AFSTAAN VAN PERSOONLIJKE INFORMATIE: KRITIEK OP GEINFORMEERDE TOESTEMMING IN EEN DIGITAAL TIJDPERK

Bachelor Eindwerkstuk

Jaimy Hartog
4163419
Begeleider: Joel Anderson

Juni 2016

Universiteit Utrecht

Bron: NASA

AFSTAAN VAN PERSOONLIJKE INFORMATIE: KRITIEK OP GEINFORMEERDE TOESTEMMING IN EEN DIGITAAL TIJDPERK

Bachelor Eindwerkstuk
Jaimy Hartog
4163419
Begeleider: Joel Anderson
Juni 2016

Aantal woorden: 7228

Inhoudsopgave

AFSTAAN VAN PERSOONLIJKE INFORMATIE: KRITIEK OP GEINFORMEERDE TOESTEMMING IN EEN DIGITAAL TIJDPERK

Jaimy Hartog
4163419
Aantal woorden: 7056

Samenvatting: In een tijdperk van moderne technologie neemt het belang van informatie in een samenleving sterk toe. Elkaar steeds sneller opvolgende technische innovaties hebben in korte tijd geleid tot de digitale infrastructuren die vandaag onze informatiemaatschappij mogelijk maken. Ook de informatie die we persoonlijk achten, ontkomt niet aan deze ontwikkeling. In veel gevallen heeft het individu in die samenleving daar geen enkele invloed op. Echter, in sommige gevallen krijgt de consument of burger de mogelijkheid expliciet te kiezen om al dan niet persoonlijke informatie af te staan. Het is goed denkbaar, juist vanwege het groeiende belang van data en informatie, dat dergelijke situaties in de toekomst vaker zullen ontstaan. De veronderstelling die bij dit soort keuzemomenten noodzakelijkerwijs door bedrijf of overheid wordt gedaan, is dat het individu in staat is hierover een goede keuze te maken. Ik betoog dat dit in het digitale tijdperk lang niet altijd waarschijnlijk is: de kenmerkende eigenschappen van de technologie bemoeilijken cruciaal inzicht in de gevolgen voor de eigen informationele privacy op korte en lange termijn. Met de vraag om toestemming ontstaat een gat tussen dat wat wordt vereist van de capaciteiten van individuen en waar zij daadwerkelijk toe in staat zijn. Dit gat toont niet alleen een probleem aan voor geïnformeerde toestemming in een digitale context, maar kan ook grond zijn voor alternatief beleid. De belangrijkste kritiek op basis van de 'autonomy gap' is dat het bij regelgeving over geïnformeerde toestemming in een digitale context gaat om een vorm van collectief zelfbedrog, die de pretentie van een autonome keuze niet waar kan maken.

Het belang van privacy krijgt een nieuwe impuls wanneer informatie door ontwikkelende digitale techniek verandert. Ik betoog dat geïnformeerde toestemming, een belangrijke methode om privacy te beschermen, juist in een digitale context slecht in staat is deze bescherming werkelijkheid te maken. De belangrijkste kritiek krijgt vorm in een 'autonomy-gap', die volgt uit de analyse van zowel geïnformeerde toestemming en digitale data. Bovendien impliceert het introduceren en onderhouden van beleid waarbij van zo'n autonomy-gap sprake is, het soort van collectief begrip dat vergelijkbaar is met zelfdeceptie.

Allereerst beschrijf ik kort de context van de informatiesamenleving en privacy waarin gevallen van geïnformeerde toestemming kunnen worden begrepen. Geïnformeerde toestemming is een van de manieren om de burger of consument de kans te geven invloed uit te oefenen op de eigen privacy. Ik stel vast dat begrip van consequenties cruciaal is om te kunnen spreken van een autonome keuze. Dit komt ook naar voren en drie cases van toestemming die ik vervolgens beschrijf: een situatie waarmee

veel van ons al regelmatig in aanraking komen, een voorbeeld van hoe persoonlijke (in dit geval medische) informatie systematisch kan worden opgeslagen en tenslotte een (nu nog) science fiction case waarin persoonlijke informatie simpelweg kan worden verkocht.

Dan ga ik over op het probleem met dit soort situaties van toestemming. Ik beschrijf hoe de roep om privacy en transparantie in contrast staat met een praktijk waarin met ogenschijnlijk veel gemakzucht persoonlijke informatie wordt afgestaan. Hoe valt dit te verklaren? Ik stel vast dat de digitale techniek waarmee informatie wordt opgeslagen en verspreid een aantal kenmerken heeft die het moeilijk maken de gevolgen van toestemming voor de eigen privacy te overzien, waarbij de cases worden heroverwogen om deze moeilijkheden te illustreren. Ze zijn van een dusdanige aard dat van consumenten of burgers niet verondersteld kan worden dat ze deze overzien. Dit resulteert in een *autonomy gap* en plaatst vraagtekens bij toestemming in de vorm zoals we die in de cases zien.

○ Informatiesamenleving, privacy en geïnformeerde toestemming

Ontwikkelingen in de verwerking en communicatie van informatie hebben in de tweede helft van de vorige eeuw aan de basis gestaan van grote transformaties in economisch, sociaal, cultureel en politiek leven.[1] De capaciteiten om informatie te produceren, op te slaan en te verspreiden explodeerden kort na de millenniumwisseling en nemen sinds die tijd alleen maar toe.[2] Elkaar steeds sneller opvolgende technische innovaties, met als hoogtepunten de computer en het internet, hebben in korte tijd geleid tot de digitale infrastructuren die vandaag onze informatiemaatschappij mogelijk maken. De nieuwste ontwikkelingen maken al deze technologie bovendien vrijwel overal toegankelijk, waarmee het bereik en de invloed op de samenleving eens te meer wordt versterkt.

Waar een maatschappij zo aan verandering onderhevig is, is het ondenkbaar dat de ethiek niet voor nieuwe uitdagingen komt te staan. Het is dan ook aan de relatief moderne gebieden in de ethiek als *computer ethics* en *information ethics* om het hoofd te bieden aan de problemen die de wereld van de creatie, verspreiding, communicatie, opslag, beveiliging en gebruik van digitale data voortbrengt.[3] Zo is de nieuwe techniek, waarvan de precieze werking vaak nog maar beperkt wordt begrepen, aanleiding voor

[1] Unesco (1998) p. 271
[2] Hilbert & López (2011) p. 60
[3] Floridi (2008) p. 3

nieuwe vragen over betrouwbaarheid, toegang en verantwoordelijkheid. De status en kwaliteit van informatie die zich niet langer op één plek bevindt en overal toegankelijk is, vraagt bijvoorbeeld niet alleen om een hernieuwd concept van intellectueel eigendom, maar dwingt ons ook na te denken over mogelijke sociale ongelijkheden die ontstaan wanneer bepaalde groepen toegang wordt ontzegd.

Privacy: nog altijd belangrijk en relevant

Ook het concept van *privacy* krijgt voor het individu in de moderne informatiesamenleving opnieuw betekenis. Een eerste en zeer invloedrijk begrip van privacy, opgetekend door Samuel Warren en Louis Brandeis in "The Right to Privacy" (1890), werd al geformuleerd als reactie op de belangrijkste technologische ontwikkelingen van de tijd: de opmars van fotografie en kranten creëerde nieuwe mogelijkheden voor de ongewenste verspreiding van persoonlijke informatie en laster. In een zoektocht naar de grenzen van begrippen als publiek belang, reputatie en toestemming werd privacy in de kern beschreven als "the right to be let alone"[4].

