

HIER VLOEKT MEN NIET,
FACEBOOK ZIET ALLES

HIER VLOEKT MEN NIET,
FACEBOOK ZIET ALLES

Sociale netwerken ontrafeld

Rob Heyman, Annet Daems, Dorien Baelden en Jo Pierson

Met een voorwoord van Dominique Deckmyn

 **DAVIDSFONDS**
UITGEVERIJ



agentschap voor Innovatie
door Wetenschap en Technologie

Rob Heyman, Annet Daems, Dorien Baelden en Jo Pierson
Hier vloekt men niet, Facebook ziet alles. Sociale netwerken ontrafeld

© 2013, Rob Heyman, Annet Daems, Dorien Baelden, Jo Pierson en Davidsfonds Uitgeverij nv
Blijde Inkomststraat 79, 3000 Leuven
www.davidsfondsuitgeverij.be
[www.twitter.com/davidsfonds](https://twitter.com/davidsfonds)
www.facebook.com/davidsfondsuitgeverij

Vormgeving cover: Davidsfonds Uitgeverij
Vormgeving binnenwerk: Smets & Ruppel
D/2013/0240/64
ISBN 978-90-6306-647-5
NUR 740, 810



Alle rechten voorbehouden.

Niets uit deze uitgave mag worden verveelvoudigd,
opgeslagen in een geautomatiseerd gegevensbestand
en/of openbaar gemaakt in enige vorm of op enige wijze,
hetzij elektronisch, mechanisch, door fotokopieën, opnamen
of op enige andere manier zonder voorafgaande schriftelijke
toestemming van de uitgever.

INHOUD

Voorwoord	7
Inleiding	13
1. Facebook kijkt mee	21
2. Waarom is Facebook gratis?	47
3. Kinderen, jongeren en sociale media: over risico's, regelgeving en empowerment	77
4. Identiteit en privacy	105
5. <i>Roadmap</i> voor socialemediawijsheid	125
Conclusie: sociale media en empowerment	131
Werkten mee aan dit boek	139
Noten	141

VOORWOORD

Dominique Deckmyn

Privacy. Het is niet meteen een woord dat van de tong rolt. Een lelijk, ongemakkelijk leenwoord voor een stoffig begrip. Wie over zijn 'privacy' begint, klinkt al snel als een zeurpiet. Erger nog: een ouwe zeurpiet. Want privacy, daar zijn de 'millennials', de 'digital natives' toch niet mee bezig?

De digital natives, zij die hun hele leven al met het internet vertrouwd zijn, die leiden hun leven ongegeneerd in het publiek. En daarin hebben ze per definitie gelijk, want uiteraard hebben de natives het internet beter begrepen dan de 'digital immigrants', die pas op volwassen leeftijd met het web kennismaakten. Of niet soms?

Het web, 'the cloud', dat is modern en opwindend. Privacy is een vaag, abstract begrip waar we niet eens een Nederlands woord voor hebben – dus hoe belangrijk en hoe relevant kan het zijn?

Het lijkt ook geen rationeel begrip te zijn. Wie zijn terughoudendheid tegenover, pakweg, Facebook wil verdedigen, die klinkt weinig overtuigend. Als iemand anders daar dan tegenover stelt dat je van Facebook tenslotte toch een heel nuttige dienst krijgt, helemaal voor niets, en dat je dus niet moet zeuren, dan klinkt dat heel nuchter en redelijk.

Er bestaan ook preciezere begrippen, zoals die in de wetgeving kunnen worden gebruikt. Het begrip persoonsgegevens, bijvoorbeeld. Ook dat is niet onduidelijk, want het kan ons leiden naar een eindeloze discussie over wat wel en niet een persoonsgegeven is. Onze naam en ons straatadres zijn dat zeker. Maar wat met ons IP-adres? Dat IP-adres laat toe om ons uniek te identificeren. En wat met een foto van ons gezicht? Uiteindelijk blijkt dat heel veel schijnbaar 'anonieme' informatie in feite gebruikt kan worden om ons uniek te identificeren – mocht iemand daar de nodige tijd in willen steken. Dus ook met het begrip 'persoonsgegevens' komen we niet heel veel verder.

