwamen

Raij en collega's die bewust twee groepen met en zonder persoonlijk aandeel creëerden zoals hierboven al vermeld werd (Raij e.a., 2011). De twee andere onderzoeken die tot hiertoe vermeld werden maakten niet bewust onderscheid tussen groepen met en zonder persoonlijk aandeel, maar lieten alle deelnemers telkens voor een periode persoonlijke data capteren. Zo interviewde Klasnja e.a. (2009) 24 deelnemers na een periode van drie maanden waarin de deelnemers hun activiteit registreerden. Prasad e.a. (2012) bestudeerden hoe 41 deelnemers hun Fitbit-data deelden en vulden deze kwantitatieve gegevens aan met interviews. Hier was dus ook steeds sprake van een persoonlijk aandeel.

De bevinding dat een confrontatie met de eigen data van invloed is op de privacybezorgdheden, plaatst echter wel een kanttekening bij een vooronderzoek van Prasad e.a. (2011) dat bestond uit een focusgroepgesprek met deelnemers die nog nooit een toepassing gebruikten. Ze kregen vier scenario's voorgeschoteld waarin een gezondheidstoepassing werd gebruikt om persoonlijke informatie te verzamelen, die vervolgens naar een website werd doorgestuurd en gedeeld werd met hulpverleners, familie of vrienden. Na het overbrengen van de scenario's aan de focusgroepdeelnemers, werd hen gevraagd naar voor- en nadelen van de gezondheidstoepassingen in de scenario's, bezorgdheden, personen met wie ze al dan niet bepaalde informatie wensten te delen,... Uit de antwoorden die de deelnemers gaven, bleek een zekere mate van bezorgdheid, hoewel die niet bijzonder uitgesproken was en eerder als abstract te categoriseren valt. Zo waren de deelnemers meer bereid hun informatie met hun dokter te delen omdat ze van hem een confidentiële behandeling verwachten. Ze stelden ook dat de overheid, verzekeraars en adverteerders pas toegang zouden mogen krijgen als daar toestemming voor wordt gegeven. Sommigen zijn zich er wel van bewust dat men tegenwoordig heel vaak ongeïnformeerd toestemming verleent. Deze deelnemers gebruikten dus nog nooit een fitness- of gezondheidstoepassingen en werden zodus ook niet geconfronteerd met persoonlijke data. Als we Raij e.a. (2011) zouden mogen geloven zouden de resultaten uit dit focusgroepgesprek uitgesprokener zijn indien we de deelnemers eerst zelf hun data lieten verzamelen en hen er daarna mee zouden confronteren. Ze zouden met andere woorden bezorgder zijn.

Klasnja e.a. (2009) maken nog een ander onderscheid dan Raij en collega's (2011). Als we Klasnja's redenering namelijk volgen (2009), op basis van het onderzoek van Nguyen, Kobsa en Hayes (2008), kunnen we veronderstellen dat natuurlijke gebruikers, in tegenstelling tot gebruikers die op vraag van de onderzoekers een toepassing gebruiken, minder privacybezorgdheden zullen hebben omdat ze zo vertrouwd zijn met de technologie.

Nguyen en collega's (ibid.) bevroegen 54 deelnemers aan de hand van een survey en een vervolginterview over alledaagse volgtechnologieën zoals bijvoorbeeld klantenkaarten. Alvorens de survey kon ingevuld worden, werden de deelnemers ingelicht over de RFID-technologie, ongeacht eventuele voorkennis. Dit gebeurde omdat het eerste luik van de vierdelige survey peilde naar de attitudes ten opzichte van RFID en het een relatief nieuwe technologie is die nog niet bekend is bij het brede publiek. RFID staat voor Radio-Frequency Identification. Met behulp van radiogolven kan informatie worden opgeslagen en afgelezen. Er zit bijvoorbeeld een RFID-tag op de vervoersbewijzen van pendelaars in de Parijse metro's (Bertels, 11.03.2015), maar ook op de MOBIB-kaarten van NMBS (Commissie voor de bescherming van de persoonlijke levenssfeer, 2009). Het tweede luik van de survey onderzocht de attitudes ten opzichte van informationele privacy in het algemeen. Hiermee doelen de onderzoekers op de privacy met betrekking tot persoonlijke gegevens. Een derde luik richtte zich, in tegenstelling tot de nieuwe RFID-technologie, op de attitudes ten opzichte van bekende alledaagse volgtechnologieën waaronder kredietkaarten, klanten-kaarten, elektronische tolheffing, browsegeschiedenis en camera-beveiliging. Het laatste luik focuste tenslotte op de demografische gegevens. De resultaten maakten duidelijk dat men tegelijk vrij bezorgd kan zijn wat betreft het abstracte concept van informationele privacy (gemiddeld 6 op een 7-puntenschaal) en de minder vertrouwde RFID-technologie (5,1 op een 7-puntenschaal), maar minder bezorgd of zelfs onbezorgd is (2,85-4,43 op 7-puntenschaal) wat betreft allerlei alledaagse volgsystemen zoals klantenkaarten en beveiligingscamera's waarmee men wel dagelijks in contact komt. Uit de interviews blijkt dat de deelnemers zich goed bewust zijn van de voordelen die de technologieën bieden. Zo levert een klantenkaart een voordeel op en maakt een kredietkaart betalingen erg makkelijk.

Negatieve gevolgen verbonden ze er echter niet aan. Ze denken niet dat hun consumptiegedrag door iemand misbruikt zou worden. Ze geloven niet dat de volgtechnologieën een bedreiging vormen voor mensen die niets verkeerd doen en niets te verbergen hebben. Ondanks hun onbekommerdheid, geven sommige deelnemers aan dat ze wel bezorgd zouden moeten zijn. Zij die meer verontrust zijn, vermijden het om aan de mogelijke bedreigingen te denken. De onderzoekers suggereren dat de belangrijkste reden voor de onbezorgdheid te wijten is aan het feit dat de deelnemers nog nooit effectief schade hebben ondervonden van enig misbruik van hun data.

De conclusies die tot dusver aan bod kwamen, zijn niet afkomstig van onderzoek met natuurlijke gebruikers van gezondheidstoepassingen zoals bij Nguyen e.a. (ibid.) wel het geval is. Ofwel gebruikten ze nog nooit een gezondheidstoepassing zoals bij het vooronderzoek van Raij e.a. die in een focusgroep peilde naar de bezorgdheden, ofwel gebruikten ze een toepassing op vraag van de onderzoekers. Misschien zijn natuurlijke gebruikers van gezondheidsapplicaties en -toepassingen, gebruikers die met andere woorden uit eigen beweging zulke apps en toepassingen aanwenden, helemaal niet bezorgd om hun privacy. De twee volgende onderzoeken behandelen daarom, in lijn met Nguyen, de privacybezorgdheden die natuurlijke gebruikers al dan niet ervaren. Het eerste onderzoek omvat een inhoudsanalyse van de online reacties van gebruikers over verschillende wearables. Gezien de verwantschap van gezondheidsapplicaties en smartphones, is het relevant om vervolgens een onderzoek aan te halen over de privacybezorgdheden van smartphonegebruikers met betrekking tot app-gebruik dat niet specifiek handelt over gezondheidsdata.

1.5.5 Onderzoek bij natuurlijke gebruikers

Motti en Caine (2014) stelden vast dat er nog maar weinig onderzoek is gedaan naar de privacybezorgdheden die ervaren gebruikers of geïnteresseerde toekomstige gebruikers van wearables zoals smartwatches en virtual reality-brillen ervaren. Ze opteerden voor een kwalitatieve inhoudsanalyse van online reacties gerelateerd aan 38

verschillende wearables op 59 verschillende websites: van technologieforums tot webshops. Een onderzoeker selecteerde uit alle reacties diegenen die met privacy te maken hadden. Vervolgens werden al de geselecteerde reacties nogmaals gelezen om het type bezorgdheid uit te maken. Ook werd nagegaan of die bezorgdheid verbonden was met een specifieke functie van de wearable.
De bevindingen komen in grote mate overeen met de conclusies uit de onderzoeken met de opgelegde gebruikers die hierboven besproken werden. Het type verzamelde data en hun gevoeligheid, de mogelijkheid om te delen en de consequenties (zoals imagoschade of misbruik door derden) beïnvloedden de privacybezorgdheden. Zo wordt ook hier de schijnbaar onschuldige informatie die activiteitstrackers verzamelen zoals hartslag, polsslag en aantal stappen, niet als een bedreiging van iemands privacy ervaren. Over de activiteitstrackers die louter de hartslag en het aantal stappen registreren lijken namelijk minder bezorgdheden te worden geuit. De wearables die uitgerust zijn met een camera, microfoon en GPS veroorzaken daarentegen serieuzere privacybezorgdheden (ibid). Deze bevindingen lijken er met andere woorden niet op te wijzen dat natuurlijke gebruikers minder bezorgd zouden zijn, zoals we verwachtten op basis van Nguyen e.a. (2008) en Klasnja e.a. (2009). Dit is misschien te wijten aan de methodologie van het onderzoek van Motti en Caine. Het betreft hier namelijk een kwalitatieve inhoudsanalyse van online reacties van zowel ervaren als onervaren (maar geïnteresseerde) gebruikers. De onervaren, maar geïnteresseerde gebruikers hebben met andere woorden dus nog geen gebruik gemaakt van zulke toepassingen. Ze zijn nog geen natuurlijke gebruikers, ze zijn nog niet vertrouwd met de technologie. Daarenboven verschillen de gebruikers die online reacties plaatsen van de gebruikers die daar geen behoefte aan hebben. Tenslotte werden ook reacties bestudeerd van een niet-exhaustieve lijst van wearables (ibid.).

Shklovski, Mainwaring, Skuladottir en Borgthorsson (2014) onderzochten de attitudes van smartphonegebruikers met betrekking tot datalekken. Gebruikers van mobiele apps zijn zich er namelijk vaak niet van bewust waar hun data terecht komen en waar ze eigenlijk toestemming voor verlenen wanneer ze zich akkoord verklaren met de gebruiksvoorwaarden en een app installeren. Zo

verzamelt de Flashlight-app bijvoorbeeld locatie, telefoonnummer en informatie over andere apps. Om naar de attitudes te peilen, interviewden de onderzoekers dertien personen tussen 27 en 55 jaar met een Android smartphone. Het eerste luik handelde over smartphones en applicaties in het algemeen, waarbij de deelnemers gevraagd werd om te demonstreren hoe ze gewoonlijk een app downloaden. Verder werden de attitudes en overtuigingen met betrekking tot data-privacy, of informationele privacy zoals het eerder werd verwoord, onder de loep genomen. In een tweede luik overliep de interviewer de gebruiksvoorwaarden van enkele populaire apps. Ook werd aan de deelnemers een app geïntroduceerd die als hulpmiddel kan dienen bij het lezen van gebruiksvoorwaarden. Tot slot werden de deelnemers gevraagd de app "*Fruit Ninja"* te installeren. Nadien lichtte de interviewer toe waar de deelnemer toegang toe had verleend. Drie weken na het interview volgde een follow-up-interview via e-mail of telefoon. Naast de dertien kwalitatieve interviews, vond ook een kwantitatieve survey plaats waar 187 respondenten aan deelnamen. De survey peilde naar de attitudes omtrent app stores, gepersonaliseerde marketing, dataverzameling door bedrijven en door smartphone-apps en tot slot naar de mate van privacybezorgdheid.

Tijdens de interviews sloegen alle deelnemers het lezen van de gebruiksvoorwaarden over wanneer hen gevraagd werd een app te installeren, ondanks privacybezorgdheden die ze eerder hadden geuit tijdens het interview. Ze deden dit naar eigen zeggen ten eerste omdat ze nog nooit negatieve gevolgen hadden ondervonden, zoals ook Nguyen e.a. (2008) aanhaalde als belangrijkste verklaring voor de beperkte bezorgdheid rond krediet- en klantenkaarten. Ten tweede overtroefde de drang naar de app die ze op het punt stonden te downloaden een mogelijke bezorgdheid. De onderzoekers merkten dat de bezorgdheid van de deelnemers toenam naarmate het interview vorderde. Na de bespreking van de gebruiksovereenkomst die ze hadden goedgekeurd wanneer ze *"Fruit Ninja"* installeerden, werd de wanverhouding duidelijk tussen wat men verwachtte dat zo'n app verzamelde en wat hij effectief verzamelde. Zo verzamelde "*Fruit Ninja"* onder andere de locatie van de gebruiker, iets wat niet binnen de verwachtingen ligt voor een app waarbij je fruit in stukken moet snijden. Deze mismatch veroorzaakte ongemak, het gevoel misleid te

zijn. De deelnemers leken er dus misvattingen op na te houden over de toegang waartoe de apps die ze gebruikten gerechtigd zijn.
In het vervolginterview stelden sommigen dat ze na het interview wel aandachtiger probeerden te zijn wanneer ze apps downloaden en gebruikten. De meerderheid had *"Fruit Ninja"* dan ook al verwijderd. Verder hadden ze echter hun gebruik niet aangepast. Ze installeerden nog steeds allerhande apps en investeerden nog steeds geen tijd in het lezen van de gebruiksvoorwaarden. Ook de in het interview besproken hulpmiddelen werden niet aangewend. De resultaten van de survey lagen in dezelfde lijn als de resultaten van de interviews. De respondenten stelden dat ze zich bewust waren van dataverzameling en de verspreiding ervan naar derden. Ook waren ze er van overtuigd dat er meer data verzameld werd dan nodig. Slechts weinig respondenten beperkten echter effectief de toegang tot hun data. Wel verwijderde 57% ooit een app uit privacyoverwegingen en annuleerde 62% de installatie van een app hiervoor.

Deze resultaten, zowel van het kwalitatieve als het kwantitatieve luik, weerspiegelen wat men in de academische wereld de privacyparadox noemt (Norberg, Horne & Horne, 2007; Büschel, Mehdi, Cammilleri, Marzouki & Elger, 2014; Baek, 2014) en die ook verder nog aan bod zal komen. Hoewel de deelnemers zeggen bezorgd te zijn om hun privacy, ondernemen ze zelf geen actie om hun privacy ook daadwerkelijk te beschermen. De intenties met betrekking tot privacy weerspiegelen de gedragingen niet. Hoewel ze zich zorgen maken over de bescherming van hun persoonlijke gegevens, geven mensen toch nog ontzettend veel persoonlijke data vrij (Norberg e.a., 2007). De privacybezorgdheden worden overstemd door andere factoren die in een (onbewuste) kosten-batenanalyse de overhand nemen. Voorbeelden van zulke factoren zijn bijvoorbeeld de gratis dienst die de app verleent, de tijd en moeite die het kost om zich door de gebruiksovereenkomst te worstelen of het gebrek aan ervaring met negatieve gevolgen (Shklovski e.a., 2014).

Uit de interviews van Shklovski e.a. (2014) blijkt dat sommige respondenten echter wel gegronde redenen zien die derden kunnen hebben voor het gebruik van hun data. Enerzijds kunnen de gebruikers van apps en toepassingen beter bediend worden met een zekere mate van personalisering zoals aanbevelingen of zodat iemands BMI bijvoorbeeld juist berekend kan worden. Anderzijds

begrijpt een groot deel van de geïnterviewden dat de informatie die zo verzameld wordt een bron van inkomsten is voor gratis apps (ibid.). Het besef dat de klant tegenwoordig het koopwaar is, neemt de bezorgdheden echter wel niet weg. Ze zien het als een product van de tijd, iets waar zij geen impact op hebben, iets wat hoort bij het smartphonegebruik, iets wat ze moeten aanvaarden als de prijs voor de gratis dienst (ibid.). Hun attitude ten opzichte van grootschalige dataverzameling mag dan wel negatief zijn, het gebruik van allerhande apps verandert niet (ibid.). Hoewel ze een strengere regulering en meer transparantie wensen en beter geïnformeerd willen worden over de risico's wat betreft dataverzameling door derden, minderen ze zelf hun app-gebruik niet noch lezen ze de gebruiksvoorwaarden (ibid.). Dus hoewel de meeste gebruikers verontwaardigd zijn over het gebruik dat van hun data wordt gemaakt, verloopt het app-gebruik volgens zijn gewone gang van zaken.

Dit kan geïnterpreteerd worden als goed nieuws voor de app-ontwikkelaars want gebruikers blijven gewoon persoonlijke informatie delen ondanks het gebrek aan vertrouwen omdat hun motivatie niet groot genoeg is om hun gedrag ook effectief te veranderen. Uit het vervolginterview bleek namelijk dat geen van de deelnemers effectief zijn gedrag had veranderd, hoewel ze tijdens het interview aangaven misleid te zijn. Dit is echter helemaal geen goed nieuws volgens de onderzoekers want geen enkel businessmodel is stevig als er geen vertrouwen is bij zijn gebruikers. Dit maakt de status van de smartphone in onze samenleving onzeker (Shklovski e.a., 2014) en bij uitbreiding het gebruik van fitness- en gezondheidstoepassingen.

1.6 Invloed technologie op gebruik

In wat volgt zal ik verder nog een onderzoek bespreken over hoe de standaard privacyinstellingen van locatie-gebaseerde apps als Foursquare en Glympse de perceptie van controle over iemands persoonlijke data beïnvloeden en daarnaast ook het gebruik van die applicaties. Ten eerste omdat sommige gezondheidsapps zoals het populaire Runkeeper of de Fitbit ook gebruik maken van de

locatievoorzieningen. Ten tweede omdat het ook relevant is om te weten hoe de privacyinstellingen het gebruik van de toepassing beïnvloeden.

Coppens, Veeckman en Claeys (2014) bestuderen in lijn met wat Akrich (ibid.) het script van een technologie noemt hoe de privacyinstellingen van locatie-gebaseerde applicaties het gebruik ervan beïnvloeden, in dit geval Foursquare en Glympse. Ze onderzoeken in eerste instantie de technologie en dan met name de gevraagde persoonlijke informatie, de standaard privacy-instellingen en de aanpassingsmogelijkheden ervan. In tweede instantie werd bekeken hoe de gebruikers met de technologie omgingen. Gedurende een periode van drie weken gebruikten de deelnemers de applicaties door verschillende opdrachten uit te voeren zoals "Check in op een willekeurige plaats en deel het met je vrienden op Facebook of Twitter. Tag indien mogelijk een vriend." In een latere fase van het onderzoek werd in een interview dieper ingegaan op de opdrachten om zo te begrijpen welke beslissingsprocessen de deelnemers doorliepen. Glympse is een locatie-gebaseerde applicatie en is vrij privacy-invasief daar het je constante locatie doorgeeft. Deze applicatie biedt wel de mogelijkheid om elke keer te kiezen met wie en voor hoe lang je dit wil delen. Foursquare biedt deze optie tot selecteren niet, maar werd controleerbaarder geacht door de deelnemers omdat je elke locatie bewust deelt in tegenstelling tot Glympse waarmee je continu gevolgd wordt (ibid.). Voor je de informatie invoert, denk je er bewust over na. Dat maakt Foursquare ook gebruiksvriendelijker omdat de gebruiker niet elke keer weer de tijdrovende privacyinstellingen moet doorlopen en op die manier geconfronteerd wordt met het feit dat hij op het punt staat persoonlijke informatie te delen (ibid.).

Coppens e.a. merken uit de interviews op dat hoewel veel deelnemers privacy en controle over hun persoonlijke gegevens belangrijk achten, ze zich niet bewust waren van de informatie die op hun Foursquare-profiel beschikbaar was, de privacyinstellingen en het desbetreffende privacybeleid. Wanneer hen namelijk wordt gevraagd welke informatie er op hun profiel zichtbaar is, moeten verschillende respondenten daarvoor teruggrijpen naar hun instellingen. De onderzoekers stelden verbaasd vast dat de meeste respondenten nog nooit naar de privacyinstellingen hadden gekeken.

Dit sluit aan bij de privacyparadox. Ook uit een recent privacyrapport van Symantec (2015), waarvoor 7000 respondenten uit zeven Europese landen bevraagd werden, blijkt dat hoewel 57% bezorgd is over de veiligheid van zijn data, amper 25% van de respondenten de gebruiksvoorwaarden leest wanneer ze online een dienst of product kopen. In aansluiting met de bevindingen van Coppens e.a (2014) en Shklovski e.a. (2014) komt ook Liu (2014) tot de constatatie dat inderdaad nog al te vaak mensen de privacyvoorwaarden niet lezen. Aan de hand van een survey bevroeg ze 100 universiteitsstudenten over het privacybeleid van mobiele apps. Geen van de deelnemers gaf aan ooit een privacybeleid te lezen. Toch gaan ze er door een simpele klik mee akkoord waardoor wordt verondersteld dat ze er mee instemmen. Het is vaak tijdrovend om het hele privacybeleid van een app te lezen, dat bovendien vaak is opgesteld in een moeilijk juridisch jargon. Daarenboven zijn er niet veel andere opties dan het goedkeuren ervan, want een afwijzing zou resulteren in het niet kunnen gebruiken van de applicatie. Liu ziet dan ook geen heil meer in *'notice and consent'*. Het is eigenlijk geëvolueerd tot het blind geven van toestemming. Nochtans is dit wel de hoeksteen van de verschillende privacy- en data protectie-wetgevingen en -reguleringen (art. 7 en 10 Richtlijn 95/46EG inzake bescherming persoonsgegevens). Het *notice and consent*-principe is een lege doos geworden omdat het zo onnadenkend gebeurt.

1.7 Ontwerpvoorstellen privacyvriendelijke gezondheidsapps

In het onderzoek van Coppens e.a. (2014) ontwikkelden enkele deelnemers zelf innovatieve strategieën, los van de technologie, om hun privacy te garanderen. Zo zorgde iemand ervoor dat een derde met slechte intenties geen routines uit zijn data zou kunnen afleiden door nooit op hetzelfde moment thuis in te checken. Een andere strategie bestond er in om verschillende accounts te creëren om zo *"zijn digitale voetafdruk te verkleinen"*. Hoewel sommige gebruikers zelf innovatieve technieken verzinnen om hun privacy te waarborgen, zouden we toch een stap verder moeten gaan dan de huidige gebruiken inzake privacybescherming om de privacy van alle gebruikers te beschermen, want zoals hierboven werd

beargumenteerd, is het *notice and consent*-principe voorbijgestreefd. In plaats van achteraf simpelweg goedkeuring te vragen voor het privacybeleid zouden we de privacyvereisten reeds van bij aanvang van de ontwikkeling van de technologie moeten integreren in de hard- en software. Dit is de *privacy by design*-filosofie (van Lieshout, Kool, Schoonhoven & de Jonge, 2011). Hierbij aansluitend zouden technologieën de transparantie moeten bevorderen. Van Lieshout spreekt in dit geval over *"transparency tools"* die de gebruiker duidelijk kunnen maken wie wat met zijn data doet (ibid.). De onderzoekers van bovenvermelde studies komen dan ook met verschillende ontwerpvoorstellen.

