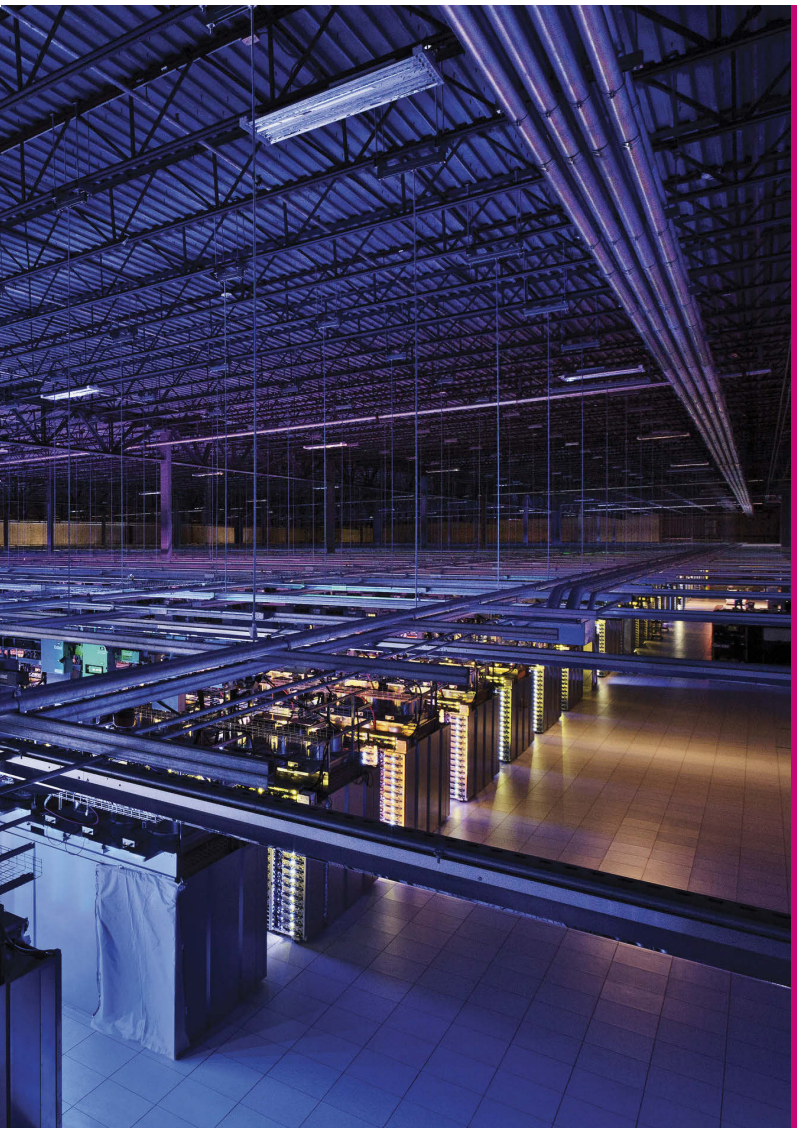
Centraal Planbureau

Meer keuze voor burgers | *Meer ruimte voor bedrijven*



CPB Policy Brief | 2014/04

Kiezen voor privacy

Hoe de markt voor persoonsgegevens beter kan

Michiel Bijlsma
Bas Straathof
Gijsbert Zwart

Samenvatting

Bedrijven en overheden verzamelen steeds meer persoonsgegevens en zij gebruiken deze ook steeds intensiever. Vaak hebben mensen daar voordeel van, maar niet altijd. Iedereen denkt verschillend over privacy en bedrijven gebruiken persoonsgegevens op verschillende manieren. De afweging tussen de voor- en nadelen hiervan kan daarom het beste door de betrokken partijen zelf gemaakt worden. Meer keuzevrijheid voor burgers en bedrijven stimuleert innovatief gebruik van persoonsgegevens, waarbij mensen zelf kunnen bepalen hoeveel privacy zij willen behouden. Een markt voor gebruiksrechten van persoonsgegevens brengt burgers en bedrijven bij elkaar.

De markt voor persoonsgegevens kan in de praktijk niet goed functioneren zonder overheidsbeleid. Zo is het moeilijk te controleren wat bedrijven met data doen en is het kostbaar om passende privacyovereenkomsten tussen bedrijf en klant af te sluiten. Het bevorderen van vertrouwen is een belangrijke doelstelling van het kabinet.[1] Het werk van de toezichthouder, het College Bescherming Persoonsgegevens (CBP), is essentieel voor dit vertrouwen. Maar het gaat niet alleen om vertrouwen: er moet ook voldoende ruimte zijn voor keuzes en ondernemerschap. We bespreken een aantal beleidsopties hiervoor. Deze opties hebben betrekking op het recht om te wissen, de vormgeving van privacyovereenkomsten, gebruik van persoonsgegevens zonder toestemming, Europees toezicht, keurmerken en technologie die burgers meer controle geeft over hun persoonlijke gegevens.

[1] Brief Kabinetsvisie op e-privacy: naar gerechtvaardigd vertrouwen, 24 mei 2013.

1 Inleiding

In juni 2013 speelde Edward Snowden tienduizenden geheime documenten van de Amerikaanse inlichtingendienst NSA door aan verschillende kranten. Snowden's onthullingen toonden aan dat veiligheidsdiensten veel meer persoonsgegevens verzamelden dan experts voor mogelijk hielden,[2] en maakten burgers bewust van de grote hoeveelheden persoonsgegevens die derden over hen hebben. Waarom zou de NSA de enige zijn? De ontwikkeling van informatie- en communicatietechnologie en het internet zorgen voor een snelgroeiende stroom aan gegevens die herleidbaar zijn tot personen. Wat weten grote online bedrijven als Google, Amazon of Facebook, maar ook meer traditionele bedrijven als banken en supermarkten, eigenlijk over ons? Technologische verandering zet aan tot een continue discussie over privacy.

