REGIOPLAN

NIETS TE VERBERGEN EN TOCH BANG

Nederlandse burgers over het gebruik van hun gegevens in de glazen samenleving

- eindrapport -

Drs. J. Koffijberg
Drs. S. Dekkers
Drs. G. Homburg
Dr. B. van den Berg

Amsterdam, januari 2009
Regioplan publicatienr. 1774

Regioplan Beleidsonderzoek
Nieuwezijds Voorburgwal 35
1012 RD Amsterdam
Tel.: 020 - 5315315
Fax : 020 - 6265199

Onderzoek, uitgevoerd door Regioplan Beleidsonderzoek in opdracht van het College bescherming persoonsgegevens

INHOUDSOPGAVE

Samenvatting ..... **I**

1 Inleiding: onderzoek onder burgers over privacy **1**
1.1 Aanleiding van het onderzoek 1
1.2 Onderzoeksvragen 1
1.3 Opzet van het onderzoek 2
1.4 Literatuur 3
1.5 Invloeden privacybewustzijn 5
1.6 Opbouw van het rapport 7

2 Bewustwording versus gedragsverandering **9**
2.1 Groepsgesprekken 9
2.2 Uitwerking thema's 10
2.3 Niet-privacybewusten trekken ook grenzen 11
2.4 De opvattingen van privacybewusten 15
2.5 Conclusie 16

3 Burgers over privacybewustzijn **17**
3.1 Inleiding 17
3.2 Achtergrondkenmerken respondenten 17
3.3 Privacybewustzijn 18
3.4 Opinie privacy 19
3.5 Praktijksituaties 21
3.6 Concreet handelen 22
3.7 Conclusie 22

4 Technologisch-maatschappelijke ontwikkelingen en privacy **25**
4.1 Inleiding 25
4.2 Verwijsindex risicojongeren 25
4.3 Rekeningrijden 27
4.4 Overige thema's 29
4.5 Conclusie 33

5 Informatie en privacybewustzijn **35**
5.1 Inleiding 35
5.2 Informatie en privacybewustzijn: algemeen 36
5.3 De invloed van het type informatie 37
5.4 Conclusie 42

6 Conclusie **43**

Bijlagen **45**
Bijlage 1 Gespreksverslagen 47
Bijlage 2 Achtergrondkenmerken van respondenten..... 59
Bijlage 3 Informatie VIR en rekeningrijden in vragenlijst 63

SAMENVATTING

In opdracht van het College bescherming persoonsgegevens (CBP) heeft Regioplan Beleidsonderzoek een onderzoek uitgevoerd naar opvattingen van burgers over de bescherming van persoonsgegevens.
Het onderzoek moest de volgende vragen beantwoorden:

1. Welke factoren zijn van invloed op opvattingen van burgers over privacy, in het bijzonder met betrekking tot een afstandelijke en toegeeflijke houding tegenover een potentiële aantasting van de bescherming van persoonsgegevens?
2. Op welke manier en in hoeverre komen deze factoren tot uitdrukking in de attitude van burgers ten opzichte van de verwerking van persoons-gegevens in een aantal actuele technologisch-maatschappelijke ontwikkelingen?
3. Op welke manier leidt informatie over feitelijk en potentieel gebruik van verwerkte gegevens tot nuancering van standpunten over de aantasting van de privacy bij een aantal actuele technologisch-maatschappelijke ontwikkelingen?

Het onderzoek is uitgevoerd door middel van een beknopte literatuurstudie, zes groepsgesprekken (waarbij de veertig deelnemers vooraf gescreend waren op een privacybewuste dan wel privacyonbewuste attitude) en een enquête onder ruim 2000 burgers.

De groepsgesprekken laten zien hoeveel verschillende factoren en omstandigheden een rol spelen bij de ontwikkeling van het privacybewustzijn en privacybewust handelen. Het doorspreken van risico's van gegevensverwerkingen leidt tot bewustwording en bij een opeenstapeling van maatschappelijk-technologische ontwikkelingen waarbij de privacy in het geding is, tot een schrikreactie. Deze schrikreactie leidt er echter niet toe dat de deelnemers zeggen hun gedrag te gaan veranderen. Dit vraagt te veel aanpassingen in hun dagelijks leven.

De enquête onder 2016 burgers bevestigt dit beeld. Mensen zijn zich over het algemeen redelijk bewust van hun privacy en hechten belang aan de wijze waarop met hun persoonsgegevens wordt omgegaan. Hun bezorgdheid over de verwerking van hun gegevens is echter niet erg groot en zij zeggen hun persoonsgegevens in het algemeen gemakkelijk te verstrekken.
Als belangrijke factor voor de acceptatie van de verstrekking en verwerking van persoonsgegevens komt vooral 'controle en transparantie' naar voren. Als vooraf om toestemming voor gegevensverwerking wordt gevraagd en informatie over het doel wordt verstrekt, gaan burgers eerder akkoord. Als het gaat om een zorgvuldige verwerking van gegevens, hebben burgers overigens meer vertrouwen in de overheid dan in het bedrijfsleven. Toch plaatsen ze ook

de nodige vraagtekens bij het koppelen van bestanden door overheids-organisaties en een ruim gebruik van het burgerservicenummer.

Het verstrekken van informatie over de verwerking van persoonsgegevens blijkt mensen aan het denken te zetten en het privacybewustzijn te beïnvloeden. Informatie rond ‘controle en transparantie’ heeft meer invloed dan andere onderzochte factoren.

Voor privacybeleid vloeien enkele belangrijke ideeën uit het onderzoek voort:

- Informatie over technologisch-maatschappelijke ontwikkelingen is belangrijk en helpt bij de vorming van attitudes.
- Controle en transparantie is wezenlijk voor acceptatie van gegevens-verwerking door burgers.
- Eenvoudige en toegankelijke bezwaarprocedures kunnen helpen om gelatenheid te vervangen door positieve acceptatie.
- Burgers stellen regelmatige overzichten van over hen geregistreerde persoonsgegevens zeer op prijs.

Zowel in de groepsgesprekken als in de enquête laat het onderzoek een mee-gaande houding van burgers in termen van de verstrekking van persoons-gegevens zien. De gedachte dat deze meegaande houding voort zou komen uit de gedachte niets te verbergen te hebben, wordt door het onderzoek niet bevestigd. Met name in de groepsgesprekken bleken respondenten flink te schrikken als ze met risico’s van de verwerking van persoonsgegevens worden geconfronteerd. Ze zeggen echter niet dat dit tot verandering van hun gedrag leidt. Dit vraagt te veel inspanning en de consequenties zijn in hun ogen te groot. Het gedrag van burgers moet dus eerder in termen van een gevoel van onvermijdelijkheid en gelatenheid dan in termen van vertrouwen in een correct gebruik van de gegevens worden beoordeeld.

1 INLEIDING: ONDERZOEK ONDER BURGERS OVER PRIVACY

1.1 Aanleiding van het onderzoek

Het College bescherming persoonsgegevens (CBP) heeft behoefte aan een verdiept inzicht in de verschillende opvattingen die mensen hebben over het belang van de bescherming van hun persoonsgegevens in relatie tot achterliggende waarden (voorkomen van hinder, schade en discriminatie, het waarborgen van persoonlijke vrijheid en gelijke behandeling, een faire informatiepositie voor de burger en consument). Vanuit deze behoefte heeft het CBP een onderzoek laten uitvoeren naar opvattingen over privacy in de context van de snelle technologisch-maatschappelijke ontwikkelingen die leiden naar een samenleving waarin mensen vrijwel overal en altijd in beeld zijn, gevolgd kunnen worden en veelzeggende digitale sporen achterlaten. Met andere woorden, het onderzoek vindt plaats in de context van de actuele situatie gespiegeld aan tal van nieuwe en actuele ontwikkelingen, zoals het rekeningrijden (en het registreren van voertuigbewegingen), de OV-chipkaart (met de registratie van reizigersbewegingen), het elektronisch patiënten-dossier (wie mag erbij?), het elektronisch kinddossier en het vastleggen van gegevens over internet- en e-mailgedrag en telefoonverkeer.

1.2 Onderzoeksvragen

Het doel van het onderzoek is het geven van inzicht in de verschillende opvattingen die mensen hebben over het belang van de bescherming van hun persoonsgegevens. Het inzicht moet bruikbaar zijn voor het verkrijgen van aandacht voor het belang van het beschermen van persoonsgegevens, in het bijzonder in de context van de actuele en snelle technologisch-maatschappelijke ontwikkelingen waarbij de privacy in het geding is.

De hoofdvragen van het onderzoek zijn:

1. Welke factoren zijn van invloed op opvattingen van burgers over privacy, in het bijzonder met betrekking tot een afstandelijke en toegeeflijke houding tegenover een potentiële aantasting van de bescherming van persoonsgegevens?
2. Op welke manier en in hoeverre komen deze factoren tot uitdrukking in de attitude van burgers ten opzichte van de verwerking van persoons-gegevens bij een aantal actuele technologisch-maatschappelijke ontwikkelingen?
3. Op welke manier leidt informatie over feitelijk en potentieel gebruik van verwerkte gegevens tot nuancering van standpunten over de aantasting van de privacy bij een aantal actuele technologisch-maatschappelijke ontwikkelingen?

1.3 Opzet van het onderzoek

In het onderzoek zijn drie onderdelen te onderscheiden. Deze lichten we hieronder kort toe.

Voorbereiding
In de voorbereidende fase is literatuur bestudeerd en zijn interviews gehouden met enkele thema-experts om grip te krijgen op de belangrijkste ontwikkelingen op het gebied van privacy. In een discussiebijeenkomst met medewerkers van het CBP is gebrainstormd over de thematiek van het onderzoek en over de opzet van het verdere onderzoek. De begripsvorming in deze voorbereidende fase heeft richting gegeven aan het verdere onderzoek. Paragraaf 1.5 geeft hierover meer informatie.

Groepsgesprekken
Er hebben zes groepsgesprekken plaatsgevonden met burgers over hun opvattingen over privacy. De deelnemers zijn op basis van screeningsvragen vooraf ingedeeld in de categorie ‘privacybewust’ en ‘niet-privacybewust’. De eerste vier gesprekken zijn gehouden met deelnemers die zich in het algemeen weinig of geen zorgen maken over de aantasting van de bescherming van de privacy. De twee andere gesprekken vonden plaats met deelnemers die zich daar wel of in enige mate zorgen over maken. De groepsgesprekken dienden om de ideeën uit de eerste fase te toetsen en verder te ontwikkelen en te concretiseren. In totaal hebben veertig burgers aan de gesprekken deelgenomen. Een verdere uitwerking van de gebruikte thematiek in de groepsgesprekken kunt u lezen in hoofdstuk 2.

Enquête onder burgers
Na de groepsgesprekken is een enquête gehouden onder een representatieve groep van burgers, met name gericht op de beïnvloedbaarheid van privacy-attitudes aan de hand van de thema’s die we ook in de groepsgesprekken gebruikten. Het basisstramien was dat we burgers eerst vroegen naar hun opvattingen over het belang van privacybescherming. Vervolgens legden we een aantal concrete situaties voor die zich in de praktijk van de gegevensverwerking zouden kunnen voordoen. Dit gebeurde enigszins verborgen, zodat de respondenten niet wisten dat naar de invloed van de situaties op hun attitudes werd gevraagd. Hiermee toetsten we in hoeverre attitudeverandering door bepaalde factoren wordt gestimuleerd.

Het onderzoek is uitgevoerd in de periode september – november 2008.

1.4 Literatuur

De term privacy wordt in het dagelijks taalgebruik op verschillende manieren gebruikt. Er kunnen drie gangbare betekenissen worden onderscheiden[1]:
1. in de betekenis van ruimtelijke privacy;
2. in de betekenis van intimiteit of individuele zelfbeschikking;
3. in de betekenis van informationele privacy.

Van ruimtelijke privacy is bijvoorbeeld sprake wanneer iemand privacy opeist in de zin van afzondering en rust. Van privacy als intimiteit is sprake wanneer het begrip uitdrukkelijk wordt gebruikt in verband met het persoonlijke leven (in de zin van relaties en seksualiteit van personen). Informationele privacy heeft te maken met de bescherming van persoonsgegevens. In dit rapport hebben we het over privacy in deze laatste betekenis.

Uit onderzoek van TNS Nipo[2] in opdracht van het CBP blijkt dat de meeste Nederlanders wel eens nadenken over de risico's met betrekking tot het gebruik van hun persoonsgegevens. Uit interviews die TNS Nipo hield blijkt dat, hoewel mensen risico's kunnen benoemen met betrekking tot het gebruik van hun persoonsgegevens, ze toch laconiek omgaan met het gebruik van hun persoonsgegevens. Mensen geven vrij gemakkelijk inzage in hun gegevens onder het motto dat ze niets te verbergen hebben, en dat organisaties toch al alles van hen weten dus dat er niets te beschermen valt. Factoren die van belang zijn bij het omgaan met persoonsgegevens zijn volgens TNS Nipo de bewaartermijn, het doel, het type organisatie, de transparantie, het type bron, controle en zelfbeschikking en eigen ervaringen. Het zich bewustzijn van de risico's van het gebruik van persoonsgegevens blijkt zich in gematigde bezorgdheid te vertalen. Meer dan de helft van alle burgers uit het onderzoek van TNS Nipo was redelijk tot zeer bezorgd over het gebruik van hun persoonsgegevens, 43% was hier niet erg bezorgd over.

Uit een onderzoek van het Rathenau Instituut[3] blijkt dat privacy in relatie tot persoonsgegevens een complex begrip is dat samenhangt met negen achterliggende waarden: zelfstandigheid, bewegingsvrijheid, ongestoord leven, vrij blijven van stigmatisering; vrij blijven van manipulatie; eigenwaarde; gelijkheid; integriteit en autonomie. Het begrip privacy heeft geen eenduidige betekenis voor alle burgers. Iedere burger gebruikt een eigen set van waarden voor zijn of haar definitie van privacy. Op basis van deze set waarden toetst iemand een casus waarin een situatie met mogelijke privacyaantasting wordt

[1] Bron: Koops, B.J. en Vedder, A. (2001) *Opsporing versus privacy: de beleving van burgers*. Den Haag, Sdu Uitgeverij.

[2] Bron: Schildmeijer, R. e.a. (2005) *Burgers en hun privacy, opinie onder burgers.* Amsterdam, TNS Nipo.

[3] Bron: Smink, G. e.a. (1999) *Privacybeleving van burgers in de informatiemaatschappij.* Den Haag, Rathenau Instituut.

voorgelegd. De ene burger beoordeelt een mogelijke bedreiging van de privacy in een bepaalde casus ook anders dan de andere.
Burgers kunnen volgens het onderzoek van het Rathenau Instituut op basis van hun beleving van privacy grofweg in drie groepen worden ingedeeld. Ten eerste een groep burgers die nauwelijks privacyproblemen ondervindt door de informatietechnologie. Deze burgers definiëren privacy relatief eenvoudig (weinig waarden). De tweede groep burgers vindt dat aan informatie-technologie privacyproblemen kleven. Zij berusten hier tot op zekere hoogte in omdat zij van mening zijn dat dit in de huidige maatschappij nu eenmaal nodig is. Ze hanteren een iets complexere definitie van privacy dan de eerste groep (meer waarden). De derde groep hanteert de meest complexe definitie van privacy (alle waarden). Deze burgers vinden dat informatietechnologie privacy-problemen met zich meebrengt en dat dit te voorkomen is omdat het gebruik van informatietechnologie vaak niet nodig is.
Het oordeel over de ernst van de schending van de privacy in een bepaalde situatie hangt behalve van iemands individuele waardenset af van een aantal criteria. Dit zijn:

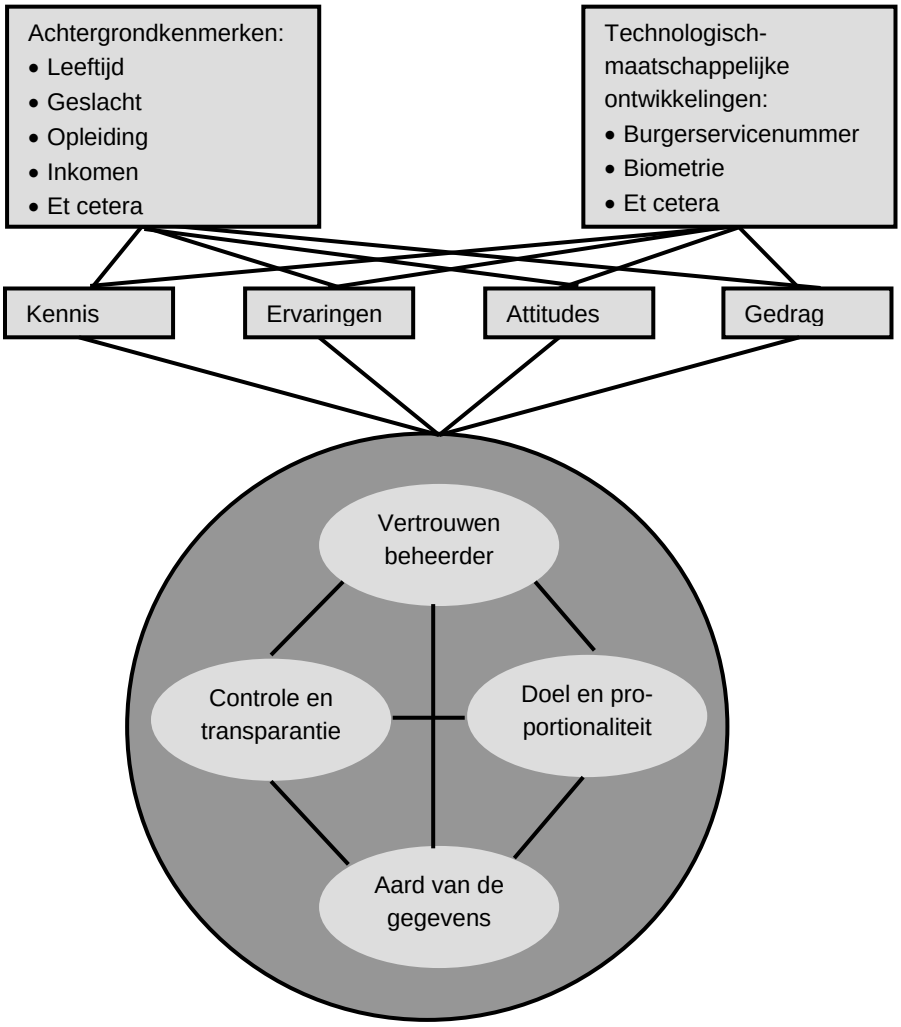
- de mate waarin men het doel van het verzamelen en gebruiken van de persoonsgegevens belangrijk vindt. Voor belangrijke doelen vindt men het gebruik van persoonsgegevens eerder goed dan voor onbelangrijke doelen.
- de gevoeligheid van de gevraagde persoonsgegevens;
- de relevantie van de persoonsgegevens voor het bereiken van het beoogde doel;
- de mate waarin burgers zelf controle hebben over wat er met hun persoonsgegevens gebeurt;
- hoe de informatie wordt behandeld en door wie. Met name de juistheid van de gegevens en welke instantie over welke persoonsgegevens beschikt, zijn daarbij belangrijke criteria.

De criteria op basis waarvan de invulling van een bepaalde casus wordt beoordeeld, verschillen qua belang. Het relatieve belang blijkt echter verschillend te zijn voor verschillende burgers. Burgers die niet of nauwelijks privacy-problemen ondervinden door het gebruik van informatietechnologie, beoordelen allereerst het doel en de relevantie van de gegevens voor het betreffende doel en hechten met name belang aan het onderhoud van de gegevens en het vertrouwen dat zij stellen in de verzamelaar. Burgers die daarentegen veel privacyproblemen verwachten door het toenemende gebruik van informatietechnologie vinden dit ook belangrijke criteria maar zij eisen bovenal dat zij toestemming moeten kunnen geven voordat zij worden opgenomen in een systeem, dat zij de mogelijkheid moeten hebben om zich uit het bestand te laten verwijderen en dat zij zelf moeten kunnen bepalen wie inzage mag hebben in hun gegevens. Met andere woorden, deze burgers hechten veel sterker aan hun zelfbeschikking (controle) over persoonlijke gegevens dan de eerstgenoemde burgers.