Wat precies onder privacy wordt verstaan, blijft sinds Warren en Brandeis dus ook steeds onderhevig aan verandering. Het begrip heeft een dynamische component: het is een ontwikkelend concept waarvan de inhoud continue wordt bepaald door de politieke en technologische eigenschappen van een samenleving.[5] Bovendien is de opvatting over hoe privacy het beste kan worden begrepen sterk afhankelijk van de vraag of het gaat om een belang of een recht. Waar het in vroegere wetgeving vooral gaat om vrijheid van fysieke of lichamelijke inbreuk, ontwikkelt het zich, bijvoorbeeld in Amerikaanse wetgeving, gedurende de negentiende en twintigste eeuw steeds meer tot de vrijheid om zonder verstoring of bemoeienis keuzes te maken.[6] Hieraan verwant ontstaat dan al snel de opvatting dat men vrij moet kunnen zijn van invloed op het denken en ideeën geuit moeten kunnen worden zonder de druk van buitenaf om zich te conformeren.

Vervolgens gaat privacy in de tweede helft van de twintigste eeuw steeds vaker over kwesties rondom persoonlijke informatie, die dan steeds gemakkelijker wordt verzameld en elektronisch wordt opgeslagen en verspreid.[7] We spreken dan ook wel van *informatie-* of *informationele privacy*: de vrijheid van epistemische interferentie, die wordt

[4] Warren & Brandeis (1890)
[5] Moor (2006) p. 114
[6] Tavani (2008) p. 135
[7] Ibid.

gerealiseerd wanneer er sprake is van een beperkte toegang tot onbekende feiten over een persoon.[8] Die feiten kunnen bijvoorbeeld gaan over onze dagelijkse activiteiten, persoonlijke levensstijl, financiën, medische geschiedenis of academische achtergrond. Deze informatie kan ergens op een vaste plek zijn opgeslagen, of uitgewisseld worden tussen partijen met behulp van elektronische middelen. De invloed die ontwikkelingen in digitale technologie hebben op het begrip van informationele privacy en hoe deze zou moeten worden beschermd, is uiteraard zeer groot. Globaal is deze op vier fronten waar te nemen[9]: de toenemende *capaciteit* om grote hoeveelheden persoonlijke informatie op te slaan; de *snelheid* waarmee informatie kan worden uitgewisseld; de *kwaliteit* en *duurzaamheid* van de opgeslagen informatie; en het *soort* van informatie dat kan worden verzameld. Wanneer de techniek bijvoorbeeld de mogelijkheid voor *big data* schept, is het noodzakelijk dat een theorie van privacy de status kan beschrijven van informatie die voortkomt uit het gebruik van internet of mobiele telefoons.

Veel analyses van informationele privacy richten zich op de centrale principes van *beperkte toegang* en *controle*.[10] Van beperkte toegang is sprake in een situatie waarin een individu beschermd is tegen indringing, interferentie en toegang van informatie door anderen.[11] Hiertoe behoren ook situaties waarin mogelijk sprake is van observatie of verzamelen van gegevens. De belangrijkste discussie over toegang richt zich op de rechtvaardiging en de grenzen van deze bescherming. De tweede pijler onder benaderingen van informationele privacy, controle, gaat over te vraag hoe en in welke mate een individu in staat is haar eigen privacy te beheren. Mensen hebben een bepaalde mate van controle nodig om overwegingen, keuzes en correcties te kunnen maken ten aanzien van de toegang van hun persoonlijke informatie.[12] Het principe van *geïnformeerde toestemming* is hier het belangrijkste uitwerking van.

Geïnformeerde toestemming

Het principe van geïnformeerde toestemming hangt nauw samen met privacy en is een belangrijk thema in literatuur in de filosofie, rechten en medische wetenschappen. Als reactie op medische experimenten met menselijke proefpersonen, maar ook politieke gebeurtenissen en misdaden, zijn verschillende richtlijnen ontstaan voor het vragen om

[8] Floridi (1999) p. 52
[9] Floridi (2005) en Tavani (2007)
[10] Tavani (2008) p. 141
[11] Moor (1997) p. 30
[12] Tavani (2008) p. 145

toestemming in tal van situaties. De conceptuele discussies richten zich in de basis op de voorwaarden, het bereik en de status van de vereisten om om toestemming te vragen en op dat wat noodzakelijk is voor een individu om een goede keuze te kunnen maken.

Faden et al. formuleren een invloedrijke theorie van geïnformeerde toestemming, die voor een gedeelte is gebaseerd op de lange geschiedenis van het begrip en deels uitgaat van een aantal fundamentele, filosofische denkbeelden.[13] Centraal in deze theorie staat *autonomie*: geïnformeerde toestemming is in de kern een proces dat een proces van zelfbeschikking en autonome keuze mogelijk maakt en beschermt. Wanneer we kunnen onderscheiden wat precies noodzakelijk is voor deze autonomie, dan is het mogelijk om vast te stellen in welke situaties sprake is van echte geïnformeerde toestemming. Op dit punt is het voor Faden en Beauchamp noodzakelijk een onderscheid te maken tussen autonome *personen* en autonome *handelingen*: een persoon kan aan de hand van een aantal aanwezige vereisten omschreven worden als 'autonoom', maar dit sluit niet dat haar handelen toch niet voldoet aan wat we een 'autonome' keuze zouden noemen.[14] De capaciteit om autonoom te handelen impliceert niet dat deze ook benut wordt. Dus wat is noodzakelijk voor een autonome handeling?

De drie voorwaarden voor een autonome handeling kunnen als volgt worden beschreven: een handeling als autonoom als deze *intentioneel* is, met *begrip* wordt uitgevoerd en dit zonder *controlerende invloeden* gebeurt.[15] De begrippen hangen nauw met elkaar samen. Een handeling is *intentioneel* wanneer de uitvoerder, bij de reflectie op de handeling, zou kunnen zeggen dat de handeling gedaan is zoals vooraf gepland.[16] Gevallen waarin handelingen per ongeluk worden gedaan, onbewuste gewoonten of handelingen die plaatsvinden door bijvoorbeeld fysieke dwang van een ander persoon, zijn niet intentioneel. Bij intentionaliteit is er geen verschil tussen willen, bereid zijn of tolereren: of iemand een bepaald risico opzettelijk *wil* nemen, *bereid is* om deze te nemen of het bestaande risico *tolereert*, maakt een handeling niet minder intentioneel.[17] Hier wordt direct de nauwe samenhang met *begrip* duidelijk: in hoeverre is iemand in staat risico's, lasten en andere gevolgen te begrijpen?