Liu (2014) stelt ten eerste voor de privacyinstellingen interactiever te maken en de gebruiker duidelijk uiteen te zetten welke gegevens vereist worden voor elke functie van een app (zie figuur 6). Zo maakt de gebruiker een bewustere afweging of hij echt zijn gegevens wil prijsgeven in ruil voor de functionaliteit van de dienst. Een tweede mogelijkheid is het sturen van pushberichten en meldingen telkens wanneer er gebruik gemaakt zal worden van specifieke persoonlijke gegevens (ibid.). Ten derde zou de data alleen opgeslagen mogen worden wanneer er een relevante activiteit plaatsgrijpt (Klasnja e.a., 2009). Zo zou een smartwatch bijvoorbeeld alleen de locatie van de gebruiker mogen registreren wanneer hij sport en niet wanneer hij tv-kijkt of werkt. Daarmee samenhangend moet hij ook enkel de informatie verzamelen die nodig is om de toepassing te laten werken (ibid.).

Category of information	Purpose of the collection	On/off in general	Allow only when this is function is in use (delete or anonymise immediately when it is OFF)
Information about your mobile equipment, IP address, user ID	These are basic items of information for the basic function of the app	On/off	
Location data	Map function	On/off	On/off
Contacts	Help find contacts that are using a similar app	On/off	On/off
Credit card number	Making payment	On/off	On/off
Album	Publish or PS pictures	On/off	On/off
…	…	…	…

Figuur 6: interactieve privacyinstellingen
Bron: Liu, 2014, p.527.

Verder zou de basisfunctionaliteit standaard zo minimaal invasief mogelijk moeten functioneren zodat de gebruiker zelf extra functionaliteiten kan toevoegen indien hij bereid is daar wat meer privacy voor op te geven (ibid.). Ten zesde raden Raij e.a. (2011) aan combinaties van gezondheidsdata met contextfactoren, zoals plaats- en tijdsaanduidingen, te vermijden, om met andere woorden een zekere mate van abstractie in te voeren. De auteurs wijzen er wel op dat zo de bruikbaarheid van de data aangetast wordt in het opzicht van de dataverwerker. In de afweging moet dus zowel in zekere mate rekening gehouden worden met de privacy van de gebruiker als met de vereisten van de dataverwerker. Voorts benadrukken Raij en collega's dat iemands psychologische staat en stressniveau van nature privé zijn (ibid.). Dit is namelijk niet zichtbaar met het blote oog. Bijgevolg is dit een zeer gevoelig type informatie dat verzameld kan worden via *personal sensing* en is voorzichtigheid geboden. Ten slotte benadrukken Prasad e.a. (2012), ondersteund door de resultaten die voortvloeiden uit de interviews met de deelnemers die vijf dagen een Fitbit gebruikten, dat een *one size fits all*-privacyinstelling niet volstaat. Het soort informatie en de personen met wie informatie al dan niet gedeeld mag worden verschilt niet alleen van persoon tot persoon, maar varieerde daarenboven ook binnen de gebruiker. Zo beslisten verschillende deelnemers van de gebruikersstudie van Prasad om na verloop van tijd hun privacyinstellingen toch verder te beperken. Daarom is een *flexibele interface* vereist zodat iedereen zijn privacyinstellingen voor zichzelf kan bepalen en indien nodig nog kan aanpassen. Zo'n interface geeft idealiter duidelijk weer welke informatie verzameld wordt en wie die op welke wijze te zien krijgt. Op die manier is de gebruiker in staat precies te bekijken wat zijn moeder kan zien en welke informatie is voortgevloeid naar een derde partij. Zo kan hij weloverwogen beslissen met wie hij zijn persoonlijke informatie wenst te delen. Ook Motti en Caine (2014) moedigen zulke afstellingsmogelijkheden aan. Niet alleen heeft de gebruiker recht op controle wat betreft het delen van zijn persoonlijke informatie, maar moet hij ook in staat zijn te beslissen welke data überhaupt verzameld mogen worden. Eventueel kan de interface een bepaalde instelling aanbevelen op basis van de achtergrondinformatie van de gebruiker. De interface moet gebruiksvriendelijk en intuïtief zijn (hij begrijpt het snel en zonder training), expressief (de gebruiker

kan namelijk zelf zijn ideale instellingen uiteenzetten) en transparant (hij ziet duidelijk wat met wie gedeeld wordt) (Prasad e.a., 2012).

Veel van deze voorstellen sluiten aan bij het *privacy by design*-principe. Dit principe zien we ook terugkomen in de nieuwe verordening van de Europese Commissie die afgerond zou moeten zijn tegen 2016-2017 (Vedder, 25.02.2015; Valcke, 04.03.2015). De verordening zal de huidige richtlijn 95/46EG inzake bescherming van persoonsgegevens vervangen (ibid.). In wat volgt zal ik kort de relevantste en belangrijkste veranderingen in vergelijking met de huidige richtlijn gegevensbescherming aanhalen. De eerste verandering die meteen opvalt is dat het nu een verordening betreft. In tegenstelling tot een richtlijn die louter een doel vooropstelt waarvan de lidstaten zelf kunnen bepalen hoe ze daar in hun wetgeving invulling aan geven, is een verordening een bindend besluit dat in de hele Europese Unie van toepassing is (ibid.). Zo gelden overal dezelfde regels. Een verordening heeft met andere woorden rechtstreekse werking. Ook het feit dat men nu een verordening ontwerpt inzake gegevensbescherming is veelzeggend: men vindt het duidelijk een belangrijp onderwerp in het big data-tijdperk (ibid.). Ten tweede zal aan de bijzondere categorieën van persoonsgegevens die extra beschermingsmaatregelen genieten in de nieuwe verordening de nieuwe categorie "genetische en biometrische gegevens" toegevoegd worden (ibid.), relevant in de context van deze masterproef over fitness- en gezondheidsdata. Ten derde vereist artikel 5 van de nieuwe verordening dat de gegevensverwerking rechtmatig, eerlijk en transparant gebeurt (ibid.). Daarnaast staat ook het principe van dataminimisatie centraal: de verwerking van persoonsgegevens en het bijhouden ervan moet beperkt blijven tot wat minimaal nodig is voor het beoogde doel (ibid.). Ten vierde evolueren de rechten van de betrokkene in de nieuwe verordening zodanig dat hij meer controle en invloed heeft op de verwerking van zijn persoonsgegevens (ibid.). Zo moet de verantwoordelijke voor de verwerking de nodige transparantie bieden over wat hij verzamelt en hoe hij de gegevens die hij verzamelt, zal verwerken. Daarnaast heeft het individu recht op informatie en toegang tot zijn gegevens met daarenboven het recht om zijn gegevens aan te passen en te laten wissen (ibid.). Verder beschrijft de verordening ook de plichten van de verantwoordelijke. Deze moet de privacy van zijn gebruikers

reeds indachtig houden van bij het begin van de ontwikkeling van zijn technologie via het reeds vermelde *privacy by design*-principe (ibid.). Ook moeten de privacyinstellingen de privacy van de gebruiker standaard (*by default*) beschermen en met andere woorden standaard op zo minimaal invasief mogelijk ingesteld staan (ibid.). Tenslotte voorziet de verordening ook in strenge straffen en boetes die kunnen oplopen tot 100 000 000 euro of 5% van de jaaromzet indien de bepalingen van de verording niet worden nageleefd (ibid.).

De Europese Unie wilt ten eerste dus dat de ontwikkelaars meer aandacht besteden aan de privacy van hun gebruikers. Enerzijds door transparant te zijn over het gebruik en de verwerking en de verzameling tot het minimum te beperken (dataminimisatie). Anderzijds door al van bij het begin van de ontwikkeling van toepassingen mechanismen ter bescherming van de privacy in te bouwen. Het principe van dataminimisatie sluit goed aan bij de voorstellen die hierboven besproken werden. De onderzoekers stelden namelijk voor alleen tijdens de relevante activiteiten data te registreren en ze slechts bij te houden voor zolang nodig is. Ook het privacy-by-default-principe sluit aan bij de eis van Klasnja e.a. (2009) om de functionaliteit zo minimaal invasief mogelijk te laten werken. Ten tweede beoogt Europa de gebruiker meer controle te bieden. De voorstellen van Prasad e.a. (2012) en Motti e.a. (2014) voor een flexibele interface waar de gebruiker door middel van een overzicht van zijn data zelf kan bepalen met wie hij welke data deelt, sluiten daar bij aan.

1.8 Conclusie

Op basis van het overzicht van de literatuur dat ik hier probeerde te schetsen, kunnen we al deels een antwoord formuleren op de vraag hoe men staat tegenover het verzamelen en gebruiken van data uit fitness- en gezondheidstoepassingen. Academici, professionals en beleidsmakers zien er potentieel in: het kan de gezondheidszorg verlichten en er kunnen interessante inzichten gedestilleerd worden uit de big data die de gezondheidstoepassingen opleveren. Er dienen echter wel eerst enkele hindernissen overwonnen te worden. De interpretatie van de gegevens vraagt een digitale geletterdheid die

nog niet bij iedereen aanwezig is. Daarnaast moet de adoptiegraad hoger, wil de hele samenleving van de voordelen kunnen genieten. Het belangrijkste punt waar rekening mee gehouden moet worden in de context van deze masterproef, is de bescherming van de privacy van de gebruikers. Indien we de privacybezorgdheden kunnen wegnemen door privacyvriendelijke apps te ontwikkelen, zal mogelijks ook de adoptiegraad van fitness- en gezondheids-toepassingen toenemen. Want als de privacy van de gebruiker niet gegarandeerd kan worden en alle verzamelde gegevens te grabbel komen te liggen, zal niemand gebruik willen maken van de vele apps en toepassingen (Klasnja e.a., 2009; Prasad e.a., 2012; Motti e.a., 2014).

Dus alvorens we privacyvriendelijke apps kunnen ontwikkelen, zullen we eerst de privacybezorgdheden van de gebruikers moeten kennen zodat we ze kunnen verhelpen. Daarom is het belangrijk om naast de visies van de academici, professionals en beleidsmakers, ook het standpunt en de bekommernissen van de eindgebruiker te kennen. Uit onderzoek blijkt dat de privacybezorgdheden van eindgebruikers variëren afhankelijk van het type informatie dat verzameld wordt. Zo zijn ze bijvoorbeeld niet bezorgd om hun privacy wanneer het algemene fitnessdata betreft die een accelerometer of barometer registreerde, maar zijn ze al bezorgder wanneer ook hun locatie wordt bijgehouden. Ook variëren de bekommernissen afhankelijk van het gebruik dat van de data gemaakt zal worden en de persoon die de informatie te zien krijgt. Zo vinden de gebruikers het niet erg bepaalde informatie te delen als dit hen een voordeel oplevert. Ook zijn ze bereid hun data beschikbaar te stellen voor onderzoekers, maar ze delen dan weer niet graag informatie met het grote publiek. Tot slot kwam ook nog aan bod hoe de privacybezorgdheden afnamen indien de data op een abstractere manier gedeeld konden worden, indien de data maar voor een beperkte duur werden bijgehouden en indien aan de data geen identiteit werd gekoppeld. Aan deze bekommernissen kunnen *privacy- en transparency enhancing technologies* tegemoet komen zoals bijvoorbeeld interactieve privacyinstellingen waarbij de gebruiker op een overzichtelijke manier kan zien wie over welke data beschikt.

2. Onderzoeksvragen

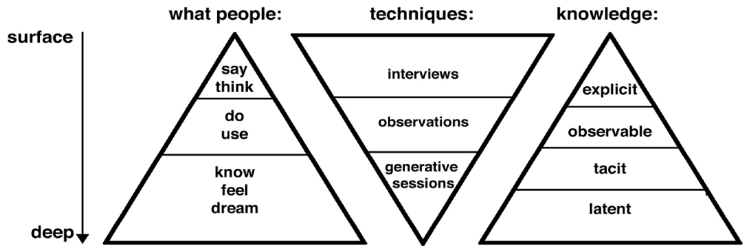
Op de vraag hoe natuurlijke gebruikers van gezondheidstoepassingen staan tegenover het gebruik van hun fitness- en gezondheidsdata, is tot nu toe nog geen sluitend antwoord gegeven. Klasnja e.a. (2009) suggereert, op basis van het onderzoek van Nguyen en collega's (2008) naar de privacybezorgdheden omtrent alledaagse trackingtechnologieën, dat natuurlijke gebruikers die uit eigen beweging gebruik maken van gezondheidstoepassingen misschien helemaal niet bezorgd zijn om hun privacy. Uit het onderzoek van Shklovski e.a. (2014) bleek dat (natuurlijke) smartphonegebruikers zich wel zorgen maakten om hun privacy, maar zich er bij hebben neergelegd dat hun data verzameld wordt. De bezorgdheden die naar voor kwamen uit de online reacties van geïnteresseerde gebruikers en effectieve gebruikers van allerlei wearables (die ik dus benoem als natuurlijke gebruikers) leken aan te sluiten bij de bekommernissen die naar voor kwamen uit de onderzoeken met "gedwongen" gebruikers.

In deze masterproef wordt gekozen voor interviews met natuurlijke gebruikers van fitness- en gezondheidstoepassingen, omdat het bestuderen van de online reacties op enkele limieten stuitte. Hier werden namelijk zowel de reacties van effectieve gebruikers als van louter geïnteresseerde gebruikers bestudeerd. Onze interviews gebeuren alleen met gebruikers die uit eigen beweging effectief al gebruik maken van fitness- en gezondheidstoepassingen. Daarenboven zijn de gebruikers die online reacties plaatsen niet representatief voor alle gebruikers. Zij zijn mogelijks heel enthousiast of juist heel bezorgd. Tenslotte peilden ze enkel naar de bekommernissen die optreden bij het gebruik van een niet-exhaustieve lijst wearables. In mijn onderzoek komen naast wearable-gebruikers ook gebruikers van apps aan het woord.

Er wordt in een interview gepeild naar hoe de natuurlijke gebruikers zich verhouden tegenover de dataverzameling van gezondheidsdata en of ze zich überhaupt bewust zijn van het feit dat hun data waarde heeft en verzameld en gebruikt wordt door derden. Daarnaast wordt gepeild naar welke informatie ze als persoonlijk en privé beschouwen en aldus niet bereid zijn te delen. Strookt dit ook met hun huidige gebruik? Tot slot wordt hen gevraagd hoe er meer

vertrouwen gecreëerd kan worden in de apps en toepassingen. Dus in tegenstelling tot de onderzoeken van Klasnja e.a. (2009), Raij e.a. (2011) en Prasad e.a. (2012) waar de deelnemers gevraagd werden een toepassing te gebruiken, worden hier gebruikers bevraagd die er zelf voor kozen fitness- en gezondheidstoepassingen te gebruiken. Dit ligt in lijn met het onderzoek van Nguyen e.a. (2008), Shklovski e.a. (2014) en Motti e.a. (2014) die gebruikers met ervaring bevroegen. Maar zoals hierboven uiteengezet werd, willen we in dit onderzoek een stap verder gaan dan het bestuderen van online reacties. Daarom wordt gekozen voor interviews.

Omdat we in eerste instantie peilen naar hun huidige opinies, meningen en gedachten in verband met dataverzameling en in het bijzonder de verzameling van fitness- en gezondheidsdata, is een interview op zijn plaats. Zoals figuur 7 duidelijk maakt, blijven we met interviews redelijk aan de oppervlakte. We peilen naar wat de deelnemers denken over de tegenwoordige dataverzameling en hoe ze er tegenover staan. In tweede instantie vragen we echter ook naar mogelijke oplossingen of factoren die in de toekomst de privacybezorgdheden kunnen reduceren en met andere woorden zouden kunnen bijdragen tot meer vertrouwen. We gaan op zoek naar latente noden. Dit zijn behoeftes waarvan men zich nog niet bewust is (Sleeswijk Visser, Stappers, van der Lugt & Sanders, 2005). Daarom kregen de interviews ook een generatieve toets. Zo maakten de deelnemers een week voor het eigenlijke interview een bundel met enkele generatieve opdrachten. Op die manier probeerden we de deelnemers alvast bewust te maken van de dataverzameling en de voor- en nadelen hiervan, zodat het interview vlot zou kunnen verlopen. Ook werd aan de deelnemers een open vraag gesteld waar ze creatief en inventief op konden antwoorden, maar hier zal in de methodensectie uitgebreider op teruggekomen worden. Figuur 7 geeft dit onderscheid tussen interviews en generatieve technieken goed weer. Het verduidelijkt de verbondenheid tussen de kennis die we willen vergaren en de techniek die we ervoor gebruiken.



Figuur 7: verband tussen techniek en te vergaren kennis
Bron: Sleeswijk Visser, Stappers, van der Lugt & Sanders, 2005, p.123.

3. Methode

3.1 Deelnemers

Aan het onderzoek namen tien personen deel. Dit is geen groot aantal gezien de beperkte tijd en middelen, maar het saturatiepunt werd wel bereikt, in die zin dat het laatste interview geen nieuwe informatie meer opleverde (Guest, Bunce & Johnson, 2006). Het betreft daarenboven een kwalitatief onderzoek waarbij we niet op grote schaal wensten te toetsen of de attitudes representatief zijn voor een grote populatie. Wel probeerden we de motivaties en attitudes diepgaand te begrijpen. De deelnemers werden gerekruteerd via een bericht in de Quantified Self Brussel Meetup-groep (zie bijlage 1). De overigen bereikte ik via mijn persoonlijk netwerk en kennissen van mijn contacten. Het voornaamste inclusiecriterium voor de deelnemers was het gebruik van een of meer fitness- en gezondheidstoepassingen. Mensen die uit medische noodzaak gebruik maken van gezondheidstoepassingen, zoals bijvoorbeeld diabetespatiënten die hun glucosegehalte moeten monitoren, vallen buiten het bestek van deze masterproef.

Het gebruik van fitness- en gezondheidstoepassingen werd heel breed opgevat en omvatte zowel het gebruik van apps als wearables, minstens een keer per maand. De uiteindelijke deelnemers gebruikten de volgende gezondeidstoepassingen: Runkeeper, Strava, de calorieënteller van MyFitnessPal of Lifesum, Personal Body Plan, HealthKit, Nike+ Running, Bodymedia en Jawbone UP. Onder de

deelnemers zaten 3 mannen en 7 vrouwen en de leeftijden varieerden tussen 21 en 53 jaar, met een overgewicht voor de categorie van 39 tot 53 jaar (zie tabel 1). Deze verdeling weerspiegelt de resultaten die Flurry (2014) bekwam na de analyse van de gebruiksdata van 6800 fitness- en gezondheidsapps voor iPhone of iPad. Zo blijkt de meerderheid van de gebruikers vrouwen (62%) te zijn en zijn de 25- tot 54-jarigen oververtegenwoordigd. De deelnemers werden bewust geselecteerd omdat zij beantwoorden aan de relevante karakteristieken voor dit onderzoek: geslacht, leeftijd en gebruik van een gezondheidstoepassing. Representativiteit werd zoals reeds gesteld, niet nagestreefd.

Tot slot is het nog belangrijk toe te voegen dat de steekproef enkele interessante personen bevatte voor dit onderwerp. Zo waren er verschillende deelnemers werkzaam in de "databusiness" zoals een statisticus, een student cross media management, een zaakvoerder van een bedrijf gespecialiseerd in online banking en een docent die daarenboven betrokken is bij de R&D van gezondheidstoepassingen. Daarnaast bevatte de steekproef ook een psychiater die vanuit zijn job juist meer op zijn privacy gesteld was. Hierbij moet opgemerkt worden dat alle deelnemers hoger opgeleid zijn.

	21 jaar
	39 jaar
	52 jaar
	21 jaar
	24 jaar
	24 jaar
	41 jaar
	44 jaar
	53 jaar
	53 jaar
3x  7x 	4x jong*, 6x oud ** jong = < 25 jaar*

Tabel 1: verdeling geslacht en leeftijd van de deelnemers

3.2 Materiaal en procedure

Om de deelnemers al op voorhand te laten nadenken over big data en grootschalige dataverzameling werd hen gevraagd een week voor het eigenlijke interview een opdrachtenbundel te maken. Deze sensitisatiefase diende om zowel de kwaliteit als de kwantiteit van de antwoorden van de deelnemers tijdens het interview te bevorderen

(Sleeswijk Visser, Stappers, van der Lugt & Sanders, 2005). De bundel bevatte vijf opdrachten die elk 5 tot 10 minuten in beslag namen (zie tabel 2 voor een overzicht van de opdrachten). Het was de bedoeling dat de opdrachten voor de respondenten leuk waren om te doen (zoals bijvoorbeeld de opdracht waarbij ze stickers mochten plakken bij de momenten in hun dagoverzicht waar ze data hadden vrijgegeven). We probeerden de deelnemer niet alleen bewust te maken van de tegenwoordige dataverzameling, maar hen ook te stimuleren om de verschillende voor- en nadelen ervan af te wegen. Ik veronderstelde immers dat big data geen alledaags onderwerp was waar de deelnemers al een uitgesproken opinie over hadden. Het gebruiken van een gezondheidstoepassing is namelijk nog iets anders dan het hebben van kennis over big data. Naast het stimuleren tot het afwegen van de voor- en nadelen bestond een van de andere opdrachten eruit een mindmap te maken van het begrip privacy (dat als een van de nadelen van big data gepercipieerd kan worden) om na te gaan wat dit voor hen betekent of zou kunnen betekenen (zie bijlage 3 voor de opdrachtenbundel). De kern van de opdrachten doorstonden een piloottest, maar ze dienden wel anders geformuleerd en gepresenteerd te worden zodat het voor alle deelnemers duidelijk zou zijn. Zo werd voor opdracht 1 een tabel met tijdsaanduidingen voorzien, omdat uit de piloottest bleek dat een leeg blad niet stimulerend werkte en er zo relevante activiteiten vergeten werden. Ook werd voor opdracht 3 al een machtigingenvenster getoond, waar ze het in de eerste versie van de opdrachtenbundel zelf moesten opzoeken.