1.5 Invloeden privacybewustzijn

In figuur 1 zijn invloeden op het privacybewustzijn in onderlinge samenhang weergegeven. De begrippen zijn gebruikt om de gesprekken met zes groepen burgers vorm te geven en aan te sturen.

Figuur 1 Privacybewustzijn: invloeden



Het idee achter de samenhang binnen het stelsel van begrippen is als volgt: Achtergrondkenmerken zoals leeftijd, geslacht, opleiding, inkomen, maar ook gezondheid en woonsituatie, et cetera beïnvloeden de kennis over, de ervaringen met, de attitudes ten aanzien van en uiteindelijk het gedrag met betrekking tot het uitwisselen van persoonsgegevens en de privacyaspecten daarvan. Kennis, ervaringen, attitudes en gedrag zijn uiteindelijk van invloed op het privacybewustzijn. Dat geldt ook voor technologisch-maatschappelijke ontwikkelingen zoals de toepassing van biometrie, de verdere ontwikkeling van het burgerservicenummer (BSN) et cetera.

Het privacybewustzijn is weergegeven in de grote cirkel en is samengesteld uit vier onderling aan elkaar gerelateerde aspecten. Het is daarmee een containerbegrip dat uit verschillende aspecten bestaat en dat wordt gevoed door diverse factoren.

De vier aspecten (vertrouwen gegevensbeheerder, controle en transparantie van het uitwisselingsproces, aard van de gegevens oftewel de mate van 'gevoeligheid' van de gegevens en het doel en de proportionaliteit van de gegevensuitwisseling) bestaan elk uit verschillende deelaspecten (zie hieronder). In het onderzoek relateren we de vier hoofdaspecten en de bijbehorende deelaspecten aan specifieke inhoudelijke onderwerpen (technologisch-maatschappelijke ontwikkelingen), zoals het vastleggen van verplaatsingsgedrag door middel van rekeningrijden, het gegevens-uitwisselingsgedrag van burgers op sociale netwerksites, de ontwikkeling van het BSN tot centrale schakel in diverse (overheids)administraties, et cetera.

Bij de vier hoofdaspecten passen de volgende deelaspecten:

Vertrouwen in hoe de beheerder van persoonsgegevens met deze gegevens omgaat

- Vertrouwen in de 'overheid' versus vertrouwen particulieren/bedrijfsleven.
- Vertrouwen onderscheiden naar diverse overheden (departement, provincie, gemeenten, diverse zelfstandige bestuursorganen (ZBO's, zoals de Belastingdienst), politie, justitie).
- Vertrouwen in de overheid in het algemeen (los van rol van beheerder).
- Vertrouwen onderscheiden naar gebruiksdoel.

Doel en proportionaliteit van de gegevensverzameling

- Doel waarvoor gegevens worden vastgelegd (administratief, dienstverlening overheid, zakelijk particulier, algemeen belang (bijvoorbeeld veiligheid), privé- versus publieksgebruik).
- Mate van gepercipieerde rechtvaardigheid doel (goedaardigheid).
- Mate van nabijheid van het doel (betrokkenheid op de eigen, persoonlijke situatie, wij-zijgevoel).
- Mate waarin doel appelleert aan centrale waarden zoals vrijheid, individualiteit en zelfbeschikkingsrecht.

Controle en transparantie

- Mogelijkheid van invloed uitoefenen op gegevensvastlegging en verstrekking.
- De zichtbaarheid van gegevens, mate waarin burgers (gevraagd/ongevraagd) met de gegevens worden of kunnen worden geconfronteerd.
- Mate waarin derden toegang hebben tot de gegevens.
- Mate waarin gegevens kunnen worden gekoppeld aan andere gegevens.

Aard van de gegevens

- Onderscheid naar type gegevens (medisch, financieel, sociaal/economisch, justitieel, et cetera).
- Binnenkant- versus buitenkantgegevens. Onder binnenkantgegevens wordt inhoudelijke informatie verstaan, onder buitenkantgegevens alleen het feit dat er gegevens zijn vastgelegd. In een dossier kan bijvoorbeeld worden vastgelegd dat meneer Jansen op 23 maart naar de huisarts is geweest vanwege pijn in zijn rug. Dan worden zowel binnen- als buitenkant gegevens vastgelegd. Als er in een dossier staat dat meneer Jansen op 23 maart naar de huisarts is geweest, zonder dat vermeld is waarvoor precies, betreft het alleen buitenkantgegevens.
- Statisch/dynamisch karakter van gegevensverzameling. Een statisch karakter houdt in dat de gegevens één keer worden verzameld en daarna niet meer worden aangepast. Bij de dynamische variant van gegevens verzamelen worden gegevens regelmatig geactualiseerd.
- Mogelijk schadelijk karakter van de gegevens (voor een burger zelf, voor derden), gepercipieerde kans op misbruik.
- Bewaartermijn gegevens.

1.6 Opbouw van het rapport

In hoofdstuk 2 wordt verslag gedaan van de zes groepsgesprekken met veertig burgers, hun privacybewustzijn en de invloed die maatschappelijk-technologische ontwikkelingen daarop uitoefenen. Het gaat hierbij om kwalitatieve gegevens. De hoofdstukken 3 tot en met 5 zijn gebaseerd op de enquête onder 2016 burgers en gaan respectievelijk over het privacy-bewustzijn (hoofdstuk 3), opvattingen over privacy in relatie tot maatschappelijk-technologische ontwikkelingen (hoofdstuk 4) en de invloed van informatie op het privacybewustzijn (hoofdstuk 5). In hoofdstuk 6 worden de uitkomsten van de groepsgesprekken en de enquête in samenhang besproken.

2 BEWUSTWORDING VERSUS GEDRAGSVERANDERING

2.1 Groepsgesprekken

Om de ideeën en begrippen uit de literatuurstudie nader uit te werken, hebben we met veertig burgers in zes bijeenkomsten gesproken over opvattingen over privacy en factoren die het privacybewustzijn beïnvloeden.
We zijn hierbij op zoek gegaan naar factoren die beïnvloeden of burgers zich wel of geen zorgen maken over de aantasting van hun privacy. We hebben hierbij vier begrippen centraal gesteld: de aard van de gegevens, het doel en de proportionaliteit van de gegevensverzameling, het vertrouwen in het type organisatie dat de gegevens verzamelt en de controle op en transparantie van de gegevensverzameling.
Tevens hebben we de burgers concrete casussen voorgelegd en ze gevraagd of ze zich bij de betreffende casus al dan niet zorgen maken over de aantasting van de privacy. Op deze manier zijn we op zoek gegaan naar een 'omslagpunt' in het denken over privacy: welke factoren maken dat burgers veranderen van een toegeeflijke houding naar een defensieve houding tegenover een potentiële aantasting van de bescherming van persoons-gegevens?

We hebben de volgende casussen in de groepsgesprekken behandeld:
- het vastleggen van verplaatsingsgegevens;
- het publiceren van gegevens op internet;
- de relatie tussen werkgevers en werknemers;
- elektronische dossiers met patiëntgegevens en informatie over risicojongeren;
- het vastleggen van locatie-informatie via telecomtoepassingen;
- biometrie;
- datamining;
- het burgerservicenummer (BSN).

Deze thema's lichten we toe in paragraaf 2.2.

De deelnemers aan de groepsgesprekken zijn vooraf gescreend op hun privacybewustzijn en privacybewust handelen. Voor vier groepsgesprekken zijn burgers uitgenodigd waarbij uit de screening bleek dat ze niet erg privacybewust zijn en hun persoonsgegevens makkelijk aan derden geven. Deze groep noemen we in de rest van het hoofdstuk 'de niet-privacy-bewusten'. Voor de twee overige groepsgesprekken zijn burgers uitgenodigd die aangaven wel privacybewust te zijn en hun persoonsgegevens ook goed beschermen. Deze noemen we in de rest van dit hoofdstuk de 'privacy-bewusten'.

In bijlage 2 is een overzicht van de achtergrondkenmerken van de respondenten opgenomen.

2.2 Uitwerking thema's

Het vastleggen van verplaatsingsgegevens
Door nieuwe technieken wordt het mogelijk verplaatsingsgegevens vast te leggen, bijvoorbeeld in het geval van de OV-chipkaart en rekeningrijden. Interessante kwesties bij dit thema zijn de verschillende doelen waarvoor deze gegevens mogelijk zouden kunnen worden gebruikt naast het afhandelen van betalingen voor het reizen met het openbaar vervoer of met de auto, welke gegevens precies bewaard mogen worden en hoe lang, of burgers inzage willen in het databestand van hun reisgegevens en het vertrouwen in de beheerder van de bestanden met reisgegevens.

Het publiceren van gegevens op internet
Burgers publiceren steeds meer over zichzelf op internet, bijvoorbeeld door een profiel op een sociale netwerksite aan te maken, door het bijhouden van een weblog of door goederen via internet te kopen of verkopen. Burgers plaatsen daarbij verschillende soorten gegevens over zichzelf op internet. Deze kennen hun eigen risico's. Op internet gepubliceerde informatie is via zoekmachines nog jaren later vindbaar. Iedereen met een internetaansluiting heeft toegang tot deze gegevens en kan ze voor verschillende doelen gebruiken.

De relatie tussen werkgevers en werknemers
Hoe ver mag een werkgever gaan om een werknemer te controleren? Mag de werkgever bijvoorbeeld de e-mails van een werknemer bekijken? Of bijhouden waar een werknemer met een bedrijfsauto zich bevindt als deze gebruikmaakt van de auto? En mag een werkgever gegevens van een medewerker opzoeken door zijn/haar naam in te toetsen in een zoekmachine op internet?

Elektronische dossiers met patiëntgegevens en informatie over risicojongeren
Elektronische patiëntendossiers staan op het punt te worden ingevoerd. Er wordt gesproken over het koppelen van deze dossiers met bijvoorbeeld een verwijsindex voor risicojongeren. Welke informatie mag worden vastgelegd in deze elektronische patiëntendossiers? En op welke gronden mag een jongere in een verwijsindex worden opgenomen? Wie mogen deze gegevens inzien en hoe lang mogen deze bewaard blijven?

Het vastleggen van locatie-informatie via telecomtoepassingen
Telecomproviders kunnen traceren waar iemand met een ingeschakelde mobiele telefoon zich bevindt. Waar mag deze locatie-informatie voor worden gebruikt? Mag deze bijvoorbeeld worden gebruikt voor opsporingsdoeleinden? Mogen er commerciële toepassingen aan worden gekoppeld zodat winkels consumenten die zich in de buurt van de winkel bevinden een sms met de nieuwste aanbiedingen sturen? En wat vinden burgers van GPS-toepassingen op een mobiele telefoon waarbij je aan vrienden zichtbaar kunt maken waar je je op dat moment bevindt?

Biometrie
Bij het gebruik van biometrische gegevens gaat het om het vastleggen van meetbare gegevens van levende wezens. Het kan hierbij gaan om vingerafdrukken, irisscans, DNA et cetera. Biometrische toepassingen worden bijvoorbeeld gebruikt in paspoorten of bij het regelen van betalingsverkeer (betalen met een vingerafdruk). Hoe denken burgers over het gebruiken van biometrische gegevens voor dit soort toepassingen? En wat vinden zij van gezichtsherkenning door middel van het gebruik van 'intelligente camera's' waarbij bijvoorbeeld voetbalsupporters voor ze een stadion binnen mogen een gezichtsscan moeten laten maken door zo'n camera?

Datamining
Datamining is het hergebruiken van beschikbare data. Hierbij wordt bijvoorbeeld geprobeerd om op een geautomatiseerde manier patronen en relaties te herkennen in grote hoeveelheden gegevens. Om deze patronen te herkennen, kunnen bestanden aan elkaar worden gekoppeld om risicoprofielen te ontwikkelen. Een andere mogelijkheid is het versturen van op de consument toegesneden reclameboodschappen (op basis van monitoring van koopgedrag met RFID-technologie (microchips)) in de supermarkt.

Het BSN: 'u bent een nummer'
Het burgerservicenummer (BSN) is een persoonsnummer. Het heeft het sofinummer per 26 november 2007 vervangen. Alle overheidsorganen mogen het BSN gebruiken. Ook huisartsen, apothekers, verzekeraars et cetera. kunnen dit nummer gebruiken. Dit is een verschil met het oude sofinummer: dit nummer mocht alleen worden gebruikt door een overheidsorgaan als dit in een wettelijke regeling was opgenomen. Het burgerservicenummer zou ook kunnen worden gebruikt in een context waarin men het niet verwacht, bijvoorbeeld door het bedrijfsleven. Hoe denken burgers hierover? En hoe groot is de kans op fraude, het opnemen van foutieve gegevens en bijbehorende schade? Vertrouwen burgers erop dat elke individuele ambtenaar die toegang heeft tot persoonsgegevens hier geen misbruik van maakt?

2.3 Niet-privacybewusten trekken ook grenzen

2.3.1 Factoren die het privacybewustzijn beïnvloeden

In onze benadering wordt het privacybewustzijn door vier factoren beïnvloed: vertrouwen in de beheerder van gegevens, doel en proportionaliteit, aard van de gegevens, controle en transparantie. In de gesprekken zijn we nagegaan of we deze factoren terugzien bij het maken van de afweging wel of niet over te gaan tot het verstrekken van de persoonsgegevens. Dit blijkt inderdaad zo te zijn. Hieronder lichten we de rol die elk van deze factoren speelt afzonderlijk toe.

- Voor een doel dat burgers persoonlijk aanspreekt (bijvoorbeeld veiligheid of onderzoek naar ziekten) zijn zij eerder geneigd over te gaan tot het verstrekken van persoonsgegevens. Ook eigenbelang speelt een rol: als een onderzoek bijvoorbeeld in dienst staat van de verbetering van de dienstverlening van een organisatie waarvan mensen zelf gebruikmaken, verlenen burgers eerder hun medewerking. Bij het element proportionaliteit blijkt het belangrijk dat er niet meer gegevens worden gevraagd dan voor het oorspronkelijke doel noodzakelijk is.

- Burgers zijn het voorzichtigst met het verstrekken van medische en financiële gegevens. Opvallend is dat zij meer risico's zien bij het prijsgeven van beeldmateriaal dan van teksten. Concreet betekent dit bijvoorbeeld dat zij verspreiding van foto's waarop zij in benevelde toestand staan riskanter vinden dan het verspreiden van geschreven teksten (bijvoorbeeld hun mening over een politicus). Beeldmateriaal is achteraf moeilijker te nuanceren dan geschreven tekst, vinden de respondenten.

- Wat betreft het soort organisatie valt het op dat de meeste respondenten meer vertrouwen hebben in de overheid dan in particuliere bedrijven wanneer het gaat om het op een goede manier omgaan met hun gegevens. Zij verwachten dat de overheid zich beter aan bestaande wet- en regelgeving houdt en dat de overheid alleen de echt noodzakelijke gegevens verzamelt waar burgers uiteindelijk zelf ook beter van worden. De zelfstandige ondernemers zijn hierop een uitzondering: zij hebben een fors wantrouwen ten opzichte van de overheid.

- Het element controle en transparantie wordt door de respondenten niet spontaan genoemd bij de afwegingen die zij maken. Bij het bespreken van de thema's komt dit element echter wel als belangrijk naar voren. Burgers hechten dus wel waarde aan controle en transparantie, maar noemen deze factor niet spontaan.

Naast deze vier hoofdelementen komen ook de andere factoren die in het vorige hoofdstuk zijn benoemd terug in de gesprekken. Kennis en ervaring blijken een belangrijke rol te spelen in de afweging die mensen maken om wel of niet hun gegevens te verstrekken. Zo geven mensen die veel van computers weten (zoals een student interactieve media) hun gegevens gemakkelijker via internet dan personen die weinig kennis hebben van ICT. Mensen met computerkennis weten naar eigen zeggen goed waar ze op moeten letten (bijvoorbeeld of het versturen van gegevens via een specifieke internetpagina beveiligd is of niet).
Ook eigen ervaringen spelen een belangrijke rol: burgers die negatieve ervaringen hebben met schending van de privacy zijn aanmerkelijk sterker privacybewust. Een deelnemer wiens vriendin door een ex is gestalkt, publiceert bijvoorbeeld zo min mogelijk over zichzelf op internet.

2.3.2 Omslagpunten niet-privacybewusten

Een groot deel van de respondenten is weinig privacybewust en verstrekt gegevens redelijk makkelijk. Ze hebben er vertrouwen in dat organisaties zich aan wetten en regels houden, denken dat er weinig met hun gegevens kan gebeuren of staan niet zo stil bij wat er zou kunnen gebeuren. Ze willen hier ook niet bij stilstaan, want ‘dan kun je je overal wel druk om maken’ en ‘word je gek’. Bovendien heerst er grote gelatenheid: sommige ontwikkelingen kun je toch niet tegenhouden, bepaalde regels (zoals het opnemen van vinger-afdrukken in het biometrisch paspoort) worden gewoon ingevoerd en je kunt er verder niets aan doen, is een veelgehoorde opvatting.

Bij het bespreken van de thema’s met de niet-privacybewusten zijn wel situaties ter sprake gekomen waar een deel van de burgers wel degelijk een grens trekt. Ze denken dus niet in alle gevallen lichtzinnig over het verstrekken van persoonsgegevens. Hieronder worden de situaties beschreven die de niet-privacybewusten onwenselijk achten met het oog op de bescherming van privacy:

Casus vastleggen van de verplaatsingsgegevens:
- Het opsporen van grote misdrijven mag wel, het opsporen van bijvoorbeeld belasting- of uitkeringsfraude gaat een aantal mensen te ver.
- Het combineren van gegevens over reisgedrag met koopgedrag (bijvoorbeeld de OV-chipkaart als betaalmiddel) is onwenselijk.

Casus publiceren van persoonlijke gegevens op internet:
- Het door iemand publiceren van een foto waar je zelf ook op staat zonder dat hiervoor toestemming is gegeven mag niet.
- Het door een krant publiceren van foto’s van omgekomen militairen die zonder toestemming van een netwerksite zijn geplukt mag absoluut niet.
- Netwerksites zouden gebruikers actief moeten informeren voordat hun privacypolicy verandert (en de beheerders van de sites ineens gegevens door mogen verkopen).

Casus relatie werkgever-werknemer
- De meeste respondenten vinden veel geoorloofd, slechts een enkeling trekt de grens bij het afluisteren van telefoongesprekken en meelezen van e-mails zonder dat hier toestemming voor is gegeven.

Casus elektronisch kinddossier (EKD)
- Een enkeling vindt dit een gevaarlijke ontwikkeling omdat gegevens met één druk op de knop kunnen worden verspreid.
- Het EKD mag niet eindeloos bewaard blijven maar moet worden vernietigd op iemands achttiende verjaardag.
- Het EKD mag alleen ‘harde’ medische gegevens bevatten en niet worden gekoppeld aan een verwijsindex risicojongeren.

- Niet elke hulpverlener mag alle informatie zien, maar alleen de informatie die voor die specifieke hulpverlener relevant is.
- Er wordt veel belang gehecht aan transparantie en het recht op correctie.

Casus vastleggen locatie-informatie via telecomtoepassingen

- Niet gebruiken ter preventie, alleen voor opsporingsdoeleinden.
- Alleen gebruiken voor opsporing van zware misdrijven, niet voor belasting- of uitkeringsfraude.
- Het zou voor commerciële partijen niet mogelijk moeten zijn dat zij gebruikmaken van deze gegevens.
- Het via GPS kenbaar maken aan vrienden waar je bent, vindt iedereen een belachelijk idee, wellicht alleen handig om toe te passen bij kleine kinderen.