Toch is het belangrijk dat we in heldere termen leren nadenken en spreken over de gegevens die heel dicht bij onze identiteit liggen. Dat wordt zelfs steeds belangrijker, en wel omdat een steeds groter deel van de economie juist rond die gegevens draait.

De voorbije vijf jaar is een economie ontstaan waarin we niet betalen met geld maar wel met gegevens over onszelf. In een klassieke economische transactie zijn twee partijen betrokken: klant en leverancier, koper en verkoper. Vraag en aanbod, die, in een economisch systeem, naar een evenwicht streven. Maar in deze nieuwe economie zijn er bijna altijd drie partijen: de leverancier van de diensten, de afnemer van de diensten en de partij die voor de dienst betaalt – meestal een adverteerder. De afnemer van de diensten beschouwt zichzelf als de ‘klant’ van de leverancier, maar is dat eigenlijk niet. Wij zijn met z’n allen niet de klanten van Facebook. Wij zijn het product dat door Facebook aan zijn echte klant, de adverteerder, wordt aangeboden.

Dat de adverteerder voor een dienst betaalt, is natuurlijk niet nieuw. Het is al decennialang het basisprincipe achter commerciële televisie. Maar er is wel een verschil, namelijk in de ‘tegenprestatie’ die van de consument wordt verwacht in ruil voor de ‘gratis’ dienst. Bij commerciële televisie ‘betaalt’ de kijker met zijn tijd: enkele minuten per uur moet hij zich overleveren aan de commerciële boodschappen van de adverteerder. Die krijgt in die minuten de kans om ons te overtuigen, of om onze keuzes op een of ander niveau te beïnvloeden. Als het niet werkte, zouden ze dat geen halve eeuw lang hebben volgehouden.

In dit nieuwe economische model betaalt de consument ook nog met iets anders: met gegevens over zichzelf. Dat is een fantastische, nieuwe munteenheid, met unieke eigenschappen. Hij is, bijvoorbeeld, onuitputtelijk. Of zo lijkt het toch. Een euro kun je maar één keer besteden, een minuut tijd ook. Maar mijn e-mailadres kan ik elke keer opnieuw geven, in ruil voor een gratis dienst. En hoe vaak ik ze ook uitgeef, ik word niet armer. Ik ben niets ‘kwijt’.

Maar hoe werkt die transactie precies? We hebben nog niet veel tijd gehad om deze ruilhandel met persoonsgegevens te analyseren. Vergeet niet dat de pioniers van de economische wetenschap er enkele eeuwen over gedaan hebben om de mechanismen van vraag en aanbod echt te doorgronden. De mechanismen van dit nieuwe economische systeem zijn zich nog volop aan het ontwikkelen. En dus is het ook verdraaid moeilijk om te zeggen of de drie partijen er wel op een gelijke manier voordeel uit halen. Krijgen we van Facebook een geweldig cadeau? Worden we door de sociale netwerken opgelicht en van onze meest

intieme gegevens beroofd? Of is het een evenwichtige deal?

Er zijn wel een paar cijfers die houvast geven. Maar dat is rekenwerk op de achterzijde van een envelop. Het bedrijf Facebook is bijna 50 miljard euro waard. Het heeft 1 miljard gebruikers. Een beetje kort door de bocht kunnen we zeggen dat elke gebruiker 50 euro waarde vertegenwoordigt. Of dat meent de collectieve intelligentie van alle beleggers toch – zij kunnen zich daar natuurlijk ook in vergissen. Maar tot iemand met een beter cijfer komt, kunnen we aannemen dat alle gegevens die Facebook over ons bezit 50 euro waard zijn.