Iemand kan in staat zijn intentioneel te handelen, maar zelf toch niet in

[13] Faden et al. (1986)
[14] Faden et al. (1986) p. 237
[15] Ibid. p. 238
[16] Ibid. p. 243
[17] Ibid. p. 246

controle zijn over de handeling. Het principe van *non controle* geeft rekenschap van invloed van buitenaf op de persoon die handelt.[18] In een proces van geïnformeerde toestemming kan sprake zijn van dwang, manipulatie of overtuiging. Hun impact op autonomie kan worden begrepen door middel van *invloed* en *weerstand*: daar waar dwang van grote invloed is op handelen en er geen ruimte is voor weerstand, is de controle door de ander groot; in het geval van overtuiging is het individu in staat meer weerstand te bieden tegen die invloed. Ook hier kan weer worden vastgesteld dat *begrip* van relevante zaken een belangrijke rol speelt, zeker wanneer het gaat om het verschil tussen manipulatie en overtuiging. De scheidslijnen tussen dwang, manipulatie en overtuiging zijn dun, maar de belangrijkste functie van *non controle* is dat een onderscheid kan worden gemaakt tussen controlerende en niet-controlerende invloeden. Dergelijke analyses kunnen echter tot de conclusie leiden dat sommige vormen van manipulatie compatibel zijn met het concept van een autonome handeling.[19] Meer hierover in de cases.

Het principe van *begrip* als noodzakelijkheid voor autonomie is complex, maar van relatief groot belang. In het ideale geval van compleet begrip zou een persoon alle relevante proposities of verklaringen moeten begrijpen die het karakter van de handeling beschrijven, en daarbij alle mogelijke consequenties en uitkomsten van het wel of niet instemmen moeten overzien.[20] Een dergelijke definitie zou weinig autonome handelingen laten bestaan. Een betere optie zou dus zijn om een principe van *voldoende* begrip te formuleren. Hiervoor zijn beschrijvingen nodig van wat Faden et al. noemen *materiële* eigenschappen van de situatie.[21] Materieel betekent hier net zoveel als *belangrijk voor het subject*: een subjectief begrip dat gegrond is in de onmiddellijke overtuigingen en verlangens, duurzame waarden, behoeften en belangen van een persoon; de beschrijvingen die voor haar het overwegen waard zijn. Het belang van deze beschrijvingen is dus niet intrinsiek aan het object waarover toestemming gegeven wordt en is dus ook niet hetzelfde als *relevantie*: dingen kunnen relevant zijn als het om het object gaat, maar niet relevant *voor de persoon* (*materieel* voor de keuze van deze persoon).[22]

○ Drie cases: persoonlijke informatie vrijgeven

[18] Ibid. p. 256
[19] Faden et al (1986) p. 360
[20] Ibid. p. 300
[21] Ibid. p. 302
[22] Ibid. p. 304

Om te illustreren hoe geïnformeerde toestemming, zoals we die hier formuleerden, vorm kan krijgen in een informationele privacy context, gaan we over tot een drietal voorbeelden. De cases hebben overeenkomstig dat toestemming moet worden gegeven om bepaalde persoonlijke informatie af te staan, waarbij verschillende afwegingen een rol spelen. Het mogelijk vrijgeven van de informatie levert steeds een ander type voordeel op en ook het soort informatie dat al dan niet kan worden vrijgegeven wisselt.

Het principe van *begrip* als noodzakelijkheid voor een autonome handeling neemt hierbij een primaire positie in, zoals die ook de basis zal zijn voor de verdere uitwerking van de centrale claim. Faden et al. onderschrijven dit relatief grote belang van begrip: een niet geslaagde vorm van geïnformeerde toestemming is zelden het resultaat van het niet voldoen aan *slechts* de eisen van intentionaliteit of non controle; veelal (niet altijd) is er dan ook een probleem met het voldoen aan de eis van begrip.[23] Andersom geldt dat, wanneer er sprake is van voldoende begrip, er in veel gevallen weinig voor nodig is ook aan de overige twee eisen voor een autonome handeling te voldoen.[24]

Cookiewet

Sinds de zomer van 2012 is in Nederland artikel 11.7a van de Telecommunicatiewet, ook wel de Cookiewet genoemd, van kracht.[25] Deze wet schrijft voor dat websites met bezoekers uit Nederland hun gebruikers moeten inlichten over de gegevens die worden verzameld bij gebruik van de website. Hiertoe moeten bezoekers ten minste een keer toestemming geven. Dit kan bijvoorbeeld gebeuren door middel van een venster binnen de website, waarin men door middel van knop aangeeft in te stemmen. Hierbij gaat het om beperkte hoeveelheden data, kleine tekstbestanden, die op de computer wordt opgeslagen en die op een later moment kan worden gebruikt om analyses over websitebezoek uit te voeren, advertenties te tonen of toepassingen van software binnen de website te ondersteunen. Het voordeel voor de gebruiker ligt in het goed functioneren van de betreffende website: gegevens hoeven niet steeds opnieuw te worden ingevoerd, instellingen en aanbevelingen worden gepersonaliseerd en alle belangrijke toepassingen werken. Het voordeel voor websitebeheerders is de mogelijkheid om gebruiks- en gebruikersanalyses uit te voeren.

De theorie van geïnformeerde toestemming geeft de handvatten om een aantal aspecten van *begrip* in deze context te beschrijven. Een bruikbaar onderscheid is hier

[23] Faden et al. (1986) p. 299
[24] Ibid.
[25] *Telecommunicatiewet* (2016). *Wetten.overheid.nl*. Geraadpleegd 2 juni 2016, http://wetten.overheid.nl/

bijvoorbeeld tussen begrip *waarover* voor toegestemd en begrip *dat* wordt toegestemd.[26] Toestemming voor het gebruik van cookies vindt plaats wanneer een gebruiker voor het eerst een website bezoekt, iedere individuele website opnieuw. Veelal is niet instemmen gecompliceerder: een duidelijk aanwezige knop in een pop-up venster geeft de mogelijkheid tot accepteren, maar volledige informatie en alternatieve instellingen vereisen doorklikken naar uitgebreide webpagina's over privacy beleid. Wanneer de vraag om toestemming bij iedere website aan de bezoeker wordt voorgelegd en het meest prominente visuele aspect aan die vraag de mogelijkheid tot accepteren is, is het legitiem de vraag te stellen of een gebruiker begrijpt *dat* hij toestemt. Macht der gewoonte of de interpretatie van de 'accepteren'-knop als slechts een bevestiging om de betreffende website daadwerkelijk te willen bezoeken, kunnen worden gezien als beperkt *begrip*. Van een autonome keuze om informatie over websitegebruik af te staan zou geen sprake zijn.

Hieraan verwant is de vraag in hoeverre een dergelijke geïnformeerde toestemmingscontext de bezoeker van voldoende *materiële* informatie voorziet.[27] Voorbeelden van materiële informatie zouden kunnen zijn in welke mate opgeslagen cookies terug te voeren zijn op een individu, wie toegang heeft tot de data voor analyses, wat de data precies beschrijft en hoelang deze opgeslagen blijft. De algemene vraag zou zijn: wat is er over mij en mijn websitegebruik bekend en bij wie? Faden et al. introduceren op dit punt het concept van *in staat stellen*: omdat *materialiteit* uitgaat van een subjectieve begrip van belang is het niet langer zinvol om te traditionele vraag te stellen welke informatie een autoriteit verplicht is te ontsluiten, maar eerder hoe een autoriteit een individu *in staat kan stellen* een autonomie keuze te maken.[28] Dat wat een autoriteit verplicht is te vermelden hoeft immers niet die informatie te omvatten die materieel is voor een individu. In de context van cookies zou dit kunnen betekenen dat getoonde informatie niet slechts dat beschrijft wat wettelijk verplicht is, maar duidelijk maakt wat er met individuele data over internetgebruik mogelijk is. Veel websites hanteren bijvoorbeeld standaardverklaringen die uitgaan van de redenen waarom cookies worden gebruikt en dit gebruik rechtvaardigen. De uitzonderingen op de regel, die meer uitgaan van materiële motieven voor gebruikers, zijn veelal te vinden bij grote bedrijven als Google en Facebook.