De privacydiscussie loopt al decennia langs twee lijnen, die elkaar overigens niet uitsluiten. Aan de ene kant een juridische benadering met de grondwettelijke verankering van de eerbiediging van de persoonlijke levenssfeer. Hieruit vloeit volgens de aanhangers voort dat privacyovereenkomsten precies moeten aangeven voor welk doel gegevens gebruikt mogen worden. De andere kant is een economische benadering van privacy, waarin de verschillende mogelijkheden centraal staan om gebruiksrecht op persoonsdata vorm te geven. De basishouding is hier dat een ieder vrij is te doen met zijn persoonsgegevens wat hij of zij wil.

Deze scheidslijn is ook geografisch, in de Europese Unie (EU) heerst de algemene juridische aanpak, in de Verenigde Staten (VS) is meer ruimte voor de economische benadering. De Europese Data Beschermingsrichtlijnen uit 1995[3] en het recente voorstel voor regulering van databescherming[4] leggen de nadruk op de rechten van burgers.[5] In de VS bestaat geen generieke privacywetgeving, kunnen privacywetten per staat verschillen en speelt het belang van bedrijven een grotere rol. Wel handhaaft de Federal Trade Commission (FTC) sectorspecifieke privacywetten.[6] Bedrijven kiezen voor een privacybeleid en opereren op basis van *notice and consent*, dat wil zeggen dat consumenten expliciet gevraagd wordt in te stemmen met hun beleid. Verkoop en openbaar maken van data kan zelfs vallen onder het First Amendment, het recht op vrije meningsuiting.

[2] Bruce Schneier, een vooraanstaande expert op het gebied van cybersecurity en in het bezit van documenten van Snowden, blogde een tijd lang iedere week over een andere, onbekende techniek van de NSA (www.schneier.com).
[3] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
[4] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
[5] De ontwerpverordening die bij de Europese Raad ligt, zal deze rechten verder versterken.
[6] De Federal Trade Commission (FTC) handhaaft een aantal privacywetten, zoals de Fair Credit Reporting Act, de Gramm-Leach-Bliley Act, de Children's Online Privacy Protection Act, the CAN-SPAM Act, de Health Insurance Portability and Accountability Act Privacy Rule of de Telemarketing and Consumer Fraud and Abuse Prevention Act.

In deze policy brief wordt onderzocht of de benaderingen van de EU en de VS bij elkaar zijn te brengen. Een economische benadering van de kosten en baten van privacybeleid, met daarin een belangrijke rol voor de verhandelbaarheid van persoonsgegevens, sluit namelijk privacy als grondrecht niet uit.[7] Ook een juridische benadering vereist keuzes over vormgeving van privacybeleid, met een rol voor economische argumenten.[8]

Privacywetgeving kan een groot effect hebben op de welvaart. Te strikte wetgeving kan burgers schaden, bijvoorbeeld als bedrijven te veel worden beperkt in hun innovatie. Het gebruik van Big Data, het zoeken naar nieuwe toepassingen van eerder verzamelde (persoons-)gegevens, is dan nagenoeg verboden. Te sobere wetgeving is schadelijk als dit mogelijk maakt dat bedrijven zonder medeweten of toestemming informatie gebruiken en personen daarvan nadeel ondervinden. Of wanneer informatie voor andere doeleinden wordt gebruikt dan waarvoor toestemming is gegeven.

2 De waarde van persoonsgegevens en de privacyparadox

Het Amerikaanse telecombedrijf AT&T biedt voor zijn glasvezelnetwerk in Austin, Texas een abonnement aan voor 99 dollar per maand. Maar klanten kunnen ook kiezen voor een abonnement van 70 dollar per maand, maar dan mag AT&T gegevens over surfgedrag gebruiken om klantspecifieke aanbiedingen en reclame aan te bieden.[9] Dit voorbeeld illustreert dat persoonsgegevens economische waarde hebben voor bedrijven. Dat is op zich niets bijzonders. Wel nieuw is de schaal waarop bedrijven persoonsgegevens verzamelen, opslaan, samenvoegen en analyseren en de economische waarde die dit lijkt te vertegenwoordigen. De marktkapitalisatie van bedrijven als Google of Facebook is daardoor nu vergelijkbaar met reuzen als Exxon of Walmart.

Persoonsgegevens ontstaan vrijwel continu: als mensen gebruik maken van sociale netwerken of zoekmachines, als cookies informatie over hun surfgedrag op internet verzamelen en doorgeven, als apps op mobiele telefoons het gedrag of de locatie van de gebruiker registreren en doorgeven, als supermarkten bijhouden wanneer je welke producten koopt, als zorgaanbieders zorggebruik registreren, als beeldmateriaal uit de publieke ruimte wordt opgeslagen, of als je betaalt met je pinpas.

Informatie over personen creëert op verschillende manieren waarde voor bedrijven. Als eerste stelt het gebruik van persoonsgegevens bedrijven in staat vraag en aanbod beter op elkaar af te stemmen. Bedrijven kunnen potentiële klanten identificeren en gerichte aanbiedingen doen. Dit verhoogt de kans dat iemand daadwerkelijk een passende aanbieding

[7] Ook als privacy een grondrecht is, kunnen persoonsgegevens verhandelbaar zijn. Daarbij is het belangrijk om op te merken dat er verschillend tegen het begrip privacy wordt aangekeken: privacy kan worden gezien als synoniem voor geheimhouding van persoonsgegevens, maar privacy kan ook worden gezien als de *mogelijkheid* om persoonsgegevens geheim te houden. In het laatste geval is het vrijwillig delen van persoonsgegevens geen beperking van de privacy.
[8] Denk bijvoorbeeld aan de reikwijdte van doelbinding.
[9] http://arstechnica.com/information-technology/2013/12/att-offers-gigabit-internet-discount-in-exchange-for-your-web-history/

krijgt, waardoor voor bedrijven de opbrengst per advertentie stijgt. Daarnaast kunnen bedrijven persoonsgegevens gebruiken om risico's te managen. Bedrijven kunnen bijvoorbeeld het risico op wanbetaling bij kredietverstrekking beter inschatten als ze meer informatie hebben over betalingsgedrag van klanten, de kans op fraude verminderen door gegevens van klanten op juistheid te controleren met alternatieve databronnen, en hun voorraadbeheer verbeteren door trends in de vraag op tijd te signaleren.