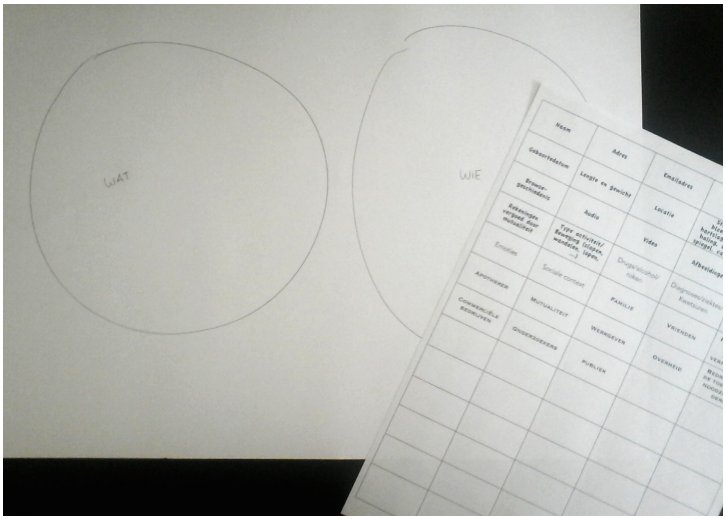
Het effectieve interview bestond uit vier luiken. In het eerste luik werd de opdrachtenbundel overlopen met de deelnemer. Hieruit moest duidelijk worden of de deelnemers zich bewust waren van de tegenwoordige dataverzameling en hoe ze hiertegenover staan. In het tweede luik kreeg de deelnemer een A3-blad voor zich met twee cirkels en een stickervel (zie figuur 8). Op het stickervel stonden 22 soorten informatie die een typische gezondheidsapp vaak verzamelt, gaande van leeftijd, geslacht en adres tot lengte, gewicht en locatie. Deze types informatie kwamen aan bod in bovenvermelde literatuur of worden standaard gevraagd door een fitness- of gezondheids-toepassing.

Opdracht	Doel
Opdracht 1: De deelnemer beschrijft hoe zijn vorige dag er uitzag en plakt de bijgevoegde stickers bij de momenten waarop hij sporen heeft achtergelaten.	De deelnemer bewust maken van de alomtegenwoordigheid van dataverzameling.
Opdracht 2: De deelnemer beschrijft hoe hij zelf gebruik maakt van zijn verzamelde data. Hij denkt na over hoe de overheid de big data kan gebruiken. Hij bedenkt hoe een commercieel bedrijf de big data kan aanwenden.	De deelnemer bewust maken van de voor- en nadelen van big data. De deelnemer laten nadenken over hoe data gebruikt en misbruikt kunnen worden.
Opdracht 3: De deelnemer beoordeelt een screenshot van een machtigingenvenster dat verschijnt voor het installeren van een Calorieënteller-app.	Te weten komen wat de deelnemer goed en minder goed vindt aan het machtigingenvenster. Hier wordt tijdens het interview op teruggekomen. Zo heeft hij er al over nagedacht.
Opdracht 4: De deelnemer noteert waar hij aan denkt bij een reeks van zes krantenkoppen over big data.	De deelnemer bewust maken van de voor- en nadelen van big data.
Opdracht 5: De deelnemer maakt een mindmap rond de term privacy.	Te weten komen wat privacy voor de deelnemer betekent en wat hij er mee associeert.

Tabel 2: oplijsting opdrachten met bijbehorend doel

Naast de soorten informatie, bevatte het stickervel ook 11 stickers met personen met wie ze hun data al dan niet zouden willen delen. Er werd ook voorzien in lege stickers voor het geval de deelnemers zelf nog aan iets dachten (zie bijlage 4 voor het volledige stickervel). De deelnemers moesten de informatie-stickers in de wat-cirkel kleven als

ze dit type informatie als persoonlijk beschouwden en bijgevolg niet wensten te delen. Anders behoorden ze de stickers buiten de eerste cirkel te plakken. De personen met wie ze de informatie in de wat-cirkel wel wilden delen, plakten ze in de wie-cirkel. Personen die hun informatie niet mochten weten, werden buiten de wie-cirkel gekleefd. Tijdens het kleven motiveerde de interviewer de deelnemer om luidop te denken en peilde hij naar de motivatie om de stickers op die welbepaalde plek te kleven. Zo kwamen al enkele voorwaarden ter sprake, maar daar werd na het kleven van de stickers nog eens apart op in gegaan. Door de deelnemers op deze manier te bevragen, probeerden we het interview niet alleen boeiender, maar ook overzichtelijker te maken. De deelnemers konden duidelijker stellen wat ze wel en niet als privé beschouwden en met wie ze al dan niet hun persoonlijke informatie wensten te delen. Wanneer dit louter mondeling zou verlopen, zouden ze dit misschien niet zo helder kunnen overbrengen.



Figuur 8: wie- en wat-cirkel met bijbehorende stickers

Tijdens het derde luik werd de huidige techniek van *notice and consent* onder de loep genomen. De interviewer greep eerst terug naar opdracht 3 uit de opdrachtenbundel waar de deelnemer de voor- en nadelen beschreef van het machtigingenvenster dat gebruikers te zien krijgen wanneer ze op het punt staan een app te installeren. Vervolgens werd een fictieve gebruiksovereenkomst besproken (zie bijlage 5). Deze werd opgesteld op basis van de gemeenschappelijkheden uit het privacybeleid van Runkeeper, Fitbit, Fjuul, MyFitnessPal en Lifesum. Tenslotte werd in het laatste luik een open vraag gesteld waarop de deelnemers vrij en creatief mochten antwoorden: "Hoe zou je er voor zorgen dat je een gezondheidsapp met een gerust hart kan gebruiken? Wat zou maken dat je een bepaalde app met 100% vertouwen zou gebruiken?" (zie bijlage 6). Om de deelnemers aan te moedigen de platgetreden paden te vermijden verzekerde de interviewer dat ze aan alles mochten denken: zowel aan regelgeving, technologie als normen in de samenleving. Indien het stroef verliep, vroeg de interviewer naar aspecten van het fictieve privacybeleid die ze liever zouden willen aanpassen en hoe ze deze vervolgens konden veranderen.

Alle interviews verliepen face-to-face, behalve een dat via skype werd afgenomen. De interviews werden allemaal opgenomen met een dictafoon en duurden tussen 49 en 79 minuten met een gemiddelde van 63 minuten.

3.3 Analyse

Alvorens aan de analyse begonnen kon worden, werden alle interviews getranscribeerd (zie bijlage 7 voor een link naar de getranscribeerde interviews). Daarna werden de interviews nogmaals gelezen om verder met de data te familiariseren. Vervolgens werd gekozen voor een thematische analyse. Er werden patronen en clusters van betekenis gezocht in de data in functie van de onderzoeksvragen (Courtois, 18.11.2014). Eerst werden de interviews opgebroken in de kleinst codeerbare eenheden. Daaraan werden vervolgens codes gegeven op basis van de topiclijst en de literatuur. De initiële codes waren onder andere de types informatie en personen met wie er al dan niet persoonlijke informtie gedeeld

mag worden (zie bijlage 8: de codes in het vet zijn de initiële codes). Daarnaast doken er tijdens het coderen ook nieuwe codes op. Daarom moest er iteratief gecodeerd worden: de nieuwe codes moesten indien nodig ook aan de voorgaande stukken tekst toegeschreven worden (zie bijlage 8). Voor de analyse werd gebruik gemaakt van het softwarepakket NVivo. Tijdens de analyse werd ook teruggegrepen naar de visuele artefacten van de respondenten waaronder de opdrachtenbundel en het cirkel-schema ter aanvulling van de transcripten. Zo maakte het cirkelschema het mogelijk eenduidig uit te maken of iets al dan niet als privé gecategoriseerd werd.

4. Resultaten

In wat volgt zal ten eerste besproken worden hoe de respondenten zich verhouden ten opzichte van de tegenwoordige dataverzameling en het gebruik van de verzamelde data. Daarna komen de resultaten aan bod van de opdracht waarbij de respondenten gevraagd werden de verschillende types informatie in of uit de wat-cirkel te kleven. Hieruit blijkt dat de inschatting van het private karakter niet alleen afhangt van het type informatie, alsook van enkele voorwaarden, maar vooral ook van het gebruik dat er van gemaakt zal worden. Vervolgens zal blijken in welke mate de respondenten zich konden vinden in het fictieve privacybeleid. Tot slot zal ik bespreken wat volgens de respondenten mogelijkheden zijn om meer vertrouwen te genereren in het gebruik van fitness- en gezondheidstoepassingen.

4.1 Houding ten opzichte van tegenwoordige dataverzameling en het gebruik ervan

Het is voor de deelnemers vaak geen verrassing dat er tegenwoordig heel veel data verzameld wordt. De respondenten zijn zich in bepaalde gevallen erg bewust dat ze data vrijgeven. Bijvoorbeeld wanneer ze toepassingen gebruiken zoals een calorieënteller waarbij ze eigenhandig hun voeding ingeven. In de meeste gevallen echter, zijn ze zich niet bewust dat ze persoonlijke informatie achterlaten,

maar komen ze tot het besef dat er persoonlijke data werd bijgehouden als ze nadien gerichte marketing ontvangen.

> Je gaat iets opzoeken op internet, maar na een tijd vraag je je wel af: "Waarom komt nu... Ik heb daarstraks ergens een site bezocht over handtassen en nu zie ik hier op mijn Facebook allemaal spullekes van handtassen." Op die moment weet je dat wel, maar je staat er echt niet bij stil dat ze alles vergaren. (Deelnemer 9)

Eigenlijk zijn de respondenten zich onbewust wel bewust van de grootschalige dataverzameling, zoals een van de respondenten dit goed uitdrukte.

> Onbewust ben je je daar van bewust. Ik zal het zo zeggen. Hahaha. Op die moment denk je daar niet aan, maar je weet het uiteindelijk wel, dat dat bezig is allemaal. Dat is een feit. (Deelnemer 8)

Of ze nu al dan niet bewust informatie vrijgeven of al dan niet geconfronteerd worden met persoonlijke advertenties, het verwondert hen niet dat er tegenwoordig heel veel informatie wordt opgeslagen. De respondenten ervaren de tegenwoordige dataverzameling als een onderdeel van de hedendaagse maatschappij.

> Je kan het niet vermijden. Zoals nu op het internet ook: je zit daar op en je weet dat dat gebeurt. Je kunt dat toch niet tegenhouden he. (Deelnemer 8)

Het feit dat er informatie verzameld wordt, vinden de meeste respondenten niet erg. Dat heeft mogelijks te maken met het feit dat ze nog nooit negatieve gevolgen hebben ondervonden. Die onwetendheid maakt dat ze geen problemen hebben met de dataverzameling. Er zijn natuurlijk uitzonderingen die de regel bevestigen. Zij die effectief ooit iets hebben meegemaakt, maakten zich meer zorgen en pasten hun privacyinstellingen aan.

> Locatie plak ik hier omdat ik daar onlangs ook nog wat mee heb meegemaakt. Dat stond op mijn facebook. Als ik met mijn gsm een bericht stuurde konden mensen dat zien. En zo was iemand achter mijn adres gekomen die ik eigenlijk niet kende. En daarmee heb ik dat nu

> vorige week aangepast. Die zei ineens van "ja, ik weet u wel wonen." En ik zei van "Huh? Hoe weet jij dat?" En dan had die daar inderdaad een screenshot van doorgestuurd waarin dan effectief Google Maps met zo een bolleke [aanduidt] waar je bent en dat was juist. En daarmee was ik daar dan zo van verschoten dat dat zo correct was. (Deelnemer 1)

Net zoals deelnemer 1 zelf besloot zijn instellingen aan te passen, beklemtonen de respondenten de eigen verantwoordelijkheid. Als de gebruiker niet wil dat er iets geweten is, moet hij het zelf afschermen of niet op het internet zetten en prijsgeven. Ze hebben het gevoel dat ze zelf bepalen wat ze delen en wat niet. Daarnaast hanteren enkele respondenten ook nog andere mechanismen om hun privacy te waarborgen: een valse naam opgeven, de browsegeschiedenis wissen of zaken opzoeken die je eigenlijk niet interesseren.

> En als ik er op let, online, ga ik ook naar exotische dingen gaan kijken die buiten mijn gedrag vallen, juist om het algoritme wat in de war te brengen. Haha. Dat zijn mogelijkheden om dingen te vermijden he. (Deelnemer 5)

Ze vinden de dataverzameling niet alleen niet erg omdat ze er nog nooit negatieve gevolgen van hebben ondervonden en omdat ze het als hun eigen verantwoordelijkheid beschouwen om hun privacy te beschermen, maar ook omdat ze vertrouwen hebben in de overheid, wetten en de bedrijven. Ze geloven namelijk niet dat er verkeerd gebruik zal gemaakt worden van hun informatie en dat ze de data heel persoonlijk zullen gebruiken om informatie over specifieke personen te weten te komen. Je bent gewoon een van de miljarden onbekende nummers waardoor je verdwijnt in de massa. Wanneer er sprake is van deviant of crimineel gedrag mag er wel op de individuele data ingezoomd worden. De respondenten geloven met andere woorden dat als je niets te verbergen hebt, alles geweten mag zijn.

> Ik denk dat ik dat allemaal niet zo erg vind omdat er niks is dat mij achtervolgt. Dat je niks hebt wat mensen niet mogen weten. Maar stel dat ik naar pornosites zou gaan, dat ik dat kei tof vind en niemand mag

> dat weten en plots weet iedereen dat, dan zou dat heel erg zijn. (Deelnemer 4)

Het verkeerd gebruik, in tegenstelling tot de loutere verzameling van de data, wordt daarentegen wel als storend en verontrustend ervaren. Verschillende respondenten ergeren zich aan de gepersonaliseerde aanbevelingen van commerciële bedrijven, hoewel er ook enkelen zijn die deze op maat gemaakte reclame net handig vinden.

> Als je bijvoorbeeld "Italiaans restaurant" zoekt en ik ben ofwel in Antwerpen ofwel bij mij thuis, dan krijg ik andere resultaten. Ik had daar nog niet echt bij stil gestaan, maar ik vind dat op zich wel handig als je nu bijvoorbeeld inderdaad dringend iets nodig hebt. Bijvoorbeeld: er is iets en je wilt naar het ziekenhuis, als je dan googlet "ziekenhuis" is het gemakkelijk als je direct het ziekenhuis in de buurt krijgt. Dus op zich zie ik daar geen probleem in. (Deelnemer 1)

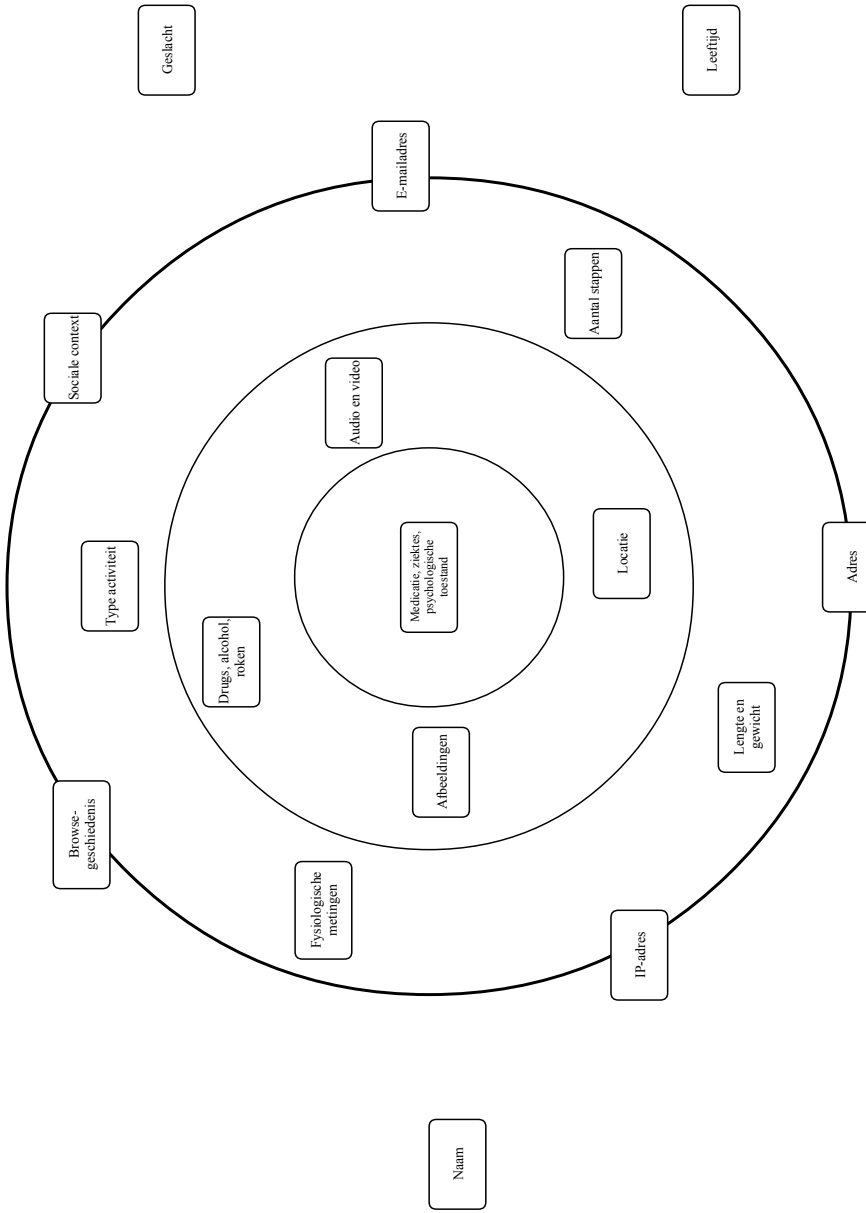
Niet alleen private bedrijven kunnen misbruik maken van de data die ze verzamelen, ook als de data in handen vallen van een individu met slechte bedoelingen dreigen er potentiële gevaren, zeker als dit individu verbonden is aan de staat.

> Want stel nu, er komt terug iemand aan de macht zoals Hitler, en die beslist van alle aanhangers of sympathisanten van een bepaald idee, die gaan we vergassen. Awel, dat is heel simpel, die moet maar gewoon gaan kijken naar uw webgeschiedenis of op wat je geabonneerd bent en met een knopje kan die zeggen: "Hier is de lijst, ga ze maar vergassen." (Deelnemer 9)

Tot dusver kunnen we besluiten dat de respondenten zich in zekere mate bewust achten van de tegenwoordige dataverzameling. Ze vinden dit niet erg zolang er geen misbruik van gemaakt wordt. Ze hebben ideeën van het mogelijke wangebruik, maar aangezien ze nog nooit te maken kregen met andere negatieve gevolgen dan reclame, zijn ze vrij gerust dat er op een goede manier met hun persoonlijke data wordt omgegaan. Daarenboven leggen zij ook de verantwoordelijkheid bij de gebruiker die zichzelf en zijn privacy kan beschermen.

4.2 Welke verzamelde informatie is privaat en welke is publiek?

De afweging die de respondenten maken tussen de informatie en het gebruik dat ervan gemaakt zal worden zien we nog uitgesprokener terugkomen wanneer gepeild werd naar welk type informatie de respondenten privé vinden. Dit bleek een opdracht die veel nuancering vergde, maar globaal genomen kunnen we stellen dat elk type informatie wel gedeeld kan worden indien het op een goede manier gebruikt wordt. Figuur 9 geeft een samenvatting weer van welke informatie de respondenten niet zomaar met iedereen wensen te delen en de types informatie die minder privaat zijn. Ze zijn bereid alle informatie in de cirkels te delen met een app of toepassing als dit nodig is, maar willen deze info niet zomaar in de openbaarheid brengen. Hoe verder een bepaald type informatie zich van het centrum bevindt, hoe meer geneigd ze zijn om het te delen met anderen. De buitenste cirkel is de grens tussen privé en publiek. De types informatie die buiten de cirkel staan, hebben voor de meeste respondenten geen privaat karakter. Over de types informatie die zich op de rand van de cirkel bevinden, zijn de respondenten het niet eens. Ze zien er het nut niet van in waarom een fitness- of gezondheidstoepassing deze informatie nodig zou hebben of welk voordeel dit hen kan opleveren. Op basis van de antwoorden van de respondenten is het niet mogelijk ze eenduidig als privaat of publiek te categoriseren, maar wel is duidelijk dat ze de meerwaarde ervan niet zien. Daarom staan ze op de rand van de cirkel die we niet alleen als grens tussen privé en publiek kunnen beschouwen, maar die we ook als nutsgrens opvatten. Alles wat namelijk in de cirkel staat is privé, maar zijn ze wel bereid te delen als het een nut heeft. Het onderscheid tussen de types informatie buiten de cirkel, in de cirkel en op de cirkel maakt dus het verband duidelijk tussen de inschatting van het private karakter van een bepaald type informatie op basis van het gepercipieerde nut ervan. De privé-publieksgrens kan namelijk verschuiven volgens de inschatting van het nut. Zo vinden respondenten hun locatie bijvoorbeeld gevoelige materie, maar zijn ze wel bereid hun locatiedata vrij te geven om hun looproute te registreren. Ook het medicatiegebruik is erg privé, maar in een afgeschermde app waar verder alleen de arts toegang toe heeft, willen



Figuur 9: overzicht van de gradaties in het privaat karakter van verschillende types persoonlijke informatie

ze die wel invoeren. Indien de gebruikers dus overtuigd worden van de bruikbaarheid van de types informatie op de rand, kan het zijn dat ook zij in de cirkel terechtkomen.

Het is echter wel belangrijk te benadrukken dat deze figuur louter een samenvatting is van de opinies die bij de tien respondenten leven. Het is een simplificatie en dat betekent dus dat niet elke respondent zich noodzakelijk in dit diagram vertegenwoordigd ziet. De indeling blijkt dus niet alleen afhankelijk van het type informatie, maar ook van het gebruik dat er van gemaakt zal worden. Verder hebben de respondenten ook nog enkele voorwaarden voor de omgang met de persoonlijke data die mee de privacybezorgdheden beïnvloeden. Deze drie beïnvloedende factoren worden nu achtereenvolgens besproken.