Dat klopt natuurlijk niet helemaal. Facebook biedt adverteerders in feite twee dingen: gegevens over de gebruikers, maar ook de mogelijkheid om die gebruikers advertenties te tonen die afgestemd zijn op die gegevens. Het ene is niets waard zonder het andere. In de praktijk maakt Facebook momenteel ongeveer 4 miljard euro omzet op jaarbasis. In het afgelopen jaar heeft Facebook dus ongeveer 4 euro verdiend aan de adverteerders die u willen bereiken. Dat is overigens een piepklein bedrag. Een commerciële zender als VTM verdient ongeveer het tienvoudige aan elke Vlaamse kijker.

Maar of het nu enkele euro's is, of enkele tientallen euro's, of misschien zelfs veel meer: wij beschikken in ieder geval over een behoorlijk startkapitaal om te gaan shoppen in deze nieuwe sociale economie.

We moeten er wel rekening mee houden dat er nog andere betrokkenen zijn in deze markt, behalve alleen onszelf, Facebook, en de adverteerder. Wie kijkt er allemaal mee naar ons digitale bestaan? Tja, wie niet, eigenlijk? Oplichters, inbrekers, stalkers, kinderlokken, belastingcontroleurs – en vul maar aan met uw favoriete boeman. Uiteraard leren we onze kinderen om daar mee om te kunnen gaan. Maar hoe goed je ook vertrouwd bent met de privacyinstellingen van Facebook, je kunt niet meedraaien in de nieuwe digitale samenleving zonder overal sporen na te laten.

Pour vivre heureux, vivons cachés, zegt een Frans spreekwoord. Facebook vertelt ons net het omgekeerde: we zullen gelukkiger zijn als we steeds meer dingen in het openbaar doen. Ons digitale leven is hoe dan ook in hoge mate zichtbaar. Zelfs als we vaardig omgaan met de privacyinstellingen van Facebook. Dat we liever geen dronken foto's van onszelf met de hele buitenwereld delen, dat hebben heel wat jongeren ondertussen wel begrepen (en de anderen leren het snel genoeg). Maar het gaat om veel meer dan dat. Een voorbeeld? Elke foto van ons gezicht die op het internet te vinden is en waar onze naam bij staat, kan morgen worden gebruikt om ons te herkennen op straat. De technologie daarvoor

bestaat, het is maar afwachten tot iemand ze inbouwt in, bijvoorbeeld, zo'n Google Glass-bril. Handig, nietwaar?*

Een restauranthouder of een fondsenwerver zal u meteen uit de voorbijgangers kunnen pikken als iemand die houdt van Mexicaans eten of van Amnesty International.

Zijn we verplicht om dit spelletje mee te spelen? Om mee te draaien in deze economie waarin we zelf de munteenheid zijn? Niet altijd. In sommige gevallen kunnen wij beslissen om echt geld te betalen voor een dienst, in plaats van deze ruilhandel met gegevens over onszelf. Voor de meeste 'gratis' apps en webdiensten bestaat wel een betalend alternatief dat onze privacy beter respecteert. Maar net in het geval van Facebook is dat moeilijk. Er zijn best wel andere sociale netwerken, maar je dreigt daar in je eentje te zitten, terwijl je vrienden elkaar via Facebook uitnodigen voor feestjes waar jij niets van weet. Tenzij je al je vrienden kunt overtuigen om mee te verhuizen.

Hoe dan ook: als u beslist om een profiel aan te maken op Facebook, voegt u 50 euro toe aan de waarde van dat bedrijf. Een niet onaardig bedrag. Vindt u dat het gebruik van Facebook u ook 50 euro aan waarde heeft opgebracht? En vindt u dat de risico's die u oploopt door uw gegevens daar te kijken te zetten, daarmee in evenwicht zijn? In dat geval is het een faire deal. Er is bovendien nog een tweede significante vraag om te stellen: mocht u die optie krijgen, zou u dan 50 euro betalen om één jaar – of voor altijd – Facebook te mogen gebruiken? Maar dan een Facebook zonder gepersonaliseerde reclame?