Meer precieze informatie over (potentiële) klanten stelt een bedrijf ook in staat om een hogere prijs te vragen aan consumenten die bereid zijn om meer voor een product te betalen. Een verzekeraar kan bijvoorbeeld risicovolle klanten meer laten betalen dan minder risicovolle klanten. Door dit soort prijsdiscriminatie kunnen vraag en aanbod beter op elkaar worden afgestemd, wat bijdraagt aan efficiëntere marktuitkomsten. Hierbij is het wel onvermijdelijk dat sommige klanten er hierdoor op achteruit gaan.

Tot slot kunnen bedrijven persoonsgegevens gebruiken om nieuwe producten te ontwikkelen. Zakelijke sociale netwerken als LinkedIn bieden nieuwe mogelijkheden voor zowel werkzoekenden als bedrijven op zoek naar personeel.[10] Internetzoekmachines gebruiken eerdere zoekopdrachten van hun klanten om hun zoekalgorithmes te perfectioneren. Bel- en twittergedrag geven informatie over files en wordt gebruikt voor crowdmanagement bij grote evenementen. Bedrijven volgen Facebook en Twitter om te zien of hun klanten tevreden zijn. E-health toepassingen stellen mensen in staat hun gezondheid te monitoren of diagnoses te stellen.

Veel mensen krijgen echter een diepgeworteld gevoel van onbehagen als onbekenden toegang hebben tot hun privé-informatie. Een ruime meerderheid van de Amerikaanse internetgebruikers zegt zich oncomfortabel te voelen bij de wetenschap dat hun gedrag gevolgd wordt op de website die zij doorzoeken (Turow et al., 2009). Daarbij maakt het wel uit waar die informatie voor wordt gebruikt. Wanneer surfgedrag wordt gebruikt voor gerichte kortingsacties is dit voor een grote groep meer acceptabel dan wanneer het gaat om advertenties. Onbehagen kan een weerspiegeling zijn van een risico op werkelijke schade. Het bedrijf waaraan iemand zijn gegevens heeft toevertrouwd, kan die schade aanrichten, maar ook derden als gevolg van verlies of doorverkoop van gegevens. Als iemand denkt dat de kans groot is om slachtoffer te worden van fraude of diefstal na het achterlaten van zijn adres of bij een creditcardbetaling, zal hij of zij minder snel een internetaankoop doen. Daarnaast kunnen mensen schade oplopen als specifieke kenmerken publiek worden. Werkgevers nemen zwangere vrouwen minder snel aan voor een nieuwe baan. Als je vaak betrokken bent bij verkeersincidenten, betaal je een hogere verzekeringspremie.

Dit gevoel van onbehagen staat wel in schril contrast met het gemak waarmee mensen hun persoonsgegevens soms weggegeven. Velen gaan akkoord met privacyovereenkomsten zonder dat ze goed weten wat daarin staat. Via Facebook delen sommige mensen elk detail van hun persoonlijk leven en het is bijna volledig geaccepteerd dat Google e-mails leest

[10] Met implicaties voor de efficiëntie van de arbeidsmarkt, zie bijvoorbeeld van den Berg (2006).

waarvan de verzender of ontvanger een gmail-adres heeft. Er lijkt sprake van een privacyparadox.

Deze kloof tussen de zorg om privacy in de publieke opinie en de waarde die mensen in de dagelijkse praktijk aan privacy hechten, blijkt ook uit empirisch onderzoek. Consumenten die vrezen voor een inbreuk op hun privacy, blijken voor enkele tientjes bereid te zijn om persoonsgegevens over te dragen. In experimenten bij aankoopbeslissingen vinden veel consumenten het geen probleem om hun gegevens aan de verkoper prijs te geven, zelfs wanneer dat eenvoudig te vermijden zou zijn.[11] De maatschappelijke onrust die onlangs ontstond over ING past in deze paradox: de plannen van ING zijn echter bescheiden in het licht van wat Google, Facebook, of diverse apps op mobiele telefoon doen met persoonsgegevens, zoals het populaire Whatsapp.[12]

3 De markt voor persoonsgegevens

Een van de mogelijke verklaringen voor de privacyparadox is dat de waarde die mensen aan hun persoonsgegevens hechten, nogal uiteenloopt. Daarbij verschillen bedrijven in de waarde die zij aan dezelfde persoonsgegevens toekennen. Grote ondernemingen die al veel persoonsgegevens bezitten, kunnen bijvoorbeeld meer afleiden uit een nieuw persoonsgegeven dan bedrijven die weinig gegevens bezitten. Een verhandelbaar gebruiksrecht op persoonsgegevens kan recht doen aan de verscheidenheid aan situaties en voorkeuren.

In een ideale economische wereld zouden bedrijven persoonsgegevens alleen mogen gebruiken als de totale baten van dit gebruik hoger liggen dan de totale kosten. Is dat niet het geval, dan is het juist wenselijk om die gegevens niet te gebruiken. Voor de overheid is het ondoenlijk om dit per geval vast te stellen. Het ligt daarom voor de hand om mensen en bedrijven zelf in staat te stellen om de kosten en baten tegen elkaar af te wegen.