[26] Faden et al. p. 300
[27] Faden et al (1986) p. 302
[28] Ibid. p. 305

In dergelijke verklaringen staan bijvoorbeeld vragen over waarom, waar en wie cookies gebruikt centraal en hoe de bezoeker van de website hier controle over kan uitoefenen.[29]

Elektronisch patiëntendossier

Vanwege de aard van het systeem is informatie over internetgedrag zoals cookies niet denkbaar in een niet-digitale vorm. Maar steeds vaker worden vormen van persoonlijke informatie gedigitaliseerd die voorheen nog voornamelijk analoog werden opgeslagen en beheerd. Als gevolg hiervan ontstaan grootschalige digitale structuren die deze informatie toegankelijk maken. Een voorbeeld is het elektronisch patiëntendossier, waarin medische gegevens van individuen binnen in zorginstelling kunnen worden opgeslagen. Dit type database kreeg in 2008 veel aandacht toen het initiatief voor een Landelijk Schakelpunt voor deze systemen (EPD-LSP) werd geïntroduceerd, waarmee zorgverleners landelijk gegevens zouden kunnen uitwisselen.[30] Waar het in eerste instantie zou gaan om impliciete toestemming door patiënten (standaard maakte men deel uit van de database, tenzij bezwaar werd gemaakt), zou in latere voorstellen expliciete toestemming nodig zijn. Uit veiligheidsoverwegingen vond de daadwerkelijke invoering echter nooit doorgang en in 2011 werd het voorstel door de Eerste Kamer definitief afgekeurd. Toch is het niet onmogelijk dat vergelijkbare infrastructuren in de toekomst vaker deel uit zullen maken van de maatschappij, zeker wanneer door technische ontwikkeling veiligheidszorgen worden verkleind.

Een belangrijk verschil met de context van cookies is de mogelijke ruimte die in dit geval zou bestaan voor communicatie. We stelden eerder vast voor Faden et al. de vraag centraal staat hoe een autoriteit het individu *in staat kan stellen* een autonome keuze te maken en dat dit los staat van de vraag wat die autoriteit slechts verplicht is te ontsluiten. Hierbij speelt een proces van deliberatie een belangrijke rol.[31] Hiermee ontstaat ruimte voor wederzijds begrip van de belangrijkste informatie die door de autoriteit of 'toestemmingszoeker' wordt verschaft, maar wordt ook duidelijk welke materiële redenen en consequenties mogelijk niet door deze informatie worden ondervangen. Manson en O'Neill spreken ook wel van 'transactionele toestemming', waarbij de strikte regelgeving

[29] *Cookies Policy*. (2016). *Facebook.com*. Geraadpleegd 12 juni 2016, https://www.facebook.com/policies/cookies/
[30] *Dossier Elektronisch Patiëntendossier*. (2016). *Medischcontact.nl*. Geraadpleegd 13 juni 2016, http://www.medischcontact.nl/Kennis/Dossiers/EPD.htm
[31] Faden et al. (1986) p. 316

rondom toestemming wordt verbonden met de rechten en behoeften van het individu.[32] Zo is het bijvoorbeeld denkbaar dat in deze situatie een zorgverlener meer inzicht kan geven in de gegevens die met het LSP toegankelijk zouden worden, wie er in theorie bij zou kunnen komen en welke voordelen dit oplevert. In gesprek kan dan bijvoorbeeld duidelijk worden dat er voor de patiënt aanvullende materiële consequenties zijn, zoals de mogelijke toegang tot de data door bepaalde familieleden die werkzaam zijn in de zorg en waarmee de patiënt een moeizame relatie onderhoudt.

Inzicht in rijgedrag tegen vergoeding

Het is goed denkbaar dat het afstaan van persoonlijke informatie in de toekomst niet alleen leidt tot het goed functioneren van systemen als het internet of goede zorg, maar daadwerkelijk verkocht kan worden. In oktober 2015 bedacht zorgverzekeraar Achmea een nieuwe dienst, waarbij consumenten korting zouden krijgen op de premie van een autoverzekering, wanneer zij een apparaatje in hun auto lieten plaatsen die rijgedrag in kaart brengt.[33] De consument kon zo profiteren van een financieel voordeel, terwijl de verzekeraar gegevens over schade in kaart kon brengen. Rustig rijgedrag zou meer korting opleveren, waarbij bijvoorbeeld hard remmen en gas geven minpunten opleverden. Hieraan verwant bestonden ideeën over apparatuur in huis die gegevens over bijvoorbeeld thermostaat of rookmelders konden doorgeven. Het idee zou in deze vorm niet worden gerealiseerd, mede door de publieke discussie die de aankondiging teweeg bracht. De dienst was echter niet in strijd met enige regelgeving.

Een belangrijk onderscheid met de beide andere cases is dat het voordeel in de vorm van financieel gewin begrepen kan worden als een vorm van manipulatie of dwang, waarvan de mate waarin die succesvol is bovendien afhangt van de economische situatie van de consument. Fisher beschrijft dit type voordelen in geïnformeerde toestemming als ‘structurele dwang’.[34] Hij beschrijft hoe bredere sociale, economische en politieke contexten niet alleen invloed heeft op het proces waarin het individu tot toestemming overgaat, maar ook op de manier waarop autoriteiten die processen vormgeven. In dit geval wordt de situatie gevormd door een samenleving waarin geld een belangrijk goed is en waar sommigen in grote mate van afhankelijk zijn. In het laatste geval kan amper nog

[32] Manson & O'Neill (2007)
[33] *Achmea biedt korting in ruil voor privédata*. (2016). *Volkskrant.nl*. Geraadpleegd 13 juni 2016, http://www.volkskrant.nl/tech/achmea-biedt-korting-in-ruil-voor-privedata~a4154347/
[34] Fisher (2013) p. 356

gesproken worden van een vrije of autonome keuze. De situatie draait om: er is niet langer van een sprake van een keuze om informatie af te staan, maar bij voldoende financiële middelen kun je je informationele privacy veroorloven. Des te belangrijker wordt het om begrip te hebben van de mogelijke gevolgen van het weggeven van informatie, zelfs als geld een zeer relevante en materiële reden is.

○ Autonomy-gaps: het probleem met geïnformeerde toestemming

In ieder van de hierboven beschreven cases is sprake van een ander soort persoonlijke informatie, te behalen voordeel en digitaal systeem. Toch zit er gemeenschappelijkheid in de noodzaak voor een zekere mate van begrip over de aard van de informatie en de werking van het digitale systeem om te kunnen spreken van een autonome handeling in geïnformeerde toestemming situaties. Of het nu gaat om cookies, medische gegevens of informatie over rijgedrag, steeds is het redelijk te veronderstellen dat deze aspecten van privacy in digitale contexten *materieel* zijn voor consument, burger of patiënt.