Misschien zal Facebook zich ooit gedwongen voelen om een privacyoptie toe te voegen. Een optie waarbij, ik zeg maar wat, al je Facebook-profielinformatie versleuteld is, op een manier dat alleen je Facebook-vrienden die kunnen lezen – en niet Facebook zelf. En waarbij er geen advertenties staan op Facebook. Technisch is dat niet moeilijk. Misschien zal Facebook die optie ooit aanbieden, onder druk van de markt. Op dat moment zul je echt keuze hebben. Het zou ook interessant zijn om te zien hoeveel zo'n optie zou kosten. Het zou waarschijnlijk meer zijn dan 4 euro per jaar, maar niet zo heel veel meer.

In tussentijd betalen we dus met die vreemde nieuwe, schijnbaar onuitputtelijke munteenheid. Als ik mijn gegevens aan Facebook geef, om het nieuws van mijn vrienden te kunnen zien, dan is er niets verdwenen. Ik kan dezelfde gegevens ook

* Op het moment van schrijven heeft Lambda Labs een API gelanceerd die hiertoe in staat is. Google heeft bewust gekozen om deze functionaliteit niet te implementeren, maar het verbiedt zijn ontwikkelaars niet om dit te doen. <http://techcrunch.com/2013/05/23/lambda-labs-is-launching-a-facial-recognition-api-for-google-glass/>

nog eens aan Google geven. Wat je 'kwijt' bent, heeft alleen maar die oubollige naam: privacy.

Precies daarom hebben bedrijven als Facebook en Google er nu alle belang bij om u de indruk te geven dat privacy in feite niet bestaat. En dat u dus helemaal niets opgeeft als u beslist om uw leven voor een flink stuk in het openbaar te leiden, via hun websites. Toch is dat onzin. Persoonsgegevens zijn de munteenheid van een hele sector van de economie geworden. Wie zijn persoonsgegevens te grabbel gooit, die gooit dus geld weg – bijna letterlijk.

Het zou nuttig zijn als we een wat hipper woord hadden voor privacy. Maar belangrijker dan dat is dat we dit nieuwe economische systeem beter doorgronden. Dat we een beter zicht krijgen op wat we precies (op)geven wanneer we ons aansluiten bij een dienst als Facebook, en wat we daarvoor terugkrijgen.

Net daarom was er dringend een boek zoals dit nodig. In ons achterhoofd zit ieder van ons met vage bezorgdheden over wat er met onze gegevens gebeurt als we ze aan een sociaal netwerk als Facebook overhandigen. In dit boek worden veel van die bezorgdheden bevestigd, gerelativeerd of tegengesproken. En zo leren we wat Facebook ons werkelijk kost. Niet om ons te overtuigen om er voortaan maar weg te blijven – al zou dat voor sommigen onder ons best weleens het effect kunnen zijn. Wel om ervoor te zorgen dat – welke beslissing we ook nemen – het tenminste een geïnformeerde beslissing zal zijn.

INLEIDING

Annet Daems, Dorien Baelden, Rob Heyman

L'histoire se répète?

Een halve eeuw geleden, in 1963 om precies te zijn, voorspelde sciencefictionauteur Philip Kindred Dick volgend toekomstscenario: 'Er zal een tijd komen waarin we niet langer zullen zeggen "Ze bespioneren me via mijn telefoon", maar wel "Mijn telefoon bespioneert me".*' Het is haast jammer dat de auteur, op wiens werk de film *Blade Runner* werd gebaseerd, het niet meer meemaakt – hij overleed in 1982 – want vijftig jaar na het verschijnen van zijn beroemde uitspraak lijkt dit toekomstscenario niet langer te behoren tot de sciencefiction, maar wel tot de realiteit. We leven in een snel veranderende, gemediatiseerde wereld waarin informatie- en communicatietechnologieën (ICT's), waaronder het internet, een steeds prominentere rol spelen. Met de opkomst van web 2.0, het interactieve net zeg maar, evolueerde het internet van een statisch naar een dynamisch netwerk, waarin de gebruiker een upgrade kreeg van consument naar producent. Naast het consumeren van media-inhouden kunnen gebruikers nu ook zelf informatie produceren en online verspreiden. Hoewel die evolutie vele voordelen heeft en bijgevolg vaak bejubeld wordt – denk maar aan de selfmade artiesten via YouTube, het organiseren van protestmarsen via sociaalnetwerksites en het snel verspreiden van nieuws via Twitter – heeft de medaille ook een keerzijde. Want wat gebeurt er met al de informatie die gebruikers online verspreiden? Wie heeft er toegang toe en hoe kunnen gebruikers zich beschermen tegen misbruik ervan? Hebben gebruikers, zoals voorspeld door Dick, (onbewust) de controle over hun gegevens overgedragen aan de communicatiediensten waarvan ze gebruikmaken?