Wanneer mensen zelf kunnen beslissen over toestemming voor het gebruik van hun gegevens voor een specifiek doel, kunnen zij een afweging maken tussen de baten en de kosten van het toegankelijk maken van gegevens. Die afweging kan positief uitvallen wanneer hij zelf direct baat heeft bij het gebruik door het bedrijf van zijn gegevens, maar ook wanneer het bedrijf hem voldoende compenseert voor de nadelen ervan.

Vanuit consumentenperspectief kan bijvoorbeeld een korting op de prijs een goede vergoeding zijn voor persoonsgegevens, een gratis dienst, of een rechtstreekse betaling. Er is dan sprake van een uitruil: in ruil voor het gebruiksrecht op zijn gegevens krijgt de persoon in kwestie een voor hem waardevol product of vergoeding. Op deze manieren kunnen de voor- en nadelen van het gebruik van persoonsgegevens per geval worden gewogen.

[11] Grossklags en Acquisti (2005).

Wat is er nodig om tot zo'n afweging te komen? Alleen wanneer gebruiksrechten zijn vastgelegd voor zowel gegevensverschaffer (de persoon) als gegevensgebruiker (het bedrijf), is het mogelijk te onderhandelen over mogelijke herschikking van die rechten. Zonder overdraagbare gebruiksrechten rest slechts een 'one-size-fits-all' oplossing die geen rekening houdt met individuele voorkeuren. Dan wordt ook het datagebruik gefrustreerd waarbij beide partijen baat hebben bij overdracht.

De meeste goederen en diensten zijn eenvoudig te verhandelen. Ook handel in informatie, zoals persoonsgegevens, is mogelijk. Een bijzonder kenmerk van informatie is dat meer partijen gebruik kunnen maken van dezelfde informatie. Daarom wordt niet de informatie zelf verhandeld, maar het recht op het gebruik ervan. Dit stelt de eigenaar in staat om de persoonsgegevens los te koppelen van het gebruik ervan door anderen. Hierdoor kan ongewenst gebruik worden voorkomen.

Bij privacyovereenkomsten wordt een gebruiksrecht op persoonsgegevens verhandeld. Er zijn ook andere voorbeelden waarbij gebruiksrechten het mogelijk maken om informatie te verhandelen. Een patent stelt een uitvinder in staat om zijn uitvinding aan potentiële kopers te onthullen zonder dat de uitvinding in waarde vermindert. Op deze manier krijgen bedrijven de prikkel om te investeren in innovatie, zelfs als ze de baten van zulke innovaties niet direct zelf kunnen verwezenlijken.

Verhandelbare gebruiksrechten zijn ook een oplossing voor andere verdelingsproblemen van immateriële goederen. Zo werken vissers in Nieuw-Zeeland sinds 1986 met verhandelbare visquota.[13] Om de visstand te beschermen, is er een beperking op de vangst van verschillende soorten. Door de visquota verhandelbaar te maken, loont het voor efficiëntere visbedrijven om rechten te kopen van minder efficiënte collega's. Beiden gaan er op vooruit: de koper kan meer vis vangen, terwijl de verkoper beter af is met de vergoeding die hij ontvangt voor zijn visquota dan met de winst die hij zou maken wanneer hij deze zelf zou benutten. En de maatschappij is beter af wanneer besparing daar plaatsvindt waar dat het goedkoopst is.

Gebruiksrechten op persoonsgegevens maken het mogelijk dat privacyregels rekening houden met de mogelijkheid dat verschillende personen en bedrijven verschillende waarde hechten aan het delen van informatie. Wanneer individuen zelf kunnen bepalen hoe en in welke omstandigheden hun gegevens gebruikt mogen worden, komen precies die transacties tot stand komen die tot wederzijds voordeel leiden. Maar dit is de theorie, hoe werkt het in de praktijk?

4 Waar faalt de markt?

In de praktijk faalt de markt dikwijls: de markt voor persoonsgegevens werkt niet goed of komt zelfs niet van de grond. Zo is het niet eenvoudig en erg duur om op individuele leest geschoeide contracten op te stellen. Daarnaast is het moeilijk te controleren hoe bedrijven en de overheid met persoongegevens omgaan en of mensen correcte persoonsgegevens verstrekken. Bovendien zijn burgers niet altijd in staat voor zichzelf optimale beslissingen te nemen.

Transactiekosten maken het onmogelijk afzonderlijke, op de persoon en situatie toegesneden, overeenkomsten op te stellen. Het kost inspanning en tijd voor een consument om zich vertrouwd te maken met het privacybeleid van elke aanbieder: alleen al het lezen van alle privacyovereenkomsten zou de gemiddelde Amerikaan 200 uur per jaar kosten (Campbell et al., 2013) en leidt niet tot begrip bij het merendeel van die lezers (McDonald et al., 2009). Het uitonderhandelen van een op maat gemaakte overeenkomst is voor de meeste consumenten ondoenlijk en zulke onderhandelingen kunnen bovendien mislukken door verschillen in inzichten over de waarde van gegevens. Het is dan ook zaak om gebruiksrechten zo te standaardiseren dat het niet vaak nodig is om van de standaard af te wijken om tot een efficiëntere verdeling van rechten te komen.[14]

Ook zijn er verschillen in onderhandelingspositie tussen persoon en bedrijf. Om de internetreuzen kan een consument moeilijker heen, dan om andere bedrijven die hevig concurreren om de aandacht van consumenten.[15] Concurrentie disciplineert immers ook het privacybeleid van die bedrijven. Bovendien kunnen verschillende productaanbieders zich differentiëren in de mate waarin zij persoonsgegevens verzamelen. Dan blijft er ook op dat gebied meer te kiezen voor de consument.