Voor een belangrijk gedeelte geeft dit aan *waarom* deze geïnformeerde toestemming situaties eigenlijk bestaan: iedere case kan op deze manier begrepen worden tegen de achtergrond van een maatschappij waarin waarden gelden als privacy, die bijvoorbeeld als essentieel wordt verondersteld voor democratie en vrijheid, waarbij de bescherming van persoonlijke gegevens functioneert als schild.[35] De cases zijn hier illustraties van: met de gelaten keuzes voor eventuele toestemming wordt gehoor gegeven aan de roep om controle over de eigen privacy en inzicht in de werking van systemen die steeds vaker deel uitmaken van onze leefwereld. De drang naar deze transparantie en de verontwaardiging wanneer bijvoorbeeld blijkt dat zonder toestemming gegevens zijn verzameld, duiden op een evenredig groeiend gewicht dat aan afzondering en beslotenheid wordt toegekend.[36] De cases laten zien hoe de keuzemomenten zijn ingericht waarin individuen de mogelijkheid hebben om weloverwogen informatie af te staan en hun eigen privacy af te bakenen en te beschermen.

‘The great giveaway’

Dus wat valt nu te verwachten van geïnformeerde toestemming situaties waarin informationele privacy op het spel staat? Zoals gezegd is een belangrijke reden voor het laten van de keuze de veronderstelling dat de burger of consument controle en inzicht eist

[35] Moor (2006) p. 114
[36] Frissen (2016) p. 15

bij eventuele openbaring. Het is immers mogelijk dat, alles overwegend, een individu bepaalde data niet vrij zou willen geven. Maar in hoeverre zouden we de situaties van geïnformeerde toestemming ook daadwerkelijk gebruiken om onze privacy te beschermen?

Anita Allen stelt vast dat een 'nieuwe generatie' onder invloed van ontwikkelende technologie als het internet juist het openbaar maken van informatie tot de standaardoptie heeft gemaakt.[37] Informationele privacy wordt steeds vaker verworpen of geherformuleerd en maakt het huidige tijdperk tot de 'Era of Revelation'.[38] Meer en meer geven mensen persoonlijke data weg aan vreemden vanwege variërende zelfzuchtige, altruïstische en maatschappelijk betrokken redenen in een grootschalig proces dat Allen de 'Great Privacy Give-Away' noemt.[39] We zijn continue bezig met het zoeken, verzamelen en publicatie van informatie over anderen en onszelf: we houden er van rond te snuffelen in dat wat verstopt is en te verspreiden wat we weten, denken en voelen. Op deze manier geven mensen routinematig ogenschijnlijk onschadelijke stukjes informatie weg, die samen blijvende digitale records vormen en die snel en uitgebreid kunnen worden gedeeld.[40]

Is dit een probleem? Allen is een voornaam verdediger van de positie dat privacy een goed is dat individuen veel beter zouden moeten verzorgen dan op dit moment gebeurt en er in sommige gevallen een beschermende rol is weggelegd voor bijvoorbeeld een overheid.[41] Het is volgens haar zelfs mogelijk te verdedigen dat het individu de morele plicht heeft minder passief op te treden wanneer het gaat om het verdedigen van de eigen privacy.[42] De schijnbare onverschilligheid ten aanzien van 'digitale broodkruimels' is volgens haar dan ook alarmerend: privacy is te belangrijk om aan het toeval of persoonlijke smaak over te laten.[43] Hiertegenover staan auteurs als Posner, die verdedigen dat het juist goed is voor een samenleving wanneer individuen er voor kiezen persoonlijke informatie te delen.[44]

Ongeacht de normatieve beoordeling van het relatief makkelijk delen van

[37] Allen (2013) p. 848
[38] Allen (2013)
[39] Ibid. p. 847
[40] Moor (1997)
[41] Allen (2011)
[42] Allen (2013) p. 865
[43] Allen (2011) p. 196
[44] Posner (2011)

informatie, lijkt deze ontwikkeling op maatschappelijk niveau in ieder geval moeilijk te rijmen met de eerdere vaststelling dat er nog altijd veel behoefte is aan transparantie en controle over de eigen privacy. Hoe valt Allens 'big giveaway' te verklaren in het licht van de geldende waarde 'privacy', waaruit geïnformeerde toestemming situaties ontstaan? We vinden het antwoord in het concept van *begrip* als noodzakelijkheid voor *autonomie* en de discrepantie tussen de veronderstelde en daadwerkelijke aanwezigheid van beide.

Digital literacy: de oncontroleerbaarheid van digitale data

De cases illustreren situaties waarin de burger of consument expliciet persoonlijke informatie in digitale vorm verruilt voor verschillende soorten voordelen. Als we Allen volgen in de analyse dat persoonlijke informatie een goed is waar we over het algemeen weinig zuinig mee lijken om te springen, dan is het van belang processen van geïnformeerde toestemming in de traditionele betekenis juist in dit soort contexten goed te analyseren. Omdat het individu deze keuze wordt voorgelegd en zij vrij is hierin een beslissing te maken, mag aangenomen worden dat door de 'toestemmingszoeker' wordt verondersteld dat zij in staat is een voor haar goede beslissing te maken: er wordt een zekere mate van *autonomie* verondersteld bij het laten van de keuze. We zagen eerder dat *begrip* hiervoor noodzakelijk is. Als dit begrip echter ontbreekt, leidt dit niet alleen tot problemen voor de totstandkoming van autonome handelingen, maar vormt dit ook de aanleiding om het beleid ten aanzien van de betreffende toestemming situatie te heroverwegen.

In de casebeschrijvingen formuleerden we steeds een aantal materiële redenen en consequenties die het afwegen waard zouden kunnen zijn. Deze richtten zich steeds op de specifieke situatie en de mogelijke afwegingen over gebruik en misbruik van de betreffende informatie. Voor het te buiten gaan dan die contexten was op de afzonderlijke keuzemomenten zelf ook geen directe rede. Het is echter juist het digitale karakter van de persoonlijke data die goed *begrip* in deze situaties bemoeilijkt: unieke eigenschappen aan de nieuwe technologie leiden tot gevolgen die zeer waarschijnlijk materieel zijn voor individuen, maar op de beslissingsmomenten zelf slecht te overzien. Dit inzicht in de werking van digitale systemen wordt tegenwoordig ook wel *digital literacy* genoemd.[45]

[45] Jenkins (2009) p. 28

Plaats: 'Greased' informatie

Computers maken het mogelijk om informatie op verschillende manieren eindeloos te manipuleren: sorteren op talloze eigenschappen, lokaliseren op basis van verschillende soorten input en weergave met ontelbare mogelijkheden. Hier plukken we in het dagelijks leven steeds meer te vruchten van en we zouden waarschijnlijk niet meer zonder kunnen. Maar volgens Moor schuilt hierin ook een gevaar: wanneer informatie wordt gedigitaliseerd wordt *gesmeerd* ('greased').[46] Informatie kan zodanig worden bewerkt dat het steeds gemakkelijker en sneller kan worden opgeroepen. Dezelfde systemen die het terugvinden van data snel en comfortabel maken, scheppen in potentie de mogelijkheid voor ongepaste blootstelling.[47] Waar telefoonboeken eerder nummers en achternamen bevatten, zijn databases bijvoorbeeld steeds vaker in staat telefoonnummers aan adressen, online profielen en bedrijven te koppelen. De aaneenschakeling van zenders en ontvangers heeft de kenmerken van een doolhof en is potentieel oneindig, waarbij instituten geheel of zijdelings betrokken raken waarvan de verantwoordelijkheden beperkt beschreven of begrepen worden.[48]

In het geval van het EPD-LSP wordt hiermee duidelijk hoe consequenties die voor een patiënt op het eerste oog vrijwel onmogelijk te overzien zijn, weldegelijk materieel zouden kunnen zijn voor toestemming. Veronderstel bijvoorbeeld de mogelijkheden die een dergelijk systeem in vergevorderd stadium biedt voor de meta-analyse van gegevens: analyses als deze zouden met toenemende nauwkeurigheid voorspellingen kunnen doen aan de hand van het persoonlijke medische dossier, op basis van het geheel aan data. Als deze analyses vervolgens invloed zouden hebben op de geboden zorg en een patiënt volgens berekeningen bijvoorbeeld niet meer in aanmerking komt voor bepaalde medicijnen, dan is dit vrijwel zeker een materiële consequentie. De manipulatie van digitale data creëert op deze manier dus een context waarin de informatie een andere betekenis en functie krijgt.