4.2.1 Inschatting privaat karakter afhankelijk van het type informatie

4.2.1.1 Vanzelfsprekende kenmerken: naam, leeftijd, geslacht

Hun naam op zich vinden de respondenten niet privé. Voor- en achternaam worden dan ook makkelijk ingevuld wanneer toepassingen of diensten er naar vragen. Belangrijk is echter te benadrukken dat andere types informatie zoals bijvoorbeeld het medicatiegebruik en het gewicht dan weer niet aan hun naam gekoppeld mogen worden, maar daar zal in wat volgt verder op worden ingegaan. We kunnen dus stellen dat louter de naam niet als privé wordt gepercipieerd.

> Dat is zo'n beetje de truc he. Als ze uw naam weten, op zich vind ik het niet erg dat ze mijn naam weten, maar dan zou ik, denk ik, andere dingen niet prijsgeven. (Deelnemer 7)

Ook geslacht, leeftijd en geboortedatum ervaren de respondenten niet als privé, hoewel velen toch afwegen wat ze er mis mee zouden kunnen doen en wat het nut er van is voor de dienst aan wie ze het zullen verschaffen. Ze beseffen namelijk dat de toepassing accuratere

gegevens zal opleveren indien het algoritme gebaseerd is op het juiste geslacht en de juiste leeftijd.

> Mijn leeftijd vind ik niet zo erg als ze dat weten. Daar zijn ze eigenlijk ook niet echt zoveel mee he. Net als mijn geslacht, dat volgt meestal ook gewoon uit uw naam. (Deelnemer 2)

4.2.1.2 Gevoelige informatie: lengte, gewicht, fysiologische metingen, activiteit

De deelnemers volgen dezelfde redenering wat betreft lengte en gewicht en zijn bereid deze informatie met de toepassing te delen omdat ze er het nut van inzien. Desondanks zijn lengte en gewicht voor sommigen wel een gevoeliger type informatie dan geslacht en leeftijd, kenmerken die vrij makkelijk af te leiden zijn uit iemands fysieke verschijning. Hun gewicht willen ze wel in de app, maar niet in de openbaarheid brengen. Dit heeft mogelijks te maken met het feit dat positieve zaken en ervaringen liever gedeeld worden dan negatieve. Overgewicht wordt immers als iets negatief beschouwd.

> Lengte en gewicht? Ja, want dan kunnen ze zo berekenen hoeveel calorieën je verbruikt. Dus dat wil ik ook geven. (Deelnemer 5)

Ook fysiologische metingen als hartslag, ademhaling en bloeddruk worden aan dezelfde redenering onderworpen: is het nuttig voor de dienst die ik op het punt sta te gebruiken? Indien dit het geval is, is vrijwel iedereen bereid ook deze informatie te delen met de toepassing. De respondenten menen dat het voor fitness- en gezondheidstoepassingen logisch is dat het type activiteit (zoals lopen, wandelen of slapen) en het aantal stappen geregistreerd kunnen worden en zijn zodus ook bereid deze data vrij te geven.

> Bloeddruk, ademhaling, ... goh. Als dat zo een programma is voor dieet enzo, dan is dat wel interessant dat ze dat weten. (Deelnemer 4)

4.2.1.3 Gevoeligere informatie: locatie, audio, video, afbeeldingen, drugs, roken, alcohol

Locatiedata is gevoeligere materie, zoals ook figuur 9 duidelijk maakt. De deelnemers zijn bereid hun locatie prijs te geven, maar alleen om de toepassing te laten werken, want het voortdurend real-time traceren vinden alle deelnemers onaangenaam. Ze hebben het gevoel gevolgd te worden.

> Je hebt zo bij iPhone nu Family Sharing, dat je zogezegd de leden van je familie kunt volgen en op real-time weet waar ze zijn. Ik denk zelfs dat ik het niet zou aanzetten voor mijn kinderen ook al zou ik willen weten waar ze zijn. Uit principe zou ik het nooit aanzetten. Omdat ... dat vind ik echt ver gaan. Zo dat traceren van waar iemand is. (Deelnemer 10)

Voor de beperkte duur van hun sportactiviteit zijn ze wel bereid deze functie in te schakelen omdat dit hen nuttige informatie oplevert. Deze informatie wordt wel enkel met de app gedeeld of niet in real-time in de openbaarheid gebracht.

> De enige momenten dat mijn gsm mijn locatie gebruikt, is als ik ga lopen. Dat vind ik niet zo erg dat hij dan mijn locatie gebruikt, want ik wil weten hoelang en hoeveel ik gelopen heb. (Deelnemer 7)

Audio en video worden door sommigen als privé ervaren omdat dit persoonlijker is: hun stem en gezicht zijn zichtbaar. Ze vinden het te invasief. Indien het gebruik van audio en video echter van nut is voor de toepassing die ze gebruiken, kan het gebruik ervan wel weer door de beugel, maar dan alleen wanneer het echt nodig is. Wanneer een app bijvoorbeeld de slaap monitort aan de hand van de microfoon, mag dit tijdens de nacht aanstaan, maar moet deze functie erna uitgezet kunnen worden. Zo zijn de gebruikers zich bewust van wanneer ze data vrijgeven.

> Maar microfoon vind ik wel wat eng. Ja, ik zou niet weten hoe dat anders werkt zonder microfoon. Maar ik vind dat ze dan zouden moeten zeggen als je het echt aanzet: “de microfoon staat nu aan”. Dat ze het zeggen terwijl je het aanzet. Dat het niet zo is van het kan altijd

> op staan. Dat ze echt waarschuwen. Of als ze de video gebruiken dat ze zeggen van: “nu gaat de videotoepassing aan” of “nu word je opgenomen”. Ja. Dan zou ik het okee vinden. Dan kies je er ook echt voor, dat je weet dat je wordt afgeluisterd tijdens uw slaap.
> (Deelnemer 5)

Enkele weigerachtige respondenten stellen dat ze in de toekomst misschien wel gemakkelijker een app toegang zouden verlenen tot hun microfoon en camera als deze praktijk meer ingeburgerd geraakt. Anderen maken zich hier nu al geen zorgen over omdat ze niet geloven dat er ook effectief op zo’n persoonlijke manier gebruik gaat gemaakt worden van die data.

> Ik ben niet zo paranoia zoals sommige mensen dat ze hun webcam altijd afplakken, daar geloof ik niet in. Daar heb ik geen last van. (Deelnemer 10)

Ook afbeeldingen beschouwen de meeste respondenten als privé omdat ze er niet altijd het nut van inzien waarom een gezondheidsapp toegang nodig heeft tot hun persoonlijke afbeeldingen. Indien ze zelf kunnen kiezen welke afbeelding ze vrijgeven beschouwen ze de nodige toegang niet als een probleem, maar anderen krijgen geen vrije toegang tot al hun afbeeldingen. Ze willen met andere woorden zelf de controle behouden.

> Als bijvoorbeeld die calorie-app mijn locatie nodig heeft, die moet dat niet hebben. Of mijn contacten. Voor zo’n dingen, ja dat is niet nodig, dus dan geef ik dat niet. Maar als die bijvoorbeeld wel mijn camera wilt voor foto’s of een fotodagboek van uw eten te verzamelen, daar ga ik dan wel toegang tot geven. (Deelnemer 2)

Drugs-, alcoholgebruik en roken worden door de meeste respondenten als privé gecategoriseerd. Dit heeft waarschijnlijk weer te maken met het feit dat positieve dingen graag worden gedeeld in tegenstelling tot negatieve zaken want de respondenten die niet roken en geen alcohol en drugs gebruiken vinden dit niet privé. Van hen mag iedereen dit weten, terwijl de anderen ondere andere hun alcoholgebruik willen afschermen. Dit kan hen namelijk negatieve

gevolgen opleveren zoals onder andere imagoschade, ontslag of vervolging voor een misdrijf.

> Mijn alcoholverbruik. Dat zou ik liever eigenlijk privé houden. Maar ik weet niet, gewoon, ja dat hangt er... ja, drugs en roken doe ik al niet, dus dat mogen ze weten. (Deelnemer 5)

4.2.1.4 Gevoeligste informatie: medische informatie

Medicatiegebruik, behandelingen, diagnoses, ziektes en kwetsuren vallen voor de respondenten onder het medisch geheim. Het kan echter wel ingegeven worden in een app of toepassing die daarvoor ontwikkeld is, indien die echter wel goed afgeschermd is voor derden, met uitzondering van het medisch personeel dat wel toegang mag krijgen tot die data. We zien hier dus weer terugkomen hoe het gebruik dat van de data gemaakt zal worden een invloed heeft op de inschatting van het private karakter, maar daar zal in paragraaf 4.2.2 verder op ingegaan worden.

Enkele respondenten gaan hierin nog een stap verder en benadrukken dat niet alleen de app daarvoor ontwikkeld moet zijn en alleen bevoegden toegang mogen hebben tot hun data, daarenboven moet de dataverzameling een specifiek doel hebben en moet de periode van dataverzameling afgebakend zijn. Ze willen niet alles zomaar lukraak, automatisch en zonder nut verzamelen en doorsturen naar de arts, maar dat zal in wat volgt geïllustreerd worden.

Over het algemeen willen ze een positieve gemoedstoestand wel delen. Ze beseffen echter dat indien die slecht is (wanneer ze bijvoorbeeld depressief zijn) ze die waarschijnlijk niet zullen willen delen. Daarnaast vragen ze zich opnieuw af wat het nut hiervan is voor een fitnesstoepassing zoals Runkeeper.

> Ik zet mijn psychologische toestand soms wel in die app, moet ik eerlijk toegeven, als ik zo echt blij ben. Maar als het negatief is, zet ik die daar nooit in. [...] Op de een of andere manier vind ik negatieve emoties meer privé dan blije emoties. (Deelnemer 7)

4.2.1.5 Wat is het nut van adresgegevens, socialie context, IP-adres en browsgeschiedenis voor een fitness- en gezondheidstoepassing?

De adresgegevens zijn een bijzonder kwestie. De adresgegevens omvatten de persoonlijke levenssfeer waar vreemden buiten moeten blijven. De respondenten beschouwen deze informatie als privé, maar zien vooral geen nut in het delen van hun adres met een gezondheidsapp, in tegenstelling tot de locatiegegevens die hen wel handige informatie kunnen opleveren zoals hun snelheid, afgelegde afstand en looproute. Het vrijgeven van de adresgegevens overschrijdt, zoals figuur 9 weergeeft, de nutsgrens niet. Daarenboven houdt het vrijgeven van hun adres ook potentiële risico's in zoals inbraak, diefstal, stalking en opdringerige reclame. Deze risico's zijn volgens de respondenten niet verbonden aan de locatiedata omdat de gebruiker daar weer weg zal zijn na een bepaalde tijd.

> Maar uw adres, dat is echt zo een specifieke plek. En uw locatie niet. Dat kan eerder waar zijn. Dus dat kan ook hier bijvoorbeeld zijn of daar. (Deelnemer 2)

Twee respondenten stellen echter wel vast dat adresgegevens vandaag de dag relatief eenvoudig te vinden zijn en beschouwen dit type informatie dan ook niet als privé.

> Locatie en adres, uiteindelijk... dat kunnen ze overal vinden he. [...] Als je iemand zijn naam hebt... Awel, je opent gewoon.. hoe noemt dat, 1911. Awel ja, je tikt gewoon die naam in en je vindt die mens, waar ze wonen en dan ga je naar Google Streetview en je ziet hoe zijn huis is. [...] En uw adres, ja, op zich is daar nog niks verkeerd mee he. (Deelnemer 9)

Over het delen van iemands persoonlijk e-mailadres bestaat minder eensgezindheid bij de respondenten. Daarom staat dit type informatie op de rand van de cirkel in figuur 9. De respondenten vallen uiteen in twee groepen. De ene groep stelt vast dat er vaak geen andere keuze is dan het invullen van hun e-mailadres en zien er geen graten in. De andere groep beschouwt dit als minder privé dan de adresgegevens omdat dit geen fysieke ruimte is, maar storen zich aan de negatieve gevolgen die het vrijgeven van hun e-mailadres met zich kan meebrengen: het ontvangen van spam. In een ideale wereld zijn alle respondenten dus wel bereid hun e-mailadres vrij te geven, maar dan wensen ze geen spam te ontvangen.

Sociale context en IP-adres zijn andere soorten persoonlijke informatie waar evenzeer geen eensgezindheid over bestond. Sociale context verraadde volgens sommigen weinig over hun persoonlijkheid, terwijl anderen juist stelden dat hun data zo een persoonlijker karakter kreeg. Over het IP-adres werd eveneens geen unanimiteit bereikt, maar dat is te wijten aan de gebrekkige kennis over wat dit juist is en kan.

> IP-adres, ja, als ze daar iets mee zijn. Ik vind dat niet zo iets heel persoonlijk, mijn IP-adres. Ik weet niet wat ze daar mee kunnen doen. (Deelnemer 5)

> IP-adres, dat is, dat weet ik niet wat ze daar allemaal mee kunnen misdoen. Ze kunnen dat gebruiken voor dingen aan te kopen. Ik weet het eigenlijk niet. Dus dat is ook zoiets, waarschijnlijk heeft dat niks met uw app te maken. Niet echt handig voor die app, dus zou ik het ook niet vrijgeven als dat niet automatisch zou gebeuren. Ik weet het niet. (Deelnemer 4)

Wat betreft de toegang tot de browsegeschiedenis van de gebruiker, vragen de deelnemers zich af wat hier de noodzaak van is. Ook hier maken ze in hun bepaling van het private karakter van dit type informatie een afweging op basis van het nut ervan. Daarenboven benadrukken verschillende respondenten dat de gebruiker zelf verantwoordelijk is voor het vrijgeven van zijn browsegeschiedenis want indien hij dit als gevoelig categoriseert kan hij zijn browsegeschiedenis makkelijk verwijderen.

Hier zien we echter een paradox: de respondenten die hun browsegeschiedenis privé vinden, doen er niks aan terwijl ze wel weten dat het kan.

> Interviewer: En uw browsegeschiedenis?
> Deelnemer 7: Die moeten niet weten op welke website ik zit.
> Interviewer: En wis je dan vaak uw cookies?
> Deelnemer 7: Nee. Helaas. Ik wist tot vorige week zelfs niet dat dat ging. Tegenwoordig krijg je wel heel vaak op je scherm: "deze site maakt gebruik van cookies." Dan denk ik altijd: "Aahja!". Maar weet ik veel wat cookies zijn. Ik had al wel door dat dat geen koekjes waren om op te eten.

4.2.2 Inschatting privaat karakter afhankelijk van het gebruik dat er van gemaakt zal worden

Zoals blijkt uit het bovenstaande houden de respondenten naast het type informatie ook allemaal rekening met wat er met hun data zal gebeuren. Dit hangt logischerwijze samen met de persoon met wie de data gedeeld zullen worden. Het gebruik dat er van gemaakt zal worden, beïnvloedt dus sterk hun intentie tot het vrijgeven van hun persoonlijke informatie. Wanneer gepeild werd naar de personen met wie ze hun data al dan niet wensten te delen, zien we die afweging met betrekking tot het gebruik van hun data nog uitgesprokener terugkomen. Zo vinden de respondenten het geen probleem om hun persoonlijke fitness- en gezondheidsdata te delen met hulpverleners zoals de huisarts en specialist, omdat deze data wel belangrijk zouden kunnen zijn bij het stellen van de juiste diagnose.

> Deelnemer 6: Ja, dus met mijn huisarts doe ik dat wel. Hij weet dat ik dat doe en dat is eigenlijk wel handig. Ik moet niet zo veel... Ik ben niet zo veel ziek. Maar door het feit dat ik mijn slaap monitor... En ik voel dat ik echt heel goed slaap, maar toch mij 's morgens niet goed voel, dat is ook een signaal. Dus als dat dan langere dagen duurt, dan ga ik daar met hem wat over praten. Meestal is dat wel correct, want dan is er een infectie ofzo.
> Interviewer: En hij analyseert dan de data die jij hebt verzameld?
> Deelnemer 6: Nee, ik vertel mijn data aan hem. Hij heeft geen access.

> Ik denk dat dat belangrijk is dat ze alles weten. Alles wat ik hier zie staan. Ik denk dat alles relevant kan zijn. (Deelnemer 3)

Enkele respondenten stellen dat die informatie inderdaad handig kan zijn voor de arts, maar ze beklemtonen dat het voor hen niet lukraak moet worden verzameld en doorgestuurd naar de arts, zoals hierboven al werd aangehaald.

> Moest mijn cardioloog zeggen van "ja, maar u loopt en uw hart en wat voor hartslag hebt u dan als u aan het lopen bent?". Dan heb ik er geen probleem mee om hem mijn voorbije loopsessies te tonen. [...] Maar ik zou hem dat niet op continue wijze doorsturen. Ik zou niet zeggen vanaf nu krijgt u dat elke dag. [...] Het zou in het kader van een concrete vraag of behandeling moeten zijn. Niet systematisch, ik teken vanaf nu een akkoord om al mijn gezondheidsapps... alles wordt gepusht naar mijn huisarts en hij zal dan wel mij bellen als hij denkt dat er een probleem is. (Deelnemer 10)

Ook zien ze er wel het nut van in als bepaalde informatie, zoals het medicatiegebruik, gedeeld wordt met de apotheker omdat hij kan waarschuwen voor bepaalde foute combinaties met andere geneesmiddelen bijvoorbeeld. Belangrijk is te benadrukken dat de apotheker niet in dezelfde mate toegang moet hebben tot de fitness- en gezondheidsdata als de arts. Zo kan de arts baat hebben bij het zien van de patiënts hartslagmetingen op basis waarvan hij bepaalde medicatie voorschrijft, maar die gedetailleerde metingen hoeven niet zichtbaar te zijn voor de apotheker.

Met een beperkte kring van familie en vrienden mogen de fitness- en gezondheidsdata ook gedeeld worden. De respondenten beklemtonen hier wel het onderscheid tussen verre familie en het gezin en vrienden en kennissen. Ook met de overheid en onderzoekers mogen de persoonlijke data gedeeld worden als ze aangewend worden voor het algemeen belang en de vooruitgang. Met de werkgever willen de respondenten hun fitness- en gezondheidsinformatie niet delen omdat dit hen negatieve gevolgen zou kunnen opleveren zoals imagoschade of zelfs ontslag. Indien het werk er onder zal lijden vinden de respondenten het wel aangewezen de werkgever er van op de hoogte te brengen.

> Eigenlijk aan de werkgever niet veel. Ik zou altijd wel schrik hebben dat ze er iets negatief kunnen uithalen. Als je alcoholgebruik ofzo... Ik denk dat niemand wilt dat zijn werkgever dat weet. En medicatiegebruik enzoverder ook niet. (Deelnemer 5)

Wat betreft het verkopen van persoonlijke informatie aan commerciële bedrijven kunnen we twee groepen onderscheiden. De ene groep is absoluut niet bereid zijn fitness- en gezondheidsdata met de commerciële bedrijven te delen omdat zij alleen uit winstbejag opereren. Zij verdienen geld met de informatie van de gebruikers. Anderzijds zijn enkele respondenten wel bereid hun informatie geanonimiseerd aan hen vrij te geven omdat ze beseffen dat ook die bedrijven hun informatie ergens moeten halen. Aangezien hun data anoniem is, zullen ze er ook geen last van ondervinden, zo luidt de redenering. Tenslotte werd gepeild naar welke informatie al dan niet met het grote publiek gedeeld mocht worden, met andere woorden welke informatie in de openbaarheid gebracht mag worden. De vanzelfsprekende informatie als naam, leeftijd en geslacht mogen voor de meeste respondenten publiek zijn. Zonder naam zouden alle gegevens openbaar mogen zijn, maar ook hier stellen enkele respondenten zich de vraag wat daar het nut van is.

4.2.3 Inschatting privaat karakter afhankelijk van de omgang met de data

Zoals uit het bovenstaande al tussen de regels door af te leiden viel, is de inschatting van het privaat karakter ook afhankelijk van hoe er met data zal omgegaan worden. De belangrijkste eis is die van anonimiteit. Zolang de persoonlijke informatie niet aan hun naam gekoppeld wordt, hebben de deelnemers niet het gevoel dat hun privacy geschonden wordt.

> Als ze mijn naam er niet aan vasthangen, mag van mij eigenlijk zo goed als alles geweten zijn. Allee, buiten dan adres en e-mailadres, maar op basis van leeftijd, geslacht en al de rest kunnen ze toch niet achterhalen wie je bent. (Deelnemer 7)

Wanneer de respondenten gewezen werden op de mogelijkheid tot reïdentificatie door het koppelen van datasets waardoor de beloofde anonimiteit teniet wordt gedaan, leken ze niet te geloven dat zij daar effectief slachtoffer van zouden worden. Dit sluit aan bij wat hierboven al aan bod kwam. Ze geloven namelijk niet dat er effectief op zo'n persoonlijke manier naar de data gekeken wordt en zeker niet als ze niets te verbergen hebben.

De respondenten geloofden niet dat ze meer geneigd zouden zijn informatie vrij te geven als die voor een beperktere duur zou bijgehouden worden of als deze abstracter was. Een voorbeeld van abstractere informatie is het doorgeven van een daggemiddelde van een bloeddruk in plaats van de bloeddruk ieder uur door te geven. Of het verzamelen van locatiedata, maar zonder tijdsaanduidingen. Maar zoals gezegd, beïnvloedde dit volgens de respondenten hun intentie tot delen niet.

We kunnen dus besluiten dat wat ze als privé beschouwen heel contextafhankelijk is. Er zijn eigenlijk geen types informatie die absoluut privé zijn. Zo kan alles wel in een bepaald kader gedeeld worden afhankelijk van wat er mee gebeurt en wie er mee in contact komt. Belangrijk is dat de gebruiker deze informatie bewust kan geven en niet dat zijn data overal terechtkomen zonder dat hij er weet van heeft.

4.3 Het privacybeleid van fitness- en gezondheidstoepassingen

De informatie over welke data de toepassing verzamelt, waarom en hoe er gebruik van gemaakt zal worden is te vinden in het privacybeleid. Wanneer de respondenten gevraagd werd of ze ooit al een privacybeleid hadden gelezen, gaven ze toe dit nooit te doen. Zij die het ooit wel al lazen, deden dit beroepsmatig. De vaakst voorkomende reden voor het niet lezen was de lengte van het privacybeleid, of in ieder geval het idee over de lengte ervan want vaak openden ze het niet eens maar gingen ze er van uit dat het een lijvig stuk tekst zou zijn.