Moreel gevaar is een tweede probleem. Het is voor een individuele consument nauwelijks te controleren of het bedrijf zich aan de overeengekomen afspraken over de reikwijdte van het gebruik houdt. Zelfs wanneer de klant op de hoogte is van verlies of ongeautoriseerd gebruik van zijn gegevens, is het niet eenvoudig de schade te verhalen. Dit speelt ook een rol bij overheden, de andere grote verzamelaars van persoonsgegevens, bijvoorbeeld ten behoeve van effectievere belastingheffing of bestrijding van misdaad. Affaires als die van de NSA maken duidelijk dat ook overheden daarbij grenzen kunnen overschrijden. Ook als gegevens met goede intenties worden verzameld, kunnen ze onbedoeld op straat komen te liggen, of ten prooi vallen aan criminele hackers. Veilingsite Ebay kwam onlangs in opspraak doordat een datalek toegang bood tot de gegevens van mogelijk 145 miljoen gebruikers.[16] De Diginotar-affaire[17] heeft laten zien dat ook persoonsgegevensoverdracht naar de overheid

[14] Standaardisatie van privacyovereenkomsten kan ook helpen om de informatie in die overeenkomsten beter te laten landen bij de lezer, zoals Kelley et al. (2010) laten zien in een experiment met meer gebruikersvriendelijke privacybijsluiters.
[15] Zulke intermediairs met marktmacht romen bovendien een deel van de waarde van gegevensoverdracht naar adverteerders en bedrijven af, wat efficiënte transacties verstoort. Zie ook Athey (2014).
[16] http://www.reuters.com/article/2014/05/21/us-ebay-password-idUSBREA4K0B420140521
[17] Het bedrijf verzorgde de beveiligingscertificaten voor verschillende overheidsdiensten. Na een hack, en kritiek op de beveiligingsprocedures van het bedrijf, staakte de overheid in 2011 het gebruik van deze dienst.

niet zonder lekrisico's is. Burgers en consumenten zijn afhankelijk van de zorgvuldigheid waarmee bedrijven en de overheid omgaan met hun persoonsgegevens. Dat kunnen zij zelf onvoldoende controleren.

Om dit moreel gevaar te ondervangen zijn consumenten in de praktijk afhankelijk van de reputatie van het bedrijf of overheid, en/of van de publieke handhaving van afspraken en veiligheidsnormen door een toezichthouder als het College Bescherming Persoonsgegevens. Reputatie werkt alleen als het verliezen van reputatie schade oplevert voor een bedrijf. Extern toezicht lukt alleen als de gebruiksvoorwaarden voor persoonsgegevens tot op zekere hoogte gestandaardiseerd zijn. Wanneer elke consument een opmaatgemaakte privacyovereenkomst sluit met zijn internetprovider, wordt het te ingewikkeld voor een toezichthouder om namens hen te verifiëren of het internetbedrijf zich aan de afspraken houdt.

Een derde obstakel voor een efficiënte markt voor persoonsgegevens is dat keuzevrijheid veronderstelt dat burgers keuzes maken die in hun belang zijn. In de praktijk blijkt dat mensen slechts beperkt in staat zijn om zulke keuzes te maken of dat ze besluiten om zich niet te verdiepen in alle details van hun keuzes. Keuzes hangen bijvoorbeeld af van de wijze van presentatie. Ook kunnen mensen niet alle gevolgen van hun keuzes overzien of deze betrekken bij hun beslissingen. Ten slotte zijn mensen bij beslissingen die gevolgen hebben op lange termijn, niet altijd voldoende alert op de consequenties. Bij de vraag[18] wie inzicht heeft in de creditcardgegevens na een online-aankoop denkt slechts een kleine minderheid van de geënquêteerden aan de mogelijkheid dat hackers mee kunnen kijken. Een deel vergeet dat ook hun bank op de hoogte is van die transactie. Privacybeleid dient burgers dan ook te beschermen tegen te grote schade door verkeerde beslissingen.

Vrijheid om gebruiksrechten te verlenen op persoonsgegevens doet recht aan de individuele keuzes en voorkeuren. Maar ongebreidelde vrijheid leidt dus niet tot optimale uitkomsten. De vraag is hoe privacybeleid deze twee werelden kan verenigen. Hoe kan regelgeving ruimte laten voor aanpassing aan de individuele voorkeuren en situatie, en anderzijds burgers beschermen tegen de tekortkomingen van de markt?

[18] in een onderzoek van Acquisti en Grossklags (2005)

5 Opties voor beleid

De Wet bescherming persoonsgegevens en de Europese richtlijn leggen het gebruiksrecht voor persoonsgegevens voornamelijk bij het betreffende individu. Ook liggen de voorwaarden waaronder persoonsgegevens gebruikt mogen worden, grotendeels vast en zijn contracten dus in grote mate gestandaardiseerd. Zowel mensen als bedrijven hebben weinig mogelijkheden om af te wijken van deze bij wet geregelde standaardcontracten. De nieuwe Europese privacyverordening[19] breidt de rechten van personen nog verder uit, onder andere door het 'recht om te wissen' ook te laten gelden voor data die volledig volgens privacyovereenkomsten gebruikt worden.[20] Dit strengere privacybeleid, met een nadruk op juridische bescherming, kan de kans op ongewenst gebruik van persoonsgegevens verkleinen. Tegelijk beperkt het de mogelijkheden voor het gebruik van persoonsgegevens waar individuele burgers geen problemen mee hebben. Zoals hierboven uiteengezet leidt dat tot maatschappelijke kosten.

De overheid kan op vier manieren de falende markt voor persoonsgegevens beter laten functioneren:

- Door gebruiksrechten duidelijk vast te stellen en overdraagbaar te maken
- Door transactiekosten te verlagen
- Door moreel gevaar te bestrijden
- Door onwenselijke gevolgen van de beperkte rationaliteit van consumenten te ondervangen.