* Vrije vertaling van: 'There will come a time when it isn't "They're spying on me through my phone" anymore. Eventually, it will be "My phone is spying on me".' Philip K. Dick, 1963.

Een belangrijk thema in Dicks oeuvre was – het zal u niet verbazen – gewijd aan de zogenaamde ontspoorde technologische vooruitgang, of, vrij vertaald, aan de snelle ontwikkelingen in technologie en de risico's die daarmee samenhangen. De ongerustheid die gepaard gaat met de introductie van nieuwe mediatechnologieën is natuurlijk niet nieuw. Veel van de discussies die oplaaien omtrent de voor- en nadelen van internet-gebaseerde technologieën verschillen nauwelijks van de debatten gevoerd rond de introductie van radio en televisie tijdens de eerste helft van de 20ste eeuw. Denk bijvoorbeeld aan de discussies omtrent de sociale en educatieve mogelijkheden van radio en televisie versus de gevaren gerelateerd aan de blootstelling aan ongewenste media-inhouden.¹

Oude wijn in nieuwe vaten dus? Niet helemaal. Ondanks het feit dat de introductie van internet-gebaseerde technologieën een aantal van de oude bezorgdheden weer doet oplaaien, kunnen er ook een aantal nieuwe bekommernissen geïdentificeerd worden. Die bekommernissen vloeien voort uit een aantal aspecten eigen aan de architectuur van ICT's. In tegenstelling tot de meer klassieke (analoge) media zijn nieuwe (digitale) media steeds vaker gekoppeld in netwerken. Die netwerkinfrastructuur maakt de automatisering van processen, het overbruggen van tijd en ruimte, en interactiviteit (communicatie en de productie en distributie van inhoud) mogelijk.² Naast de vele voordelen die deze nieuwe eigenschappen bieden, rijzen er met de toenemende participatie van de gebruiker ook een aantal vragen over onder meer de voorwaarden waaronder gebruikers participeren, de gegevens die zij online zetten, en de controle over de netwerken.

De geschiedenis leert dat discussies omtrent opportuniteiten en uitdagingen van nieuwe mediatechnologieën vaak in twee kampen zijn op te delen. Dit zijn utopische en dystopische denkbeelden waarbij de waarheid doorgaans in het midden te vinden is. Dat is ongetwijfeld het geval voor internettechnologieën. Gezien hun unieke eigenschappen lijkt een kritische blik op de wisselwerking tussen technologie en gebruiker ons echter niet overbodig. Zonder in de val te willen trappen van technologisch deterministische denkpatronen behandelt dit boek de bezorgdheden die gepaard gaan met het gebruik van internettechnologieën. Meer in het bijzonder focust het op het ontrafelen van de mechanismen van sociaalnetwerksites en de implicaties van deze mechanismen voor de gebruiker.

Sociaalnetwerksites: een hoera-verhaal zonder meer?