> Dat is gewoon lang en de helft van de tijd snap je er toch niks van. (Deelnemer 7)

Ook het feit dat er geen andere keuze is dan het goedkeuren van het privacybeleid van de app of toepassing die ze op het punt staan te installeren, maakt dat de respondenten het niet lezen. Ook al ben je niet akkoord met wat er in staat, als je de toepassing graag wilt gebruiken en er zijn geen alternatieven, dan zit er niets anders op dan je akkoord te verklaren. Dan heeft het dus weinig zin om ook te lezen wat er in staat.

> Je wilt voort he. Je bent dat aan het downloaden. Je wilt dat hebben. Je wilt niet heel den bazaar nog eerst een halve dag lezen. (Deelnemer 4)

Enkele respondenten vermoeden daarenboven dat er altijd hetzelfde instaat. Ze veronderstellen dat het in orde is en in lijn is met wat er van technologieontwikkelaars verwacht wordt. Andere redenen waarom privacyvoorwaarden vaak niet worden gelezen zijn de kleine lettertjes, het moeilijke taalgebruik, bovendien vaak in het Engels.

Na het overlopen van het fictieve privacybeleid blijken alle deelnemers bereid dit beleid goed te keuren, mits een kleine wijziging aan het recht van aanpassen dat de app-ontwikkelaars zich toe-eigenen. Zij behouden zich het recht om het privacybeleid eender wanneer aan te passen, waarop ze vervolgens enkel de datum van laatste update zullen aanpassen. De gebruiker wordt geacht op de hoogte en akkoord te zijn met iedere wijziging. Deze clausule beschouwen de respondenten als een gevaarlijk addertje onder het gras en ze wensen dan ook duidelijker op de hoogte gebracht te worden van eventuele wijzigingen met een expliciete melding in de vorm van een mail of pushbericht. Daarnaast zijn er voor enkele respondenten nog wat pijnpunten, maar die worden niet door de anderen aangehaald. Zo is de manier waarop de gebruiker zijn recht op inzage, aanpassing en verwijdering van zijn persoonlijke gegevens kan uitoefenen niet gebruiksvriendelijk volgens twee respondenten. Daarnaast benadrukken twee andere respondenten dat het vaak niet binnen de mogelijkheid ligt van de dataverzamelaars om de data effectief te verwijderen. Onder andere door wetsbepalingen die eisen dat de data voor een bepaalde duur wordt bijgehouden. Een laatse struikelblok is de toegang die de fictieve gezondheidsapp zich toe-

eigent tot de contactenlijst van de gebruiker. De respondent die dit probleem aanhaalde, wenste daar zelf volledige controle over.

4.4 Oplossingen voor meer vertrouwen in fitness- en gezondheidstoepassingen

Eigenlijk is er onder de natuurlijke gebruikers die geïnterviewd werden al een behoorlijke mate van vertrouwen in de apps die ze gebruiken. Wanneer bij de respondenten gepeild werd naar mogelijke oplossingen waarop fitness- en gezondheidstoepassingen in de toekomst meer vertrouwen zouden kunnen genereren stelde iemand voor de apps labels te geven zodat duidelijk wordt of de app zorgvuldig met je data zal omspringen en je privacy zodus gewaarborgd kan worden. Een respondent nuanceert echter het gebruik van labels. Het feit dat er een label aanhangt, houdt voor hem niet noodzakelijk in dat de data correct behandeld zullen worden.

> Kan je dat allemaal vertrouwen? Pffff. Je kan daar wel opzetten "privacyproof", maar is dat dan wel zo? Dat weet je nooit he. En dat gaan we nooit weten ook. (Deelnemer 8)

Een andere mogelijkheid die aangehaald werd was de expliciete toestemming vragen voor elke functie apart met bijbehorende uitleg over elke functie. Hierbij aansluitend zou eventueel ook gewerkt kunnen worden met schuifbalkjes zodat de gebruiker ook hier op basis van de nodige informatie kan kiezen of hij toestemming verleent voor het verzamelen van die specifieke informatie.
Een derde oplossing voor meer vertrouwen is het bieden van een duidelijk overzicht van welke data bij wie is terechtgekomen, zodat de gebruiker op basis van deze informatie zijn instellingen kan wijzigen.

> Dat je misschien zelf ook inzage hebt in de gegevens die zij verzamelen en wat ze er mee doen. Hoe dat dat moet opgelost worden, dat weet ik niet. Misschien dat je ergens via een account dan zo kan raadplegen wat ze hebben en wat er mee gebeurt. En dat je er eventueel inspraak in hebt, dat je zegt: "Hoo stop! Hier gaat het te ver." En dat je dan op stop of delete duwt, dat dat daar dan stopt. Wat hebben ze en dit

> gebeurt er mee. Ja, dan, dat zou al inderdaad een pak meer vertrouwen geven. (Deelnemer 8)

Het bewust geïnformeerd vrijgeven van persoonlijke informatie lijkt de gemeenschappelijke noemer van deze drie oplossingen. Het bewust delen van fitness- en gezondheidsdata, gebaseerd op de nodige informatie blijkt dus de belangrijkste behoefte voor de gebruikers op weg naar meer vertrouwen. Zij willen op de hoogte zijn van wat er door wie met welke data zal gebeuren. Ze willen perfect weten waarom ze die informatie geven. Ze zijn baas over eigen data. Niettegenstaande horen we in de interviews regelmatig terugkomen dat de gebruiker impliciet toestemming geeft aan derden voor het gebruik van zijn data door die online te plaatsen of in te voeren in de app. Dit is het tegenovergestelde van het bewust geïnformeerd vrijgeven van persoonlijke informatie, maar enkele gebruikers lijken hier toch mee akkoord te gaan.

> Ik vind dat ik toestemming geef door het zelf online te zetten, dat zij het mogen gebruiken. Want ik zet het online, al mijn vrienden kunnen het zien. Dan vind ik dat zij er ook mee mogen doen wat ze willen. (Deelnemer 5)

Ook de professionele look van de toepassing, de naamsbekendheid en gebruiksvriendelijkheid spelen een belangrijke rol in het genereren van vertrouwen. Daarnaast blijkt persoonlijk contact een factor die meer vertrouwen kan inboezemen.

> Bodymedia is eigenlijk een vrij nauwkeurig toestel, maar als ik daar mijn moeder mee begon te meten werkte dat niet. Dus dat was heel afwijkende data en ik heb natuurlijk geluk dat ik contact heb met dat bedrijf dus ik heb dan wel al gemaild naar hen en dan heb ik dat gevraagd [...]. Maar ik vind dat wel belangrijk dat als er iets fout gaat dat je dat kan vragen hoe dat dat komt. (Deelnemer 6)

Er heerst momenteel vertrouwen in de overheid en de Europese Unie. Bijkomende wetten en verbodsbepalingen bieden niet noodzakelijk meer vertrouwen. Respondenten gingen er van uit dat zij wel toezicht houden op het verzamelen en gebruiken van persoonlijke informatie.

> Maar ik veronderstel dat daar ook wel controle op zit op zo'n dingen, nee? (Deelnemer 2)

Enkele respondenten beseffen echter wel dat het feit dat er een wet of verbod is op bijvoorbeeld reïdentificatie, dit het effectieve slechte gebruik niet kan vermijden. Persoonlijke data kan nog steeds misbruikt worden en je privacy kan zo geschonden worden, alleen zullen diegenen daar dan wel voor gestraft worden. De respondenten hebben met andere woorden niet al hun hoop op de wetgevende macht gevestigd en zijn daar redelijk nuchter in.

> Ik vind, opnieuw, datzelfde, als ik aan een site al mijn geheimen geef en daar staat in "ik ga het niet gebruiken". Ja, je moet niet naïef zijn. Je hebt ze wel gegeven. Dus, je moet er van uitgaan dat het kan zijn dat iemand die gebruikt. (Deelnemer 10)

4.5 Conclusie

Op basis van deze resultaten kunnen we besluiten dat de respondenten de tegenwoordige dataverzameling zien als een element van onze 21e-eeuwse samenleving en zich erbij hebben neergelegd. Er is geen type informatie dat ze absoluut als privé beschouwen want de respondenten zijn zelfs bereid medische informatie te delen afhankelijk van de manier waarop er met de informatie wordt omgegaan en het doel waarvoor het gebruikt wordt. Tot slot kunnen we stellen dat ze meer geneigd zullen zijn om hun data vrij te geven als het doel en het gebruik duidelijk gespecifieerd worden. Zo kunnen ze zelf beslissen hun data daar al dan niet voor prijs te geven.

5. Discussie

5.1 Zijn de natuurlijke gebruikers zich bewust van de dataverzameling?

Dit onderzoek probeerde een bijdrage te leveren aan de huidige stand van zaken in de literatuur door natuurlijke gebruikers van fitness- en gezondheidstoepassingen te bevragen. Enkele studies (Raij e.a.,

2011; Prasad e.a., 2012; Klasnja e.a., 2009) bevroegen namelijk personen die op vraag van de onderzoekers de technologie voor een bepaalde periode moesten gebruiken. Nguyen e.a. (2008) stelden vast dat mensen minder bezorgd waren over volgsystemen waarmee ze dagelijks in contact komen, zoals klantenkaarten bijvoorbeeld, dan over nieuwe technologieën waar ze weigerachtiger tegenover staan. Op basis van dit onderzoek van Nguyen veronderstelden Klasnja e.a. (2009) dat natuurlijke gebruikers van fitness- en gezondheidstoepassingen die al uit zichzelf gebruik maken van allerlei sensoren om hun activiteit te monitoren, minder bezorgd zouden zijn om het prijsgeven van hun data. Door het feit dat ze vertrouwd zijn met de voordelen ervan en nog geen negatieve gevolgen hebben ondervonden, zijn ze meer bereid gebruik te maken van zulke technologieën.

Alvorens te bespreken hoe de natuurlijke gebruikers uit dit onderzoek zich nu effectief verhouden ten opzichte van de tegenwoordige dataverzameling, is het belangrijk te weten of de gebruikers beseffen dat er zoveel persoonlijke informatie verzameld wordt. Dat besef is er volgens de respondenten wel degelijk. Dat sluit aan bij de resultaten van Shklovski e.a. (2014). Uit zijn survey bleek namelijk dat de respondenten zich bewust achten van de dataverzameling en het doorgeven van hun informatie aan derden. Of de inschatting van onze respondenten echter gegrond is, is op basis van ons onderzoek niet uit te maken. We peilden namelijk niet naar hun feitelijke kennis over de tegenwoordige dataverzameling. Het besef is echter wel eerder een onbewust besef. Dat lijkt paradoxaal, maar het betekent gewoon dat de respondenten leken in te zien dat dataverzameling alomtegenwoordig is. Ze beschouwen het als een facet van de wereld waarin we nu leven, net zoals de deelnemers aan het onderzoek van Shklovski e.a. (2014). Het feit dat dataverzameling als normaal wordt beschouwd, houdt echter niet in dat de gebruikers zich dan ook bewust zijn van ieder spoor dat ze achterlaten. In sommige gevallen beseffen ze natuurlijk dat ze informatie vrijgeven, zoals bijvoorbeeld bij het invoeren van hun maaltijd in een calorieënteller. Maar het is vooral door de gevolgen van de dataverzameling waardoor men ondervindt dat er wel degelijk veel informatie wordt vergaard. Zo krijgen ze gerichte reclame op basis van de webpagina's die ze bezochten of krijgen ze

aanbiedingen van restaurants in hun buurt. Eigenlijk weten de respondenten dus wel dat er heel veel data worden verzameld en opgeslagen, maar ze zijn zich er op het moment dat ze data vrijgeven vaak niet van bewust.

5.2 Hoe staan de natuurlijke gebruikers tegenover de dataverzameling van persoonlijke gegevens?

Het feit dat de respondenten de tegenwoordige dataverzameling als een element van de hedendaagse samenleving beschouwen, bepaalt mee hoe ze zich hier tegenover verhouden. Door de dataverzameling als logisch te kaderen, is er voor hen geen andere keuze dan het te aanvaarden. Ze hebben zich erbij neergelegd. Ze vinden het normaal. Ze staan er niet negatief tegenover.

Dat heeft ten eerste, net zoals Nguyen e.a. (2008) en Shklovski e.a. (2014) al stelden, vooral te maken met het feit dat ze nog nooit zeer negatieve gevolgen hebben ondervonden van het prijsgeven van persoonlijke informatie en bovendien ook niet met negatieve verhalen geconfronteerd willen worden. Die onwetendheid houdt hun niet-afkerige houding in stand.

Ten tweede hebben ze vertrouwen in degenen die gebruik maken van hun data. Dat sluit aan bij de bevindingen van Nguyen e.a. (2008). Uit zijn onderzoek bleek namelijk dat de geïnterviewden niet veronderstelden dat er effectief misbruik gemaakt zou worden van hun consumptiegedrag, zoals geregistreerd door klantenkaarten. De deelnemers aan ons onderzoek zijn zich er wel van bewust dat hun data in handen van een crimineel of dictator nefaste gevolgen kan hebben, maar ze hebben vertrouwen in de huidige praktijken en politiek. Buiten dan het overmatig spammen en de gepersonaliseerde aanbevelingen, hebben ze niet het gevoel dat er misbruik gemaakt wordt van hun data. Daarnaast zien we bij de respondenten de klassieke gedachtegang opduiken dat dataverzameling geen probleem is omdat ze toch niks te verbergen hebben. Ook de deelnemers uit het onderzoek van Nguyen e.a. (2014) geloofden dat de volgtechnieken geen bedreiging vormen voor mensen die niks verkeerd doen. Ook Greenwald (2014) merkt op dat velen deze redenering volgen als het

gaat over privacy, maar benadrukt dat privacy wel voor iedereen van belang is, ook als je niets te verbergen hebt.

Ten slotte beschouwen de respondenten het als hun eigen verantwoordelijkheid om hun data te beschermen en hebben ze het gevoel daar wel controle over te hebben. Het feit dat de respondenten het gevoel hebben dat zij controle hebben over wat er met hun data gebeurt, draagt ook bij tot hun niet-afkerige houding ten opzichte van dataverzameling.

We kunnen dus stellen dat de natuurlijke gebruikers de tegenwoordige dataverzameling als een element van de 21e eeuw beschouwen en hier niet negatief tegenover staan. Dat ligt in lijn met wat Klasnja e.a. (2009) verwachtte op basis van de resultaten van Nguyen e.a. (2008), maar we kunnen niet uitmaken of de natuurlijke gebruikers er ook effectief positiever tegenover staan dan mensen die er niet mee vertrouwd zijn omdat die hier niet bevraagd werden.

5.3 Wat vinden de natuurlijke gebruikers privé?

5.3.1 Inschatting privaat karakter afhankelijk van het type informatie

Welke informatie de gebruikers als privé categoriseerden, bleek zowel afhankelijk van het type verzamelde informatie, het gebruik dat er van wordt gemaakt, als ook van drie voorwaarden voor de behandeling van de data (anonimiteit, abstractie, beperkte duur bijhouden). Dat zagen we ook al opduiken in de literatuur. Deze factoren zijn daarenboven communicerende vaten. In de afweging of een bepaald type persoonlijke informatie al dan niet privé is, namen de respondenten namelijk ook altijd de manier waarop er met de data omgegaan werd en het nut mee in rekening. Daarom staan er in figuur 9 vijf types informatie op de rand van de cirkel. Over het algemeen zien de respondenten het nut niet in van het delen van deze types informatie (adres, e-mailadres, IP-adres, browsegeschiedenis en sociale context) met een fitness- of gezondheidstoepassing. Net zoals de types informatie op de rand, vinden ze de types informatie binnen de cirkel ook privé, maar zijn ze wel bereid deze info te delen met bevoegden en indien het hen iets oplevert, als het - met andere

woorden - nut heeft. Zo beschouwen ze het medicatiegebruik als privé, maar willen ze het bijvoorbeeld wel delen met een app die hen er aan herinnert hun pillen in te nemen. In tegenstelling tot de informatie op de rand van de cirkel en de informatie in de cirkel, beschouwen de respondenten de informatie buiten de cirkel als openbare kenmerken en beschouwen ze die dus doorgaans niet als privé. Dat wordt geïllustreerd door figuur 9.

Alle types informatie binnen de cirkel zijn globaal genomen dus privé en zouden de deelnemers niet openbaar maken als hun identiteit er aan gekoppeld is. Ze zijn echter wel bereid deze info met een gezondheidstoepassing te delen als dit van enig nut is. Er zijn echter gradaties van bereidwilligheid afhankelijk van het type informatie. Zo waren de respondenten weigerachtiger wat betreft het vrijgeven van de locatie-, audio- en videodata, dan wat betreft de data waar men van een gezondheidsapp kan verwachten dat hij ze verzameld - zoals lengte, gewicht en aantal stappen. De informatie in het centrum van de cirkel beschouwen de respondenten als medisch geheim en willen ze dan ook enkel delen met medisch bevoegden.

Die gradaties in de bereidwilligheid van de respondenten om al dan niet persoonlijke data te delen afhankelijk van het type informatie sluit aan bij de bevindingen van Klasnja e.a. (2009) waarbij de respondenten ook meer bezorgd waren over de GPS-data en de data die de microfoon verzamelde dan over de data die vergaard werden door de accelerometer en de barometer. Ook zij vonden net als onze respondenten het verzamelen van audio-data te persoonlijk en hebben bij het vrijgeven van locatiedata opnieuw, net als enkele van onze deelnemers, het gevoel gevolgd te worden. Daarenboven vreesden ook enkele deelnemers aan de studie van Klasnja e.a. (ibid.) voor negatieve gevolgen wanneer deze data in criminele handen terechtkomen. Een bekommernis die ook opdook in ons onderzoek. Motti en Caine (2014) stelden eveneens vast dat het verzamelen van de hartslag en polsslag niet als een bedreiging van iemands privacy werd ervaren. Ook Raij e.a. (2011) vonden dat hun respondenten het meest bezorgd waren over de inferenties over hun psychologische toestand.

5.3.2 Inschatting privaat karakter afhankelijk van het gebruik van de data

Niet alleen het type informatie speelt een rol bij de afweging van de mate van gevoeligheid, maar ook het gebruik dat er van gemaakt zal worden. Ten eerste gaat het hier om het gebruik dat de persoon in kwestie er zelf van kan maken. Hij is doorgaans bereid zijn persoonlijke data in te voeren in de app of het te laten registreren indien het hem iets oplevert: informatie over zijn eet- of slaappatroon, zijn looproute, -afstand en -snelheid of een gepersonaliseerde berekening zoals een BMI of het aantal verbrande calorieën. Ook uit de interviews van Shklovski e.a. (2014) bleken de respondenten het nut in te zien van een zekere mate van personalisering. Onze resultaten sluiten ook aan bij de resultaten van Klasnja e.a. (2009) die stelden dat wanneer de gebruikers gevraagd werden naar de aanvaardbaarheid van een bepaalde functionaliteit, zij een kosten-batenanalyse maakten van de voor- en nadelen die het gebruik van de toepassing hen opleverde.

Ten tweede speelt ook het gebruik dat anderen er van zullen maken een rol. Over het algemeen kunnen we stellen dat onze respondenten bereid zijn elk type informatie te delen zolang er geen misbruik van gemaakt wordt. De data mogen opgaan in het grote geheel om daaruit trends en inzichten te destilleren, maar mogen niet op een persoonlijke manier gebruikt worden om individuen te discrimineren. Zo zouden bijvoorbeeld alle mensen met een ongezonde levensstijl verplicht kunnen worden een hogere verzekeringsbijdrage te betalen of zou de werkgever zijn medewerker kunnen ontslaan omwille van choquerende foto's. Positieve zaken willen ze wel delen, in tegenstelling tot negatieve elementen zoals het alcoholgebruik. Omwille van de potentiële negatieve gevolgen vinden de respondenten het dan ook belangrijk dat anonimiteit gegarandeerd wordt. Dat sluit aan bij de instrumentele waarde van privacy (Vedder, 25.02.2015). De gebruikers hechten waarde aan hun privacy omdat ze op die manier negatieve gevolgen kunnen voorkomen. Men kan als denkoefening deze redenering natuurlijk ook omdraaien en stellen dat mensen met een gezonde levensstijl positief gediscrimineerd worden en de werknemer met flatterende foto's en goede contacten net meer kans maakt op promotie. Mag de

privacy met andere woorden wel geschonden worden indien dit een positieve uitkomst impliceert? Als we de redenering van Greenwald (2014) zouden volgen, hangt het eigenlijk niet af van het gebruik dat er van de persoonlijke informatie gemaakt wordt. Zodra er toezicht is - of in dit geval kennisname van iemands persoonlijke informatie - is de privacy namelijk al geschonden.

Het gebruik dat anderen er van zullen maken hangt logischerwijze samen met wie die andere is. We zien dan ook dat met een beperkte kring van vrienden en familie vrijwel alle persoonlijke informatie gedeeld mag worden. Het gaat hier wel degelijk om een beperkte kring van vrienden en familie, want de respondenten benadrukten zelf het onderscheid tussen vrienden en kennissen en het gezin en de ruimere familie met neven, nichten en tantes. De intentie informatie te delen is zoals Prasad e.a. (2012) het formuleren dus afhankelijk van de relatie die de gebruiker heeft met zijn vrienden en familie.

Onze respondenten waren ook bereid hun persoonlijke informatie met het medisch bevoegd personeel te delen. Dat zou namelijk een betere zorgverlening mogelijk maken, aangezien ze geloven dat alle informatie relevant kan zijn voor het stellen van de juiste diagnose. In de literatuur werd echter niet specifiek gepeild naar het doorgeven van data uit fitness- en gezondheidstoepassingen aan de behandelende arts.

De persoonlijke informatie mag eveneens gedeeld worden met de overheid en onderzoekers als dit ten goede komt aan de maatschappij. Voor het algemeen belang mogen de persoonlijke data dus gedeeld worden, hoewel verschillende respondenten toch anonimiteit vereisen. Hoewel, zoals de deelnemers aan de studie van Raij e.a. (2011), ook onze respondenten minder bezorgd waren wanneer hun persoonlijke data alleen met onderzoekers zouden worden gedeeld dan met het grote publiek.

Wat betreft het vrijgeven van (anonieme) persoonlijke data aan commerciële bedrijven, zagen we twee partijen tegenover elkaar staan. De ene groep was niet bereid zijn informatie prijs te geven zodat een commercieel bedrijf daar vervolgens winst mee kon maken. Bij de andere groep heerste het besef dat ook de commerciële bedrijven hun informatie ergens moeten halen. Zij legden ze zich er bij neer dat hun anonieme data verzameld en verkocht werden. Het

feit dat ze dat beseffen neemt de bezorgdheden echter wel niet weg. Dit wantrouwen tegenover commerciële bedrijven is geen goede basis voor het gebruik van allerlei apps, zo stellen Shklovski e.a. (2014).