Hieronder bespreken we zes aanpassingen van het huidige beleid (inclusief de nieuwe privacyverordening) waarmee bovenstaande subdoelen beter bereikt kunnen worden.

Beleidsoptie 1. Aanpassing van het uitgebreide recht om te wissen

Als een burger gebruik maakt van het recht om te wissen van rechtmatig verkregen en gebruikte gegevens, zou het bedrijf een vooraf vastgestelde compensatie moeten kunnen krijgen.

Een burger in Nederland heeft al het recht om in te zien welke gegevens er over hem geregistreerd zijn.[21] Ook is er het recht om gegevens te laten verbeteren, verwijderen en aan te vullen, mits de gegevens niet kloppen, onvolledig of niet nodig zijn voor het beoogde gebruik van de gegevens.[22] Het recht om te corrigeren kan dus niet zomaar gebruikt worden door burgers om nadelige informatie over henzelf te verdoezelen. Ook kan dit recht niet gebruikt worden om eenzijdig privacyovereenkomsten op te zeggen. De aangekondigde Europese verordening over databescherming gaat nog een stap verder. In het huidige voorstel krijgen burgers het recht om gegevens te laten wissen - ook als ze eerder expliciet

[19] Het Europees Parlement is na aanpassingen akkoord gegaan met een voorstel van de Europese Commissie voor de Algemene verordening gegevensbescherming. De Europese Raad moet op moment van publicatie nog akkoord gaan met het voorstel.
[20] Aanvankelijk werd een "recht om vergeten te worden" voorgesteld, dat nog verder zou gaan.
[21] Artikel 35 Wbp.
[22] Artikel 36 Wbp.

toestemming voor het gebruik daarvan hebben gegeven.[23] Het recht om te wissen geeft burgers de mogelijkheid om hun vergissingen te herstellen en biedt hen zo meer controle over het gebruik van hun gegevens. Dit kan ten goede komen aan de bereidwilligheid om persoonsgegevens met anderen te delen.

Het uitgebreide recht om te wissen heeft ook een nadeel: het ontneemt burgers de mogelijkheid om een geloofwaardig contract af te sluiten over het gebruik van hun gegevens. Dit kan de werking van de markt voor persoonsgegevens verstoren. Voor bedrijven betekent het recht om te wissen dat persoonsgegevens minder waard zijn, omdat het gekochte gebruiksrecht zonder opgaaf van redenen en zonder vergoeding kan worden ontnomen. Dat maakt het onaantrekkelijk voor bedrijven om vergoedingen te bieden of diensten te verlenen in ruil voor persoonsinformatie. De consument kan immers na het ontvangen van de vergoeding of dienst direct de afgestane informatie laten wissen.

Een betere manier om een balans te vinden tussen de voor- en nadelen van het recht om te wissen is om in privacyovereenkomsten standaard een compensatie af te spreken als de burger eenzijdig de privacyovereenkomst opzegt. Bij een abonnement op een website zou dit kunnen betekenen dat een consument maandelijks een hoger bedrag kwijt is als hij niet meer wil dat zijn persoonsgegevens gebruikt worden. In het eerdere voorbeeld van telecombedrijf AT&T zou het contract de mogelijkheid kunnen geven aan de klant om terug te keren naar het duurdere abonnement zonder gegevensverzameling. Op deze manier kunnen mensen eenvoudig hun beslissing ongedaan maken en hebben bedrijven meer zekerheid over de duurzaamheid van het gebruiksrecht.

Beleidsoptie 2. Standaardcontract zonder doelbinding

Sta een standaardcontract toe waarin doelbinding wordt vervangen door meer algemene voorwaarden voor gebruik, zodat toestemming gegeven kan worden voor hergebruik van gegevens.

Doelbinding houdt in dat de privacyovereenkomst tussen een burger en een bedrijf altijd specifiek moet aangeven voor welk doel de persoonlijke gegevens gebruikt worden. Niemand kan dus een overeenkomst met een bedrijf sluiten waarbij alleen algemene voorwaarden worden gesteld aan het gebruik van persoonsgegevens. Het voordeel is dat voor alle partijen eenduidig is welk gebruik van gegevens is toegestaan. Burger, bedrijf en toezichthouder weten exact wat het bedrijf wel en niet met gegevens mag doen. Doelbinding kan er zo aan bijdragen dat consumenten zich bewust zijn van waar hun gegevens voor worden gebruikt.[24] Doelbinding maakt verder het toezicht op het gebruik van persoonsgegevens goedkoper omdat contractbreuk eenvoudig te constateren is. Het nadeel is dat hergebruik van persoonsgegevens erg kostbaar is, omdat doelbinding vereist dat er voor een nieuw doel ook een nieuwe privacyovereenkomst moeten worden afgesloten. In veel gevallen betekent het opnieuw afsluiten van privacyovereenkomsten een stevige

[23] In artikel 17 van de ontwerpverordening over gegevensbescherming (“recht om te wissen”) staat dat de betrokkene (“data subject”) het recht heeft om zijn toestemming om persoonsgegevens te gebruiken zoals bedoeld bij punt (a) van artikel 6(1) in te trekken. In dit laatste artikel staat dat persoonsgegevens gebruikt mogen worden voor één of meerdere specifieke doelen als de betrokkene daar toestemming voor gegeven heeft.
[24] Tenzij doelbinding tot complexe contracten leidt - dan is het omgekeerde waarschijnlijker.

kostenpost die gepaard gaat met vertraging en onzekerheid over de reactie van rechthebbenden. Op deze manier maakt doelbinding innovatie op basis van hergebruik van persoonsgegevens onaantrekkelijk.