Om de werking van sociaalnetwerksites te ontrafelen en inzichten te verwerven in de risico's die gepaard kunnen gaan met het gebruik ervan, is het uiteraard belangrijk te begrijpen wat het begrip inhoudt. Een sociaalnetwerksite is een internetdienst waar een persoonlijk profiel kan worden aangemaakt door te registreren. Dat profiel wordt een digitale identiteit – bestaande uit persoonlijke gegevens – die gekoppeld kan worden aan profielen van andere gebruikers. Op die manier ontstaan er online netwerken die onderling verbonden deelnemers toelaten om contact te onderhouden, berichten te sturen, en multimediamateriaal zoals foto's en video's uit te wisselen. Een aantal bekende sociaalnetwerksites zijn Facebook, LinkedIn en Twitter. Online sociale netwerken zijn erg populair in Vlaanderen: minstens zeven op de tien Vlamingen zijn actief op één of meerdere sociaalnetwerksites. Momenteel is Facebook de populairste netwerksite (62,9% Vlamingen heeft een Facebook-account) gevolgd door Twitter (26,9%) en LinkedIn (21,5%). Zowat de helft van alle Vlamingen met een sociaalnetwerkkaccount (56,6%) zegt geen dag zonder sociale media te kunnen.³

Die populariteit doet vermoeden dat gebruikers heel wat voordelen zien in het gebruik van sociaalnetwerksites. Inderdaad, de voordelen zijn legio en kunnen globaal gezien onderverdeeld worden in aspecten eigen aan sociale netwerken (denk bijvoorbeeld aan sociale contacten, steungroepen, entertainment, toegang tot informatie, identiteitsontwikkeling, enzovoort), welke vertaald worden naar een online omgeving, en aspecten eigen aan de unieke kenmerken van nieuwe mediaplatformen. Die laatste kunnen best uitgelegd worden aan de hand van wat de Spaanse socioloog Manuel Castells – een autoriteit op het gebied van nieuwe media – bestempelde als massa-zelfcommunicatie. Waar communicatie vroeger voornamelijk binnen familie- en vriendenkringen bleef, kan ze vandaag via sociale media openbaar gemaakt worden en bijgevolg een veel groter bereik krijgen. Massa-zelfcommunicatie, waarbij een individu iets meedeelt aan een groot publiek via het internet, is een nieuwe vorm van communicatie die is ontstaan met de intrede van (onder andere) sociaalnetwerksites. Door deze vorm van massa-zelfcommunicatie krijgen gebruikers de mogelijkheid om naast consumenten ook producenten van media-inhouden te worden. In vergelijking met pakweg tien jaar geleden kunnen gebruikers immers op een eenvoudiger manier veel meer informatie online zetten en verspreiden. Nieuwe mediaplatformen hebben met andere woorden de drempel verlaagd om inhoud te creëren, te selecteren en

te verspreiden. Voor Castells is dit een positieve evolutie. Hij onderstreept het emanciperend potentieel voor gebruikers die socialemediaplatformen, zoals sociaalnetwerksites, kunnen aanwenden om zichzelf uit te drukken en een publiek te vinden.⁴

Die voordelen en emanciperende aspecten van online sociale netwerken ten spijt kan het gebruik van sociaalnetwerksites ook een aantal risico's inhouden. Met behulp van krachtige computers, complexe algoritmes en geautomatiseerde processen worden socialemediaplatformen voortdurend geanalyseerd.⁵ Op die manier worden de verbanden en structuren van deze netwerken ontrafeld: wie praat met wie; wie zijn aanstokers en onrustzaaiers; wie zijn de volgers? Maar ook informatie over politieke en ideologische overtuiging, seksuele oriëntatie, interesses en hobby's, opleiding, burgerlijke staat, en nog veel meer kan gevolgd en geanalyseerd worden. Als gevolg van de enorme hoeveelheden persoonlijke informatie, foto's, video's, interesses, meningen en activiteiten die online gedeeld worden, komen er steeds meer bezorgdheden over privacy aan de oppervlakte. Want wat als sociaalnetwerksites alles van u zien?

Dit boek is ontsprongen aan de behoefte om die bezorgdheden het hoofd te bieden. Hoewel het voornamelijk focust op de mechanismen van sociaalnetwerksites – met Facebook als casus – en de implicaties ervan voor de gebruiker, moet dit boek niet opgevat worden als een manifest tegen sociaalnetwerksites. Het dient gelezen te worden als een gids naar geletterdheid over sociale media; een gids die de gebruiker een aantal inzichten wil verschaffen om op een bewuste manier te kunnen genieten van de vele voordelen die sociaalnetwerksites zoals Facebook bieden.