De meeste van onze respondenten wilden de gevoeligere informatie in de cirkel (zie figuur 9) enkel met het publiek delen indien hun data geanonimiseerd waren, net zoals bij het onderzoek van Raij e.a. (2011) en Prasad e.a. (2012). Dan nog stelden enkelen zich de vraag welk nut het had om hun data voor het grote publiek beschikbaar te stellen. Welk gebruik zouden zij er van kunnen maken?

5.3.3 Inschatting van privaat karakter afhankelijk van de omgang met de data

Dat anonieme data wel in de openbaarheid gebracht mogen worden, sluit aan bij het laatste aspect dat een rol speelt bij de afweging van het al dan niet delen van persoonlijke informatie: de manier waarop er met de data omgegaan wordt. Indien anonimiteit geboden kan worden, zijn de respondenten meer bereid persoonlijke informatie te delen. Zo hebben ze het gevoel dat het eventuele misbruik en de negatieve gevolgen waarover hierboven al sprake was niet of minder mogelijk zijn. Als hun naam bijvoorbeeld niet verbonden wordt aan hun medicatiegebruik kan niemand weten dat zij het zijn die lijden aan een bepaalde ziekte. Zo riskeren ze niet anders behandeld te worden. Het belang van anonimiteit is niet verrassend, en sluit aan bij de bevindingen van Raij e.a. (2011) en Prasad e.a. (2012). Het is wel belangrijk te benadrukken dat de naam an sich, los van alle informatie die daaraan gekoppeld kan worden, niet als privé wordt beschouwd.

Naast de anonimiteit van de gegevens, bleek ook uit de literatuur dat de mate van abstractie van de data en de beperkte duur van het bijhouden ervan de bereidheid tot delen beïnvloedde. Met een hogere mate van abstractie wordt het doorgeven van minder precieze gegevens bedoeld. Bijvoorbeeld een daggemiddelde van de bloeddruk in plaats van ieder uur de bloeddruk te meten. Of door bijvoorbeeld locatiegegevens niet te vergezellen van

tijdsaanduidingen. Wanneer hier bij de respondenten echter naar gepeild werd, gaven zij aan dat zolang de data anoniem doorgegeven zouden worden, een hogere graad van abstractie hen niet meer vertrouwen zou inboezemen. Ook geloofden ze niet dat een beperking op de duur van het bijhouden van de data hen meer vertrouwen zou bieden.

Deze bevindingen zijn tegengesteld aan de resultaten van Raij e.a. (2011) en Prasad e.a. (2012) waar de mate van abstractie de bezorgdheden wel kon temperen. Daarnaast sluiten ze ook niet aan bij Klasnja e.a. (2009) die merkten dat de bekommernissen afnamen indien de data maar voor zolang als nodig bijgehouden zouden worden. Dat heeft waarschijnlijk te maken met methodologische verschillen. De onderzoeken die wel merkten dat deze factoren van invloed waren, waren gebruikersstudies waarbij de deelnemers effectief een gezondheidsapp gebruikten en bepaalde informatie op een abstractere manier konden doorgeven (Prasad e.a., 2012) of op een overzichtelijke manier met hun data geconfronteerd werden alvorens ze een survey invulden (Raij e.a., 2011) of een interview gaven (Klasnja e.a., 2009). Ons onderzoek bestond louter uit interviews zonder enige visualisatie of mogelijkheid om de deelnemers effectief gebruik te laten maken van een toepassing die het mogelijk maakt abstractere data door te geven. Spreken over een bepaald gedrag is niet noodzakelijk gelijk aan het stellen van dat gedrag. Hiermee bedoel ik dat de deelnemers misschien wel meer bereid zouden zijn hun data te delen als dit kon op een abstractere manier of indien de data voor een beperkte duur werden bijgehouden.

We kunnen besluiten dat de bevraagde natuurlijke gebruikers niet alle soorten informatie die typische fitness- en gezondheidstoepassingen verzamelen over dezelfde kam scheren wanneer hen gevraagd wordt welke informatie ze privé vinden. Bepaalde data zoals het aantal stappen zijn beduidend minder gevoelig dan medische data zoals het medicatiegebruik en diagnoses. Wanneer deze data echter niet misbruikt kunnen worden en alleen toegankelijk zijn voor bevoegden, nemen de bezorgdheden af. Als het vrijgeven van de data de gebruiker daarenboven iets oplevert - zoals een gepersonaliseerde berekening van het aantal calorieën - is hij eveneens meer bereid deze data met een app te delen. Ook wanneer de data geanonimiseerd zijn, zijn de gebruikers meer bereid

data vrij te geven. Indien de gebruiker zelf bewust kan kiezen om persoonlijke informatie al dan niet te delen in tegenstelling tot het automatisch verzamelen van data, nemen de bekommernissen eveneens af. Deze bevindingen bieden steun voor het contextuele integriteitsmodel van Nissenbaum (in Shklovski e.a., 2014). Zo is voor een bepaald type informatie niet eenduidig uit te maken of dit privé is of niet. Het is heel erg afhankelijk van het gebruik dat ervan gemaakt zal worden en de manier waarop er mee omgegaan wordt.

5.4 Strookt wat de natuurlijke gebruikers als privé beschouwen ook met hoe er gebruik wordt gemaakt van hun persoonlijke data?

Om enigszins antwoord te krijgen op de vraag of de overtuigingen van de respondenten met betrekking tot wat ze privé achten overeenstemmen met hun gebruik van gezondheidstoepassingen, werd de inhoud van een fictief privacybeleid overlopen. De deelnemers verklaren zich namelijk doorgaans akkoord met zulke privacyvoorwaarden. Maar strookt de inhoud waar ze zich akkoord mee verklaren ook met hun bovenvermelde privacyopvattingen?

Eerst en vooral blijkt, zoals ook reeds uit verschillende onderzoeken naar voren is gekomen (Shklovski e.a., 2014; Coppens e.a., 2014; Symantec, 2015; Liu, 2014), dat de respondenten nooit, tenzij beroepsmatig, het uitgebreide privacybeleid van hun gezondheidstoepassing lezen. Ze gaan er dus blindelings mee akkoord. Dit vooral omwille van de lengte van de beschrijving en het ontbreken van een andere keuze dan het goedkeuren ervan. Deze motivaties bleken ook bij Liu (2014) en Shklovski e.a. (2014) verklarende factoren. Ook de moeilijkheidsgraad van de tekst speelde een rol, net als bij Liu (2014). Een ander obstakel voor onze respondenten was de taal: een privacybeleid is namelijk vaak in het Engels geschreven. Ten slotte veronderstelden onze deelnemers dat wat er in zou staan wel in orde zou zijn.

Het feit dat de respondenten de gebruiksvoorwaarden meestal nooit lezen, ondanks hun wens voor een beperkt en goed gebruik van hun persoonlijke data, sluit aan bij de privacyparadox (Norberg e.a., 2007; Büschel e.a., 2014; Baek, 2014; Coppens e.a., 2014; Shklovski

e.a., 2014). Ze willen graag controle over hun data, maar benutten die mogelijkheid niet ten volle. Zoals hierboven al vermeld werd, beschouwen ze het deels als hun eigen verantwoordelijkheid om hun privacy te beschermen en geen persoonlijke data vrij te geven als ze dit niet willen. Ondanks het feit dat ze dus niet al hun data zomaar wensen prijs te geven, nemen ze dus toch niet altijd het heft in handen. Hun gedragingen weerspiegelen met andere woorden hun overtuigingen niet.

Na het overlopen van het fictieve privacybeleid waarin beschreven stond wat de ficitieve gezondheidsapp zou verzamelen en hoe hij er gebruik van zou maken, waren de meeste respondenten bereid dit beleid goed te keuren. Dat is tegengesteld aan de bevindingen van Shklovski e.a. (2014), waar de respondenten na het overlopen van het privacybeleid van een spelletjesapp het gevoel hadden misleid te zijn. Dit is mijn inziens te wijten aan het feit dat het in ons onderzoek om een gezondheidsapp ging, in tegenstelling tot de spelletjesapp bij Shklovski e.a. (2014). Daarnaast werden er in het fictieve privacybeleid dat in ons onderzoek werd gebruikt, andere zaken vermeld. De data die de fictieve app in ons onderzoek verzamelt, is namelijk nodig voor het verlenen van de functionaliteit. Er wordt uitgelegd hoe de data gebruikt worden en met wie ze gedeeld zullen worden. Hierbij wordt benadrukt dat alleen gedeïdentificeerde data verkocht zullen worden. De spelletjesapp uit het onderzoek van Shklovski e.a. (2014) verzamelde daarentegen overbodige informatie voor de functionaliteit die hij beloofde, zoals de locatiegevens. Hoewel sommigen, zoals reeds vermeld, niet wilden dat hun data doorverkocht werden aan derden zodat het bedrijf achter de toepassing er winst op kon maken, zien we deze bezorgdheid niet opduiken wanneer het fictieve privacybeleid overlopen werd. Hier stond nochtans in dat de gedeïdentificeerde data doorverkocht kunnen worden. In de meeste gevallen keurt men het privacybeleid goed zonder het te lezen. Desondanks blijkt de inhoud van het fictieve privacybeleid toch grotendeels overeen te stemmen met hoe ze willen dat er gebruik wordt gemaakt van hun data, aangezien ze allemaal bereid zijn het goed te keuren. Vermits het fictieve beleid opgesteld werd op basis van de privacyvoorwaarden van een aantal populaire fitness- en gezondheidsapps, hebben we redenen om te geloven dat het gebruik

van hun data door de apps die ze gebruiken wel strookt met hun opvattingen.

5.5 Hoe meer vertrouwen genereren in fitness- en gezondheidstoepassingen?

Aangezien we een grotere adoptiegraad van fitness- en gezondheidstoepassingen willen bekomen en dit mogelijks verhinderd wordt als de gebruikers niet zeker weten dat er op een goede manier met hun persoonlijke gegevens wordt omgegaan, werden de respondenten gevraagd hoe we meer vertrouwen kunnen genereren in zulke toepassingen. De meeste respondenten stelden dat ze in de toepassingen die ze gebruiken wel al een behoorlijk vertrouwen hebben. Dat is eigenlijk wat je zou verwachten op basis van Nguyen (2008) en Klasnja (2009). Zij veronderstelden namelijk dat zij die al vertrouwd zijn met een bepaalde technologie hier minder bezorgd over zijn. Daarom zou toekomstig onderzoek kunnen nagaan wat niet-gebruikers tegenhoudt om fitness- en gezondheidstoepassingen te gebruiken. Niettegenstaande het heersende vertrouwen, hadden de respondenten wel enkele suggesties waardoor de apps hen meer vertrouwen zouden kunnen inboezemen en een paar verklaringen voor hun bestaande vertrouwen. Twee respondenten benadrukken wel dat 100% vertrouwen in een technologie nooit mogelijk is.

Zoals hierboven al aan bod kwam, blijkt het anonimiseren van de persoonlijke data bij te dragen tot minder bezorgdheid. Mayer-Schönberger en Cukier (2013) beschreven echter hoe we in een big data-tijdperk niet meer volledig kunnen steunen op de de-anonimisering omdat het door het koppelen van verschillende datasets mogelijk is de identiteit af te leiden uit de geanonimiseerde data. Wanneer onze respondenten echter op de hoogte gebracht werden van de mogelijkheid tot reïdentificatie, maakte het hen niet bezorgder. Ze geloofden namelijk niet dat zij daar effectief het slachtoffer van zullen worden. Een tweede factor die momenteel al bijdraagt tot meer vertrouwen bij de respondenten is de naamsbekendheid, de look en de gebruiksvriendelijkheid van de app of toepassing. Aan een app waar ze nog nooit van gehoord hebben en

die er onbetrouwbaar uitziet, zullen ze geen data vrijgeven. Ten derde bleek uit de anekdotes van enkele respondenten dat ook het persoonlijk contact met de mensen achter de toepassing veel vertrouwen inboezemt. Ten slotte blijkt uit de interviews dat verschillende respondenten geloven dat ze impliciet toestemming geven aan derden om hun data te gebruiken door de data online te plaatsen. Dat betekent daarom echter niet dat zij de mensen die hun data gebruiken ook 100% vertrouwen. Verschillende respondenten halen dan ook het gebruik van interactieve schuifbalkjes en pushberichten aan waarbij de ontwikkelaars telkens expliciet toestemming vragen voor het gebruik van onder andere de locatiedata. Idealiter wordt hierbij extra uitleg verschaft over het waarom en het specifieke gebruik van de nodige data. Dit expliciet verlenen van toestemming voor specifieke functionaliteiten op basis van de nodige informatie, kan dus mogelijks ook extra vertrouwen scheppen in fitness- en gezondheidstoepassingen.

Het expliciet verlenen van toestemming kan eigenlijk als een interactieve versie van het *notice and consent*-principe beschouwd worden, dat ook al voorgesteld werd door Liu (2014). Het *notice and consent*-principe voorziet de gebruiker van informatie op basis waarvan hij vervolgens beslist zich hier al dan niet mee akkoord te verklaren. Momenteel wordt die informatie verschaft in de vorm van een uitgebreid privacybeleid en geeft de gebruiker vaak toestemming zonder het te lezen. Als we dit korter en interactiever maken, zal de gebruiker wellicht beter geïnformeerd zijn en explicieter toestemming geven dan nu vaak het geval is. Hoewel de kans bestaat dat hij nog steeds geen tijd zal nemen voor het doornemen van de informatie. Omdat de gebruikers hun data al dan niet willen vrijgeven afhankelijk van het gebruik dat ervan gemaakt zal worden, is het nodig om het gebruik duidelijk te specifiëren zodat de gebruiker bewust kan beslissen of hij zijn informatie al dan niet wenst vrij te geven. Ondanks het feit dat deze informatie ook vandaag al beschikbaar is in de uitgebreide gebruiksovereenkomsten en privacyvoorwaarden, worden die vandaag de dag nauwelijks gelezen en verklaart de doorsnee gebruiker zich er mee akkoord zonder het te bekijken. Daarom zie ik heil in deze explicietere en interactievere manier van akkoord verklaren.

Volgens Mayer-Schönberger en Cukier (2013) en Bertels (11.03.2015) is het geven van informatie in een big data-context echter moeilijk vol te houden. Vaak is op voorhand namelijk nog niet duidelijk hoe bepaalde data inzichten kunnen opleveren. Het liefst verzamelen data-analisten zoveel mogelijk data en komen ze daarna tot interessante conclusies en verdere toepassingen.

Daarom moeten we misschien streven naar het bieden van 100% transparantie zodat de gebruiker niet op voorhand al moet goedkeuren waar zijn data voor gebruikt mogen worden, maar dat hij het gebruik op de voet kan volgen en het vrijgeven van zijn data een halt kan toeroepen vanaf het moment dat hij vindt dat het niet meer bij zijn overtuigingen aansluit. Dat kan misschien door de gebruiker een overzicht te bieden van wie welke data te zien krijgt, zoals de interface uit Prasads onderzoek (zie figuur 4 en 5). Een andere mogelijkheid is het toekennen van privacylabels aan de verschillende apps die duidelijk maken of de privacy al dan niet gewaarborgd wordt. Dit idee tot het bevorderen van de transparantie sluit aan bij de bepalingen uit de nieuwe Europese verordening die meer transparantie eisen over de dataverwerking, zodat de gebruiker meer controle en invloed heeft over zijn data (Vedder, 25.02.2015; Valcke, 04.03.2015). De bovenvermelde ideeën zijn daarenboven ook illustraties van de *privacy-* en *transparancy-enhancing technologies* die Van Lieshout e.a. (2011) voorstellen en die de nieuwe Europese verordening ook wil stimuleren.

Naast deze suggesties van de respondenten polste de interviewer of ook een strengere regulering meer vertrouwen zou genereren. Dat blijkt niet noodzakelijk het geval. Verschillende respondenten stelden namelijk dat een strengere straf misbruik echter niet onmogelijk maakt. Dit is tegengesteld aan de resultaten van Shklovski e.a. (2014) waar de deelnemers wel geloofden in een strengere regulering. Ook de EU zet hier op in, want ze heeft in de nieuwe verordening een artikel toegevoegd dat zware boetes oplegt voor iedereen die zich niet houdt aan de regels die vooropgesteld staan in de verordening (Valcke, 04.03.2015).

Een laatste aspect dat ik wil aanhalen dat ook bijdraagt tot de mate van vertrouwen is het feit dat de natuurlijke gebruikers die aan dit onderzoek deelnamen, nooit zware negatieve gevolgen hebben ondervonden van het vrijgeven van hun data. Met uitzondering van

twee respondenten die naar aanleiding van een privacyinbreuk hun privacyinstellingen aanpasten in restrictieve zin. Het vertrouwen dat er nu heerst, is, zoals Shklovski en zijn collega's (2014) stellen, gebaseerd op de (vrijwillige) onwetendheid en het aanvaarden van de huidige praktijken omdat er geen andere keuze is. Dat onwetendheid het vertrouwen bevordert, is belangrijk als we denken aan sensibiliseringscampagnes om de gebruikers op de hoogte te brengen van de gevaren die het online vrijgeven van persoonlijke data inhoudt. Dat zal namelijk het vertrouwen bemoeilijken. Het is natuurlijk nodig om de samenleving mediawijsheid bij te brengen, maar we moeten ons ervan bewust zijn dat het confronteren van de gebruikers met negatieve gevolgen - en hen met andere woorden uit de onwetendheid halen- repercussies heeft voor het vertrouwen dat de gebruikers zullen hebben in de virtuele wereld. Ik pleit niet voor het verder stimuleren van de heersende onwetendheid, ik suggereer alleen dat wanneer we de gebruiker inlichten over de risico's, dat hem mogelijk kan afschrikken en zijn vertrouwen kan aantasten. Daardoor zal hij misschien geen gebruik meer willen maken van allerlei apps en toepassingen. Daarom zal het belangrijk zijn de gebruiker ook de mogelijkheid te bieden en hem ervan te overtuigen dat hij in staat is controle uit te oefenen over zijn data. Hiervoor moeten we privacyvriendelijke en transparante toepassingen aanbieden, zodat gebruikers op basis van de nodige informatie kunnen beslissen hun persoonlijke data vrij te geven of terug te trekken.

5.6 Limieten en toekomstig onderzoek

De bijdrage die dit onderzoek wilde leveren, was het in kaart brengen van de attitudes van natuurlijke gebruikers van fitness- en gezondheidstoepassingen ten opzichte van dataverzameling. Daarbij werd verondersteld dat de natuurlijke gebruikers door hun ervaring met zulke toepassingen aanbevelingen konden hebben voor toekomstige, meer privacyvriendelijke fitness- en gezondheidsapps.

Een eerste beperking van dit onderzoek heeft te maken met de keuze voor interviews. Hoe de gebruikers de toepassingen willen gebruiken is niet noodzakelijk gelijk aan hoe ze in het interview

beschreven gezondheidstoepassingen te gebruiken. Toekomstig onderzoek zou een volledig generatief onderzoek kunnen zijn waarin de deelnemers wordt gevraagd een concrete transparante privacyvriendelijke app voor de toekomst te ontwikkelen. Deze mogelijkheid paste nu niet binnen het tijdsbestek van deze masterproef, aangezien naast de latente noden ook naar huidige opinies met betrekking tot dataverzameling werd gepeild.

Ten tweede was het vaak moeilijk voor de respondent om een antwoord te geven op de vraag welke informatie een fictieve alleswetende gezondheidsapp al dan niet mocht verzamelen. Daarom is het aan te raden in vervolgonderzoek gebruik te maken van scenario's. De resultaten van dit onderzoek kunnen wel een aanzet zijn tot de ontwikkeling van mogelijke scenario's.

Ten slotte zou toekomstig onderzoek kunnen nagaan welke factoren de niet-gebruikers tegenhouden in hun adoptie van fitness- en gezondheidstoepassingen. Heeft dit met privacyissues te maken?

6. Conclusie

De big data die fitness- en gezondheidstoepassingen opleveren, bieden heel veel potentieel. Niet alleen kunnen de toepassingen de gebruiker aanmoedigen om gezonder te leven, ook de arts-patiëntrelatie wordt verlicht. De big data kunnen bovendien interessante inzichten opleveren zodat we preventief actie kunnen ondernemen. Maar daarvoor moeten eerst enkele belangrijke hindernissen overwonnen worden. Ten eerste staan de artsen momenteel nog wat weigerachtig tegenover het gebruik van gezondheidstoepassingen in de gezondheidszorg en is de interpretatie vaak niet eenvoudig voor zij die daarin niet geschoold zijn. Ten tweede maakt de volledige bevolking nog geen gebruik van zulke toepassingen. Ten derde zullen we ook aandacht moeten besteden aan de privacy van de gebruikers. De privacy staat namelijk onder druk door de alomtegenwoordige dataverzameling. Als we echter een grotere adoptiegraad willen bereiken van fitness- en gezondheidstoepassingen, zullen we ervoor moeten zorgen dat de gebruikers er meer vertrouwen in hebben dat hun privacy gewaarborgd wordt. Zo wierp de vraag zich op hoe de gebruikers van

fitness- en gezondheidstoepassingen denken over hun privacy in de context van zulke toepassingen, welke informatie zij als privé beschouwen en hoe we hen meer vertrouwen kunnen bieden.

De bijdrage die dit onderzoek wilde leveren, bestond erin dat hier natuurlijke gebruikers bevraagd werden, in tegenstelling tot ander onderzoek waar deelnemers een fitnesstoepassing gebruikten op vraag van de onderzoekers. Uit ons onderzoek bleek dat de deelnemers zich onbewust wel bewust zijn van de dataverzameling en zich hierbij hebben neergelegd. Ze staan er echter niet negatief tegenover, veelal omdat ze er nog geen kwalijke gevolgen van ondervonden hebben. Wat we daarnaast zowel uit de literatuurstudie als uit dit onderzoek vooral moeten onthouden is het contextuele karakter van het privacybegrip van de gebruiker. Welke informatie iemand als privé beschouwd is heel erg afhankelijk van het gebruik dat ervan gemaakt wordt.