Casus Burgerservicenummer

- Er is verontwaardiging over de uitbreiding van de toepassing zonder informatie hierover te hebben ontvangen.
- Men heeft twijfels over de veiligheid van de gebruikte techniek, verder is er opvallend veel vertrouwen in de naleving van regels over het niet mogen koppelen van bestanden.

Casus biometrie

- Mensen hebben dubbele gevoelens over het vastleggen van vingerafdrukken en irisscans.
- Het vervangen van sociale/menselijke controle door apparaten (bijvoorbeeld vingerafdruk in de crèche) keurt men af, niet zozeer vanwege privacy, maar meer vanwege de manier van inrichten van de samenleving.
- Slimme camera's die gelaatsscans kunnen maken en linken aan een database in de openbare ruimte vindt men te ver gaan. Het gebruik van deze camera's om hooligans uit voetbalstadions te weren, vindt men wel een goed idee.

Casus datamining

- Burgers hebben veel vertrouwen in wet- en regelgeving waarin staat dat bestanden niet zomaar mogen worden gekoppeld. Het is geen prettig idee dat het wel zou kunnen.
- Met name wanneer gegevens in handen kunnen komen van commerciële partijen baart dit mensen zorgen.

2.3.3 Bewustwording en gedragsverandering

Opvallend is dat een deel van de niet-privacybewuste respondenten na afloop van de gesprekken zegt te zijn geschrokken van de gebruikte gespreksvoorbeelden. Ze zeggen 'paranoïde' of zelfs 'depressief' naar huis te gaan. Toch zorgt dit naar eigen zeggen niet voor een gedragsverandering. De bewustwording duurt maar even en zal geen effect hebben op hun dagelijkse leven, zeggen de deelnemers. Volgens hen kun je er eenvoudigweg niet te lang bij

blijven stilstaan, want je gedrag aanpassen vanwege privacy is praktisch gezien niet mogelijk: soms is het verplicht gegevens door te geven en een leven zonder internet is in de huidige tijd niet meer mogelijk. Als je wel te veel bij privacykwesties stil staat 'word je gek' zegt een groot deel van de groep. Toch worden er in twee gesprekken wel gegevens uitgewisseld over websites als infofilter.nl (waar burgers kunnen aangeven niet gebeld te willen worden door bedrijven) en heeft een klein aantal mensen het website-adres van het CBP gevraagd omdat ze geïnteresseerd zijn in de wet- en regelgeving omtrent privacy en in de organisatie die de privacy bewaakt.

2.4 De opvattingen van privacybewusten

De respondenten die wel privacybewust zijn, zeggen dat dit komt door hun opvoeding, berichten in de krant of door negatieve ervaringen van henzelf of anderen in hun nabijeomgeving. Voorbeelden van deze negatieve ervaringen zijn: dat je meerdere malen per dag wordt gebeld door energieleveranciers, of dat je e-mailadres of computer gehackt is.
De respondenten uit deze groepen gaan zeer bewust om met het verstrekken van hun eigen gegevens. Toch zijn ze in sommige gevallen juist weer opvallend mild in hun beoordeling van nieuwe ontwikkelingen. Een groot deel van de privacybewusten vindt bijvoorbeeld het EKD een goed idee. Hieronder volgen de belangrijkste uitkomsten van de gesprekken met de privacybewusten:

EKD

- Een EKD zou alleen voor kinderen met problemen moeten worden aangelegd als het ook niet-medische gegevens gaat bevatten.
- Het is niet vanzelfsprekend dat ouders altijd inzake mogen hebben in het dossier (sommige zaken zoals het gebruiken van een anti-conceptiepil zouden ook voor de ouders verborgen moeten kunnen blijven).
- Hulpverleners hebben veel te macht bij het EKD, zij kunnen er ook onjuiste informatie in zetten.

Biometrie

- Men vreest fraudegevoeligheid en koppeling aan andere bestanden.
- De mogelijkheid van het maken van gelaatsscans zorgt voor het idee je hele leven te worden gevolgd.
- Biometrische toepassingen leiden ertoe dat mensen gaan denken over een scenario waarin iedereen in de toekomst een chip in de huid krijgt. Dit scenario wordt als zeer onwenselijk bestempeld.

Locatie-informatie via telecomtoepassingen

- Een deel van de groep reageert hierop opvallend mild: wat voor kwaads kan er gebeuren als derden de beschikking hebben over gegevens betreffende je verblijfplaats. Een ander deel vindt het geen prettig idee traceerbaar te zijn.

- De mogelijkheid van het ontvangen van reclame-smsjes in de buurt van bepaalde winkels wordt gezien als vervelende consequentie maar niet als ernstige aantasting van de privacy.
- Traceerbaarheid via GPS gaat een deel van de groep echt te ver.

Datamining

- Men is zich ervan bewust dat bestanden kunnen worden gekoppeld, maar is er ook laconiek over. De deelnemers vinden het met name vervelend dat ze zelf geen controle hebben over de gegevens die bij anderen bekend zijn.

2.5 Conclusie

Bij de bepaling van het privacybewustzijn spelen uiteenlopende overwegingen en waardenstelsels een rol, die per burger kunnen verschillen. Door confrontatie met situaties waarin privacyrisico's een rol spelen, zeggen burgers meer stil te staan bij de mate waarin hun persoonsgegevens al dan niet beschermd zijn. Dit betekent niet dat zij hun gedrag aanpassen. Dit vraagt immers veel: veel gegevensverstrekkingen hebben een verplicht karakter. Voor zover dat niet zo is, vergt het een flinke aanpassing van de levensstijl om zich aan de gegevensverstrekking te onttrekken. Daarnaast is het moeilijk om alle consequenties van de verstrekking van gegevens te doorgronden. Al met al is daardoor sprake van een zekere gelatenheid. Burgers veranderen hun gedrag hooguit mondjesmaat, ook al zijn ze soms bezorgd over hun privacy.

3 BURGERS OVER PRIVACYBEWUSTZIJN

3.1 Inleiding

In het vorige hoofdstuk is gerapporteerd over de uitkomsten van de groepsgesprekken met respondenten. In dit hoofdstuk en de twee volgende hoofdstukken wordt gerapporteerd over de uitkomsten van de enquête. Als wordt gesproken over respondenten dan wordt hier dus een andere groep respondenten mee bedoeld dan in hoofdstuk 2.

Aan de respondenten is gevraagd in welke mate zij stilstaan bij het beschermen van hun persoonsgegevens en hier hun gedrag op afstemmen. We noemen dit privacybewustzijn en privacybewust gedrag.
In dit hoofdstuk maken we een onderverdeling in een aantal aspecten, namelijk:

- het bewustzijn zelf, ofwel de mate waarin burgers wel eens nadenken over of stilstaan bij privacy;
- de opinie over privacy en de mate waarin burgers belang hechten aan privacybescherming;
- de praktijk waarin burgers te maken hebben met privacyvraagstukken;
- het concrete handelen van burgers ten aanzien van hun privacy.

Deze onderdelen zijn in deze paragraaf uitgewerkt. Als er opvallende verschillen zijn naar achtergrondkenmerken wordt hierover gerapporteerd. Verder wordt waar mogelijk een vergelijking gemaakt met het onderzoek dat TNS Nipo in 2004 in opdracht van het CBP heeft uitgevoerd.

3.2 Achtergrondkenmerken respondenten

In totaal hebben 2016 respondenten de enquête over privacybewustzijn ingevuld. De helft van hen is vrouw (50,4%), de gemiddelde leeftijd is 45,5 jaar. Van de respondenten heeft 45,5 procent een hbo-opleiding of universitaire studie afgerond. Hogeropgeleiden zijn daarmee oververtegenwoordigd, aangezien ongeveer een kwart van de Nederlandse bevolking een dergelijk diploma bezit (CBS, 2007).
In totaal is 8,6 procent van de respondenten van allochtone afkomst. Dit is wat minder dan in de algemene populatie waarin ongeveer 20 procent van allochtone afkomst is (CBS, 2007). Meer dan de helft van de respondenten heeft een midden-hoge of hoge sociaal-economische status (59,1%). Tot slot heeft 30 procent van de respondenten één of meer thuiswonende kinderen onder de achttien jaar.

In de vragenlijst is ook gevraagd naar een aantal andere kenmerken van de respondenten, zoals politieke interesse en internetgebruik. Ongeveer tien procent van de respondenten geeft aan sterk geïnteresseerd te zijn in politiek. Een grote groep respondenten (47,9%) zegt echter niet zo geïnteresseerd te zijn in politiek. Met betrekking tot internetgebruik valt op dat de meerderheid van de respondenten thuis iedere dag surft op het internet (59,3%). Slechts 1,6 procent van de respondenten surft nauwelijks op het internet. De meerderheid van de respondenten kijkt een tot drie uur televisie per dag (54,2%).

In bijlage 2 is een overzicht van de kenmerken van de respondenten opgenomen.

3.3 Privacybewustzijn

In tabel 3.1 is het privacybewustzijn van de respondenten weergegeven.

Tabel 3.1 Privacybewustzijn, in percentages (n = 2016)

	Vaak	Regelmatig	Soms	(Bijna) nooit
Denkt u wel eens na over de risico's met betrekking tot het gebruik van persoonsgegevens?	8	34	48	10
Staat u er wel eens bij stil als u uw gegevens verstrekt aan een organisatie (bedrijf of overheid) dat deze gegevens bewaard kunnen blijven in een databestand?	17	42	34	8
Staat u er wel eens bij stil dat gegevens die u aan een organisatie (bedrijf of overheid) verstrekt gekoppeld zouden kunnen worden aan gegevens over u die verzameld zijn in andere databestanden?	7	31	42	20

Bij de risico's van het gebruik van persoonsgegevens in het algemeen staat 42 procent van de respondenten vaak of regelmatig stil. In vergelijking met het onderzoek van TNS Nipo is dit percentage aanzienlijk hoger. In dat onderzoek dacht maar 28 procent wel eens na over deze risico's.
Mannen, respondenten met een hoog opleidingsniveau en respondenten met een hoge sociaaleconomische status denken hier vaker over na dan vrouwen, respondenten met een laag opleidingsniveau en respondenten met een lage sociaaleconomische status. Ook respondenten die meer geïnteresseerd zijn in politiek en die vaker gebruikmaken van internet denken hier meer over na dan degenen zonder interesse in politiek en die weinig gebruikmaken van internet.

Twee vijfde van de respondenten (59%) staat vaak of regelmatig stil bij het feit dat als je gegevens verstrekt aan een organisatie deze gegevens ook bewaard kunnen blijven in een databestand. Vrouwen, politiek geïnteresseerde

respondenten en respondenten die regelmatig op het internet surfen staan hier vaker bij stil.

Verder staat 38 procent vaak of regelmatig stil bij het feit dat gegevens kunnen worden gekoppeld aan gegevens uit andere databestanden. Mannen staan hier in verhouding met vrouwen vaker bij stil. Ook staat men hier vaker bij stil naarmate men ouder is, hoger is opgeleid, meer is geïnteresseerd in politiek en meer gebruikmaakt van internet.

3.4 Opinie privacy

Als de respondenten gevraagd wordt of ze bezorgd zijn over het gebruik van hun persoonsgegevens, geeft 4 procent aan zeer bezorgd te zijn, 40 procent bezorgd, 52 procent niet erg bezorgd en 4 procent helemaal niet bezorgd. Vrouwen zijn meer bezorgd over het gebruik van persoonsgegevens dan mannen. Ook is men meer bezorgd naarmate men jonger is, meer geïnteresseerd is in politiek en naarmate men meer gebruikmaakt van internet.

De meerderheid van de respondenten is dus niet erg of helemaal niet bezorgd (56%). In het onderzoek van TNS was dit 48 procent.

Als de respondenten wordt gevraagd wat zij belangrijk vinden bij de verwerking van hun persoonsgegevens, hechten zij veel belang aan alle in tabel 3.2 genoemde aspecten.

Tabel 3.2 Belang privacybescherming, in gemiddelde rapportcijfers (van 1 tot 10) (n = 2016)

Stelling	Gemiddeld cijfer	Kenmerk respondenten hogere score (meer belang)
Ik vind het belangrijk dat ik de mogelijkheid heb om mijn gegevens te laten verwijderen als ik dat nodig vind.	9,25	Vrouw, ouder, politiek geïnteresseerd
Ik vind het belangrijk dat mijn gegevens uitsluitend worden gebruikt waarvoor ik ze heb gegeven.	9,20	Vrouw, ouder, 1 of meer kinderen
Ik vind het belangrijk dat ik zekerheid heb dat mijn gegevens uitsluitend worden gebruikt waarvoor ik ze heb gegeven.	9,04	Vrouw, ouder, 1 of meer kinderen
Ik vind het belangrijk dat ik geïnformeerd word over de mogelijke consequenties van het geven van mijn gegevens.	8,89	Vrouw, ouder
Ik vind het belangrijk dat ik op de hoogte ben van het doel waarvoor mijn gegevens worden gebruikt.	8,86	Vrouw, ouder, hoger opgeleid, 1 of meer kinderen, politiek geïnteresseerd
Ik vind het belangrijk dat ik de mogelijkheid heb om mijn gegevens in te zien, zodat eventuele onjuistheden gecorrigeerd kunnen worden.	8,84	Vrouw, ouder, politiek geïnteresseerd
Ik vind het belangrijk dat ik weet wie toegang heeft tot mijn gegevens.	8,77	Vrouw, ouder, politiek geïnteresseerd

Uit de tabel blijkt dat respondenten aan alle aspecten van gegevensbescherming veel belang hechten, maar wat respondenten vooral belangrijk vinden (gemiddelde van 9 of hoger) is dat hun gegevens uitsluitend worden gebruikt waarvoor ze zijn afgegeven en dat zij hun gegevens kunnen laten verwijderen. Het onderzoek van TNS Nipo leverde nagenoeg dezelfde uitkomsten op.

We hebben gekeken naar de kenmerken van mensen die meer belang hechten aan privacybescherming. Tabel 3.2 laat zien dat vrouwen op alle stellingen over privacybescherming hoger scoren dan mannen, wat betekent dat vrouwen meer belang hechten aan privacybescherming dan mannen. Verder geldt dat hoe ouder de respondenten zijn, hoe belangrijker zij de verschillende aspecten van privacybescherming vinden. Tevens hechten respondenten met kinderen en respondenten die geïnteresseerd zijn in politiek meer belang aan privacybescherming.

Ten aanzien van het privacybewustzijn is respondenten tot slot gevraagd in welke mate zij het eens zijn met de stelling dat hun privacy steeds meer in het gedrang komt door een toenemend gebruik van informatietechnologie (computers en andere manieren van gegevens elektronisch opslaan en uitwisselen). Van de respondenten is 62 procent het hier (helemaal) mee eens, ruim een kwart staat hier neutraal in en 11 procent is het hier (helemaal) niet mee eens.

Vrouwen en oudere respondenten zijn het vaker eens met deze stelling dan mannen en jongere respondenten. Daarnaast zijn respondenten uit een hogere sociale klasse en respondenten met weinig politieke interesse het vaker eens met deze stelling dan respondenten uit een lagere sociale klasse en respondenten met meer politieke interesse.

3.5 Praktijksituaties

Behalve naar het bewustzijn van en de opinie over privacy is de respondenten ook gevraagd of zij in het dagelijks leven vaak een aantasting van de privacy beleven en of zij wel eens situaties meemaken waarin blijkt dat een organisatie gegevens over hen had, terwijl de respondent hiervan niet op de hoogte was. De resultaten staan in tabel 3.3.

Tabel 3.3 Privacyaantasting in het dagelijks leven, in percentages (n = 2.016)

	Vaak	Regelmatig	Soms	(Bijna) nooit
Komen in uw dagelijks leven vaak situaties voor waarin u het gevoel heeft dat uw privacy wordt aangetast?	1	12	50	37
Heeft u wel eens een situatie meegemaakt waarin bleek dat een organisatie (bedrijf of overheid) gegevens over u had, waarvan u niet wist dat deze organisatie die had?	5	21	43	31

Van de respondenten ervaart 13 procent vaak of regelmatig situaties waarin hun privacy wordt aangetast. 87 procent ervaart deze situatie soms of bijna nooit. Vrouwen, hogeropgeleide respondenten, politiek geïnteresseerde respondenten en respondenten die meer gebruikmaken van internet ervaren dit soort situaties vaker dan mannen, lageropgeleide respondenten, respondenten met weinig interesse in politiek en respondenten die weinig gebruikmaken van internet.

Een kwart van de respondenten heeft wel eens een situatie meegemaakt waarbij een organisatie gegevens van hen had waarvan men niet op de hoogte was. Men geeft vaker aan hiermee te maken te hebben als men vrouw, jong en hogeropgeleid is. Ook geeft men vaker aan dat men wel eens zo'n situatie heeft meegemaakt naarmate men meer geïnteresseerd is in politiek en meer gebruikmaakt van het internet.

3.6 Concreet handelen

De respondenten is gevraagd in welke mate zij privacybewust zijn. De vraag is of dit bewustzijn ook resulteert in privacybewust gedrag. In tabel 3.4 staan de resultaten van twee vragen hieromtrent.

Tabel 3.4 Privacybewust handelen, in percentages (n = 2016)

	Vaak	Regel-matig	Soms	(Bijna) nooit
Komt het wel eens voor dat een organisatie (bedrijf of overheid) om uw gegevens vraagt, maar u deze niet geeft omdat u vindt dat het uw privacy aantast?	2	13	55	30
Bent u bij het verstrekken van uw gegevens wel eens nagegaan hoe lang deze gegevens bewaard zullen blijven?	2	8	21	69

Vijftien procent van de respondenten geeft aan er vaak of regelmatig voor te kiezen gegevens niet te geven aan een organisatie omdat dit als privacy-aantasting wordt ervaren. Tien procent van de respondenten gaat bij het verstrekken van gegevens wel eens na hoe lang ze bewaard blijven. Men vertoont dit privacybewuste gedrag vaker naarmate men meer geïnteresseerd is in politiek en naarmate men meer gebruikmaakt van internet.

Als gevraagd wordt aan respondenten hoe zij doorgaans omgaan met het verstrekken van hun persoonsgegevens, antwoordt 4 procent dat hij of zij gegevens eigenlijk altijd afstaat zonder erover na te denken. 45 procent staat zijn gegevens wel af, maar denkt daarbij wel na over het doel van het gebruik van de gegevens en 52 procent van de respondenten besluit wel eens om gegevens niet af te staan na een afweging te hebben gemaakt. De uitkomsten van het onderzoek van TNS Nipo waren respectievelijk 8, 42 en 48 procent, wat betekent dat de respondenten uit dat onderzoek iets gemakkelijker omgingen met het verstrekken van hun gegevens.[1]

3.7 Conclusie

Geconcludeerd kan worden dat respondenten zich over het algemeen redelijk bewust zijn van hun privacy. De onderzoeksresultaten vergelijkend met het onderzoek van TNS Nipo, kan worden geconcludeerd dat burgers zich momenteel bewuster zijn van hun privacy dan vier jaar geleden. Verder hechten de respondenten een groot belang aan de wijze waarop met hun persoonsgegevens wordt omgegaan.

[1] Het verschil tussen de middengroepen (45%-42%) is niet significant, de overige verschillen wel.

Tegelijkertijd is de bezorgdheid over het omgaan met persoonsgegevens niet heel groot. Ook ondervinden de respondenten in de praktijk niet vaak inbreuken op hun privacy en handelen zij ook niet heel erg privacybewust. Deze bevindingen zijn in overeenstemming met de groepsgesprekken: burgers kunnen zich wel bewust zijn van privacyrisico's bij gegevensverstrekking, maar er daadwerkelijk naar handelen heeft dusdanige consequenties dat men ervoor kiest niet privacybewust te handelen.