De voor- en nadelen van doelbinding kunnen beter in balans worden gebracht door naast het huidige voorgeschreven standaardcontract met doelbinding een tweede standaardcontract toe te staan waar alleen grofweg in hoeft te worden aangegeven waar de gegevens voor gebruikt gaan worden. Iemand zou dan kunnen aangeven voor welke categorieën van toepassingen gegevens gebruikt mogen worden (bijvoorbeeld 'gerichte advertenties', 'klantenservice', 'marktonderzoek', etc.). Partijen kunnen zelf kiezen voor het standaardcontract met doelbinding - en dus beter toezicht - of voor het tweede type zonder doelbinding maar met meer flexibiliteit. Een meer flexibele overeenkomst legt wel meer verantwoordelijkheid bij bedrijven om uit te leggen wat ze met gegevens doen (Roosendaal, Van den Broek en Van Veenstra, 2014). Een bijkomend voordeel van een contract zonder doelbinding is dat bij geavanceerde producten de privacyovereenkomst eenvoudig en kort kan blijven. Dit vergroot de kans dat mensen privacyovereenkomsten daadwerkelijk gaan lezen en begrijpen, waardoor een betere afweging mogelijk is over het beschikbaar maken van hun gegevens.

Beleidsoptie 3. Maak gerechtvaardigd belang duidelijker

De toezichthouder zou voor nieuwe toepassingen van persoonsgegevens snel duidelijkheid moeten kunnen geven of een beroep op gerechtvaardigd belang kan worden gedaan, dit kan bijvoorbeeld door heldere algemene principes te formuleren waarmee bedrijven zelf kunnen inschatten wat hun mogelijkheden zijn.

Een bedrijf hoeft niet in alle gevallen toestemming te vragen voor het gebruik van persoonsgegevens. Dat is niet nodig voor de normale bedrijfsvoering of het dagelijks beheer van de organisatie. Deze doelen worden gezien als een 'gerechtvaardigd belang' voor het gebruik van persoonsgegevens. Een bedrijf moet zelf afwegen of zijn belang bij het gebruik van de gegevens opweegt tegen de belangen van de betrokkene. Een beroep op gerechtvaardigd belang is niet beperkt tot uitzonderlijke situaties, maar bedrijven kunnen zich er ook niet automatisch op beroepen.[25]

Het is onduidelijk hoe bedrijven belangen moeten wegen in situaties waarover de toezichthouder zich niet eerder heeft uitgelaten. Door algemene principes te formuleren, beperkt de toezichthouder de onzekerheid. Een dergelijke open norm ('fair use') is al te vinden in het auteursrecht. Hierdoor zijn er minder transactiekosten, komen hold-up-problemen minder vaak voor en ontstaat er meer ruimte voor innovatie. Te veel ruimte leidt tot lagere transactiekosten, maar maakt het moeilijker voor burgers om te voorkomen dat bepaalde persoonsgegevens verzameld worden. Een open norm is daarom vooral geschikt voor basale persoonsgegevens (zoals naam, adres, telefoonnummer, e-mailadres) en voor situaties waarin persoonsgegevens vrijwel onmiddellijk worden geanonimiseerd, zoals bij het tellen van passanten met behulp van wifi-tracking.

[25] Opinie 06/2014 van het samenwerkingsverband van Europese privacytoezichthouders (de "Artikel 29 werkgroep") over gerechtvaardigd belang.

Beleidsoptie 4. Keurmerk

Geef met een keurmerk aan hoeveel privacy een product biedt.

Complexe privacyovereenkomsten en moreel gevaar maken het moeilijk voor burgers om hun keuzes te baseren op privacybeleid van bedrijven. Naast de al besproken mogelijkheden kunnen toezichthouders ook bijdragen aan beter inzicht door het toekennen van keurmerken. Momenteel maakt de toezichthouder pas bekend hoe een bedrijf met persoonsgegevens omgaat wanneer er regels overtreden worden. Door met keurmerken te werken, kan een toezichthouder burgers ook vooraf informeren dat een bedrijf zich aan de regels houdt. Op deze manier kan marktfalen door moreel gevaar worden tegengegaan: bedrijven met een keurmerk zijn immers beter te vertrouwen door burgers.

Keurmerken zijn vooral voordelig voor kleine bedrijven en start-ups. Voor een klein bedrijf is het hebben van een keurmerk deels een substituut voor een eigen reputatie: een keurmerk maakt het makkelijker om te concurreren met grote ondernemingen. Keurmerken zijn overigens niet het exclusieve domein van de overheid, maar kunnen ook heel goed door private partijen worden geïntroduceerd.

Beleidsoptie 5. Privacy Enhancing Technologies (PET's)

Zorg voor een publiek identificatieplatform dat interoperabel is met private PET's en introduceer een vergunningensysteem voor cruciale PET-diensten.

Een van de reacties op de toename in het gebruik van persoonsgegevens is de ontwikkeling van software die burgers meer controle over persoonsgegevens geeft. Deze privacy-enhancing technologies (PET's) waren er in eerste instantie vooral op gericht om anoniem het internet te kunnen gebruiken, maar bij nieuwere PET's gaat het om het beheer van persoonsgegevens. Bedrijven kunnen PET's inzetten na het verkrijgen van persoonsgegevens en zo de risico's van datalekken beperken, maar PET's kunnen burgers ook rechtsreeks controle geven over welke persoonsgegevens ze aan wie verstrekken. Voorbeelden van Nederlandse PET's zijn eID, een publieke dienst die het mogelijk maakt om jezelf online te identificeren, en Qiy, een dienst die controle geeft over welke persoonsgegevens je met wie deelt.