Achter de schermen van sociaalnetwerksites: wat komt u te weten?

Dit boek is geen encyclopedisch naslagwerk, maar wel een aanzet tot het aanbieden van een aantal inzichten in de mechanismen van sociaalnetwerksites die de gebruiker kunnen ondersteunen in een bewuster en veiliger gebruik van online netwerkplatformen. Een aantal thema's en vragen staan hierbij centraal:

- In eerste instantie focust dit boek op de persoonsgebonden gegevens die gebruikers op sociaalnetwerksites plaatsen. Vragen die in dit thema behandeld worden zijn onder meer: (1) Wie heeft toegang tot de gegevens die gebruikers

online zetten?; (2) Wat gebeurt er met die gegevens?; en (3) Wat zijn de mogelijke gevolgen van het feit dat derden toegang hebben tot die gegevens?

- In tweede instantie wordt aandacht besteed aan een aantal specifieke mogelijke gevaren verbonden aan het gebruik van sociaalnetwerksites. In tegenstelling tot het vorige thema, zoomt dit thema in op kinderen en jongeren. De vragen focussen op: (1) Wat zijn de gevaren gerelateerd aan andere gebruikers van sociaalnetwerksites (vb. cyberpesten); en (2) Wat is de impact van de privacyinstellingen van Facebook op de identiteitsontwikkeling van jongeren?
- Tot slot legt het boek zich toe op de vraag wat ondernomen kan worden om persoonsgegevens beter te beschermen en de gevaren te minimaliseren. Meer concreet wordt gezocht naar antwoorden op: (1) Wat kan de gebruiker doen? Die vraag focust enerzijds op de reikwijdte van de controle van de gebruiker over zijn of haar privacy en anderzijds op de stappen die de gebruiker kan ondernemen om deze controle te vergroten; (2) Wat kan de overheid doen in termen van regulering?; en (3) Wat kan of mag verwacht worden van de industrie zelf?

De ontrafeling van de mechanismen van sociaalnetwerksites en de zoektocht naar antwoorden op de centrale vragen van dit boek zijn georganiseerd aan de hand van vier hoofdstukken. In het eerste hoofdstuk, '**Facebook kijkt mee**', bespreekt **Mathias Vermeulen** de voor- en nadelen van het vrijgeven van persoonlijke gegevens op sociaalnetwerksites in een breder maatschappelijk kader. Meer concreet bespreekt hij hoe sociaalnetwerksites aangewend kunnen worden voor zowel het ondersteunen als het tegenwerken van democratische processen en hoe de gegevens die op het platform verspreid worden aanleiding kunnen geven tot surveillancepraktijken vanuit (autoritaire) overheden en politiediensten, of misbruikt kunnen worden door criminelen. Tot slot houdt dit hoofdstuk de macht van Facebook over persoonsgegevens tegen het licht en staat het stil bij de mate waarin een bedrijf zoals Facebook zowel rechter als partij kan zijn en wat de gevolgen daarvan zijn voor privacy en vrijheid van meningsuiting.

In het tweede hoofdstuk, '**Waarom is Facebook gratis?**', onderzoekt **Rob Heyman** de impact van het zakelijke model van Facebook op de privacy van de gebruiker. Sinds de beursgang van Facebook spelen commerciële motieven een steeds

belangrijkere rol in de werking van het netwerk. Aangezien er geen financiële kost verbonden is aan het gebruik van Facebook, moet het bedrijf elders inkomsten vergaren. Dit hoofdstuk bespreekt hoe Facebook persoonsgegevens gebruikt als munteenheid en hoe die gegevens gebruikt worden voor profiling praktijken en de ontwikkeling van gepersonaliseerde reclame. Verder ontleedt dit hoofdstuk de strategieën die Facebook hanteert voor het filteren van media-inhouden op basis van gebruiksprofielen. Meer in het bijzonder beschrijft het hoe subtiele veranderingen in gebruiksinstellingen en -voorwaarden de controle van Facebook over persoonsgerelateerde gegevens enerzijds en de productie, selectie en verspreiding van inhoud anderzijds steeds weer vergroot.