4 TECHNOLOGISCH-MAATSCHAPPELIJKE ONTWIKKELINGEN EN PRIVACY

4.1 Inleiding

In de enquête zijn vragen gesteld over technologisch-maatschappelijke ontwikkelingen in relatie tot de privacy. Twee van deze ontwikkelingen, de introductie van een verwijsindex risicojongeren en het rekeningrijden, zijn het meest uitgebreid aan de orde gesteld. Daarnaast zijn vragen gesteld over het volgen van werknemers met GPS, het gebruik van locatie-informatie van telecomaanbieders, het burgerservicenummer, het koppelen van bestanden door overheidsinstanties, het gebruik van digitale vingerafdrukken in paspoorten, sociale netwerksites en het informeren van burgers over de verwerking van persoonsgegevens.

4.2 Verwijsindex risicojongeren

Een verwijsindex risicojongeren is bedoeld om signalen over probleemgedrag van jongeren bij elkaar te brengen. Verschillende hulpverleners kunnen zonder dat ze het van elkaar weten te maken hebben met dezelfde jongere. Het ministerie van Jeugd en Gezin is van plan om een systeem in te voeren waarbij hulpverleners een melding krijgen als een jongere ook in aanraking is geweest met een andere hulpverlener. Dit systeem wordt de verwijsindex risicojongeren (VIR) genoemd. Het werkt digitaal: als een onderwijzer een risicomelding doet en een politieagent doet hetzelfde over dezelfde jongere, dan ontvangen de onderwijzer en de politieagent allebei een e-mail dat er over deze jongere nog een melding is. De onderwijzer en de politieagent kunnen dan contact met elkaar opnemen. De VIR is bedoeld voor jongeren tot 23 jaar.

Voorafgaand aan het onderzoek had slechts 15 procent van de respondenten wel eens van de VIR gehoord. Respondenten die nog nooit van de VIR hebben gehoord, zijn gemiddeld ouder (50 jaar) dan respondenten die er wel eens van hebben gehoord (gemiddeld 45 jaar).

Hoewel slechts weinigen van de VIR op de hoogte zijn, staat een groot deel van de respondenten, 70 procent, positief of zeer positief tegenover het idee, 24 procent is neutraal en 6 procent is (zeer) negatief. Zeer privacybewuste respondenten zijn negatiever over de VIR. Als aan de respondenten nadere informatie over de VIR wordt voorgelegd, zijn degenen die summiere informatie ontvangen het meest positief. Respondenten die gedetailleerdere informatie lezen, oordelen minder positief.

Bijna een kwart van de respondenten is (zeer) bezorgd over de wijze waarop bij de VIR met privacy wordt omgegaan, 41 procent staat hier neutraal in en 34

procent is hier (helemaal) niet bezorgd over. Respondenten met kinderen maken zich meer bezorgd over de wijze waarop bij de VIR met privacy wordt omgegaan dan respondenten zonder kinderen. Ook respondenten die meer privacybewust zijn, maken zich hierover meer zorgen. Respondenten die summiere informatie over VIR voorgelegd hebben gekregen, zijn minder bezorgd dan respondenten die gedetailleerdere informatie kregen.

Aan de respondenten is een aantal stellingen over de VIR voorgelegd. De resultaten staan in tabel 4.1.

Tabel 4.1 Opinie over aspecten van de VIR (n = 1010)

Stelling	Helemaal mee eens	Mee eens	Noch mee eens, noch mee oneens	Mee oneens	Helemaal mee oneens
Het is voor mij belangrijk dat de gegevens uit de verwijsindex risicojongeren beheerd worden door de overheid in plaats van door een private partij	25	44	26	4	1
Ik maak me zorgen over de technische beveiliging van de verwijsindex risicojongeren, zodat mensen de systemen kunnen hacken en daardoor gegevens over mijn kinderen kunnen lezen	14	40	28	15	2
Ik vind dat hulpverleners uit verschillende beroepsgroepen informatie over een jongere zoals wat er met een jongere aan de hand is en welke behandeling hij krijgt digitaal met elkaar moeten uitwisselen	16	51	19	11	2
Ik vind het belangrijk dat ouders en jongeren inzage kunnen krijgen in de gegevens uit de Verwijsindex risicojongeren	31	48	15	6	1

Twee derde van de respondenten vindt dat hulpverleners uit verschillende beroepsgroepen informatie over een jongere digitaal met elkaar moeten kunnen uitwisselen. Het idee van de gegevensuitwisseling vindt dus weerklank. Mannen zijn deze mening vaker toegedaan dan vrouwen. Verder zijn de respondenten die het eens zijn met deze stelling intensievere gebruikers van het internet en privacybewuster dan respondenten die het niet eens zijn met deze stelling.
Ruim twee derde van de respondenten vindt het daarbij belangrijk dat de gegevens uit de VIR worden beheerd door de overheid in plaats van door een private partij. Vijf procent vindt dit (helemaal) niet belangrijk. Mannen vinden dit belangrijker dan vrouwen. Ook vinden respondenten dit belangrijker naarmate ze meer geïnteresseerd zijn in politiek.

Over de technische beveiliging van de VIR maakt ruim de helft van de respondenten zich zorgen, vrouwen meer dan mannen en jongeren meer dan ouderen. Ook respondenten met thuiswonende kinderen onder de achttien

jaar en privacybewuste respondenten maken zich meer zorgen over de technische beveiliging van de VIR.

De grote meerderheid, tachtig procent van de respondenten, vindt het belangrijk dat ouders en jongeren inzage kunnen krijgen in de gegevens uit de VIR. Respondenten die dit belangrijk vinden zijn gemiddeld ouder, hebben vaker thuiswonende kinderen en zijn meer geïnteresseerd in politiek dan respondenten die dit niet belangrijk vinden. Respondenten die informatie hebben gelezen waarin de sprake is van inzage in de gegevens, vinden het belangrijker dat ouders en jongeren inzage hebben dan respondenten die deze informatie niet hebben gekregen.

Uit de gegevens blijkt dat respondenten met thuiswonende kinderen niet meer of minder positief staan tegenover de VIR dan respondenten zonder thuiswonende kinderen. Wel zijn respondenten met thuiswonende kinderen zich bezorgder over de privacyaspecten van de VIR.

Geconcludeerd kan worden dat de respondenten het idee van een VIR waarderen en het nuttig nuttig vinden dat hulpverleners op deze wijze informatie met elkaar uitwisselen. Daarbij is het wel belangrijk dat de gegevens worden beheerd door de overheid. Meer respondenten met thuiswonende kinderen maken zich zorgen over de wijze waarop met de privacy wordt omgegaan en over de technische beveiliging van de gegevens.

4.3 Rekeningrijden

Anders dan bij de VIR was de bekendheid met het rekeningrijden voorafgaand aan het onderzoek wel heel groot. Van de respondenten had 95 procent wel eens gehoord van rekeningrijden, mannen vaker dan vrouwen en oudere respondenten meer dan jongere.

De respondenten zijn aanzienlijk minder positief over het rekeningrijden dan over de VIR. Bijna de helft is (zeer) negatief en slechts één vijfde is (zeer) positief. Respondenten zijn negatiever over rekeningrijden naarmate ze meer autorijden: respondenten die zeer positief zijn over rekeningrijden gebruiken gemiddeld 2,7 dagen per week de auto terwijl respondenten die zeer negatief zijn over rekeningrijden dit gemiddeld 4,8 dagen per week doen.
Respondenten die positief zijn over rekeningrijden zijn gemiddeld ouder en hogeropgeleid dan respondenten die niet positief zijn over het rekeningrijden.

De helft van de respondenten is bezorgd over het omgaan met de privacy bij het rekeningrijden. Respondenten met een lage sociaaleconomische status maken zich meer zorgen dan respondenten met een hoge sociaaleconomische status. Ook maken respondenten zich meer zorgen over de privacy aspecten van het rekeningrijden naarmate ze meer televisie kijken en als ze privacybewuster zijn.

Aan de respondenten is een aantal stellingen over rekeningrijden voorgelegd. De resultaten staan in tabel 4.2.

Tabel 4.2 Opinie over aspecten van rekeningrijden (n = 1006)

Stelling	Helemaal mee eens	Mee eens	Noch mee eens, noch mee oneens	Mee oneens	Helemaal mee oneens
Ik ervaar het vastleggen van rijgedrag bij rekeningrijden als het permanent in de gaten gehouden worden	23	42	18	14	3
Ik maak me zorgen over de technische beveiliging van mijn rijgegevens, zodat mensen de systemen kunnen hacken en daardoor mijn rijgedrag kunnen nagaan	18	44	25	12	2
Ik maak me er zorgen over dat mijn rijgegevens ook voor andere doelen gebruikt gaan worden dan alleen voor het opmaken van een factuur, zoals voor het doen van aanbiedingen van bijvoorbeeld te passeren wegrestaurants	17	46	20	15	2
Ik maak me er zorgen over dat mijn rijgegevens ook voor andere doelen gebruikt gaan worden dan alleen voor het opmaken van een factuur, zoals een autoverzekeringsmaatschappij die bijhoudt in welke gebieden ik precies rij en daar de verzekeringspremie op afstemt. Als een automobilist zich dan vaak in risicogebieden bevindt, wordt de premie hoger omdat dan het risico op auto-inbraak groter is	20	48	18	12	2
Ik maak me zorgen dat mijn rijgegevens lang bewaard blijven	14	38	30	15	3
Ik maak me er zorgen over dat de overheid of een privaat inningsbureau mijn rijgegevens doorgeven/-verkopen aan derden	17	42	22	16	3
Ik maak me zorgen dat ik geen inzage kan hebben in mijn eigen rijgegevens, waardoor ik geen mogelijkheid heb eventuele onjuistheden te corrigeren	22	52	17	8	1

De stellingen in de tabel betreffen zorgen die respondenten kunnen hebben ten aanzien van het rekeningrijden. Minimaal de helft van alle respondenten maakt zich zorgen over elk van de privacyaspecten uit de tabel. Bijna twee derde ervaart het vastleggen van rijgedrag als permanent in de gaten gehouden worden. Respondenten geven vaker aan dat zij dit zo ervaren naarmate zij meer privacybewust zijn. Ook rijden respondenten die dit zo ervaren meer auto (gemiddeld 4,5 dagen per week) dan respondenten die dit helemaal niet zo ervaren (gemiddeld 3,9 dagen per week).
Drie vijfde maakt zich zorgen over de technische beveiliging van de gegevens. Er zijn iets meer respondenten die zich zorgen maken over de technische beveiliging van de gegevens van rekeningrijden dan van VIR (een verschil van 8%). Men maakt zich meer zorgen over de technische beveiliging van de gegevens als men meer televisie kijkt en als men meer privacybewust is.

Verder zijn er veel respondenten die zich zorgen maken over het feit dat hun verplaatsingsgegevens kunnen worden gebruikt voor een ander doel dan waarvoor ze verzameld zijn. 63 procent is bang dat zijn gegevens ook gebruikt gaan worden voor het doen van aanbiedingen door commerciële partijen zoals wegrestaurants. Vrouwen maken zich hier meer zorgen over dan mannen. Ook maakt men zich hierover meer zorgen naarmate men meer televisie kijkt en als men meer privacybewust is.
Van de respondenten maakt 68 procent zich zorgen dat de gegevens gebruikt gaan worden door verzekeringsmaatschappijen. Respondenten met een lage SES maken zich hierover meer zorgen dan respondenten met een hoge SES. Ook maakt men zich hierover meer zorgen naarmate men meer televisie kijkt en als men meer privacybewust is. 59 procent van de respondenten maakt zich zorgen dat gegevens worden doorverkocht of –gegeven. Respondenten die zich hier zorgen over maken zijn gemiddeld ouder dan respondenten die zich hier geen zorgen over maken. Ook respondenten die meer televisie kijken en respondenten die meer privacybewust zijn maken zich hierover meer zorgen.

Ruim de helft van de respondenten maakt zich zorgen dat zijn gegevens lang bewaard blijven en driekwart dat ze geen inzage kunnen hebben in hun eigen gegevens, vooral vrouwen, ouderen en privacybewusten.

In het algemeen geldt dat respondenten zich meer zorgen maken over het beheer en het gebruik van de verplaatsingsgegevens als de beheerder een private partij is.

4.4 Overige thema's

Naast de VIR en het rekeningrijden zijn nog zeven andere technologisch-maatschappelijke ontwikkelingen aan de respondenten voorgelegd, te weten: het volgen van werknemers met GPS, het gebruik van locatie-informatie van telecomaanbieders, het burgerservicenummer, het koppelen van bestanden door overheidsinstanties, het gebruik van digitale vingerafdrukken in paspoorten, sociale netwerksites en het informeren van burgers over de verwerking van persoonsgegevens. Deze onderwerpen zijn minder uitgebreid behandeld dan de VIR en het rekeningrijden. De opvattingen van de respondenten worden in deze paragraaf besproken.

Het controleren van de verblijfplaats van werknemers via GPS
GPS-technologie maakt het voor werkgevers mogelijk om voortdurend te traceren waar werknemers zich bevinden. De meerderheid van de respondenten vindt dit acceptabel, mits de werknemers hiervan op de hoogte zijn gesteld (tabel 4.3).

Tabel 4.3 Opinie over controleren werknemers via GPS (n = 2016)

Antwoord	Percentage
Ik vind het acceptabel dat een werkgever met behulp van systemen die locatiegegevens doorgeven (zoals GPS) controleert waar een werknemer met een bedrijfsauto zich bevindt tijdens werktijd	10
Ik vind het acceptabel dat een werkgever met behulp van systemen die locatiegegevens doorgeven (zoals GPS) controleert waar een werknemer met een bedrijfsauto zich bevindt tijdens werktijd, mits de werknemer hiervan vooraf op de hoogte is gesteld	70
Ik vind het onder geen enkele voorwaarde acceptabel dat een werkgever met behulp van systemen die locatiegegevens doorgeven (zoals GPS) controleert waar een werknemer met een bedrijfsauto zich bevindt tijdens werktijd	20

Het gebruik van locatie-informatie van telecomaanbieders

De meerderheid van respondenten vindt dat locatie-informatie van telecom-aanbieders alleen gebruikt mag worden ten behoeve van opsporing door Justitie. Twee vijfde van de respondenten vindt dat deze gegevens alleen gebruikt mogen worden na toestemming van henzelf (tabel 4.4).

Tabel 4.4 Opinie over het gebruik van locatie-informatie van telecomaanbieders (n = 2016)

Antwoord	Percentage
Locatie-informatie die telecomaanbieders opslaan op basis van de signalen van mijn mobiele telefoon mag alleen gebruikt worden ten behoeve van opsporing door Justitie	59
Locatie-informatie die telecomaanbieders opslaan op basis van de signalen van mijn mobiele telefoon mag gebruikt worden door commerciële instanties die mij een sms willen sturen met reclame van de winkel waar ik me op dat moment bij in de buurt bevindt	2
Locatie-informatie die telecomaanbieders opslaan mag alleen worden gebruikt als ik daar zelf toestemming voor heb gegeven	39

Het burgerservicenummer

Bijna de helft van de respondenten vindt het burgerservicenummer een goed idee, mannen vaker dan vrouwen. Bijna een derde is er huiverig voor, omdat ze bang zijn dat onbevoegden dan gegevens kunnen inzien en een kwart denkt zelfs dat dit fraudegevoelig is (tabel 4.5).

Tabel 4.5 Opinie over het burgerservicenummer (n = 2016)

Antwoord	Percentage
Ik vind het een goed idee als alle overheidsorganen en instanties als ziekenhuizen, werkgevers en zorgverzekeraars gegevens over mij opslaan onder hetzelfde burgerservicenummer omdat dit de zorg efficiënter maakt	46
Ik ben er huiverig voor als alle overheidsorganen en instanties als ziekenhuizen, werkgevers en zorgverzekeraars gegevens over mij opslaan. Ik denk dat onbevoegden dan gegevens kunnen inzien die niet voor hen bestemd zijn	30
Ik denk dat een burgerservicenummer dat alle overheidsorganen en instanties zoals ziekenhuizen, zorgverzekeraars et cetera gebruiken fraudegevoelig is, dat wil zeggen dat onbevoegden zich toegang kunnen verlenen tot mijn gegevens en daar misbruik van kunnen maken	24

Het koppelen van bestanden door overheidsinstanties

De meerderheid van respondenten heeft er vertrouwen in dat de overheid hun gegevens niet koppelt aan andere databestanden (tabel 4.6).

Tabel 4.6 Opinie over koppelen van bestanden door overheidsinstanties (n = 2016)

Antwoord	Percentage
Als ik mijn gegevens doorgeef aan een overheidsinstantie, vertrouw ik erop dat deze instantie volgens de wetten en regels mijn gegevens behandelt. Ik ga er dan ook vanuit dat deze overheidsinstantie mijn gegevens niet aan andere bestanden (waarin ook gegevens van mij zijn opgenomen) koppelt	68
Als ik mijn gegevens doorgeef aan een overheidsinstantie, heb ik er weinig vertrouwen in dat deze instantie volgens de wetten en regels mijn gegevens behandelt. Ik ga ervan uit dat deze overheidsinstantie in sommige gevallen toch gegevens zal koppelen aan andere bestanden (waarin ook gegevens van mij zijn opgenomen), ook al is dit volgens wetten en regels niet toegestaan	23
Als ik mijn gegevens doorgeef aan een instantie, heb ik er geen vertrouwen in dat deze overheidsinstantie volgens de wetten en regels mijn gegevens behandelt. Ik ga ervan uit dat deze instantie gegevens zal koppelen aan andere bestanden (waarin ook gegevens van mij zijn opgenomen), ook al is dit volgens wetten en regels niet toegestaan	9

Een digitale vingerafdruk in paspoorten

Drie kwart van de respondenten vindt het een goed idee wanneer een digitale vingerafdruk wordt opgenomen in paspoorten, mits de beveiliging goed geregeld is. 12 procent van de respondenten maakt zich geen zorgen over deze beveiliging en een kleine minderheid, 11 procent, van de respondenten vindt deze ontwikkeling een naar idee. Respondenten die dit een naar idee vinden, zijn gemiddeld jonger dan de respondenten die dit wel een goed idee vinden (39 jaar versus 48 en 46 jaar) (tabel 4.7).

Tabel 4.7 Opinie over een digitale vingerafdruk in paspoorten (n = 2016)

Antwoord	Percentage
Ik vind het een goed idee als in paspoorten ook een digitale vingerafdruk wordt opgenomen en maak me geen zorgen over de beveiliging van deze digitale gegevens	12
Ik vind het een goed idee als in paspoorten ook een digitale vingerafdruk van mensen wordt opgeslagen, mits de beveiliging goed geregeld is	77
Ik vind het een naar idee als in paspoorten ook een digitale vingerafdruk van mensen wordt opgeslagen	11

Foto's op sociale netwerksites

Bijna de helft van de respondenten vindt het onder geen enkele voorwaarde acceptabel dat mensen foto's van hen op sociale netwerksites kopiëren en per e-mail doorsturen naar anderen. Meer vrouwen dan mannen vinden dit onacceptabel (55% versus 38%). De gemiddelde leeftijd van respondenten die dit onacceptabel vinden is hoger dan de respondenten die het acceptabel vinden en die eerst om toestemming gevraagd willen worden (48 jaar versus 43 en 44 jaar) (tabel 4.8).

Tabel 4.8 Opinie over sociale netwerksites (n = 2016)

Antwoord	Percentage
Ik vind het acceptabel dat mensen de foto's die ik op een sociale netwerksite (zoals Hyves, Facebook, Partyflock etc.) zet kopiëren en per e-mail doorsturen naar anderen	16
Ik vind het acceptabel dat mensen de foto's die ik op een sociale netwerksite (zoals Hyves, Facebook, Partyflock etc.) zet kopiëren en per e-mail doorsturen naar anderen mits men mij eerst om toestemming vraagt	37
Ik vind het onder geen enkele voorwaarde acceptabel dat mensen de foto's die ik op een sociale netwerksite (zoals Hyves, Facebook, Partyflock etc.) zet kopiëren en per e-mail doorsturen naar anderen	46

Informatie over registratie

Aan de respondenten is ten slotte gevraagd of ze prijs zouden stellen op periodieke informatie over de registratie van persoonsgegevens (tabel 4.9).