Het voordeel van PET's is dat ze de kans op moreel gevaar beperken, zodat burgers meer zekerheid hebben als ze hun gegevens delen. Bedrijven kunnen bovendien meer vertrouwen op de juistheid van die gegevens (Acquisti, 2008). Een bijkomend voordeel van PET's is dat ze de transactiekosten van privacyovereenkomsten sterk kunnen verlagen. De overheid kan het gebruik van PET's stimuleren door elektronische identificatie te faciliteren. Hoewel private partijen ook voor identificatie kunnen zorgen, heeft een overheidsrol voordelen vanwege de bijbehorende schaalvoordelen, de machtspositie van de identiteitsbeheerder, standaardisatie, en voorkoming van dubbele identiteit. PET's bieden de overheid daarom de mogelijkheid bestaande publieke taken efficiënter te vervullen.

Private PET-diensten kunnen op termijn essentieel worden bij veel soorten transacties en bij het beheer van gevoelige persoonsgegevens. Om de betrouwbaarheid van dit soort cruciale PET-diensten te borgen, zou een vergunningensysteem kunnen worden ingevoerd - net als in de financiële sector.

Beleidsoptie 6. Europese toezichthouder

Richt een centrale Europese toezichthouder op voor bedrijven die in meerdere landen opereren, nationale toezichthouders als het CBP kunnen zich dan richten op binnenlandse activiteiten.

Het toezicht in Europa is nu nationaal waardoor het controleren en eventueel sanctioneren van multinationals bovendien tot dubbel werk leidt. Om dubbel werk te beperken en de zekerheid voor burgers en bedrijven te vergroten, staat in de voorgestelde verordening dat in dit soort gevallen de verantwoordelijkheid bij één toezichthouder ligt. Dit is de zogenoemde 'one-stop-shop'.

Europese samenwerking kan nog efficiënter dan nu het geval is. Een centrale Europese toezichthouder met bevoegdheden die vergelijkbaar zijn met die van het Directoraat-generaal Mededinging van de Europese Commissie, heeft twee voordelen. Een eerste voordeel is dat nationale toezichthouders niet allemaal de technische en juridische expertise in huis hoeven te hebben om te kunnen vaststellen of een bedrijf met geavanceerde technologie in overtreding is.

Een tweede voordeel is dat een Europese toezichthouder free-ridergedrag bij toezichthouders voorkomt. Een nationale toezichthouder zal mogelijk minder urgentie zien om capaciteit te reserveren voor het controleren van bedrijven die zich niet op de binnenlandse markt richten. Ook laat een kleine toezichthouder het controleren en eventueel vervolgen van grote multinationals liever over aan grotere toezichthouders. Europees toezicht brengt daarom waarschijnlijk meer daadkracht dan een samenwerkingsverband tussen nationale toezichthouders.

6 Conclusie

De mogelijkheden voor het gebruik van persoonsgegevens in de economie zijn de afgelopen jaren sterk toegenomen. Burgers, consumenten, ondernemers en werkgevers hebben hiervan de vruchten geplukt. Er gaat ook nog regelmatig iets mis, waardoor de privacy van groepen mensen wordt geschonden. De belangen zijn groot en het ligt voor de hand dat persoonsgegevens in de toekomst nog veel intensiever gebruikt gaan worden. Goed privacybeleid is daarom doorslaggevend voor onze welvaart. De diversiteit in voorkeuren voor privacy en snelle technologische ontwikkeling betekenen dat een markt voor overdraagbare gebruiksrechten voor persoonsgegevens centraal zou moeten staan in privacybeleid. We bespreken een aantal beleidsopties die deze markt beter zouden kunnen laten werken.

Literatuur

Acquisti, A. en J. Grossklags, 2005, Privacy and Rationality in Individual Decision Making, *IEEE Security and Privacy*, vol. 3, nr. 1, pag. 26-33.

Acquisti, A., 2008, Identity Management, Privacy, and Price Discrimination, *IEEE Security and Privacy*, vol. 6, nr. 2, pag. 46-50.

Acquisti, A., L. John en G. Loewenstein, 2009, What is privacy worth, Twenty first workshop on information systems and economics (WISE), pag. 14-15.

Athey, S., 2014, Information, Privacy, and the Internet: An Economic Perspective, CPB Lecture 2014.

Berg, G.J., 2006, Revolutionary Effects of New Information Technologies, *The Economic Journal*, vol. 116, nr. 509, pag. F10-F28.

Campbell, J., A. Goldfarb en C. Tucker, 2014, Privacy regulation and market structure, *Journal of Economics and Management Strategy*.

Kelley, P.G., L. Cesca, J. Bresee en L.F. Cranor, 2010, Standardizing privacy notices: an online study of the nutrition label approach, Proceedings of the SIGCHI Conference on Human factors in Computing Systems, pag. 1573-1582.

Mcdonald, A.M., R.W. Reeder, P.G. Kelley en L.F. Cranor, 2009, A comparative study of online privacy policies and formats, Privacy enhancing technologies, pag. 37-55, Springer.

Roosendaal, A. en Tijs van den Broek Anne Fleur van Veenstra, 2014, Vertrouwen in big data toepassingen: accountability en eigenaarschap als waarborgen voor privacy, *Privacy en Informatie*, vol. 2014, nr. 3.

Turow, J., Jennifer King, Chris Jay Hoofnagle, Amy Bleakley en Michael Hennessy, 2009, Americans reject tailored advertising and three activities that enable it, Annenberg School for Communication Working Paper.

Yandle, T. en C.M. Dewees, 2008, Consolidation in an individual transferable quota regime: lessons from New Zealand, 1986–1999, *Environmental management*, vol. 41, nr. 6, pag. 915-928.

Dit is een uitgave van:

Centraal Planbureau
Postbus 80510 | 2508 GM Den Haag
T (070) 3383 380

Juni 2014 | ISBN 978-90-5833-646-0