Het derde hoofdstuk, **'Kinderen, jongeren en sociale media: over risico's, regelgeving en empowerment'**, van **Eva Lievens** werpt een licht op de gevaren die verbonden kunnen zijn aan het gebruik van sociaalnetwerksites. Meer concreet bespreekt dit hoofdstuk praktijken zoals cyberpesten (online pesten, meestal tussen leeftijdsgenoten), sexting (het versturen van seksueel getinte foto's van elkaar), grooming (het manipuleren van jongeren via sociaalnetwerksites met seksueel misbruik als doel) en de confrontatie met ongewenste media-inhouden (bijvoorbeeld pornografisch materiaal). Het hoofdstuk geeft een overzicht van de wettelijke kaders die aangewend kunnen worden om deze gevaren het hoofd te bieden. Centraal staat ook de vraag hoe wettelijke beschermingsmaatregelen kunnen worden verzoend met het recht op vrije meningsuiting en het recht op privacy van jongeren. Daarnaast besteedt het hoofdstuk aandacht aan alternatieve vormen van regelgeving, de rol van ouders en leerkrachten in het verhogen van de geletterdheid over media en privacy van jonge gebruikers en de verantwoordelijkheid van sociaalnetwerkaanbieders.

Het hoofdstuk **'Identiteit en privacy'** van **Ralf De Wolf** analyseert vervolgens welke invloed Facebook heeft op hoe gebruikers hun identiteit ontwikkelen en hun privacy beheren. Het analyseert in eerste instantie hoe de intrinsieke eigenschappen van Facebook en de complexe privacyinstellingen de privacycontrole van de gebruiker bemoeilijken. Het bespreekt vervolgens hoe deze aspecten kunnen leiden tot onzichtbare publieken op Facebook, waardoor de gebruiker geconfronteerd kan worden met een botsing van verschillende contexten (bijvoorbeeld een schoolcontext versus een vriendencontext). Het hoofdstuk onderzoekt hoe jongeren al dan niet rekening houden met onzichtbare publieken

bij de ontwikkeling van online identiteiten. Tot slot wordt aandacht besteed aan het toenemende belang van privacygeletterdheid en aan de vraag of in de toekomst controle door de gebruiker zal volstaan om privacy in de hand te hebben.

Het laatste hoofdstuk, **'Roadmap voor socialemediawijsheid'**, van **Dorien Baelden** focust op de stappen die de gebruiker zelf kan ondernemen om bewuster, veiliger, en weerbaarder te surfen op sociaalnetwerksites. De *roadmap* is geen handboek over privacyinstellingen van sociaalnetwerksites, maar wel een beslissingsboom die vragen en antwoorden in kaart brengt en die een overzicht geeft van instanties die informatie verstrekken, klachten behandelen, praktische tips geven en online ondersteuning aanbieden.

Tot slot laten we hoeveel waarheid er schuilt in de uitspraak 'Hier vloekt men niet, Facebook ziet alles' over aan uw verbeelding wanneer u dit boek leest. We staan er nauwelijks bij stil, maar we worden tegenwoordig gefilmd, beloerd, gemonitord, gescreend en gedatabased dat het een lieve lust is. Het recht op privacy is een mensenrecht, maar blijft het nog overeind? Wordt het in de driehoek afgebeelde alziende oog – de goddelijke voorzienigheid – in de online wereld vervangen door sociaalnetwerksites en andere socialemediaplatformen? 'Hier vloekt men niet' is een prent die in katholiek Vlaanderen overal, tot in de cafés, aan de muur hing. De wereld is nu groter; nieuwe vaardigheden dienen daarom te worden aangeleerd. De online wereld heeft nood aan nieuwe gedragscodes en meer bewustzijn over veranderende privacyconventies, want het oog van zowel gebruikers als aanbieders van online diensten reikt verder dan ooit.