Tabel 4.9 Opinie over het informeren van burgers over de verwerking van persoonsgegevens (n = 2016)

Antwoord	Percentage
Ik vind dat ik jaarlijks van alle instanties die gegevens van mij in hun bestand hebben staan een overzicht moet ontvangen van welke gegevens bij hen in het bestand staan	67
Ik vind dat ik jaarlijks van alle instanties die gegevens van mij in hun bestand hebben staan een overzicht zou moeten ontvangen van welke gegevens bij hen in het bestand staan maar in de praktijk zou ik deze overzichten niet uitvoering bestuderen	20
Ik vind niet dat ik jaarlijks van alle instanties die gegevens van mij in hun bestand hebben staan een overzicht moet ontvangen van welke gegevens bij hen in het bestand staan. Ik ben er niet in geïnteresseerd	12

87 procent van de respondenten vindt dat ze van alle instanties die gegevens van hen verzamelen een overzicht moeten ontvangen van welke gegevens in het bestand staan. 20 procent van de respondenten zal deze gegevens echter niet bestuderen.

4.5 Conclusie

De verschillen in de casussen VIR en rekeningrijden suggereren dat de waardering van technologisch-maatschappelijke ontwikkelingen terugkomt in opvattingen over de omgang met de persoonsgegevens. Bij het rekening-rijden, dat negatiever wordt beoordeeld dan het idee van de VIR (dat overigens weinig bekend is), is de bezorgdheid over het gebruik van de gegevens groter dan bij de VIR. Mogelijk speelt ook een rol dat het bij rekeningrijden over de ‘eigen’ gegevens gaat en bij de VIR vooral over die van ‘de ander’.
In het werkgever-werknemerverkeer wordt het gebruik van verplaatsings-gegevens zeer acceptabel geacht, tenminste als de werknemer ervan op de hoogte is gesteld. In algemene zin zien we dat bij de telecomgegevens vooral het gebruik door justitie voor veiligheidsdoeleinden positief wordt beoordeeld. Het vertrouwen in een correct gebruik van gegevens door de overheid is zeker aanwezig, al is er ook bezorgdheid over de mogelijkheden van het combineren van gegevens met het Burgerservicenummer. Controle en transparantie komen steeds terug als relevante factor. Veel burgers stellen prijs op jaarlijkse overzichten van gegevens die over hen geregistreerd zijn (ook al zullen ze die niet altijd goed bekijken). Als hen vooraf toestemming word gevraagd of als ze geïnformeerd worden over het gebruik van gegevens, gaan ze vaker akkoord met de gegevensverstrekking en –verwerking.
Opvallend huiverig zijn de burgers over het doorsturen van beeldmateriaal over het internet. In de groepsgesprekken gaven burgers als reden dat dit minder goed ongedaan kan worden gemaakt.

5 INFORMATIE EN PRIVACYBEWUSTZIJN

5.1 Inleiding

In de enquête is niet alleen gevraagd hoe burgers over verschillende technologisch-maatschappelijke ontwikkelingen in relatie tot privacy denken en welk gedrag ze daarmee verbinden. Er is ook geprobeerd na te gaan in hoeverre het geven van informatie over de technologisch-maatschappelijke ontwikkelingen invloed heeft op het privacybewustzijn en het (voorgenomen) privacybewust handelen. En zo ja, welk type informatie de burgers het meest raakt.

Het privacybewustzijn is met een aantal stellingen gemeten. Vervolgens is aan de respondenten een tekst voorgelegd. Van deze tekst bestaan tien verschillende varianten. De teksten zijn willekeurig over de respondenten verdeeld. Elke respondent kreeg dus slechts één van de teksten te lezen.

Vijf teksten gaan over de verwijsindex risicojongeren (VIR). Eén daarvan is zo neutraal mogelijk opgesteld. Twee teksten geven specifieke informatie over de aard van de verwerkte gegevens. Daarvan benadrukt één er dat de gegevens in de registraties van de verschillende deelnemende organisaties blijven (‘buitenkant-uitwisseling’). De andere speelt in op de angst voor uitwisseling van gegevens tussen verschillende partijen (‘binnenkant-uitwisseling’). De volgende twee teksten gaan over transparantie en controle. De eerste laat zien dat het voor een burger relatief eenvoudig is om inzage te krijgen in de gegevens van het eigen kind, de tweede beschrijft een situatie waarin inzage moeizaam verloopt.

De vijf andere teksten gaan over een tweede casus, het rekeningrijden. Opnieuw is er een neutrale tekst met beknopte feitelijke informatie. Twee teksten variëren op de betrokkenheid van overheid dan wel bedrijfsleven bij de verwerking van gegevens, twee andere teksten gaan over het al dan niet mogelijke commerciële gebruik van gegevens.

Op deze wijze zijn in de teksten de vier belangrijkste factoren die invloed hebben op het privacybewustzijn (afgeleid in hoofdstuk 1) verwerkt: aard van de gegevens, transparantie en controle, vertrouwen in de beheerder en doel en proportionaliteit. De teksten zijn zodanig opgesteld dat ze realistische situaties en verwachtingen weerspiegelen. Er worden dus geen extreme, niet bestaande situaties beschreven.

De gebruikte teksten zijn in bijlage 3 opgenomen. Beknopt worden ze als volgt gekarakteriseerd:

1 = Verwijsindex risicojongeren (VIR): neutraal
2 = VIR: aard van de gegevens buitenkant
3 = VIR: aard van de gegevens binnenkant
4 = VIR: controle en transparantie, veel controle
5 = VIR: controle en transparantie, weinig controle
6 = Rekeningrijden: neutraal
7 = Rekeningrijden: vertrouwen beheerder publiek
8 = Rekeningrijden: vertrouwen beheerder privaat
9 = Rekeningrijden: doel en proportionaliteit, niet commercieel
10 = Rekeningrijden: doel en proportionaliteit, wel commercieel

Nadat de respondenten de teksten hadden gelezen zijn, enigszins verdekt, opnieuw (deels dezelfde) vragen over het privacybewustzijn en gedrag gesteld. Hiermee konden we zien in hoeverre het privacybewustzijn veranderde door de confrontatie met de teksten en dus door de verstrekte informatie.

5.2 Informatie en privacybewustzijn: algemeen

De algemene hypothese die we wilden toetsen was: heeft het verstrekken van informatie over bepaalde risico's bij de verwerking van persoonsgegevens invloed op het privacybewustzijn en gedrag? Dus met andere woorden: worden mensen meer of minder bewust van of meer of minder bezorgd over hun privacy als ze worden gewezen op specifieke situaties waarin persoons-gegevens een rol spelen? En in hoeverre beïnvloedt dit hun handelen? De resultaten staan in tabel 5.1.

Tabel 5.1 Verandering in privacybewustzijn en gedrag totale groep

Vragenlijst	Voor	Na	Ver-schil	Signi-ficant?
Frequentie waarin men nadenkt over de risicio's met betrekking tot het gebruik van gegevens (lagere score is vaker)	2,60	2,66	-0.06	Ja
Frequentie waarin men bezorgd is over het gebruik van persoonsgegevens (lagere score is vaker)	2,55	2,52	0.02	Ja
Frequentie waarmee men stilstaat bij het feit dat gegevens bewaard kunnen blijven in databestand (lagere score is vaker)	2,33	2,66	-0.34	Ja
Frequentie waarin men wel eens afziet van het geven van persoonsgegevens omdat dit een aantasting van de privacy is.	3,13	3,06	0.07	Ja
Mate van belang dat men hecht aan verschillende aspecten van privacybescherming (hogere score is meer belang)	62,85	63,22	-0.37	Ja

Het blijkt dat het geven van informatie over privacyaspecten van maatschappelijk-technologische ontwikkelingen (in dit geval de verwijsindex risicojongeren en het rekeningrijden) inderdaad invloed heeft op het privacybewustzijn en op privacybewust gedrag.

De invloed is als volgt. Het geven van informatie aan burgers zorgt ervoor dat zij zeggen minder vaak na te denken over de risico's met betrekking tot het gebruik van gegevens en dat zij zeggen minder vaak stil te staan bij het feit dat gegevens bewaard kunnen blijven. Zij worden echter wel bezorgder over het gebruik van persoonsgegevens, geven aan vaker af te zien van het verstrekken van persoonsgegevens vanwege een veronderstelde privacyaantasting en gaan meer belang hechten aan verschillende aspecten van privacybescherming.

5.3 De invloed van het type informatie

Het is de vraag in hoeverre informatie over de aard van de gegevens, transparantie en controle, vertrouwen in de beheerder en doel en proportionaliteit (de vier belangrijke beïnvloedende factoren uit hoofdstuk 1) een verschillende uitwerking op het privacybewustzijn heeft.
We gaan dit na door voor alle teksten (die dus elk staan voor een bepaalde factor) na te gaan of respondenten vóór en na lezing van de teksten andere antwoorden op vragen over het privacybewustzijn geven.

Deze analyse wordt vijf keer uitgevoerd, voor elk van de vijf manieren waarop we het privacybewustzijn in de enquête hebben gemeten, steeds met een iets andere invalshoek:

- aspecten die respondenten belangrijk vinden als het gaat om de bescherming van hun gegevens;
- (wel eens) afzien van het verstrekken van gegevens;
- (wel eens) nadenken over de risico's van het verstrekken van gegevens;
- bezorgdheid over het gebruik van persoonsgegevens;
- stilstaan bij het feit dat verstrekte gegevens in een databestand bewaard kunnen blijven.

Belangrijke aspecten van privacy
De eerste manier waarop het privacybewustzijn is gemeten, inventariseert de aspecten die de respondenten belangrijk vinden als het gaat om de bescherming van hun gegevens. Deze vraag is ingedeeld in zeven stellingen. Deze stellingen zijn samengevoegd in één schaal voor het belang van privacyaspecten. De resultaten staan weergegeven in tabel 5.2.

Tabel 5.2 Belang privacyaspecten, in schaal van 7 tot 70 (7 = helemaal niet belangrijk en 70 = zeer belangrijk)

Vragenlijst	Voor	Na	Ver-schil	Signi-ficant?
1 = VIR: neutraal	62,11	62,38	-0,27	Nee
2 = VIR: aard van de gegevens buitenkant	61,95	62,42	-0,47	Nee
3 = VIR: aard van de gegevens binnenkant	62,9	63,41	-0,51	Nee
4 = VIR: controle en transparantie, veel controle	63,24	63,33	-0,08	Nee
5 = VIR: controle en transparantie, weinig controle	63,86	64,3	-0,44	Ja
6 = Rekeningrijden: neutraal	62,26	62,56	-0,3	Nee
7 = Rekeningrijden: vertrouwen beheerder publiek	62,96	63,64	-0,68	Nee
8 = Rekeningrijden: vertrouwen beheerder privaat	63,61	64,21	-0,6	Nee
9 = Rekeningrijden: doel en proportionaliteit, niet commercieel	62,53	62,43	0,1	Nee
10 = Rekeningrijden: doel en proportionaliteit, wel commercieel	63,04	63,51	-0,47	Nee

Te zien is dat alleen de factor controle en transparantie (de variant weinig controle) significant van invloed is op de mate waarin respondenten belang hechten aan verschillende aspecten van privacybewustzijn. Met andere woorden: als burgers een tekst voorgelegd krijgen waarin het moeilijk blijkt om inzage te krijgen in de eigen gegevens, gaan ze (bescherming van) de privacy hoger waarderen. Dit wijst op het belang van de factor controle en transparantie.

Meer specifiek zien we de invloed terug in één van de stellingen, die gaat over het belang van weten wie toegang tot de gegevens heeft. Bij zes van de teksten vinden de respondenten dit aspect na lezing van de teksten belangrijker dan ervoor.

De andere factoren uit het privacymodel hebben geen significante invloed op de mate van belang die respondenten hechten aan hun privacybescherming.

Het niet verstrekken van de eigen gegevens

Een tweede manier waarop privacybewustzijn is benaderd, is via de vraag naar de mate waarin het voorkomt dat respondenten zeggen de eigen gegevens vanwege de aantasting van de privacy niet te verstrekken.
Na lezing van zes van de teksten geven burgers vaker aan dat het voorkomt dat zij gegevens niet verstrekken (tabel 5.3).

Tabel 5.3 Mate waarin men afziet van het geven van persoonsgegevens op een schaal van 1 tot 4 (1 = vaak en 4 = (bijna) nooit), uitgesplitst naar type informatie

Vragenlijst	Voor	Na	Ver-schil	Signi-ficant?
1 = VIR: neutraal	3,15	3,09	0,06	Nee
2 = VIR: aard van de gegevens buitenkant	3,15	3,11	0,04	Nee
3 = VIR: aard van de gegevens binnenkant	3,20	3,13	0,08	Ja
4 = VIR: controle en transparantie, veel controle	3,04	2,95	0,10	Ja
5 = VIR: controle en transparantie, weinig controle	3,08	3,16	-0,07	Nee
6 = Rekeningrijden: neutraal	3,01	2,96	0,06	Nee
7 = Rekeningrijden: vertrouwen beheerder publiek	3,15	3,04	0,11	Ja
8 = Rekeningrijden: vertrouwen beheerder privaat	3,11	3,02	0,09	Ja
9 = Rekeningrijden: doel en proportionaliteit, niet commercieel	3,17	3,07	0,11	Ja
10 = Rekeningrijden: doel en proportionaliteit, wel commercieel	3,19	3,05	0,13	Ja

Deze verschuiving in beschreven gedrag wordt veroorzaakt door de volgende factoren:

- aard van de gegevens binnenkant
- controle en transparantie veel controle
- vertrouwen beheerder publiek
- vertrouwen beheerder privaat
- doel en proportionaliteit, niet commercieel
- doel en proportionaliteit, wel commercieel

Blijkbaar zetten juist deze factoren de burgers aan het denken over het verstrekken (en eigenlijk over het mogelijk onbedoeld gebruik of misbruik) van gegevens.

Er zijn geen significante verschillen bij de neutrale vragenlijsten. Dit is naar verwachting, omdat in de neutrale vragenlijsten geen factoren zijn verwerkt die van invloed kunnen zijn op het privacybewustzijn.

Nadenken over risico's

Een derde manier om privacybewustzijn te meten, gaat over het nadenken over de risico's met betrekking tot het gebruik van persoonsgegevens. Hierop blijkt informatie over twee factoren van invloed te zijn. Dit zijn de aard van de gegevens en controle en transparantie. Respondenten geven aan minder vaak na te denken over de risico's als alleen buitenkantgegevens in te zien zijn (dus alleen dat er bij een bepaalde instantie gegevens geregistreerd zijn, zonder dat bekend wordt welke gegevens dat zijn). Ook geven ze aan minder vaak na te denken over de risico's als er weinig controle en transparantie bij de verwerking van gegevens mogelijk is.

Tabel 5.4 Nadenken over risico's gebruik persoonsgegevens, in schaal van 1 tot 4 (1 = vaak en 4 = (bijna) nooit), uitgesplitst naar type informatie

Vragenlijst	Voor	Na	Ver-schil	Signi-ficant?
1 = VIR: neutraal	2,65	2,70	-0,05	Nee
2 = VIR: aard van de gegevens buitenkant	2,60	2,75	-0,15	Ja
3 = VIR: aard van de gegevens binnenkant	2,68	2,74	-0,06	Nee
4 = VIR: controle en transparantie, veel controle	2,59	2,64	-0,06	Nee
5 = VIR: controle en transparantie, weinig controle	2,56	2,67	-0,11	Ja
6 = Rekeningrijden: neutraal	2,60	2,59	0,01	Nee
7 = Rekeningrijden: vertrouwen beheerder publiek	2,53	2,56	-0,03	Nee
8 = Rekeningrijden: vertrouwen beheerder privaat	2,64	2,62	0,03	Nee
9 = Rekeningrijden: doel en proportionaliteit, niet commercieel	2,63	2,69	-0,06	Nee
10 = Rekeningrijden: doel en proportionaliteit, wel commercieel	2,56	2,64	-0,07	Nee

Het eerstgenoemde effect is verwacht. Dat er alleen buitenkantgegevens worden uitgewisseld, kan immers geruststellen. Het tweede effect is onverwacht. Het is wellicht toe te schrijven aan de gelatenheid, die eerder in de groepsgesprekken werd geconstateerd. Als burgers worden geconfronteerd met situaties waarin controle en transparantie beperkt zijn, kan de gelatenheid met de bijbehorende desinteresse de kop opsteken. Anders gezegd: mogelijkheden voor controle en transparantie kunnen burgers wellicht activeren. Dit kan ook anders worden geïnterpreteerd: na het lezen van de tekst over een casus waarbij weinig controle en transparantie mogelijk is, gaan mensen zich realiseren dat ze eigenlijk nauwelijks nadenken over de risico's van het gebruik van persoonsgegevens.

Mate van bezorgdheid

Een vierde manier om het privacybewustzijn te meten, heeft betrekking op de bezorgdheid van burgers over het gebruik van persoonsgegevens. Er zijn maar twee situaties waarin de respondenten zich na lezing van de teksten vaker bezorgd maken over het gebruik van persoonsgegevens. De ene is bij de neutrale tekst over rekeningrijden, die klaarblijkelijk de nodige vragen oproept. De tweede situatie is die van de tekst over rekeningrijden met betrokkenheid van een private beheerder van gegevens. Dit laatste maakt burgers klaarblijkelijk wat meer bezorgd (tabel 5.5).

Tabel 5.5 Bezorgdheid over gebruik persoonsgegevens, in schaal van 1 tot 4 (1 = vaak en 4 = (bijna) nooit), uitgesplitst naar type informatie

Vragenlijst	Voor	Na	Ver-schil	Signi-ficant?
1 = VIR: neutraal	2,63	2,58	0,05	Nee
2 = VIR: aard van de gegevens buitenkant	2,55	2,57	-0,02	Nee
3 = VIR: aard van de gegevens binnenkant	2,59	2,64	-0.05	Nee
4 = VIR: controle en transparantie, veel controle	2,51	2,53	-0,03	Nee
5 = VIR: controle en transparantie, weinig controle	2,52	2,55	-0,04	Nee
6 = Rekeningrijden: neutraal	2,51	2,42	0,09	Ja
7 = Rekeningrijden: vertrouwen beheerder publiek	2,50	2,45	0,05	Nee
8 = Rekeningrijden: vertrouwen beheerder privaat	2,52	2,42	0,10	Ja
9 = Rekeningrijden: doel en proportionaliteit, niet commercieel	2,60	2,55	0,05	Nee
10 = Rekeningrijden: doel en proportionaliteit, wel commercieel	2,54	2,52	0,02	Nee

Stilstaan bij het bewaren van gegevens

De vijfde benadering van privacybewustzijn is gericht op de mate waarin burgers stilstaan bij het feit dat gegevens bewaard kunnen blijven in een databestand. Hier zien we over de hele linie een effect. Bij alle teksten, dus bij alle factoren zeggen de respondenten na lezing van de tekst dat zij minder vaak stilstaan bij het feit dat hun gegevens bewaard kunnen blijven in data-bestanden (tabel 5.6).

Tabel 5.6 Stilstaan bij feit dat gegevens bewaard kunnen blijven in databestand, in schaal van 1 tot 4 (1 = vaak en 4 = (bijna) nooit)

Vragenlijst	Voor	Na	Ver-schil	Signi-ficant?
1 = VIR: neutraal	2,31	2,72	-0,41	Ja
2 = VIR: aard van de gegevens buitenkant	2,31	2,73	-0,42	Ja
3 = VIR: aard van de gegevens binnenkant	2,38	2,75	-0,37	Ja
4 = VIR: controle en transparantie, veel controle	2,26	2,67	-0,41	Ja
5 = VIR: controle en transparantie, weinig controle	2,32	2,76	-0,44	Ja
6 = rekeningrijden: neutraal	2,37	2,60	-0,23	Ja
7 = rekeningrijden: vertrouwen beheerder publiek	2,32	2,61	-0,29	Ja
8 = rekeningrijden: vertrouwen beheerder privaat	2,34	2,58	-0,24	Ja
9 = rekeningrijden: doel en proportionaliteit, niet commercieel	2,30	2,59	-0,30	Ja
10 = rekeningrijden: doel en proportionaliteit, wel commercieel	2,37	2,63	-0,27	Ja

Over dit effect valt alleen te speculeren. Mogelijk realiseren burgers zich na lezing van de tekst hoe weinig ze normaal gesproken stilstaan bij dit soort situaties en passen ze hun mening aan aan een vernieuwd referentiekader. Ze vinden dan zelf dat ze vrij weinig bij het bewaren van gegevens stilstaan.