Tijd: 'Documentary capacities'

Niet alleen is digitale data onbeperkt bewerkbaar en te doorzoeken, ook hebben de systemen relatief grote 'documentary capacities': door het toenemende gebruik van digitale middelen laten we continue sporen achter die in potentie lange tijd bewaard

[46] Moor (1997) p. 27
[47] Moor (1997) p. 27
[48] Barocas & Nissenbaum (2014) p. 60

kunnen worden.[49] Warren en Brandeis, die we eerder aanhaalden voor een oorspronkelijke formulering van het begrip van privacy, hadden vergelijkbare zorgen over de eerste draagbare camera's die een doorlopende verslaglegging van mensen mogelijk maakte. De hedendaagse techniek maakt uiteraard het veelvoudige mogelijk. Vast en draagbare apparatuur is in staat continue data op te slaan en te controleren, die voor onbepaalde tijd op een afgelegen plek wordt opgeslagen.[50]

Inzicht in de tijd dat informatie over surfgedrag wordt opgeslagen kan in het geval van cookies bijvoorbeeld materieel worden voor een gebruiker, wanneer informatie over bepaalde aankopen of bezoek aan specifieke fora langdurig achterblijft in databases van websitebeheerders. Maar ook in het geval van data over rijgedrag kan de oneindige capaciteit van systemen een potentieel probleem vormen. Hoe lang een consument bijvoorbeeld als chauffeur voor bepaald soort rijgedrag verantwoordelijk kan worden gehouden zal in eerste instantie bijvoorbeeld niet snel een overweging zijn. Wanneer data echter door een zorgverzekeraar systematisch wordt opgeslagen en ingezet om voorspellingen te doen over de schade gedurende een jaar, dan zou dit naar alle waarschijnlijkheid veranderen.

Data: 'Black boxing'

Ten slotte heeft digitale data de eigenschap product te zijn van techniek die het product is van menselijk handelen, maar waarvan vaak nog slechts beperkt wordt begrepen hoe die in de kern werkt. Voor het leeuwendeel van de gebruikers geldt dat er sprake is van een 'black box': op het niveau van code, algoritmen en de relatie tussen input en output is niet meer duidelijk hoe resultaten precies ontstaan.[51] Bias en een misplaatste beoordeling van patronen en verbanden als objectief zijn belangrijke problemen voor digitale systemen waarvan de werking beperkt wordt begrepen.[52] Algoritmen hebben het voordeel zonder tussenkomst van menselijke beoordeling tot conclusies te komen en op deze manier afstand te scheppen, maar zijn bij ontwerp altijd onderhevig aan menselijke waarden. Bestaande vooroordelen en categorisering worden zo systematisch gehandhaafd en uitvergroot.

Een implicatie van complexe techniek voor de case over rijgedrag is

[49] Allen (2011)
[50] Ibid.
[51] Rieder & Röhle (2012) p. 75
[52] Angwin (2016)

bijvoorbeeld dat bij het in kaart brengen van rijstijl en beweging gebruik wordt gemaakt van locatiegegevens om gemiddelde snelheden uit te rekenen. De informatie over de verblijfplaatsen van een individu maakt op zichzelf geen expliciet deel uit van de data die wordt opgeslagen of van de dienst als geheel, maar kan met kennis van de techniek worden geabstraheerd. De werkende techniek en algoritmen zijn in eerste instantie niet inzichtelijk, maar maken in een vervolgstadium wel dingen mogelijk die materieel zijn voor een consument. Bias in dit systeem zou er bovendien voor kunnen zorgen dat bepaald rijgedrag op basis van aanvullende gegevens, als geslacht of leeftijd, sneller wordt beoordeeld als roekeloos.

Autonomy gaps

We zien nu dus hoe gemakkelijk het is te onderschatten wat burger en consument zouden moeten kunnen overzien om een goed geïnformeerde, en daarmee autonome, keuze te kunnen maken over het afstaan van persoonlijke informatie aan een digitaal systeem. De moderne informatiesamenleving is er steeds meer op ingericht te antwoorden aan de roep om keuze en maatwerk, waarvan de beschreven cases voorbeelden zijn. We leven in zijn algemeenheid, onder invloed van langlopende processen van individualisme en liberalisme, in een tijdperk van onvoorwaardelijke inzet om keuze mogelijk te maken.[53] In de praktijk blijken we echter bijzonder slecht om te kunnen gaan met deze keuzevrijheid.[54] In het geval van privacy is dit, gezien de analyse van Allen, niet anders. Men wil transparantie en de eigen informationele privacy beschermen, maar lijkt daar maar zeer beperkt toe in staat.[55] Nu we inzicht hebben in de eigenschappen van digitale systemen die *begrip* van consequenties voor de eigen privacy als noodzakelijkheid voor een autonome handeling bemoeilijken, hebben we een manier om te begrijpen waarom deze paradox ontstaat. Keuzemomenten zoals we in de casebeschrijvingen zagen sluiten niet aan bij de beperkte capaciteiten van individuen om de in potentie verstrekkende gevolgen van het weggeven van persoonlijke informatie in een digitale context te overzien.

Deze discrepantie tussen de keuzestructuren die bepaalde capaciteiten veronderstellen en capaciteiten die individuen daadwerkelijk bezitten, is wat Anderson beschrijft als een *autonomy gap.*[56] Sociaal beleid, praktijken en instituten kunnen worden

[53] Anderson p. 1
[54] Ariely (2008)
[55] Frissen (2016)
[56] Anderson p. 6

gezien als gevallen van collectieve ondernemingen, waarbij min of meer specifieke aannames worden gedaan over de manier waarop die zullen werken en of redelijk is te veronderstellen dat ze gerealiseerd en onderhouden kunnen worden.[57] De meest essentiële aanname hierbij is de veronderstelling van de competentie van individuen die met deze praktijken in aanraking zullen komen. We hebben in de cases vastgesteld dat het bij geïnformeerde toestemming situaties mogelijk is om tot op zekere hoogte de voor- en nadelen van het weggeven van persoonlijke informatie te achterhalen. Wat concreet met data mag en zal worden gedaan kan bijvoorbeeld worden vastgelegd in verklaringen of in sommige gevallen gecommuniceerd met experts. Als dit niet zo zou zijn, zouden we kunnen zeggen dat de informatie over de dienst, bijvoorbeeld korting op premies, cruciale componenten mist.[58] Maar zoals we hebben gezien houdt het hier niet op: bij het laten van de keuze om persoonlijke informatie af te staan in een digitale context, wordt verondersteld dat het individu inzicht heeft de kenmerkende oncontroleerbaarheid van digitale data en de problemen die deze vormt voor informationele privacy. Een veel bredere en uitvoerigere afweging van waarschijnlijkheden en risico's is noodzakelijk om te kunnen spreken van een strategische, autonome keuze. Het is onredelijk te veronderstellen dat significant grote groepen individuen de benodigde capaciteiten hebben.