Om de gebruiker daarom bij de bescherming van zijn privacy tegemoet te komen, is het noodzakelijk hem van de nodige informatie te voorzien zodat hij zelf kan beslissen of hij zijn data voor die doeleinden beschikbaar stelt. We kunnen in lijn met de *privacy by design*-filosofie de privacybescherming al in de technologie inbouwen, zoals de Europese verordening voorschrijft en zoals onderzoekers aanmoedigen. We moeten de gebruiker de controle geven over zijn eigen data door hem goed te informeren, hoewel dit in een big data-tijdperk niet vanzelfsprekend zal zijn. We moeten de gebruikers op de hoogte brengen van de gevaren van onzorgvuldige privacybescherming, maar hen dus zeker ook oplossingen aanreiken die hen zo vertrouwen kunnen bieden. Zo komen we misschien tot een grotere adoptiegraad van fitness- en gezondheidstoepassingen zodat we de voordelen ervan ten volle kunnen benutten.

Referenties

Apple (2015). *Gezondheid. Een compleet nieuwe manier om gezondheids- en fitnessinformatie te gebruiken.* [11.04.2015, Apple: https://www.apple.com/nl/ios/whats-new/health/].

Apple (2015). *ResearchKit*. [11.04.2015, Apple: https://www.apple.com/researchkit/].

Azumio Inc (2015). *Instant Heart Rate.* [06.05.2015, Google: https://play.google.com/store/apps/details?id=si.modula.android.instantheartrate].

Baek,Y.M. (2014). Solving the privacy paradox: A counter-argument experimental approach. *Computers in Human Behavior, 38*, pp. 33-42.

Baviux (2015). *Lady Pill Reminder.* [11.04.2015, Baviux: http://baviux.com/app/lady-pill-reminder/].

Becker, S., Kribben, A., Meister, S., Diamantidis, C.J., Unger, N., & Mitchell, A. (2013). User Profiles of a Smartphone Application to Support Drug Adherence – Experiences from the iNephro Project. *PlOS ONE,* 8 (10), pp. 1-6.

Basha, B. (2015). *Birth Control Pill.* [06.05.2015, Google: https://play.google.com/store/apps/details?id=com.benbasha.pill].

Bertels, N. (Leuven, 11.03.2015). *Gastcollege ICT-recht: Big Data.* [Gastcollege N. Bertels].

Büschel, I., Mehdi, R., Cammilleri, A., Marzouki, Y., & Elger, B. (2014). Protecting Human Health and Security in Digital Europe: How to Deal with the "Privacy Paradox"? *Science and Engineering Ethics, 20*(3), pp.639-658.

Bushhousen, E. (2014). The Quantified Self Movement and Hospital Librarians. *Journal of Hospital Librarianship, 14*(1), pp. 88-93.

Cafazzo, J.A., Casselman, M., Katzman, D.K., Palmert, M.R. (2012). BANT: An mHealth App for Adolescent Type I Diabetes – A Pilot Study. *Poster Abstracts, 50*, pp. S77-S78.

Carrera, P.M., & Dalton, A.R.H. (2013). Do-it-yourself Healthcare: The current landscape, prospects and consequences. *Maturitas, 77*(1), pp. 37-40.

Carroll, A. (2014). *Medical Data Sharing and Your Tracker*. [11.04.2015, Youtube: https://www.youtube.com/watch ?v=LVQwUj1qP8s].

Chen, M., Mao, S., M., Zhang, Y., & Leung, V.C.M. (2014). *Big Data – Related Technologies, Challenges and Future Prospects*. London: Springer.

Commissie voor de bescherming van de persoonlijke levenssfeer (2009). *Advies uit eigen beweging inzake RFID*. [06.05.2015, http://www.privacycommission.be/sites/privacycommission/ files/documents/advies_27_2009_0.pdf].

Consolvo, S., Klasnja, P., McDonald, D.W., Avrahami, D., Froehlich, J., LeGrand, L., Libby, R., Mosher, K., & Landay, J.A. (2008). Flowers of a Robot Army? Encouraging Awareness & Activity with Personal, Mobile Displays. *UbiComp '08*, pp. 54-63.

Consumer Health Information Corporation (2008). *Motivating Patients to Use Smartphone Health Apps*. [06.05.2015, http://www.consumer-health.com/press/2008/NewsRelease SmartPhoneApps.php].

Coppens, P., Veeckman, C., & Claeys, L. (2014). Privacy in location-based services: user scripts & user practices. Nog niet geplubliceerd.

Courtois, C. (18.11.2014). *Communicatiewetenschappelijke onderzoeksdesigns: module kwalitatief onderzoek – analyse en rapporteren.* [Hoorcollege C. Courtois].

Cukier, K., & Mayer-Schönberger, V. (2013). The Rise of Big Data – How It's Changing the Way We Think About the World. *Foreign Affairs, 92*(3), pp. 28-40.

Dehaene, W., & Reynaert, P. (2014). Chips: meer, sneller, kleiner en wat doen we met de batterij? In B. Pattyn, & P. d'Hoine (Reds.), *Herdenken en vooruitgaan, XXI, Lessen voor de eenentwintigste eeuw* (pp. 63-70). Leuven: Universitaire Pers Leuven.

Dehzad, F., Hilhorst, C., de Bie, C., & Claassen, E. (2014). Adopting Health Apps, What's Hindering Doctors and Patients? *Health, 6*(16), pp. 2204-2217.

Diebson, F. X. (2012). *A Personal Perspective on the Origin(s) and Development of "Big Data": The Phenomenon, the Term, and the Discipline.* [12.04.2015, Diebson: http://www.ssc.upenn.edu/~fdiebold/papers/paper112/Diebold_Big_Data.pdf].

EarthFlare (2014). *Med Helper Pill Reminder*. [06.05.2015, Google: https://play.google.com/store/apps/details?id=com.earthflare.android.medhelper.lite].

Entelechyasia (14.12.2012). *Smartphone sport up to 19 sensors*. [11.04.2015, Wordpress: http://entelechyasia.com/2012/12/14/smartphones-sport-up-to-19-sensors/].

Etlinger, S. (2014). *What do we do with all this big data?* [12.04.2015, TED Conferences: https://www.ted.com/talks/susan_etlinger_what_do_we_do_with_all_this_big_data]

European Voice (2014). *Date: the new currency?* Brussel: European Voice [11.04.2015, European Voice: http://blog.digital.telefonica.com/wp-content/uploads/2014/06/Data-the-new- currency.pdf].

Europese Commissie (10.04.2014). *Green Paper on mobile Health ("mHealth")*. Brussel: Europese Commissie.

Fitbit (2015). *Fitbit.* [11.04.2015, Fitbit: https://www.fitbit.com].

FitnessKeeper (10.04.2015). *Runkeeper*. [11.04.2015, Google: https://play.google.com/store/apps/details?id=com.fitnesskeeper.runkeeper.pro].

Flurry (19.06.2014). *Health and Fitness Apps Finally Take Off, Fueled by Fitness Fanatics.* [12.04.2015, Flurry: http://www.flurry.com/blog/flurry-insights/health-and-fitness-apps-finally-take-fueled-fitness-fanatics#.VSqJj7OsW-A].

Fraser, H., Kwon, Y., & Neuer, M. (2011). *The future of connected health devices – liberating the Information Seeker*. New York: IBM.

Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management, 35*(2), pp. 137-144.

Golia, N., & O'Donnell, A. (2011). Telematics' Drive Toward Acceptance. *Insurance & Technology, 36*(3).

Greenspun, H. (2013). *Infographic – mHealth – A check-up on consumer use.* [12.04.2015, Deloitte: http://www2.deloitte.com/us/en/pages/life-sciences-and- health-care/articles/center-for-health-solutions-consumer- adoption-of-mhealth.html].

Greenwald, G. (2014). *De Afluisterstaat. Edward Snowden, de NSA en de Amerikaanse Spionage- en Afluisterdiensten.* Amsterdam: Lebowski Publishers.

Guest, G., Bunce, A., & Johnson, L. (2006). How Many Interviews Are Enhough? An Experiment with Data Saturation and Variability. *Field Methods, 18*(1), pp. 59-82.

Icahn School of Medicine at Mount Sinai (2015). *Asthma Health by Mount Sinai.* [06.05.2015, Apple: https://itunes.apple.com/WebObjects/MZStore.woa/wa/viewSoftware?id=972625668&mt=8&ls=1&v0=www-us-researchkit-itms-asthma-health].

Jawbone (2015). *Jawbone UP*. [11.04.2015, https://jawbone.com/up].

Klasnja, P., Consolvo, S., Choudhury, T., Beckwith, R., & Hightower, J. (2009). Exploring Privacy Concerns about Personal Sensing. *Pervasive Computing,* pp. 176-183.

Lane, J.E., & Finsel, B.A. (2014). Fostering Smarter Colleges and Universities: Data, Big Data, and Analytics. In J.E. Lane (Red.), *Building a Smarter University – Big Data, Innovation,and Analytics* (pp. 3-26). Albany: State University of New York Press.

Lin, J. J., Mamykina, L., Lindtner, S., Delajoux, G., & Strub, H. B. (2006). Fish'n'Steps: Encouraging physical activity with an interactive computer game. *UbiComp 2006: Ubiquitous Computing*, pp. 261-278.

Liu, Y. (2014). User control of personal information concerning mobile-app: Notice and consent? *Computer Law & Security Review: The International Journal of Technology Law and Practice, 30*(5), pp. 521-529.

Madsen, F., Ladelund, S., & Linneberg, A. (2014). High Levels of Bed Occupancy Associated With Increased Inpatient And Thirty-Day Hospital Mortality in Denmark. *Health Affairs, 33*(7), pp. 1236-1244.

Martin, J.A.C., Martinez-Perez, B., de la Torre-Diez, I., & Lopez-Coronado, M. (2014). Economic Impact Assessment from the

Use of Mobile App for the Self-management of Heart Diseases by Patients with Heart Failure in a Spanish Region. *Journal of Medical Systems, 38*(9), pp.1-7.

Martínez-Pérez, B., De La Torre-Díez, I., & López-Coronado, M. (2015). Privacy and Security in Mobile Health Apps: A Review and Recommendations. *Journal of medical systems, 39*(1), pp. 1-8.

Mayer-Schönberger, V., & Cukier, K. (2013). *De Big Data Revolutie. Hoe de data-explosie al onze vragen gaat beantwoorden.* Amsterdam: Maven Publishing.

Markowetz, A., Blaszkiewicz, K., Montag, C., Switala, C., & Schlaepfer, T. E. (2014). Psycho-Informatics: Big Data shaping modern psychometrics. *Medical Hypotheses, 82*(4), pp. 405-411.

MediSafe (2015). *MediSafe Meds & Pill Reminder.* [06.05.2015, MyFitnessPal: https://www.myfitnesspal.com/].

Motti, V.G., & Caine, K. (2014). User's Privacy Concerns About Wearables: impact of form factor, sensors and type of data collected. *fc15.ifca.ai,* pp. 1-15.

MyFitnessPal (2015). *MyFitnessPal.* [11.04.2015, MyFitnessPal: https://www.myfitnesspal.com/].

Nakajima, T., & Lehdonvirta, V. (2013). Designing motivation using persuasive ambient mirrors. *Personal and ubiquitous computing, 17*(1), pp. 107-126.

Navetta, D. (2014). Legal Implications of Big Data. *The Computer & Internet Lawyer, 31*(1), pp. 1-5.

Netatmo (2015). *JUNE.* [11.04.2015, Netatmo: https://www.netatmo.com/june].

Nguyen, D.H., Kobsa, A., & Hayes, G.R. (2008). An Empirical Investigation of Concerns of Everyday Tracking and Recording Technologies. *UbiComp '08*, pp. 182-191.

Norberg, P.A., Horne, D.R., & Horne, D.A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *The Journal of Consumer Affairs, 41*(1), pp. 100-126.

Ola, O., & Sedig, K. (2014). The Challenge of Big Data in Public Health: An Opportunity for Visual Analytics. *Online journal of public health informatics, 5*(3), pp. 1-21.

Peuteman, A., & Pironet, E. (11.03.2015). De meetbare mens. De voor- en nadelen van apps. *Knack*, pp. 86-90.

Prasad, A., Sorber, J., Stablein, T., Anthony, D., & Kotz, D. (2012). Understanding Sharing Preferences and Behavior for mHealth Devices. *WPES '12*, pp. 117-128.

PwC (2013). *Socio-economic impact of mHealth: An assessment report for the European Union.* [06.05.2015, http://www.gsma.com/ connectedliving/wp-content/uploads/2013/06/Socio- economic_impact-of-mHealth_EU_14062013V2.pdf].

Raij, A., Ghosh, A., Kumar, S., & Srivastava, M. (2011). Privacy Risks Emerging from the Adoption of Innocuous Wearable Sensors in the Mobile Environment. *CHI 2011*, pp. 11-20.

Research2guidance (06.05.2014). *mHealth App Developer Economics 2014 – The State of the Art of mHealth App Publishing*, pp. 16-17.

Research Now (17.03.2015). *Are mobile medical apps good for our health? A new study by Research Now reveals that doctors and patients say yes.* [12.04.2015, Research Now: http://www.researchnow.com/en-US/PressAndEvents/ News/2015/march/research-now-study- are-mobile-medical-apps-good-for-our-health-infographic.aspx?language=en- US].

Runtastic (2015). *Runtastic Heart Rate Monitor.* [06.05.2015, Google:https://play.google.com/store/apps/details?id=com.ru ntastic.android.heartrate.lite].

Shklovski, I., Mainwaring, S.D., Skuladottir, H.H., & Borgthorsson, H. (2014). Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use. *CHI 2014*, pp. 1-10.

Sleeswijk Visser, F., Stappers, P.J., van der Lugt, R., & Sanders, E.B.N. (2005). Contextmapping: experiences from practice, *CoDesign: International Journal of CoCreation in Design and the Arts, 1*(2), pp. 119-149.

Smolan, R., & Erwitt, J. (2012). *The Human Face of Big Data*. Californië: Against All Odds Productions.

Steinhubl, S.R., Muse, E.D., & Tropol, E.J. (2013). Can Mobile Health Technologies Transform Health Care? *JAMA,310*(22), pp. 2395-2396.

Syed, Z., Scirica, B.M., Mohanavelu, S., Sung, P., Michelson, E.L., Cannon, C.P., Stone, P.H., Stultz, C.M., & Guttag, J.V. (2009). Relation of Death Within 90 Days of Non-ST-Elevation Acute Coronary Syndromes to Variability in Electrocardiographic Morphology. *The American Journal of Cardiology, 103*(3), pp. 307-311.

Symantec (2015). *State of Privacy Report 2015*. [12.04.2015, Symantec: http://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf].

Valcke, P. (04.03.2015). *ICT-recht: Privacy – recht op vergetelheid*. [Hoorcollege professor P. Valcke].

Van der Meer, B. (Leuven, 13.03.2015). *Media en Geweld: Recherchepsychologie - Dreigingsmangement & de Rol van Media en Communicatie.* [Gastcollege B. Van der Meer].

Van Lieshout, M., Kool, L., van Schoonhoven, B., & de Jonge, M. (2011). Privacy by Design: an alternative to existing practice in safeguarding privacy. *Info, 13*(6), pp. 55-68.

Vanhaelewyn, B., Pauwels, G., Maes, M., & De Marez, L. (2014). *iMinds – digimeter 2014.* [11.04.2015, iMinds: https://www.iminds.be/nl/inzicht-in-digitale-technologie/digimeter].

Vedder, A. (Leuven 25.02.2015). *ICT-recht: Privacy*. [Hoorcollege professor A. Vedder].

Waltz, E. (2012). How I Quantified Myself. Can self-measurement gadgets help us live healthier and better lives? *IEEE Spectrum, 49*(9), pp. 42-47.

Wolf, G. (2010). *The Quantified Self.* [01.10.2014, TED Conferences:https://www.ted.com/talks/gary_wolf_the_quantified_self#t-291334]

Zuckerman, O., & Gal-Oz, A. (2014). Deconstructing gamification: evaluating the effectiveness of continuous measurement, virtual rewards, and social comparison for promoting physical activity. *Personal and Ubiquitous Computing, 18*(7), pp. 1705-1719.

Bijlagen

Bijlage 1: Rekrutering

Dear members of the Quantified Self-meetup group,

As a master student in Communication Sciences at the KU Leuven I'm writing my thesis under supervision of Professor Karin Slegers about the attitudes towards the datacollection of health data. Through interviews or a group discussion I want to develop the ideal privacy settings for health and fitness applications. For this reason I'm looking for users of such applications. If possible, participants should be speaking Dutch. I plan to have the discussions in Dutch so I can be sure I don't miss any nuance.
If you are interested to take part in my research or if you have any further questions, don't hesitate to contact me.

Kind regards,
Evelien Herelixka
evelienherelixka@hotmail.com

Bijlage 2: Introductiebrief bij opdrachtenbundel

Dag ...,

In deze envelop vind je de opdrachtenbundels ter voorbereiding van het interview.

Zorg ervoor dat je alle opdrachten hebt afgerond voor het interview plaatsvindt en dat je de bundel bij de hand hebt op de dag van het interview, zodat we hier op terug kunnen komen.

Ik zou je willen vragen elke dag een opdracht te maken, maar als je ze liever allemaal op 1 dag maakt is dat natuurlijk geen probleem. Elke opdracht neemt ongeveer 5 à 10 minuten in beslag.

Ik heb bewust veel witruimte voorzien en achteraan nog extra pagina's toegevoegd zodat je je niet beperkt voelt en vrij kan redeneren en associëren. Er zijn absoluut geen foute of juiste antwoorden.

Moest er toch iets zijn, aarzel dan niet om me te contacteren.

Groetjes,
Evelien
evelienherelixka@hotmail.com
0494/372641

Bijlage 3: Opdrachtenbundel

Opdrachtenbundel rond dataverzameling

1

Naam:

Leeftijd:

Geslacht:

Opleiding:

Job:

Ik maak gebruik van de volgende gezondheidstoepassingen:

1.1) Beschrijf hoe je dag er gisteren uit zag.

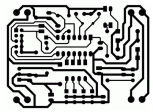
06.00		
07.00		
08.00		
09.00		
10.00		
11.00		
12.00		
13.00		
14.00		

15.00		
16.00		
17.00		
18.00		
19.00		
20.00		
21.00		
22.00		
23.00		

1.2) Plak nu de bijgevoegde stickers bij de momenten waarop je digitale informatie/sporen hebt achtergelaten. *(In de laatste kolom is er plaats voorzien voor de stickers. Indien er meerdere van toepassing zijn mag er buiten de hokjes geplakt worden.)*

Denk bijvoorbeeld aan de informatie die apps verzamelen,

je telefoniegegevens,



data die allerlei slimme apparaten opslaan (zoals een geprogrammeerde thermostaat bijvoorbeeld),

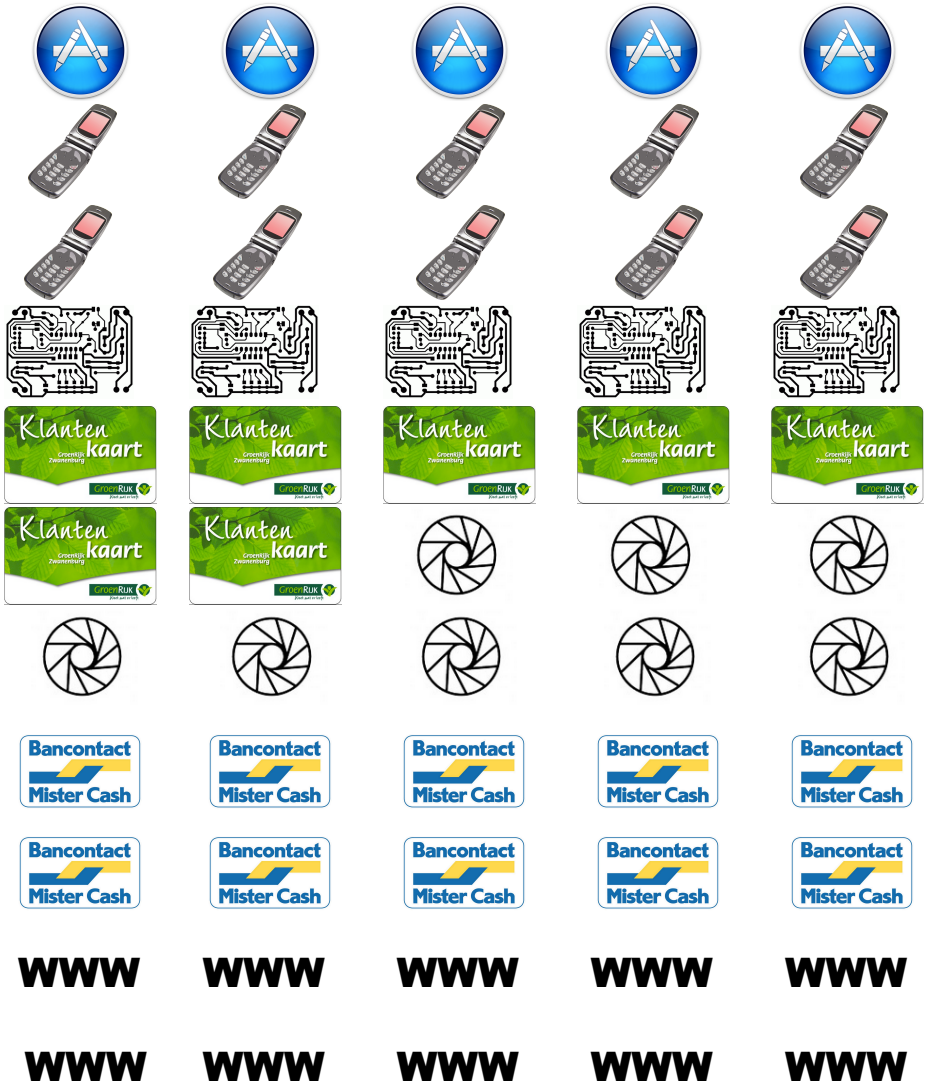
gegevens die verzameld worden via klantenkaarten en –nummers bij bijvoorbeeld tv- en elektriciteitsleveranciers,

allerhande camera's,

geldtransacties,

je browsegeschiedenis en surfgedrag op het internet,...

Gebruik de lege stickers als je nog ergens aan denkt.