5.4 Conclusie

Informatie over technologisch-maatschappelijke ontwikkelingen blijkt invloed te hebben op het bewustzijn met betrekking tot privacy. Ook volkomen neutrale informatie zet mensen aan het denken. Wat betreft de vier belangrijke invloeden op het privacybewustzijn uit hoofdstuk 1 is het vooral informatie over de factor transparantie en controle die in verschillende analyses invloed blijkt te hebben op (een verschuiving in) privacyattitudes. De andere factoren komen minder vaak terug.
In het algemeen zijn de verschuivingen in attitudes met betrekking tot de privacy als gevolg van de informatieverstrekking gering. Dit is te verklaren vanuit de aard van de informatie in de gebruikte teksten. De teksten zijn niet gericht op schokeffecten door extreme situaties, maar ze geven realistische situaties en ideeën van burgers weer.

6 CONCLUSIE

Het onderzoek is van start gegaan met het doel inzicht te geven in de verschillende opvattingen die burgers hebben over het belang van de bescherming van hun persoonsgegevens, in het bijzonder in relatie tot actuele technologisch-maatschappelijke ontwikkelingen waarbij de privacy in het geding is. De hoofdvragen van het onderzoek gaan over de factoren die opvattingen van burgers over privacy beïnvloeden, de manier waarop die factoren tot uitdrukking komen in de attitude van burgers ten opzichte van de verwerking van persoonsgegevens en de mate waarin informatie over technologisch-maatschappelijke ontwikkelingen tot verandering van de attitude met betrekking tot de privacy leidt.

Er kan worden geconcludeerd dat respondenten zich over het algemeen redelijk bewust zijn van hun privacy, zonder dat ze er erg bezorgd om zijn. Ze hechten een groot belang aan de wijze waarop met hun persoonsgegevens wordt omgegaan, maar ze ondervinden in de praktijk niet vaak inbreuken op hun privacy. Ze zeggen niet heel erg privacybewust te handelen. In vergelijking met eerder onderzoek van TNS Nipo met eenzelfde vraagstelling blijken onze respondenten aanzienlijk vaker stil te staan bij de risico's van het gebruik van persoonsgegevens dan vier jaar geleden.

Bij de vorming van het privacybewustzijn spelen uiteenlopende overwegingen en waardenstelsels een rol, die per burger kunnen verschillen. Door de confrontatie met situaties waarin privacyrisico's een rol spelen, zeggen burgers meer stil te staan bij de mate waarin hun persoonsgegevens al dan niet beschermd zijn. Dit betekent niet dat zij hun gedrag aanpassen. Dit vraagt immers veel: veel gegevensverstrekkingen hebben een verplicht karakter. Voor zover er geen verplichte gegevensverstrekking is, vergt het een flinke aanpassing van de levensstijl om zich aan de gegevensverstrekking te onttrekken. Daarnaast is het voor burgers moeilijk om alle consequenties van de verstrekking van gegevens te doorgronden. Al met al is daardoor sprake van een zekere gelatenheid. Burgers zeggen dat ze hun gedrag hooguit mondjesmaat veranderen, zelfs als ze bezorgd zijn over hun privacy. Het ziet er dus naar uit dat burgers de steeds ruimere verwerking van hun persoonsgegevens niet altijd accepteren vanuit een positieve waardering, maar zeker ook omdat ze het gevoel hebben er niet omheen te kunnen. Het overkomt ze en wie zich er erg druk om maakt, 'wordt er gek van'.

Veel burgers stellen prijs op jaarlijkse overzichten van gegevens die over hen geregistreerd zijn (ook al zullen ze die niet altijd goed bekijken). Als hen vooraf toestemming word gevraagd of als ze worden geïnformeerd over het gebruik van gegevens, gaan ze vaker akkoord met de gegevensverstrekking en -verwerking. Als gegevens worden gebruikt voor opsporing, gaan mensen hier snel mee akkoord. Mensen hebben veel vertrouwen in de zorgvuldige omgang

met gegevens door de overheid.
Opvallend huiverig zijn de burgers voor het doorsturen van beeldmateriaal over het internet. In de groepsgesprekken gaven burgers als reden hiervoor dat dit minder goed ongedaan kan worden gemaakt.

Informatie over technologisch-maatschappelijke ontwikkelingen blijkt invloed te hebben op het bewustzijn met betrekking tot privacy. De aard van de informatie maakt hierbij niet zo veel uit: ook volkomen neutrale informatie zet mensen aan het denken. Wat betreft de vier factoren uit het gehanteerde privacymodel (aard van de gegevens, transparantie en controle, vertrouwen in de beheerder en doel en proportionaliteit) is het vooral de factor transparantie en controle die in verschillende analyses invloed blijkt te hebben op (een verschuiving in) privacyattitudes. De andere factoren hebben weinig tot geen merkbare invloed.
In het algemeen zijn de verschuivingen in attitudes met betrekking tot de privacy als gevolg van de informatieverstrekking gering. Dit is te verklaren vanuit de aard van de informatie in de gebruikte teksten. De teksten zijn niet gericht op schokeffecten door extreme situaties, maar ze geven realistische situaties en ideeën van burgers weer.

Voor privacybeleid vloeien hieruit enkele belangrijke ideeën voort:
- Informatie over technologisch-maatschappelijke ontwikkelingen is belangrijk en helpt bij de vorming van attitudes.
- Controle en transparantie is wezenlijk voor acceptatie van gegevensverwerking door burgers.
- Eenvoudige en toegankelijke bezwaarprocedures kunnen helpen om gelatenheid te vervangen door positieve acceptatie.
- Burgers stellen regelmatige overzichten van over hen geregistreerde persoonsgegevens zeer op prijs.

In algemene zin komt uit het onderzoek, zowel in de groepsgesprekken als in de enquête, een meegaande houding van burgers in termen van de verstrekking van persoonsgegevens naar voren. De gedachte dat deze meegaande houding voort zou komen uit de gedachte niets te verbergen te hebben, wordt door het onderzoek niet bevestigd. Met name in de groepsgesprekken bleken respondenten flink te schrikken als ze met risico's van de verwerking van persoonsgegevens worden geconfronteerd. Ze zeggen echter niet dat dit tot verandering van hun gedrag leidt. Dit vraagt teveel inspanning en de consequenties zijn te groot. Het gedrag van burgers moet dus eerder in termen van een gevoel van onvermijdelijkheid en gelatenheid dan in termen van vertrouwen in een correct gebruik van de gegevens worden beoordeeld.

BIJLAGEN

BIJLAGE 1

GESPREKSVERSLAGEN

Gesprek 1

Niet-privacybewusten

Deelnemers
Deze groep bestaat uit mensen tussen de 18 en 40. Het opleidingsniveau van de deelnemers varieert van mbo tot wo. Een aantal van hen studeert nog.

Manier van omgaan met het verstrekken van gegevens
De deelnemers geven aan niet zomaar aan iedereen persoonlijke gegevens te verstrekken. Ze kijken onder andere naar het doel (wat gaat er met de gegevens gebeuren?) en het soort organisatie dat om gegevens vraagt. Iedere respondent maakt hierbij zijn eigen afweging: sommigen kijken of het doel hen aanspreekt (bijvoorbeeld onderzoek naar ziekten of veiligheid), anderen kijken met name of ze er zelf belang bij hebben (als het doel van een onderzoek is het verbeteren van een organisatie, kunnen ze er zelf ook van profiteren als de dienstverlening verbetert).

De meeste respondenten hebben meer vertrouwen in de overheid: de overheid is transparant en controleerbaar volgens hen. Opvallend is dat de jongere die in de horeca werkt, in de zaak van zijn vader, juist minder vertrouwen heeft in de overheid dan in particuliere bedrijven. Dit verschil komen we in andere gesprekken ook tegen: ondernemers (of mensen uit een ondernemersgezin) hebben wantrouwen ten aanzien van de overheid.
Over het algemeen zijn de deelnemers het voorzichtigst met het verstrekken van hun creditcardgegevens: als hier misbruik van wordt gemaakt, kan dit grote consequenties hebben. Kennis speelt hierbij een belangrijke rol: de mensen die veel gebruikmaken van internet verstrekken hun gegevens het makkelijkst via internet, de mensen die dit niet doen zijn ook huiverig voor het verstrekken van gegevens via internet.

Casus: vastleggen verplaatsingsgegevens
De meningen zijn verdeeld over de impact van het vastleggen van verplaatsingsgegevens op de privacy. Een deel van de groep vindt het wel een inbreuk op de privacy, met name vanwege het gevaar op het hacken van de gegevens. Een deel van de groep vindt het geen probleem, omdat de vastgelegde informatie volgens hen niet zo interessant is, er kan weinig mee gebeuren. Het merendeel van de groep ervaart het vastleggen van de reisgegevens als een black box waarin de gegevens verdwijnen en er niets

mee gebeurt, een klein aantal respondenten ervaart het vastleggen van locatiegegevens als permanent in de gaten worden gehouden.
Als de groep wordt geconfronteerd met de mogelijkheid de gegevens voor andere doeleinden te gebruiken (bijvoorbeeld het opsporen van fraude of plegers van misdrijven) brengt dit de groep aan het twijfelen. Een deel van de groep zegt dit te ver vinden gaan. Niemand heeft bezwaar tegen een lange bewaartermijn van de verplaatsingsgegevens.
Het toekennen van andere gebruikersmogelijkheden aan de OV-chipkaart dan het betalen van een reis met het OV stuit op wat praktische bezwaren. Over het combineren van de reisgegevens met bijvoorbeeld koopgedrag zijn de respondenten kritisch, deels uit praktische overwegingen, deels omdat ze het een onprettig idee vinden dat bestanden aan elkaar worden gekoppeld. Men is bang dat het einde dan zoek is en er steeds meer bestanden aan elkaar zullen worden gekoppeld.

Casus: publiceren van persoonlijke gegevens op internet
De groep heeft over het algemeen weinig problemen met publiceren van gegevens op internet. Argumenten die hiervoor worden gegeven, zijn het niets te verbergen hebben en het kunnen uitoefenen van invloed op wat er wel en niet wordt gepubliceerd. Slechts één persoon geeft aan voorzichtig te zijn met persoonlijke gegevens op internet te publiceren. Dit is gebaseerd op onprettige ervaringen die ze hiermee heeft gehad. De meeste respondenten zijn zich wel bewust van mogelijk misbruik maken van de gegevens, maar nemen hiertegen zelf maatregelen: ze schermen hun Hyvespagina af of gebruiken een nickname.

Opvallend is dat slechts één het onacceptabel en vervelend vindt als iemand anders een foto publiceert waar zij ook op staat, zonder dat ze hiervoor toestemming heeft gegeven. De anderen reageren gelaten op de mogelijkheid: je kunt er toch niets aan doen en dan kun je je wel overal druk over gaan maken.
De groep staat niet erg kritisch ten opzichte van het door machines ‘lezen’ van afgeschermde informatie uit bijvoorbeeld een weblog en op basis daarvan reclame krijgen.

Het gebruiken van gegevens op netwerksites voor opsporingsdoeleinden vindt iedereen prima. Een duidelijke grens trekken zij bij de mogelijkheid dat een krant foto’s van deze netwerksites publiceert van in oorlogsgebieden omgekomen militairen. Dit mag alleen als hier nadrukkelijk toestemming voor is gegeven.
De meeste mensen hebben er vertrouwen in dat de beheerders van netwerksites niets anders doen met hun gegevens dan voor het onderhouden van de site nodig is.

Wanneer de groep het concrete geval voorgelegd wordt dat Hyves in de privacypolicy heeft opgenomen dat ze hun policy kunnen wijzigen en dat gebruikers er zelf verantwoordelijk zijn om op de hoogte te raken van deze

wijziging, veroorzaakt dit veel onrust. De deelnemers vinden dit onacceptabel. Hyves zou hen vooraf actief moeten informeren over wijzigingen, dat is de verantwoordelijkheid van de site. Ondanks de onrust zal dit niet de manier waarop zij omgaan met het publiceren van gegevens op internet veranderen.

Gesprek 2

Niet-privacybewusten

Deelnemers
De deelnemers aan dit gesprek waren tussen de 60 en 76 jaar. Hun opleidingsniveau varieert van mavo tot vwo.

Privacy zowel beschermen als onnodige drempel
Privacy wordt door deze groep enerzijds gezien als iets dat moet worden beschermd (tegen misbruik, fraude), anderzijds als iets dat te veel beschermd wordt wanneer het niet moet (bijvoorbeeld wanneer het gaat om publiceren van foto's van winkeldieven of gegevens over pedofielen). Met name een oud-politieman is hier fel in: het belang van de veiligheid zou vaker voorop moeten staan, en niet privacy.
De meeste deelnemers verstrekken hun gegevens vrij makkelijk aan instanties, vaak is het volgens hen ook verplicht. Bij het verstrekken van gegevens via internet is men voorzichtiger: men verstrekt daar bijvoorbeeld fictieve gegevens.

Casus: relatie werkgever - werknemer
Bij het voorleggen van de casus over gegevens die een werkgever kan verzamelen over een werknemer valt op dat de groep vindt dat een werknemer in de baas zijn tijd eigenlijk geen privacy heeft. Van een groot deel van de groep mag een werkgever e-mails controleren en telefoongesprekken afluisteren. Een enkeling maakt hierbij de kanttekening dat dit alleen mag als er een verdenking bestaat of als het van te voren aangekondigd is dat de werkgever dergelijke controles houdt.
Als men expliciet wordt gevraagd zich te verplaatsen in de werknemer (hoe is het om gecontroleerd te worden) dan is men wat sceptischer. Is het inderdaad wel een goed idee om een werkgever toestemming te geven van alles te controleren? Na enige discussie besluit de groep dat het toch goed is. Misbruik van gegevens kan altijd voorkomen, maar daar is niets aan te doen.

Casus: het EKD (met koppeling aan de verwijsindex risicojongeren)
Over het vastleggen van gegevens in een EKD is het grootste deel van de groep het eens dat het nadelige gevolgen kan hebben, maar dat de ontwikkeling onvermijdelijk is. Eén persoon vindt het een gevaarlijke ontwikkeling. Men is het er over eens dat een elektronisch dossier meer risico met zich meebrengt dan een papieren dossier, omdat alles met één druk op de knop

snel kan worden verspreid.
Men vindt het belangrijk dat alleen ‘harde’ medische gegevens worden vastgelegd in het EKD. Gegevens van een psycholoog horen hier niet in thuis vindt men. Het koppelen van het EKD aan de VIR vindt men geen goede ontwikkeling: de informatie die dan opgenomen wordt, is niet ‘hard’ genoeg. Tevens vindt men het van belang dat het dossier als iemand volwassen is weer vernietigd wordt, zodat mensen niet eindeloos kunnen worden beoordeeld op jeugdzonden. Naarmate het gesprek vordert, worden mensen steeds negatiever over het fenomeen EKD: iemand zegt zelfs dat ze associaties krijgt met het boek 1984 (Orwell), en dat ze er depressief van wordt. Iemand anders vindt gegevens vastleggen in een EKD ook een gevaarlijke ontwikkeling: dingen kunnen immers ongenuanceerd worden vastgelegd en een eigen leven gaan leiden. Een deel van de groep vindt deze reacties onzin: nu zijn er ook al veel medische gegevens bekend bij allerlei instanties (arts, apotheker, bezorgdienst van de apotheker) dus het maakt weinig verschil.
Wel is men het erover eens dat het systeem zo moet worden opgebouwd dat per soort informatie de toegang van de hulpverleners moet worden geregeld: niet elke hulpverlener mag alle informatie zien.
De groep hecht groot belang aan het recht ter inzage. Gegevens zouden ook moeten kunnen worden gecorrigeerd, maar dit mogen mensen niet op eigen houtje doen. Hiervoor moet een speciale commissie worden ingesteld waar je met klachten naartoe kunt.

Bewustwording en gedragsverandering
Aan het eind van het gesprek gaven mensen grappend aan helemaal paranoïde geworden te zijn door het nadenken over het koppelen van bestanden en misbruik die er van gegevens zou kunnen worden gemaakt. Toch beïnvloedt dit hun handelen niet. De ontwikkelingen zijn onvermijdbaar denken ze. De enige manier om zo min mogelijk in allerlei systemen terecht te komen, is volgend hen zo onopvallend mogelijk leven (zorgen dat je niet met politie in aanraking komt et cetera).

Gesprek 3

Niet-privacybewusten

Deelnemers
De aanwezigen bij dit gesprek varieerden in leeftijd van 44 tot 63. Het opleidingsniveau verschilt van mavo tot wo.

Manier van omgaan met het verstrekken van gegevens
De meeste deelnemers aan dit gesprek zeggen hun persoonsgegevens vrij makkelijk te verstrekken: ze staan niet zo stil bij mogelijke nadelige consequenties. Soms maken deelnemers zich achteraf wel zorgen: zo had iemand haar gegevens inclusief gironummer gegeven aan een goed doel om lid te

worden, maar duurde het heel lang voordat ze een schriftelijke bevestiging kreeg. Toen was ze bang dat ze misschien was opgelicht, maar dit bleek uiteindelijk niet zo te zijn. Eén respondent zegt voorzichtig te zijn met het verstrekken van gegevens: 25 jaar geleden is ze opgelicht en sindsdien is ze heel alert.
De meeste deelnemers zeggen het meeste vertrouwen te hebben in overheidsinstanties en verzekeringsmaatschappijen wanneer het gaat om het zorgvuldig omgaan met hun gegevens. Zij gaan professioneel te werk en zijn gewend om met vertrouwelijke gegevens om te gaan. Een zelfstandig ondernemer geeft aan juist heel weinig vertrouwen te hebben in de overheid.
Ook in dit gesprek blijkt het doel een belangrijke factor bij het verstrekken van gegevens: als mensen het een interessant doel vinden, geven ze hun gegevens makkelijker, bijvoorbeeld aan een goed doel. Een respondent brengt ter sprake dat ook goededoelenorganisaties adressenbestanden kunnen verkopen. Dit vindt iedereen verkeerd en men is hier verontwaardigd over. Er worden tips uitgewisseld over hoe je dit doorverkopen kunt voorkomen (de website infofilter.nl wordt genoemd). Mensen vinden het vooral irritant als ze worden gebeld door instanties die ze niet zelf hun gegevens hebben verstrekt, het privacyaspect is hierbij voor hen minder van belang.

Casus: vastleggen locatie-informatie via telecomtoepassingen
Bij het voorleggen van de casus locatie-informatie via telecomtoepassingen blijkt dat een deel van de groep zich er wel van bewust is dat alle mobiele telefoons traceerbaar zijn door telecomaanbieders. Ze staan hier echter in het dagelijks gebruik niet bij stil en vinden het ook geen probleem. Als je niets te verbergen hebt, maakt het niet uit, vindt men. Eén persoon vindt het zelfs wel een veilig idee.

De politie mag de locatiegegevens alleen gebruiken van de leden van de groep als er een gericht onderzoek plaatsvindt of als er een concrete aanleiding is voor het doen van preventief onderzoek (bijvoorbeeld bijhouden wie in de buurt komt van het huis van een bedreigde politicus). Wel moet er onderscheid worden gemaakt tussen het traceren van locatiegegevens en afluisteren.
Voor opsporing mogen de locatiegegevens volgens het grootste deel van de groep wel worden gebruikt. In eerste instantie zegt men dat dit niet alleen in geval van vermissing/moord mag, maar ook in geval van belasting/uitkeringsfraude. Hierover ontstaat discussie in de groep: met name een persoon die werkt als timmerman vindt het voor het bestrijden van zwart werken wel een erg zwaar middel. Hij vindt dit te ver gaan. Een aantal deelnemers zegt enorm veel moeite te hebben met uitkeringsfraude, dus van hen mogen locatiegegevens wel worden gebruikt om dit te bestrijden. Een aantal mensen vindt dat je wel voorzichtig met dit soort gegevens om moet gaan: medewerkers van de sociale dienst hebben bijvoorbeeld geen opsporingsbevoegdheid en het wordt wel belangrijk gevonden dat personen die gebruik mogen maken van deze locatiegegevens dit wel hebben. Er zouden goede regels moeten komen om verkeerd gebruik van de informatie tegen te gaan.