Kritiek op geïnformeerde toestemming: collectief zelfbedrog

Hiermee komen we op de normatieve vraag: is het een probleem dat mensen niet-autonome keuzes maken over hun informationele privacy? Zoals we bij de analyse van Allen benoemden, is het doel niet een normatieve beoordeling te verbinden aan het vergeven of beschermen van privacy. De kritiek ligt in de paradox tussen de collectieve waarden die de grond zijn voor geïnformeerde toestemming situaties en de beperkte mate waarin uiting gegeven kan worden aan die waarden in die specifieke situaties. Zoals we zagen ontstaat geïnformeerde toestemming uit geldende waarden als privacy en democratie; door individuen controle te geven over persoonlijke informatie geven we uitdrukking aan de collectieve wil om deze waarden te beschermen. Nu we echter zien hoeveel deze situaties in feite aan inzicht vergen van individuen, is het onredelijk te veronderstellen dat zij de capaciteiten hebben tot een autonome keuze te komen: in de

[57] Ibid. p. 9
[58] Anderson p. 10

praktijk is geïnformeerde toestemming in digitale contexten dus niet in staat waarden als privacy of democratie te realiseren of beschermen.

Vrijwillig beperkt begrip

Volgens deze analyse worden we nu dus geconfronteerd met de situatie dat een veelgebruikte en basale methode, met als motivatie de bescherming van bepaalde geldende waarden en ideeën, in een context die steeds belangrijker wordt, niet op die manier functioneert. Hoe kunnen we geïnformeerde toestemming situaties dan betekenis geven? Voor ik een antwoord probeer te formuleren op deze vraag, moeten we nog de mogelijkheid overwegen dat individuen vrijwillig een beperkte mate van begrip onderschrijven. In een situatie als deze erkent het individu dat er zaken zijn waar zij geen zicht op heeft, maar besluit onder invloed van bepaalde motivaties te accepteren dat dit zo is en gaat al dan niet over tot toestemming. Een voorbeeld van een motivatie om weg te blijven van toegankelijke informatie is de angst voor de impact van een veranderende overtuiging op het eigen gedrag.[59] Het vrijwillig in het ongewisse blijven vormt in potentie een probleem voor de analyse van geïnformeerde toestemming als *autonomy-gap*: een beperkte mate van begrip als noodzakelijkheid voor autonomie is immers geen punt meer, omdat deze wel wordt erkend maar beoordeeld als ongewenst of onbelangrijk.

Opnieuw is de inzet hier niet een normatieve beoordeling te geven, maar te refereren aan de reden waarom geïnformeerde toestemming überhaupt bestaat en mogelijk is. Een centrale functie is het individu in te lichten over voordelen en risico's van het vrijgeven van persoonlijke informatie. Eventuele risico's en gevolgen kunnen immers groot zijn: de manier waarop informatie wordt beschermd en voor bepaalde doeleinden mag en kan worden gebruikt, staat mogelijkheden tot verlies of verkeerd gebruik toe.[60] De schade die dit kan veroorzaken aan de informationele privacy heeft invloed op de mate waarin een individu haar toekomst kan vormen.[61] Geïnformeerde toestemming is er op ingericht inzicht te geven in deze mogelijkheden. Het niet willen kennen van deze materiële informatie zet dus in potentie de deur open voor een informatiesamenleving waarin die geïnformeerde toestemming niet meer nodig wordt geacht: openbaring wordt, zoals Allen stelde, de standaardoptie.[62] Dit is natuurlijk mogelijk, wanneer informationele

[59] Carrillo & Mariotti (1999) p. 529
[60] Ploug & Holm (2013) p. 1098
[61] Ibid. p. 1099
[62] Allen (2013) p. 848

privacy niet meer wordt gezien als een waarde die we dienen te beschermen. Zoals ik vaststelden, is hier echter (nog) geen sprake van.

Conclusie: collectief zelfbedrog

In de betekenisgeving van geïnformeerde toestemming is de aanname dan ook aan dat het individu gemotiveerd is een zo compleet en materieel mogelijke afweging te maken en dat de situaties die door autoriteiten worden gecreëerd op deze behoefte zijn ingericht. De taak is nu dus vast te stellen waarom geïnformeerde toestemming situaties vaak worden ingericht, terwijl deze in de praktijk dus slecht in staat zijn hetgeen te beschermen waar ze voor gemaakt zijn. Een mogelijkheid is manipulatie: de toestemmingzoeker maakt keuzemomenten mogelijk en kent alle mogelijke overwegingen, maar is zich er van bewust dat het individu hierover nooit volledig geïnformeerd zal zijn. Een andere mogelijkheid is dat de toestemmingzoeker in de oprechte overtuiging leeft dat het individu een goede afweging kan maken, maar dit om de genoemde redenen niet mogelijk is. Beleid zou er dan op gericht moeten zijn de inzichten die de toestemmingszoeker heeft, beter over het voetlicht te brengen.

Aannemelijker is het echter dat zowel toestemmingszoekers, zoals overheid en bedrijven, maar ook burgers en consumenten, geen inzicht kunnen hebben in de mogelijke gevolgen van de digitale systemen die ze gebruiken, juist vanwege de genoemde kenmerken die ze moeilijk te kennen maken, maar wel weten dat die gevolgen eventueel bestaan. Dat men zich van dat laatste bewust is, of in het geringste geval een vermoeden heeft dat er risico's bestaan, zou een goede rede zijn om te verklaren waarom geïnformeerde toestemming überhaupt bestaat. Hiermee ontstaat echter de vreemde contradictie dat vanuit bestaande maatschappelijke waarden regelgeving wordt geïntroduceerd, waarvan we ons tegelijk bewust zijn dat deze maar beperkt in staat is deze waarden te beschermen of creëren.