Klanten kaart
Bancontact Mister Cash
www

2.1) Bekijk nauwkeurig je antwoord/stickers bij vraag 1.
a) Wat zou je voor jezelf met deze data doen/wat zou je hieruit concluderen?
b) Wat zou je als overheid met deze data van de hele bevolking kunnen doen?
c) Hoe zou je als bedrijfsleider van een commercieel bedrijf deze rijkdom aan informatie gebruiken?

a)

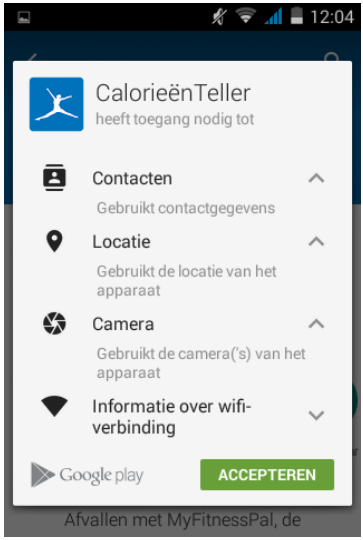
b)

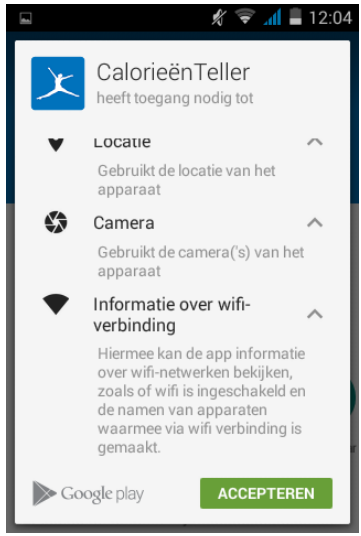
c)

2.2) Als je het zo bekijkt, zijn er dan zaken die je nu liever toch privé zou houden?

7

3) Bekijk de volgende screenshots. Deze pop-up verschijnt wanneer je de CalorieënTeller-app wilt installeren via de Google Playstore. Wat vind je hier goed aan? Wat vind je hier slecht aan?





GOED

NIET GOED

4) Lees de volgende krantenkoppen in verband met big data en noteer waar je aan denkt.

‘Big data zijn maar nuttig als je weet wat er mee aan te vangen’
De Tijd, 16 oktober 2014

Wat u koopt verraadt wie u bent
De Tijd, 31 januarie 2015

100.000 jobs dankzij ‘big data’
De Standaard, 14 oktober 2014

Cyberspionage bedreigt België
De Tijd, 7 juni 2014

Met 'big data' is een uitbraak van ebola eerder te voorspellen
Het Financieele Dagblad, 21 augustus 2014

Big data in de zorg: hoe veilig zijn onze medische data?
Trends.be, 2 december 2014

5) Maak op de volgende pagina een mindmap van alles waar je aan denk bij “privacy”.
Hier zie je een voorbeeld van een mindmap:

PRIVACY

Bijlage 4: Stickers luik 2

Naam	Adres	Emailadres	Leeftijd	Geslacht
Geboortedatum	Lengte en gewicht	Locatie	Stappen, bloeddruk, hartslag, adem-haling, suiker-spiegel, calorieën	IP-adres
Browse-geschiedenis	Audio	Video	Afbeeldingen	Medicatiegebruik, behandelingen
Rekeningen vergoed door mutualiteit	Type activiteit/ Beweging (slapen, wandelen, lopen, ...)	Drugs/alcohol/ roken	Diagnoses/ziekte /Kwetsuren	Psychologische toestand
Emoties	Sociale context	Familie	Vrienden	Hulpverleners (huisarts, specialist, verpleegster,...)
Apotheker	Mutualiteit	Werkgever	Overheid	Bedrijf achter de toepassing + noodzakelijke derden
Commerciële bedrijven	Onderzoekers	publiek		

Bijlage 5: Fictief privacybeleid

Privacy Policy Fictieve App

(o.b.v. Runkeeper, Fitbit, Fjuul, Myfitnesspal, Lifesum)
Last updated November 8, 2012

Introduction

Our goal is to help people live healthier, more active lives. Our products and services provide instant access to health and fitness data so you can track your progress, push your goals and take control of your health.
By accessing and using the Services, you acknowledge that you have read, understood, and agree to be bound by these Terms of Use and the Privacy Policy.
If you do not agree with our Privacy Policy or Terms of Use, please do note use our Services or provide us with your personal data.
We reserve the right to, update, change or modify this Privacy Policy. Any material changes to this policy will be posted on the Website and/or Applications (or You may be notified by email or other notification), and will indicate when such changes will become effective. You will be deemed to have agreed to any such modification or amendment by Your decision to continue using the Website and/or Application following the date in which the modified or amended Privacy Policy is posted on the Website.
We do not knowingly collect any personal data from children under the age of 13 and our Services do not target children under 13. If you are under 13, please do not submit any personal data through our Services. Further, we encourage parents and legal guardians to monitor their children's Internet use and to help us in enforcing our Privacy Policy by instructing their children to never provide any personal data

through our Service without their permission. If you become aware that a child under the age of 13 has submitted personal data to us, please contact us and we will do our best to delete that account from our database.

What data we collect

When you use our Services, among the personal data we may collect from you are: your email address, first and last name, height, weight, date of birth and gender. We may also, depending on your use of the Services, collect personal data about your calorie intake, weight loss goal/weight gain goal, activity/diet routines, your body measurements and BMI.
We collect industry standard log data about the browser and operating system you are using and your IP address every time you make use of our services.
We may also collect other information you provide, such as your consents, preferences and feedback, information relating to your devices and other such information you provide us with.
We use location information derived from sources such as GPS or Cell-ID to determine the location of your mobile device. Via the settings of your operating system you can turn location monitoring on and off. You can opt-out and disable location services at any time
We will access your phone's contact list for the purpose of letting you identify contacts who are Fitbit users. We do not store your phone's contact list, and it is deleted immediately after it is used for this purpose.
You can also search friends by using your Facebook credentials. In such case you will be asked to allow us to access certain information associated with your Facebook account such as your name, profile picture, gender, list of friends and other public information.

In an ongoing effort to improve our Services, additional personal data may be collected from you. In such case, we will notify you when the personal data collection takes place.

How we use your data

Personally identifiable information

Personally Identifiable Information (PII) is data that includes a personal identifier like your name, email or address, or data that could reasonably be linked back to you.
We use your personal data to:

- identify you
- provide you with our services
- analyze the usage and improve our services
- communicate with you, inform you of updates, perform market research, correct errors and problems, and prevent and investigate fraud and other criminal activities.

Except as described in this Privacy Policy we do not sell, lease, rent or otherwise disclose your personal data to a third party without your consent.
We share your personal data with the parties indicated below and for the following reasons:

- *Third party service providers*. We share your personal data with authorized third party service providers who process or manage your data for us, make customer research and the like based on our instructions and in compliance with our Privacy Policy.
- *Strategic partners*. To obtain the best benefits of the Fjuul App, you may choose to sync some of your Fjuul

App's data with a third party application. In such case we will share your personal data with that application.

- *International transfers.* Our services may be provided in various countries and have servers in different locations. If your data is transferred across international borders outside the country where you use the Fjuul App, we shall take reasonable steps to ensure that such transfer is made based on adequate protection and legal basis.
- *Lawful requests*. We may disclose your personal data to certain authorities or third parties if we are required to do so by any applicable law, to respond to legal proceedings or lawful requests.
- *Reorganization and mergers*. In the event of a reorganization of our businesses or merger, we may disclose your personal data to the relevant third party.
- *Protection of our interests and protection against fraud.* We may process or disclose your personal data, in application with applicable laws, to defend our interests or in our actions to prevent and combat fraud.

De-identified data

We may share or sell aggregated, de-identified data that does not identify you, with partners and the public in a variety of ways, such as by providing research or reports about health and fitness or as part of our Premium membership. Such data may also be used for promotional purposes. When we provide this information, we perform appropriate procedures so that the data does not identify you and we contractually prohibit recipients of the data from re-identifying it back to you.

Security

Our systems are firewall protected. We also use encryption techniques and authentication procedures to maintain the security of your personal data and prevent unauthorized access to your Account and our systems. However, no system can be 100% secure and despite our efforts, there is always a risk of unauthorized access to your personal data. By using our Services, you assume this risk.
Authorized personnel or authorized third parties who are granted access to personal data are required to keep such data confidential. When your information is stored by third parties or displayed on third parties' sites, their privacy policy and control apply.

Your rights to modify and delete your personal data

If you have an account, you can access and modify your personal information through your account, at any time. If you completely delete all such information you will not be able to access or use the website and/or applications correctly. If you would like us to delete your personal information from our system, please contact us at removal@service.com with a request that we delete your personal information from our database. We will use commercially reasonable efforts to honor Your request; however, we may retain an archived copy of Your records as required by law or for other legitimate business purposes.

Bijlage 6: Topiclijst

Luik 1: Opdrachtenbundel bespreken
>> Waren ze zich bewust van de tegenwoordige dataverzameling? Hoe stonden ze ertegenover? Hoe staan ze er nu tegenover?

- **Opdracht 1:** Zou hij even willen toelichten: Hoe is hij te werk gegaan?
- Had hij hier al eens eerder over nagedacht? Was hij zich voor de opdracht bewust van de hoeveelheid informatie die hij per dag achterlaat? Leg uit, geef een voorbeeld van iets waar hij zich niet bewust van was.
- Hoe staat hij daar tegenover?
    * Maakt hij zich zorgen (bv. over veiligheid data)?
    * Maakt dat hem bang?
    * Vindt hij het fascinerend?
    * ...
- Hoe gaat hij hier in de toekomst naar toe kijken? Gaat hij zich anders gedragen?
- Via welke app verzamelen en delen ze gezondheidsinformatie? Waarom wel/niet? Met wie wel/niet?
- **Opdracht 2:** Zou hij even willen toelichten: hoe is hij te werk gegaan?
- Waarom geeft hij dit antwoord?
- Had hij hier al eens eerder over nagedacht?
- Wat doet hij met zijn eigen persoonlijke data? Bepaald gedrag aanpassen, meer of minder stellen?
- Als je bedenkt dat de hele bevolking zoveel data genereert, dan levert dat big data op (bv. alleen al elektriciteitsverbruik van heel Vlaanderen; of alle stappen en verbrande calorieën van alle fitbit-gebruikers) Denkt hij dat zijn persoonlijke data waarde heeft? Hoe dan? Wat is er positief aan zoveel data? Wat kan je er uit halen? Wat zijn positieve gevolgen?
- Wat is er negatief aan zoveel data? Hoe kan het misbruikt worden? Wat zijn negatieve gevolgen? Baart hem dat zorgen?
- **Opdracht 3** slaan we nu over, maar daar komen we in het laatste luik op terug.
- **Opdracht 4:** Zou hij even willen toelichten: hoe is hij te werk gegaan?
- Waarom geeft hij dit antwoord?
- Had hij hier al eens eerder over nagedacht?
- Na het lezen van de krantenkoppen, wat is zijn conclusie? Is hij pro of contra verdere dataverzameling?
- **Opdracht 5:** Hoe is hij te werk gegaan?
- Aan wat dacht je meteen?

Luik 2: Gevoelige informatie?
>> Wat vinden ze privé/gevoelig/persoonlijk?

Op A3-papier 2 cirkels: wat en wie. In de cirkel plakt hij wat hij privé wilt houden en wie het wel mag weten. Ik overloop verschillende soorten typische informatie die verzameld word door populaire gezondheidsapps. Dan plakt hij die dus ofwel in of uit de cirkel, daarbij zal hij waarschijnlijk al nuanceren met wie wel en onder welke voorwaarden. De wie's mogen ze dan ook al plakken en eventueel verbinden. En de voorwaarden kort noteren. Na het overlopen van de wat, zal ik dan opnieuw terugkomen op de wie's en de voorwaarden, herhaling kan geen kwaad, alles nog eens op een rij.

- Welke informatie die gezondheidsapps verzamelen (zie stickers) vindt hij gevoelig/houdt hij liever privé?
    * 1e graad/metingen
        + naam, adres, emailadres
        + leeftijd, geslacht, geboortedatum
        + gewicht, lengte
        + locatie
        + aantal stappen, hartslag, ademhaling, bloeddruk, suikerspiegel, calorieën
        + IP-adres, browsegeschiedenis
        + audio, video, afbeeldingen
        + medicatiegebruik/ behandelingen van zorgverstrekkers
        + rekeningen vergoed door de mutualiteit
    * 2e graad/inferenties/afleidingen van gedragingen en situaties o.b.v. 1e graad
        + type activiteit/beweging (slapen, wandelen, lopen, springen,...)
        + drugs/alcohol/roken
        + diagnoses/ziektes/kwetsuren
        + psychologische toestand
        + emoties
        + sociale context
- Wat mag gedeeld worden met wie?
    * familie
    * vrienden
    * hulpverleners (huisarts, specialist, thuiszorg, verpleegster ziekenhuis,...)
    * apotheker
    * mutualiteit
    * werkgever
    * overheid
    * bedrijf achter de toepassing (Runkeeper) en noodzakelijke derden voor toepassing (bv. Google Analytics >> app verbeteren)
    * commerciële bedrijven geïnteresseerd in jouw data >> advertisen
    * onderzoekers
    * publiek
- Waarom? Wat is het verschil?
- Op welke voorwaarden?
    * toestemming
    * identificeerbare data
    * gedeïdentificeerde, geaggregeerde data
    * gedeïdentificeerd én verbod op reïdentificatie
    * gratis vs. betalend
    * zijn er bepaalde situaties waarin wel of geen data verzameld mag worden?
        + tijdens je werk (bv. psycholoog/arts)
        + controlerende partner (ziet waar je bent geweest >> jaloers)
        + extreem: spion >> niemand mag weten waar je bent geweest
        + ...

* zijn er bepaalde situaties waarin wel of geen data gedeeld mag worden?
    + wel met familie als het ze niet ongerust zal maken
    + levensbedreigende situatie
    + ...
* mate van abstractie/informatie die er uit gehaald kan worden:
    + Verandert er iets als de **combinatie** van informatiebronnen verandert?
        - Hoe bezorgd zou je zijn op een schaal van 0 tot 10 als de app bijhoudt:
            > dat je bv. sport (binair: gesport/niet gesport)
            > de tijdstippen waarop je sport (8u)
            > de plaatsen waar je gaat sporten (thuis, fitness)
            > de plaatsen en het tijdstip waarop je sport *(8u in de fitness)*
        - Wat zijn die zorgen dan? Waar is hij bang voor?
    + mate van **detail**: 5min-precisie vs. daggemiddelde
        > waarom is dat beter? Waarom minder bezorgd?
* denkt hij zelf nog aan voorwaarden

- Waarom? Wat is het verschil?
- Voor welke <u>doeleinden</u>? Wat mag er mee gebeuren?
    * dienst verlenen/zodat de app werkt
    * app verbeteren
    * doorverkopen aan commerciële bedrijven/advertisers
    * voor wetenschappelijk onderzoek
    * voor beleid
    * bij diagnose arts
    * denkt hij zelf nog aan andere doeleinden?
- Waarom? Wat is het verschil? Waarom dit wel en dat niet?

Luik 3: Privacybeleid

>> Strookt wat ze privé vinden, dus wat we net hebben besproken, ook met wat ze hebben goedgekeurd/vrijgeven?

-Ziet hij ooit beknopte versie van de machtigingen (zoals screenshots) bij downloaden app? *(alleen bij Android)*
- Bekijkt/leest hij die?
- Wat vindt hij van de screenshots van 5 apps? Kom terug op **<u>opdracht 3</u>**.
    * wat goed/niet? (inhoud/vorm (beknopt, overzichtelijk)
- Daarnaast bestaat er ook meestal/altijd nog een uitgebreid privacybeleid/privacyvoorwaarden *(uitgebreide versies tonen)*. Heeft hij ooit een zo'n privacybeleid van de verschillende toepassingen die hij gebruikt gelezen voor het gebruik ervan?
    * waarom wel/niet? wat zijn de hindernissen (taal, lengte, moeilijkheid,...)
    * Indien toch misschien ooit gelezen, heeft het hem ooit tegengehouden om de app te gebruiken/downloaden? waarom?
    * indien niet gelezen, maakt hij zich dan zorgen omdat hij het niet gelezen heeft?
    * laten lezen en eerste indruk bevragen
- Wat vindt hij van het fictieve privacybeleid? (zowel qua vorm als inhoud) Markeringen overlopen.
- Indien dit het privacybeleid is van een app die ze willen installeren, wat zou hij dan doen?
    * app installeren zonder lezen?
    * lezen?
    * goedkeuren?

Luik 4: licht generatieve opdracht
>> Hoe kunnen we het vertrouwen in het gebruik van gezondheidsapps vergroten?

- Hoe zou je er voor zorgen dat je zelf een gezondheidsapp met een gerust hart kan gebruiken? Wat zou maken dat je een bepaalde app met 100% vertrouwen zou gebruiken? *Denk daar maar 5 minuten over na. Op de achterkant van luik 2-cirkel-blad. Je mag aan alles denken:* ***technologie****/app optimaliseren/functies toevoegen/beperkingen invoeren,* ***recht*** *(privacyvoorwaarden, -beleid),* ***samenleving****/normen,... Indien stroef, aanpassingen laten aanbrengen aan fictieve beleid.*

Bijlage 7: Interviews

Link naar dropbox met getranscribeerde interviews:
https://www.dropbox.com/sh/zxzgsn4rhr0050v/AACWUorhppJa5yca3c_-4ei7a?dl=0

Bijlage 8: Codeboek

De codes in het vet zijn de initiële codes, de anderen werden tijdens het coderen toegevoegd.

- **Sporen:**
  - **App – wearable**
  - **Betaalkaart**
  - **Browsegeschiedenis**
  - **Camera**
  - **Digitale tv – slimme apparaten**
  - Geen sporen
  - **Klantenkaart**
  - Locatie
  - **Telefoniegegevens**
- **Eigen gebruik verzamelde data**
- **Bewust van dataverzameling**
- Onverschillig, neergelegd bij dataverzameling
- "Grote publiek is privacyminded"
- **Gefascineerd door mogelijkheden big data**
- **Big brother** (controle werkgever en overheid)
- Vertrouwen in overheid
- Persoonlijk vs. onpersoonlijk gebruik van de data
- Negatieve gevolgen dataverzameling:
  - Effectief
  - Potentieel:
    - In handen van dictator
    - In handen van werkgever
    - In handen van verzekeraar
    - In handen van crimineel
- Big data in de zorg:
  - Beveiligd
  - Alleen toegankelijk voor bevoegden
  - Data moeten correct zijn
  - Infrastructuur nodig
  - Reglementering

- **Privacy:**
  - **Fundamenteel recht**
  - **Schaamte – imago**
  - **Vreemde geen zaken mee – intrinsiek privacybegrip**
  - **Braaf ≠ probleem**
  - **Evolutie privacybegrip**
- Eigen verantwoordelijkheid bescherming privacy
  - Eigen verantwoordelijkheid
  - Privacyinstellingen wijzigen
  - Valse gegevens
  - Zo weinig mogelijk informatie geven
  - Algoritme verwarren
  - App is snel terug verwijderd
  - Alternatieven zoeken
- **Types informatie:**
  - **Adres**
  - **Afbeeldingen**
  - **Audio**
  - **Bloeddruk, ademhaling, aantal stappen, suikerspiegel, calorieën**
  - **Browsegeschiedenis**
  - Contacten
  - **Diagnoses – ziektes – kwetsuren**
  - **Drugs – alcohol – roken**
  - **E-mailadres**
  - **Emoties**
  - **Geboortedatum**
  - **Geslacht**
  - **IP-adres**
  - **Leeftijd**
  - **Lengte en gewicht**
  - **Locatie**
  - **Medicatie en behandelingen**
  - **Naam**
  - **Psychologische toestand**
  - **Rekeningen vergoed door de mutualiteit**

- **Sociale context**
- **Type activiteit**
- **Video** – camera

- **Delen met:**
  - **Delen met apotheker**
  - **Delen met bedrijf achter de toepassing**
  - **Delen met commerciële bedrijven:**
    - **Spammen**
      - Verwijderen / uitschrijven
    - **Gerichte marketing – profiling**
      - Handig
      - Irritant - filter bubble
    - **Data verkopen**
    - Informatie doelgroep
  - **Delen met familie**
  - **Delen met grote publiek**
  - **Delen met hulpverleners**
  - **Delen met mutualiteit**
  - Delen met onbekenden
  - **Delen met overheid:**
    - **Beleid**
    - Economie aanzwengelen
    - Gezondheidszorg
    - Misdaden bestraffen
    - Veiligheid
  - Delen met verzekeraar
  - **Delen met vrienden**
  - **Delen met werkgever**
  - Delen met niemand
- **Voorwaarden:**
  - (dataverzameling mag zolang) geen misbruik
  - nut/voordeel
  - **abstractie**
  - **afhankelijk van de situatie**
  - **anonimiteit**
  - **beperkte duur bijhouden**
  - bewust data vrijgeven – controle – ik kies

- **toestemming:**
    - **expliciet**
    - impliciet
- **gratis vs. betalend**
- positieve dingen wel, negatieve niet

- **Machtigingenvenster:**
    - **Te beknopt**
    - **Goed - duidelijk**
- **Gevolg machtigingenvenster:**
    - **Goedkeuren**
    - **App niet downloaden**
- **Privacybeleid niet lezen:**
    - Geen andere keuze dan goedkeuren
    - Altijd hetzelfde
    - Geen zin
    - **Engels**
    - Kleine lettertjes
    - **Te lang**
    - **Te moeilijk**
    - Verondersteld OK
- Privacybeleid goedkeuren
- **Bezorgd na niet lezen van privacybeleid**
- Pijnpunten privacybeleid
    - Gebruik = goedkeuren
    - Recht van aanpassen
    - Recht op inzage, aanpassen, wissen
    - Beveiliging data
- Momenteel al veel vertrouwen
- **Factoren die vertrouwen beïnvloeden:**
    - Louche look
    - Gebruiksvriendelijk
    - Goede naam
    - Overzicht waar data terechtkomt
    - Privacybeleid beschikbaar
    - Gebruik data specifiëren
    - Privacy op voorhand, niet achteraf
    - Pop-up/pushbericht

- Persoonlijk contact
- Onwetendheid
- Opslaan op telefoon i.p.v. op internet
- Labels
- Interactieve schuifbalkjes – voor alles apart toestemming
- Technologie nooit 100% betrouwbaar
- Bewustmaking – sensibilisering
- **Wetten**
    - **Verbod reïdentificatie**
    - Slecht gebruik nog steeds mogelijk