Eén persoon vindt het gebruiken van locatiegegevens voor preventie veel te ver gaan. Hij krijgt hier associaties bij van de situatie in de DDR.

Men vindt het onwenselijk als commerciële partijen gebruik zouden maken van locatiegegevens, bijvoorbeeld door het sturen van een sms zodra je in de buurt bij een bepaalde winkel bent. Dit wekt vooral irritatie.
Het scenario van vrienden via GPS laten weten waar je je bevindt, vinden mensen in eerste instantie belachelijk. Volgens hen zou geen enkele Nederlander dat willen. Na hierover wat doorgepraat te hebben, besluit men dat het voor kleine kinderen toch wel handig zou kunnen zijn. Eén groepslid maakt hierbij de kanttekening dat dit geen volwaardige vervanging is van toezicht die ouders zonder techniek zouden moeten houden.

Casus: Burgerservicenummer
Bij het introduceren van de casus ‘u bent een nummer’ ontstaat enige verontwaardiging in de groep als wordt uitgelegd dat het Burgerservicenummer door meer instanties gebruikt gaat worden dan het sofinummer, zonder dat men hierover is geïnformeerd. Na enige discussie hierover brengt iemand in dat hij zich herinnert dat de overheid hier wel informatie over heeft verstrekt, maar dat dit bij niemand dan echt goed is doorgedrongen.
Ondanks de verontwaardiging over de bredere toepassingen van het BSN is het merendeel niet bang voor het koppelen van allerlei bestanden aan elkaar. Ze vertrouwen erop dat er regels zijn die ervoor zorgen dat dit niet mag en dat het dus ook niet gebeurt. Bovendien denken ze dat het voor een belastinginspecteur helemaal niet interessant is om te weten welke medicijnen iemand gebruikt, dus dat dit in de praktijk ook niet zal leiden tot misbruik.
Dat veel gegevens die via het BSN worden vastgelegd voor het bedrijfsleven interessant kunnen zijn, wordt wel beaamd door de groep. Misbruik zou tegengehouden moeten kunnen worden door regels en gebruik van goede technologie (om hacken tegen te gaan).
De groep brengt ook de voordelen van een BSN onder de aandacht.

Bewustwording & gedragsverandering
Het gesprek komt vanzelf op het onderwerp ‘skimmen’. Een aantal respondenten heeft nog nooit van dit fenomeen gehoord en geeft aan wel huiverig te worden van dit soort berichten, maar hun gedrag toch niet aan te passen.
Bij de afsluiting van dit gesprek geven deelnemers aan nu toch wel een beetje paranoïde de deur uit te gaan. Ten slotte wordt de deelnemers voorgelegd of ze nu anders omgaan met het verstrekken van gegevens dan voor dit gesprek. Er wordt volmondig beaamd dat dit niet het geval is. Mensen verwachten snel weer in hun oude patroon te vervallen en weer in te dutten. Men geeft aan zich wel meer bewust te zijn van de risico’s, maar dat hun gedrag er niet door zal veranderen.

Gesprek 4

Niet-privacybewusten

Deelnemers
Deze groep bestaat uit personen van 19 tot 38 jaar. Hun opleidingsniveau varieert van mbo tot vwo en hbo. Twee personen weten veel van computer-technologie (de een studeert interactieve media en voor de ander zijn computers zijn hobby).

Manier van omgaan met het verstrekken van gegevens
De meeste respondenten gaan makkelijk om met het geven van hun persoonlijke gegevens. Als argument wordt hiervoor onder andere genoemd dat mensen vast geen slechte bedoelingen hebben met hun gegevens, men er niets mee kan en als iemand het echt wil men de gewenste gegevens toch wel kan achterhalen. Toch spelen de aard van de gegevens en het soort instelling wel een rol. Men heeft meer vertrouwen in de overheid en in grote bedrijven dan in kleine onbekende bedrijven. De redenen hiervoor zijn dat men verwacht dat zij zich aan de privacywetgeving houden en dat de overheid dingen zal doen met gegevens waar burgers zelf ook voordeel van hebben.

Casus: Biometrie
Over het opnemen van vingerafdrukken in een biometrisch paspoort heeft de groep gemengde gevoelens: het paspoort wordt dan minder makkelijk te vervalsen, maar als je paspoort wordt gestolen, liggen er wel erg gevoelige gegevens op straat. Tegelijkertijd zegt men dat er aan deze ontwikkeling niet valt te ontkomen: de ontwikkeling komt er onder druk van de VS en daar kun je als burger weinig aan doen. Ook over irisscans opnemen in een paspoort bestaan dubbele gevoelens. Er komt steeds meer controle en die gaat steeds verder. Het invoeren van deze technieken wordt door een kleine groep machthebbers bepaald en zijn zij eigenlijk wel te vertrouwen? De groep vindt het belangrijk dat er nog wel menselijke controle blijft (bijvoorbeeld bij de douane) en dat dit niet totaal wordt vervangen door een apparaat, want dit is toch vatbaarder voor misbruik. Dit geldt ook voor andere toepassingen van biometrische gegevens dan in het paspoort: bijvoorbeeld voor het betalen via een vingerafdruk of de vingerafdruk als controlemiddel in de crèche: het nadeel hiervan is dat het steeds onpersoonlijker wordt en het sociale contact steeds meer verdwijnt.
De grens ligt voor de meesten bij het opslaan van DNA in het paspoort. Het gevaar hiervan is vooral dat dit kan leiden tot discriminatie. Door de mensen die veel van techniek/computers weten, wordt het gevaar van hacken uitdrukkelijk naar voren gebracht. De gegevensopslag is niet waterdicht.
Het opslaan van DNA van misdadigers in een databank vindt men wel een goed idee.
Het gebruik van slimme camera's die gezichtsscans herkennen wordt handig gevonden voor de opsporing, maar het idee te kunnen worden gevolgd en dat

je dan echt herkenbaar bent, staat het grootste deel van de groep niet aan. Ook wordt getwijfeld aan het nut van de invoering van deze camera's: het is duur, maar werkt het ook echt? De zoektocht naar veiligheidsmaatregelen gaat steeds verder, terwijl de meeste mensen zich niet onveilig voelen. Eén persoon vindt het gebruik van deze camera's echter prima, mits mensen duidelijk op de hoogte worden gesteld van de aanwezigheid van deze camera's zodat men ervoor kan kiezen om niet in het gebied te komen waar ze hangen.

Casus datamining
De meeste deelnemers denken dat het koppelen van bestanden niet zomaar mag. Een enkeling denkt dat het ondanks regelgeving toch wel gebeurt. De mogelijkheid van het koppelen van allerlei (digitale) bestanden aan elkaar wordt gezien als zorgelijk. Als men er bij toeval achterkomt dat bestanden worden gekoppeld zonder dat men zich hiervan bewust was, is dit geen prettig idee (een concreet voorbeeld hierbij is de bank die van de IBG doorkrijgt of je nog wel studeert en dus een studentenrekening mag hebben). Men vindt dat voor het koppelen van bestanden eerst toestemming zou moeten worden gevraagd. Ook zou er een wet moeten zijn om te voorkomen dat dit achter je rug gebeurt. Met name gegevens die in handen kunnen komen van commerciële partijen die daar consumenten mee kunnen beïnvloeden (zoals in het voorbeeld van het casino) baart de groep zorgen. Er wordt dan met de consument gespeeld, vinden zij.

Bewustwording
De behandelde cases maken een klein deel van de groep bewuster. Zo is iemand ook nieuwsgierig geworden naar de wet- en regelgeving op dit gebied en vraagt hij naar de website van het CBP. Toch zorgt het bij de meeste respondenten niet voor een gedragsverandering: ze zullen als ze de deur uitlopen alles weer vergeten en dat willen ze ook. Want als je er te veel bij stilstaat wat er allemaal mis kan gaan, heb je geen leuk leven meer en kun je bijvoorbeeld ook niet meer op internet. Praktisch gezien is dat niet mogelijk, dus dan kun je er maar het beste je schouders over ophalen. Eén persoon voegt toe dat ze zich niet druk maakt om privacykwesties, omdat ze nu nog niet veel gegevens heeft waar mensen iets mee kunnen. Ze studeert bijvoorbeeld nog, dus haar financiële situatie is nog niet uitgekristalliseerd.

Gesprek 5

Privacybewusten

Deelnemers
Deze groep bestaat uit ouderen van 71 tot 78, die in opleidingsniveau verschillen van lbo tot hbo.

Manier van omgaan met het verstrekken van gegevens
De deelnemers aan deze groep zijn privacybewust. Dit uit zich in het niet makkelijk verstrekken van gegevens aan derden (bijvoorbeeld een valse naam opgeven bij ruilen in een winkel, aan de telefoon geen gironummer verstrekken om gebruik te maken van een bepaalde actie, het niet afgeven van een paspoort in een hotel in het buitenland en dan alleen toestaan dat men een kopie maakt). Deze bewustheid komt enerzijds voort uit eigen ervaringen, berichten uit de krant over fraude en oplichting, opvoeding en het idee dat er door allerlei instanties zoveel gegevens gevraagd worden dat deze gegevens samen heel veel prijs geven over iemands persoonlijke leven.

Het meeste vertrouwen heeft men in de overheid, vooral als één van de deelnemers zegt zelf bij de overheid gewerkt te hebben en bestanden koppelen echt niet mocht. De overheid zal de privacywetgeving wel naleven denkt men. Een persoon is sceptisch: je weet in de praktijk niet wat er met je gegevens gebeurt.
Of men gegevens verstrekt, hangt ook af van het doel: het moet te begrijpen zijn waarom een instantie gegevens nodig heeft. Als voorbeeld van situatie waarin dit niet te begrijpen is, is de bonuskaart van AH: waarom moeten zij ook je adresgegevens et cetera hebben? Het is mogelijk om een anonieme bonuskaart te krijgen, maar daar moet wel veel moeite voor worden gedaan. Mensen vinden het storend als ze reclame krijgen die op hun bestedings-patroon is afgestemd, dat gegevens kunnen worden doorverkocht aan andere instanties en dat het bekend is wat men allemaal koopt.

Digitale sporen achterlaten
De deelnemers zijn bezorgd over skimmen, vinden het onprettig dat je bij parkeren in sommige gebieden alleen kunt betalen door te chippen (want je chipknip is niet anoniem) en dat je door telecomaanbieders kan worden getraceerd. Dit geeft mensen het gevoel dat ze altijd kunnen worden gevolgd en dit beschouwt men als aantasting van de privacy.
Met het publiceren van gegevens op internet heeft de groep minder moeite: men vindt het zelfs wel handig dat ze terug te vinden zijn door oude vrienden. Alleen bij sollicitaties kan informatie op een sociale netwerksite vervelend zijn, maar je hebt ook zelf de controle over wat je erop zet en je kunt het afschermen. Het publiceren van foto’s op internet is lastiger: als iemand dat doet en jij wilt dat niet, dan moet deze eraf worden gehaald door die persoon. Anderen mogen alleen gegevens over iemand publiceren op internet als er toestemming is gevraagd (bijvoorbeeld het opnemen van naam en functie door een werkgever).

EKD
In eerste instantie ziet de groep vooral de voordelen van het EKD. Kinderen kunnen dan beter worden geholpen. De stemming slaat om in verontwaar-diging als de optie van het opnemen van niet-medische gegevens in het dossier wordt genoemd. Dan zou het dossier in elk geval vernietigd moeten worden als iemand achttien wordt. Men vindt het een beter idee als het EKD

niet automatisch voor iedereen wordt gemaakt, maar alleen voor kinderen waarmee problemen zijn. Men is het niet eens over wie inzage mag hebben in het dossier: sommige zaken moeten ook voor ouders verborgen kunnen blijven (bijvoorbeeld als een kind de pil heeft gevraagd bij de dokter). Daarom is het niet vanzelfsprekend dat de ouders altijd inzage mogen hebben in het dossier.

Biometrie
Bij het vastleggen van biometrische gegevens maken de respondenten zich vooral druk over de fraudegevoeligheid. Ook irriteert het dat de overheid veel gegevens wil vastleggen zonder dat de burger daar beter van wordt. Bij sommige respondenten bestaat de angst dat de biometrische gegevens worden gekoppeld aan gegevens uit andere bestanden.
Het vastleggen van gelaatsscans vindt een deelnemer erg fout, hij krijgt er associaties bij van het boek ‘The boys from Brazil’: je wordt je hele leven gevolgd. De anderen vinden de toepassing van gelaatsscans in voetbalstadions wel goed.

Locatieinformatie
Dat mobiele telefoons traceerbaar zijn voor telecomaanbieders is voor een deel van de groep nieuw. Men vindt het geen prettig idee. Maar aan de andere kant: wat kan er nu mis gaan met deze informatie? Er wordt door enkele deelnemers gewezen op de voordelen: je bent traceerbaar bij bijvoorbeeld een natuurramp.
Er moet onderscheid worden gemaakt in het feit dat aantasting van de privacy vervelend kan zijn (bijvoorbeeld als je reclame ontvangt van de McDonalds via sms) en misbruik dat kan worden gemaakt van gegevens wat desastreus kan zijn (bijvoorbeeld als een kind een bepaald stempel krijgt in het EKD die niet terecht is).

Gesprek 6

Privacybewusten

Deelnemers
Deze groep bestaat uit deelnemers van 20 tot 37 jaar, variërend in opleidingsniveau van mbo tot wo.

Manier van omgaan met het verstrekken van gegevens
De deelnemers uit deze groep denken goed na voor ze hun gegevens verstrekken. Ze letten er bijvoorbeeld op dat er niet meer gegevens worden gevraagd dan nodig is voor het doel, ze geven telefonisch nooit persoonlijke gegevens en zijn zich ervan bewust dat toekomstige werkgevers het internet af kunnen struinen naar informatie over hen. Het kennisniveau over privacykwesties is hoog: de groep noemt uit zichzelf voorbeelden van het

BSN, de bewaartermijn van de gegevens van de OV-chipknip en men wisselt gegevens uit over een website waar je kunt aangeven dat je niet gebeld wilt worden door bedrijven.
Over het algemeen heeft men meer vertrouwen in de overheid dan in het bedrijfsleven dat zij goed met gegevens omgaan. De kanttekening wordt geplaatst dat men geen inzicht heeft in wat de overheid met hun gegevens doet, dat ze waarschijnlijk allerlei bestanden aan elkaar koppelen en dat ze alles van je weten.

Verschillende deelnemers hebben ook slechte ervaringen met privacykwesties: zo is bij een deelnemer zijn wachtwoord voor zijn Hotmail-account gehackt, waardoor men ook zijn eBay-account kon hacken. Hij liep daardoor kans dat met zijn creditcard allerlei goederen zouden worden gekocht. Ook bij een andere deelnemer is haar computer gehackt. Een deelneemster werd meerdere malen per dag gebeld door energieleveranciers; uiteindelijk heeft ze een ander telefoonnummer genomen.
Andere voorbeelden waarbij de privacy in het geding is, zijn: een familielid die bij de politie werkt en op een speciale cursus had geleerd hoe ze afgeschermde Hyvespagina's kon bekijken (en dus op een verjaardag wist te vertellen dat de respondent in kwestie een nieuwe vriend had, wat alleen op haar Hyves stond) en een andere respondent had een vriendin wiens ex kunstmatige intelligentie studeerde en via het achterhalen van haar wachtwoorden haar ook stalkte. De meeste respondenten gaan dan ook op een bewuste manier met Hyves om (pagina's afschermen, geen 'wilde foto's' op Hyves zetten).
De groep reageert heftig op het voorbeeld van de privacypolicy van Hyves: men vindt dat Hyves gebruikers actief moet informeren over wijzigingen in deze policy. Toch geeft een aantal deelnemers toe dat mensen zelf ook te makkelijk zijn in het geven van toestemming op bepaalde sites. Sommige mensen zouden tegen zichzelf in bescherming moeten worden genomen en hier zou goede wetgeving voor moeten zijn.

Elektronisch kinddossier
Een klein aantal personen uit de groep reageert hier heftig op. Een deelneemster zegt zelfs dat ze het liefst dan nu nog een kind zou krijgen, voordat het EKD ingevoerd wordt. Nadelen die worden genoemd, zijn: Big brother is watching you, veel te veel macht voor hulpverleners, het zou niet voor elk kind moeten worden ingevoerd, er kan ook onjuiste informatie op komen te staan. Voordelen zien een aantal groepsleden ook wel.

Biometrie
In eerste instantie wordt het opnemen van biometrische gegevens in een paspoort als handig beschouwd door de groep, mits de biometrische gegevens niet aan andere bestanden kunnen worden gekoppeld. Omdat er kans bestaat dat dit wel gebeurt en er kans is op fraude, vindt men het toch maar een eng idee. Het scenario dat iedereen straks een chip in de huid krijgt wordt geschetst (en als onwenselijk beschouwd).

Slimme camera's die reageren op gelaatsscans worden als positief voor de veiligheid beschouwd, maar er zijn ook bezwaren tegen deze camera's. Het idee overal te worden gevolgd is geen prettig idee, je hebt er zelf geen controle over en de grenzen schuiven steeds meer op; alle informatie over jou ligt dan open en bloot op tafel vindt men.

Traceerbaarheid via telecomtoepassingen
Een groot deel van de groep schrikt ervan dat dit mogelijk is. Een iemand wordt zelfs boos: ze heeft er niet om gevraagd en zeker geen toestemming voor gegeven. Ze vindt het heel vervelend.
Men vreest dat dit in de toekomst ook voor commerciële doeleinden zal worden gebruikt. Dit wordt als belachelijk bestempeld. Een deel van de groep reageert echter laconiek: als je je van dit soort dingen bewust wordt dan heb je een probleem en word je er gek van. Je moet je er dus niet druk over te maken.
In traceerbaarheid via GPS ziet een persoon wel voordelen (bijvoorbeeld om te gebruiken bij festivals als je mensen kwijt bent). Anderen vinden dit een onnodige toepassing, zelfs voor kinderen. Kinderen hebben al een mobieltje tegenwoordig dus kun je ze gewoon bellen en bovendien moeten ouders zelf goed op hun kinderen letten. De sociale controle gaat tegenwoordig veel te ver, dit is een schending van de privacy.

Datamining
De meeste groepsleden zijn zich er wel van bewust dat dit kan gebeuren. Een deel ziet het als onwenselijk, een ander deel haalt de schouders er over op. Je wordt gek als je er bij stil gaat staan. Het wordt als vervelend ervaren dat je er zelf geen controle over hebt.

Bewustwording
Ook bij deze groep gaat een deel van de mensen enigszins paranoïde naar huis. Twee mensen vragen de URL van het CBP omdat ze benieuwd zijn naar de bestaande wet- en regelgeving. Het grootste deel van de groep zegt dat hun gedrag niet zal veranderen: ze zijn al redelijk voorzichtig en hebben niets te verbergen. Het gaat hen meer om de morele kant: op zich mag men wel alles van ze weten, maar ze willen er wel zelf de controle over houden.