Overweeg in het licht van deze verklaring wat Faden et al. beschrijven als een tweede *betekenis* (sense²) van toestemming.[63] Toestemmingen zijn kortweg niet altijd autonome handelingen. In sommige gevallen is eerder sprake van 'effectieve' toestemming: een beleidsgeoriënteerde vorm waarvan de condities niet louter afleidbaar zijn van het concept van autonomie, of zelfs algemene opvattingen van respect voor autonomie hoeft

[63] Faden et al. (1986) p. 280

te bevatten.[64] Deze vorm is een wettelijk of institutioneel 'effectieve' toestemming, omdat die voldoet aan de regels en procedures die binnen een specifiek instituut gelden en krijgt soms de misleidende titel 'valide'. Het voornaamste doel van deze vorm is eerder het reguleren van het gedrag van de 'toestemmingzoeker' in een kader van regelgeving, dan het individu in staat te stellen een autonome handeling te verrichten.[65] De wettelijke doctrine die 'geïnformeerde toestemming' heet belooft in die zin veel meer dan het kan waarmaken: de wettelijk opgelegde verplichting zou onderscheiden moeten worden van het *idee* van geïnformeerde toestemming dat individuen een weloverwogen en beduidende rol hebben in het besluitmakingsproces.[66]

Bekijken we nu bijvoorbeeld opnieuw de toestemming voor cookies, dan lijkt de situatie in een aantal opzichten op deze betekenis van het concept. Zo wordt de toestemming bij iedere individuele website gevraagd, waarmee de handeling routinematig wordt en de kans op een weloverwogen beslissing met de tijd zal afnemen. Stellen we ons een situatie voor waarbij een gebruiker bij het betreden van het internet toestemming dient te geven voor het opslaan van data voor alle websites gedurende een jaar, dan ligt een uitgebreidere analyse van de gevolgen meer voor de hand. Daarnaast is niet instemmen in deze situatie vaak gecompliceerd of zelfs onmogelijk, waarbij de gebruiker alleen kan aangeven kennis te hebben genomen van de cookies. Een simpele druk op een knop is voldoende voor instemming en uitgebreide informatie is in eerste instantie vaak verborgen achter links. Hoewel er in deze situatie dus wordt gesproken van 'geïnformeerde toestemming', is van substantieel begrip en daarmee een autonome handeling in veel gevallen nauwelijks sprake. Zeker in digitale contexten is vaak sprake van routinematige vorm van toestemming.[67]

Waar de pretentie van geïnformeerde toestemming is dat individuen hun informationele privacy kunnen beschermen, zijn we ons tegelijk bewust van onze collectieve beperkte capaciteiten om alle materiële risico's van digitale technologie te overzien. Het diepe probleem met beleid dat *autonomy-gaps* teweeg brengt, is dat het gebruik ervan noodzakelijkerwijs tot een contradictie leidt in onze collectieve wil[68]: de motivatie voor het introduceren van de regelgeving is de wil en de overtuiging autonoom

[64] Ibid.
[65] Ibid. p. 281
[66] Katz (1980) p. 122
[67] Ploug & Holm (2013) p. 1098
[68] Anderson p. 10

te zijn - het idee dat er sprake is van controle over de persoonlijke informatie van onszelf en anderen in een digitale context - en tegelijk het bewustzijn dat die niet of heel beperkt mogelijk is. Om te begrijpen hoe dit soort beleid ontstaat en wordt onderhouden, moeten we uiteindelijk beroep doen op het soort van denken dat centraal staat in vormen van zelfdeceptie.[69] De mens heeft een sterke neiging zeer bewerkbare 'positieve illusies' op te nemen, die noodzakelijk zijn voor meeste basale dagelijkse functioneren.[70] We willen geloven dat we controle hebben over onze informationele privacy, terwijl we weten dat dit niet daadwerkelijk mogelijk is; wat overblijft is het soort van lege geïnformeerde toestemming dat Faden et al. beschrijven in haar 'effectieve' vorm. Van het 'idee' van geïnformeerde toestemming, dat in staat is de centrale waarden te beschermen die we ermee voor ogen hebben, kan in digitale contexten echter geen sprake zijn; hiervoor zijn capaciteiten tot begrip noodzakelijk die de kenmerken van digitale data nog niet toe staan.

[69] Ibid.
[70] Taylor (1989)

Literatuur

- Allen, A. (2011). *Unpopular Privacy: What Must We Hide?*. Oxford University Press, 4:29.

- Allen, A. (2013) *An Ethical Duty to Protect One's Own Information Privacy?*. Faculty Scholarship Paper 451.

- Anderson, J. (forthcoming). *Autonomy gaps as a social pathology: Ideologiekritik beyond paternalism*. In Rainer Forst (ed.), Sozialphilosophie und Kritik. Suhrkamp

- Angwin, J. L. (2016). *Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And it's Biased Against Blacks*. ProPublica. Geraadpleegd 14 juni 2016, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

- Ariely, D. (2008). *Predictably Irrational: The Hidden Forces That Shape Our Decisions* (New York: HarperCollins.

- Barocas, S. & Nissenbaum, H. (2014). *Big Data's End Run around Anonymity and Consent*. In: Privacy, big data, and the public good (Lane, J.) pp. 44-75.

- Faden, R., Beauchamp, T., & King, N. (1986). *A history and theory of informed consent*. New York: Oxford University Press.

- Fisher, J. A. (2013). *Expanding the Frame of "Voluntariness" in Informed Consent: Structural Coercion and the Power of Social and Economic Context*. Kennedy Institute of Ethics Journal 23 (4):355-379.

- Floridi, L. (1999). *Information ethics: on the philosophical foundations of computer ethics*. Ethics and Information Technology, 1(1), 37–56

- Floridi, L. (2008) *Foundations of Information Ethics*. In: The Handbook of Information and Computer Ethics (eds K. E. Himma and H. T. Tavani), John Wiley & Sons, Inc., Hoboken, NJ, USA.

- Henkin, L. (1974). *Privacy and autonomy*. Columbia Law Review, 77, 1410–1425.

- Jenkins, Henry (2009). *Confronting the Challenges of Participatory Culture: Media Education for the 21st Century* (PDF). Cambridge, MA: The MIT Press.

- Katz, J. (1980) *Disclosure and Consent*. In: A. Milunsky and G. Annas, Genetics and the Law II (New York: Plenum Press, 1980)

- Manson, N. & O'Neill, O. (2007). *Rethinking informed consent in bioethics*. Cambridge: Cambridge University Press.

- Moor,J.H. (1997). *Towards a theory of privacy in the information age*. Computers and Society, 27(3), 27–32.

- Moor, J.H. (2006). *Using genetic information while protecting the privacy of the soul*. In: Tavani, H.T. (Ed.), Ethics, Computing, and Genomics, Jones and Bartlett, Sudbury, MA, pp. 109–119.

- Posner, E. (2011). *Liberalism and Concealment*. New Republic. Geraadpleegd 14 juni 2016, https://newrepublic.com/article/94037/unpopular-privacy-anita-allen

- Rieder, B. & Röhle, T. (2012). *Digital Methods: Five Challenges*, in: David M. Berry (ed.), Understanding Digital Humanities (Basingstoke en New York: Palgrave Macmillan, 2012) 86-103

- Rössler, Beate (2002). *Problems with autonomy*. Hypatia 17 (4):143-162.

- Rössler, B. (2013). *Autonomy, Paternalism, and Privacy: Some Remarks on Anita Allen*. APA Newsletter Philosophy and Law 13:13-17.

- Tavani, H.T. (2007). *Philosophical theories of privacy: implications for an adequate online privacy policy*. Metaphilosophy, 38(1), 1–22.

- Tavani, H. T. (2008). *Informational privacy: Concepts, theories, and controversies*. The Handbook of Information and Computer Ethics (eds K. E. Himma and H. T. Tavani), John Wiley & Sons, Inc., Hoboken, NJ, USA., 131-164.

- Taylor, S. E. (1989) *Positive Illusions: Creative Self-Deception and the Healthy Mind* (New York: Basic Books.

- Unesco. (1998). *World information report*. Paris: UNESCO Pub.

- Warren S. & Brandeis L. (1890) *The Right to Privacy* (4 Harvard L.R. 193)