BIJLAGE 2

ACHTERGRONDKENMERKEN VAN RESPONDENTEN

Tabel B2-1 Overzicht deelnemers aan de groepsgesprekken

Geslacht	Leef-tijd	Lft. kinderen	Hh*	Beroep/branche	Opleiding
Groep 1 (niet-privacybewusten)					
M	19	n.v.t.	?	Horeca	Havo
M	27	n.v.t.	1	Bankier	Vwo
V	18	n.v.t.	5	Studente	Wo
M	39	5, 5	4	Werkzoekend	Mbo
V	23	n.v.t.	1	Studente, bijbaan maatschappelijk werkster	Hbo
V	23	n.v.t.	?	In between jobs	Hbo
V	20	n.v.t.	1	Studente, horecamedewerkster	Wo
Groep 2 (niet-privacybewusten)					
M	64	n.v.t.	2	Gepensioneerd, vroeger politieagent	Mbo
M	76	n.v.t.	1	Gepensioneerd, speelt af en toe nog als acteur	Mavo
V	52	n.v.t.	2	Huisvrouw, vroeger verpleegster	Mbo
V	62	n.v.t.	2	Acupuncturist	Havo
V	66	n.v.t.	1	Gepensioneerd	Vwo
Groep 3 (niet-privacybewusten)					
M	51	14, 16	1	Bouw	Havo
M	44	8, 8	4	Dansleraar	Mbo
M	50-60	geen	1	WAO	Vwo
M	54	20	4	VUT (was militair)	Mavo
V	47	9, 12, 15	4	Datamanager ziekenhuis	Wo
V	49	13, 20, 23	4	Doktersassistente	Mavo
V	53	n.v.t.	1	Kunstenares, schilderdocente	Hbo
V	63	?	?	Verkoopster	Mbo
Groep 4 (niet-privacybewusten)					
M	22	n.v.t.	2	Student	Vwo
M	33	n.v.t.	1	Kunstenaar, horeca	Vwo
M	37	1	3	Administratief medewerker verzekeringen	Mbo
V	25	n.v.t.	2	Uitzendkracht	Hbo
V	21	1	2	Toneelschool	Vwo
M	19	n.v.t.	1	Student	Hbo

Vervolg tabel B2-1

Groep 5 (privacybewusten)					
Geslacht	**Leef-tijd**	**Lft. kinderen**	**Hh***	**Beroep/branche**	**Opleiding**
M	59	30	3	Kok	Mbo
M	53	n.v.t.	1	Consultant	Hbo
M	62	n.v.t.	2	Afdelingsmanager gemeente	Hbo
M	78	52, 42	2	Gepensioneerd, vroeger loodgieter	Lbo
V	57	n.v.t.	1	Groepsleidster kinderopvang/weefster	Havo
M	62	n.v.t.	2	Gebouwenbeheerder	Lbo
V	69	36,29	2	Vut, was docente	Hbo
V	51	n.v.t.	1	Werkzoekend	Mbo
Groep 6 (privacybewusten)					
M	18-30	n.v.t.	1	Webontwikkelaar	Hbo
M	18-30	n.v.t.	1	Student	Wo
V	37	n.v.t.	1	Docente	Hbo
M	24	?	4	Student	Mbo
V	37	6	2	Loopbaanadviseur	Wo
V	20	1	2	Studente	Mbo

* Aantal personen in huishouden waartoe deelnemer behoort.

Respons webenquête

Tabel B2-2 Demografische kenmerken respondenten (n = 2016)

Kenmerk	% (frequentie)
Vrouw	50,4 (1017)
Man	49,6 (999)
Leeftijd, gemiddeld	45,5
Leeftijdscategorieën	
18-24 jaar	9,0 (182)
25-44 jaar	38,1 (768)
45-64 jaar	43,8 (883)
65+	9,1 (183)
Opleiding	
Geen onderwijs/basisonderwijs	0,6 (13)
Lbo, vmbo, vbo, leerlingwezen	9,0 (181)
Mavo, vmbo, mulo, ulo	11,7 (236)
Mbo	23,3 (469)
Havo, vwo, wo-propedeuse	9,5 (192)
Hbo, wo-bachelor/kandidaats	32,7 (659)
Wo-doctoraal/master, KMA	12,8 (258)
Etnische achtergrond	
Allochtoon eerste generatie*	3,0 (61)
Allochtoon tweede generatie**	5,6 (113)
Autochtoon	90,7 (1829)
Sociaaleconomische status ***	
Laag	2,2 (45)
Laag-midden	17,6 (354)
Midden	21,1 (425)
Midden-hoog	38,2 (770)
Hoog	20,9 (422)
Tenminste één thuiswonend kind < 18 jaar	30,0 (544)

* Een persoon die in het buitenland is geboren.

** Een persoon die in Nederland is geboren, van wie één van de ouders in het buitenland is geboren.

*** Sociaaleconomische status is berekend op basis van opleiding en beroep

Tabel B2-3 Overige kenmerken respondenten (n = 2016)

Kenmerk	% (frequentie)
Geïnteresseerd in politiek	
Sterk geïnteresseerd	10,4 (210)
Tamelijk sterk geïnteresseerd	40,9 (41,3)
Niet zo geïnteresseerd	47,9 (965)
Aantal keer per week thuis surfen op internet	
Minder dan 1x per maand/nooit	1,6 (32)
1x per week – 1x per maand	9,9 (199)
2 – 5x per week	28,9 (582)
Iedere dag	59,3 (1196)
Aantal uren dat men televisie kijkt	
0 – 1 uur per dag	9,8 (197)
1 – 3 uur per dag	54,2 (1093)
3 – 5 uur per dag	28,4 (572)
5 of meer uur per dag	7,6 (154)

BIJLAGE 3

INFORMATIE VIR EN REKENINGRIJDEN IN VRAGENLIJST

Van de vragenlijst bestonden tien varianten. Deze verschillen uitsluitend op één onderdeel: de informatie die over twee technologisch-maatschappelijke ontwikkelingen is verstrekt. Elke respondentgroep kreeg één van de onderstaande teksten.

1. VIR: neutraal

Verschillende hulpverleners kunnen zonder dat ze het van elkaar weten te maken hebben met dezelfde jongere. Het ministerie van Jeugd en Gezin is van plan om een systeem in te voeren waarbij hulpverleners een melding krijgen als een jongere ook in aanraking is geweest met een andere hulpverlener. Dit systeem heet de verwijsindex risicojongeren. Dit werkt digitaal: als een onderwijzer een risicomelding doet en een politieagent doet hetzelfde over dezelfde jongere, dan ontvangen de onderwijzer en de politieagent allebei een e-mail dat er over deze jongere nog een melding is. De onderwijzer en de politieagent kunnen dan contact met elkaar opnemen.
De verwijsindex risicojongeren is bedoeld voor jongeren tot 23 jaar.

2. VIR: aard van de gegevens buitenkant

Verschillende hulpverleners kunnen zonder dat ze het van elkaar weten te maken hebben met dezelfde jongere. Het ministerie van Jeugd en Gezin is van plan om een systeem in te voeren waarbij hulpverleners een melding krijgen als een jongere ook in aanraking is geweest met een andere hulpverlener. Dit systeem heet de verwijsindex risicojongeren. Dit werkt digitaal: als een onderwijzer een risicomelding doet en een politieagent doet hetzelfde over dezelfde jongere, dan ontvangen de onderwijzer en de politieagent allebei een e-mail dat er over deze jongere nog een melding is. De onderwijzer en de politieagent kunnen dan contact met elkaar opnemen.
De verwijsindex risicojongeren is bedoeld voor jongeren tot 23 jaar.

Via de verwijsindex risicojongeren wordt geregistreerd dat een hulpverlener contact heeft met een jongere. Wat er precies aan de hand is of welke behandeling een jongere krijgt staat er niet in. Deze informatie houden hulpverleners in hun eigen dossier. Wel kan de politieagent die een e-mail heeft ontvangen dat een jongere ook met Bureau Jeugdzorg in aanraking is geweest, de jeugdzorghulpverlener bellen om na te gaan of het goed zou zijn om samen een plan te bedenken om de jongere te helpen.

3. VIR: aard van de gegevens binnenkant

Verschillende hulpverleners kunnen zonder dat ze het van elkaar weten te maken hebben met dezelfde jongere. Het ministerie van Jeugd en Gezin is van plan om een systeem in te voeren waarbij hulpverleners een melding krijgen als een jongere ook in aanraking is geweest met een andere hulpverlener. Dit systeem heet de verwijsindex risicojongeren. Dit werkt digitaal: als een onderwijzer een risicomelding doet en een politieagent doet hetzelfde over dezelfde jongere, dan ontvangen de onderwijzer en de politieagent allebei een e-mail dat er over deze jongere nog een melding is. De onderwijzer en de politieagent kunnen dan contact met elkaar opnemen.
De verwijsindex risicojongeren is bedoeld voor jongeren tot 23 jaar.

Op dit moment is het idee dat hulpverleners een signaal krijgen dat een andere hulpverlener ook contact heeft met de jongere. Wat er precies met de jongere aan de hand is of welke behandeling een jongere krijgt, houdt iedere hulpverlener in zijn eigen dossier. Wel kunnen hulpverleners contact met elkaar opnemen om uit te zoeken of er een gezamenlijke aanpak nodig is.

Hans heeft een zoon van veertien jaar. Hans en zijn vrouw zijn onlangs gescheiden. Hans en zijn zoon hebben het hier moeilijk mee. Hans is veel gaan drinken en zijn zoon doet het minder goed op school. Hij haalt veel onvoldoendes en is onlangs betrokken geweest bij een vechtpartij. Hans heeft psychische hulp gezocht voor zijn zoon.
Hans maakt zich zorgen over de verwijsindex risicojongeren. Hij is bang dat na een signaal de school contact op kan nemen met de jeugdhulpverlening en dan wellicht te horen krijgt welke problemen in het gezin spelen. Hans wil niet dat de school weet dat zijn zoon hulp krijgt vanwege de scheiding en zijn alcoholprobleem. Hij vindt dat dit de school niets aangaat en wil zelf de keuze hebben om dit wel of niet op school te vertellen.

4. VIR: controle en transparantie, veel controle

Verschillende hulpverleners kunnen zonder dat ze het van elkaar weten te maken hebben met dezelfde jongere. Het ministerie van Jeugd en Gezin is van plan om een systeem in te voeren waarbij hulpverleners een melding krijgen als een jongere ook in aanraking is geweest met een andere hulpverlener. Dit systeem heet de verwijsindex risicojongeren. Dit werkt digitaal: als een onderwijzer een risicomelding doet en een politieagent doet hetzelfde over dezelfde jongere, dan ontvangen de onderwijzer en de politieagent allebei een e-mail dat er over deze jongere nog een melding is. De onderwijzer en de politieagent kunnen dan contact met elkaar opnemen.
De verwijsindex risicojongeren is bedoeld voor jongeren tot 23 jaar.

Hans heeft een half jaar geleden het bericht gekregen dat over zijn zoon Jacco een melding is opgenomen van Bureau Jeugdzorg in de verwijsindex risicojongeren. Het contact met de hulpverlener van Bureau Jeugdzorg

verloopt stroef. Hans heeft geen idee wat een risicomelding inhoudt. Hans belt de informatielijn over de Verwijsindex omdat hij inzage wil in wat er over zijn zoon is vastgelegd. Bij de informatielijn verwijzen ze hem door naar de ambtenaar van zijn gemeente die als taak heeft toezicht te houden op de Verwijsindex. Via deze ambtenaar mag Hans de gegevens die opgenomen zijn over Jacco inzien.

5. VIR: controle en transparantie, weinig controle

Verschillende hulpverleners kunnen zonder dat ze het van elkaar weten te maken hebben met dezelfde jongere. Het ministerie van Jeugd en Gezin is van plan om een systeem in te voeren waarbij hulpverleners een melding krijgen als een jongere ook in aanraking is geweest met een andere hulpverlener. Dit systeem heet de verwijsindex risicojongeren. Dit werkt digitaal: als een onderwijzer een risicomelding doet en een huisarts doet hetzelfde over dezelfde jongere, dan ontvangen de onderwijzer en de huisarts allebei een e-mail dat er over deze jongere nog een melding is. De onderwijzer en de huisarts kunnen dan contact met elkaar opnemen.
De verwijsindex risicojongeren is bedoeld voor jongeren tot 23 jaar.

Hans heeft een half jaar geleden het bericht gekregen dat over zijn zoon Jacco een melding is opgenomen van bureau Jeugdzorg in de verwijsindex risicojongeren. Het contact met de hulpverlener van bureau Jeugdzorg verloopt stroef. Hans heeft geen idee wat een risicomelding inhoudt. Hans belt de informatielijn over de Verwijsindex omdat hij inzage wil in wat er over zijn zoon is vastgelegd. Bij de informatielijn verwijzen ze Hans door naar de ambtenaar van zijn gemeente die als taak heeft toezicht te houden op de Verwijsindex. Via deze ambtenaar mag Hans de gegevens die opgenomen zijn over Jacco inzien. Hans leest dan alleen dat er een melding over Jacco is van de hulpverlener van Bureau Jeugdzorg, maar niet waarom deze melding is gedaan. Daarvoor moet hij contact opnemen met de hulpverlener van Bureau Jeugdzorg met wie het contact stroef verloopt.

6. Rekeningrijden: neutraal

Het kabinet heeft besloten om rekeningrijden in te gaan voeren. Dit betekent dat u gaat betalen voor elke kilometer die u heeft gereden. Om te kunnen bepalen hoeveel kilometer u heeft afgelegd, moet u straks een kastje in uw auto plaatsen. Met behulp van satelliettechnologie communiceert dit kastje naar een centrale computer, zodat een factuur kan worden opgemaakt. Dit kastje registreert plaats, tijd en aantal gereden kilometers. Verschillende locaties en tijdstippen kennen namelijk verschillende tarieven.

7. Rekeningrijden: vertrouwen beheerder publiek

Het kabinet heeft besloten om rekeningrijden in te gaan voeren. Dit betekent dat u gaat betalen voor elke kilometer die u heeft gereden. Om te kunnen bepalen hoeveel kilometer u heeft afgelegd, moet u straks een kastje in uw auto plaatsen. Met behulp van satelliettechnologie communiceert dit kastje naar een centrale computer, zodat een factuur kan worden opgemaakt. Dit kastje registreert plaats, tijd en aantal gereden kilometers. Verschillende locaties en tijdstippen kennen namelijk verschillende tarieven.

Er komt een door het Rijk ingesteld bureau dat de betalingen zal regelen. De gegevens over uw rijgedrag gaan naar een centrale computer die wordt beheerd door de overheid. Deze zet de gegevens om in een tarief dat u moet betalen en stuurt dit door naar het inningsbureau dat de betalingen afhandelt. Het inningsbureau krijgt geen informatie over waar en wanneer u heeft gereden, maar kan op basis van de tariefinformatie wel een factuur opstellen.

Gerwin is 34 jaar, woont in Amsterdam en is vertegenwoordiger bij een bedrijf dat kantoorartikelen verkoopt. Gerwin rijdt voor zijn werk vele kilometers. Ook privé legt hij grote afstanden af, omdat zijn nieuwe vriendin in Breda woont. Hij maakt zich zorgen over het rekeningrijden, omdat hij bang is dat de overheid de gegevens over zijn rijgedrag mogelijk voor andere doeleinden gaat gebruiken. Hij is met name bang dat hij als verdachte kan worden aangemerkt van een delict wat heeft plaatsgevonden in de buurt van waar hij gereden heeft, te meer omdat hij op zoveel plekken in het land komt.

8. Rekeningrijden: vertrouwen beheerder privaat

Het kabinet heeft besloten om rekeningrijden in te gaan voeren. Dit betekent dat u gaat betalen voor elke kilometer die u heeft gereden. Om te kunnen bepalen hoeveel kilometer u heeft afgelegd, moet u straks een kastje in uw auto plaatsen. Met behulp van satelliettechnologie communiceert dit kastje naar een centrale computer, zodat een factuur kan worden opgemaakt. Dit kastje registreert plaats, tijd en aantal gereden kilometers. Verschillende locaties en tijdstippen kennen namelijk verschillende tarieven.

Een van de mogelijkheden voor de afhandeling van de betaling is dat u gebruikmaakt van een particuliere dienstverlener. De gegevens van uw kastje komen binnen op een centrale computer van de particuliere dienstverlener. Dit bureau zendt alleen het tarief dat u moet betalen door aan het inningsbureau van het Rijk. Op deze wijze kan de overheid geen inzage hebben in wanneer en waar u heeft gereden, maar alleen hoeveel geld u verschuldigd bent. U kunt ervoor kiezen om gebruik te maken van extra diensten van de particuliere dienstverlener, zoals het ontvangen van verkeers- en route-informatie op maat.

Gerwin is 34 jaar, woont in Amsterdam en is vertegenwoordiger bij een bedrijf dat kantoorartikelen verkoopt. Gerwin rijdt voor zijn werk vele kilometers. Ook privé legt hij grote afstanden af, omdat zijn nieuwe vriendin in Breda woont. Gerwin kiest er voor om het rekeningrijden te laten uitvoeren door een particuliere dienstverlener, maar hij maakt zich wel zorgen over zijn privacy. Zijn verplaatsingsgegevens komen in handen van een commerciële partij die op termijn misschien mogelijkheden ziet om geld te verdienen met de verplaatsingsgegevens waarbij de gegevens zullen worden gebruikt op een manier die hij niet prettig vindt. Hij wil bijvoorbeeld geen reclame ontvangen over zuinige auto's omdat bekend is dat hij veel kilometers rijdt.

9. Rekeningrijden: doel en proportionaliteit, niet-commercieel

Het kabinet heeft besloten om rekeningrijden in te gaan voeren. Dit betekent dat u gaat betalen voor elke kilometer die u heeft gereden. Om te kunnen bepalen hoeveel kilometer u heeft afgelegd, moet u straks een kastje in uw auto plaatsen. Met behulp van satelliettechnologie communiceert dit kastje naar een centrale computer, zodat een factuur kan worden opgemaakt. Dit kastje registreert plaats, tijd en aantal gereden kilometers. Verschillende locaties en tijdstippen kennen namelijk verschillende tarieven.

Het doel van het rekeningrijden is de files te bekorten, de betrouwbaarheid te verhogen en de reistijd van deur tot deur verminderen. Daarnaast wordt een verbetering van de kwaliteit van de leefomgeving nagestreefd door het beheersen en terugdringen van CO2-uitstoot, verbetering van de luchtkwaliteit en efficiënter energiegebruik.

10. Rekeningrijden: doel en proportionaliteit, wel commercieel

Het kabinet heeft besloten om rekeningrijden in te gaan voeren. Dit betekent dat u gaat betalen voor elke kilometer die u heeft gereden. Om te kunnen bepalen hoeveel kilometer u heeft afgelegd, moet u straks een kastje in uw auto plaatsen. Met behulp van satelliettechnologie communiceert dit kastje naar een centrale computer, zodat een factuur kan worden opgemaakt. Dit kastje registreert plaats, tijd en aantal gereden kilometers. Verschillende locaties en tijdstippen kennen namelijk verschillende tarieven.

Het doel van het rekeningrijden is het verbeteren van de bereikbaarheid in Nederland en het bevorderen van de kwaliteit van de leefomgeving. Het is echter niet ondenkbaar dat de verplaatsingsgegevens ook voor andere doelen zullen worden gebruikt, bijvoorbeeld door de Belastingdienst (voor het controleren van uw reiskosten), voor opsporingsdoeleinden (achteraf in kaart brengen wie zich rond een plaats delict bevond) of voor marketingdoeleinden (het informeren van automobilisten door wegrestaurant X met aanbiedingen).

Annet is 45 jaar, woont in Groningen en werkt als zelfstandig consultant. Haar familie en vrienden wonen allemaal in de buurt en haar klanten zijn bijna

allemaal in de provincie gevestigd. Een enkele keer moet ze voor een overleg met een opdrachtgever naar Zwolle. Annet rijdt niet heel veel kilometers per jaar, maar toch maakt ze zich zorgen over het rekeningrijden. Ze is bang dat haar rijgegevens niet alleen voor het rekeningrijden zullen worden gebruikt, maar ook voor andere doeleinden. Ze is met name bang dat ze als verdachte kan worden aangemerkt van een delict wat heeft plaatsgevonden in de buurt van waar ze heeft gereden.