Uw gegevens op straat? Over privacy bij kilometerbeprijzing

Custers, B.H.M.; Kuiper, A.; Szabo, Z.; Tops, R.

Published in:
Tijdschrift voor Vervoer en Recht

Publication date:
2008

Dr. ir. B.H.M. Custers*, drs. A. Kuiper**, drs. Z. Szabo*** en ing. R. Tops****

Uw gegevens op straat? Over privacy bij kilometerbeprijzing

1. Samenvatting

Privacy is in toenemende mate een belangrijk punt bij de invoering van een kilometerbeprijzing. De verschillende systemen voor het monitoren van voertuigen brengen uiteenlopende consequenties met zich mee voor de privacy. In dit document zullen de privacyaspecten worden beschreven van de verschillende scenario's die de Nederlandse overheid nu hanteert. Er wordt vaak gedacht dat privacy een hindernis is voor kilometerbeprijzing, maar door handige keuzes en slimme oplossingen hoeft dat niet het geval te zijn. Aan de hand van concrete technische, juridische, en organisatorische (deel)oplossingen wordt in deze bijdrage aangegeven hoe de kilometerbeprijzing privacyvriendelijk kan worden gerealiseerd.

2. Inleiding

Anders Betalen voor Mobiliteit (ABvM), dat is de nieuwste term die de overheid gebruikt voor kilometerbeprijzing. Andere termen, zoals rekeningrijden en kilometerheffing, zijn in de afgelopen jaren besmet geraakt omdat ze werden gebruikt bij plannen die niet uitvoerbaar leken of bleken. De vraag of ABvM wel uitvoerbaar is, is niet zonder meer te beantwoorden, omdat vooralsnog onduidelijk is hoe deze vorm van kilometerbeprijzing eruit komt te zien. De inrichting van ABvM is nog volop voorwerp van onderzoek en discussie. Terecht, omdat invoering van kilometerbeprijzing een groot project is, dat zorgvuldig voorbereid dient te worden. In de voorstudies zijn verschillende scenario's voorgesteld, maar het is onduidelijk welke voor- en nadelen al deze scenario's bieden op verschillende punten, waaronder kosten, beveiliging, handhaving en privacy.

In deze bijdrage wordt ingegaan op de privacy, een van de punten die in de publieke discussie steeds meer naar voren komt.[1] Hieronder worden de scenario's die op dit moment bij de overheid worden overwogen op hun privacyvriendelijkheid beoordeeld.[2] Omdat privacy een belang is dat moet worden afgewogen tegen andere belangen, zullen ook hier andere belangen worden meegenomen in de afwegingen.[3] Er wordt nogal eens gesuggereerd dat het beschermen van privacy een hindernis is voor zaken als effectiviteit, handhaving, fraudebestrijding en klantvriendelijkheid. Toch kan privacy heel goed samengaan met al deze zaken, als er voor slimme oplossingen wordt gekozen. Hieronder worden technische, juridische en organisatorische oplossingen voorgesteld die kunnen helpen bij privacyvriendelijke kilometerbeprijzing. Deze bijdrage vormt een vervolg op een eerder artikel waarin de mogelijke privacyproblemen van gegevens over voertuiglocaties werden beschreven.[4]

3. Scenario's

Op dit moment worden binnen het Ministerie van Verkeer en Waterstaat vier scenario's overwogen voor de invoering van ABvM.[5] Elk van de vier voorgestelde scenario's voor kilometerbeprijzing is gebaseerd op een plaatsbepaling met een kastje in het voertuig. Een dergelijk kastje heet een OBE, On-Board Equipment. Met behulp van dit inbouwkastje wordt het verschuldigde bedrag bepaald. Daarmee verschilt de Nederlandse aanpak aanzienlijk van enige andere vorm van kilometerbeprijzing in de rest van de wereld. In andere landen wordt vooral gebruik gemaakt van tolpoorten of *Automatic Number Plate Recognition* (ANPR), een systeem van poorten met camera's boven de snelweg dat kentekens registreert. OBE's worden in andere landen vooralsnog alleen kleinschalig in proefopstellingen gebruikt voor privaat verkeer.

In elk scenario wordt een aantal stappen doorlopen om het aantal afgelegde kilometers te beprijzen. De scenario's verschillen naar de autonomie van het kastje in het voertuig: hoeveel gebeurt er in de OBE en staan de gegevens daar opgeslagen of gebeurt dit in een centrale administratie en

* **Dr. ir. B.H.M. Custers is postdoc onderzoeker aan de Universiteit Tilburg bij het Tilburg Institute for Law, Technology and Society (TILT) en senior consultant bij Capgemini Consulting Services.**

** **Drs. A. Kuiper CMC MBT is managing consultant bij Capgemini Technology Services, Public Sector en is een van de auteurs van het rapport 'Het Kan'.**

*** **Drs. Z. Szabo is een van de opstellers van het rapport 'Trends in Mobiliteit 2008; De Randstad Voorbij'. Hij is politicoloog en sinds 2007 werkzaam als vice-president bij Capgemini Nederland B.V.**

**** **Ing. R. Tops is als business developer mobiliteit en projectleider betrokken bij het beproeven van mobiele technologie in de provincie Utrecht.**

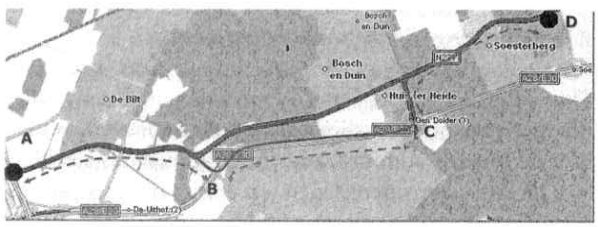
1. Zie bijvoorbeeld W. Schenk, 'Politie registreert alle auto's bij Zwolle', *Volkskrant*, 7 mei 2008.
2. *Het Kan! Techniek, organisatie, handhaving en kosten van varianten van Anders Betalen voor Mobiliteit*, 29 maart 2005 van het Ministerie van Verkeer en Waterstaat (Rapportnummer VW/DGP/ABvM/TOH20050329). Dit rapport is door LogicaCMG, Capgemini en Get ID opgesteld als achtergrondstudie voor de Commissie Nouwen (ABvM).
3. Voor aanknopingspunten voor dergelijke afwegingen, zie ook: A. Vedder, et al. *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw*, Rathenau Instituut/TILT 2007.
4. B.H.M. Custers, 'Privacy-aspecten bij de kilometerheffing', *Openbaar Bestuur*, 2008 (wordt gepubliceerd).
5. Kilometre pricing in the Netherlands (KMP), Information update, presentatie Ministerie van Verkeer en Waterstaat, 15 april 2008.

worden de gegevens daar opgeslagen en verwerkt? (zie Tabel 1)

Tabel 1. Vier scenario's (thin, slim, smart en thick) met daarin verschillende verdelingen van functies voor de OBE versus de centrale administratie.

	Thin	Slim	Smart	Thick
Verplaatsings-gegevens verzamelen	OBE	OBE	OBE	OBE
Verplaatsings-gegevens verrijken (route)	Centraal	OBE	OBE	OBE
Verplaatsings-gegevens aggregeren naar wegcategorie	Centraal	Centraal	OBE	OBE
Kilometerprijs berekenen	Centraal	Centraal	Centraal	OBE
Inning	Centraal	Centraal	Centraal	Centraal

Figuur 1: Een route met twee prijzen: lokaal en op de snelweg



Ritprijsbepaling: de afstand wordt bepaald per categorie weg (en eventueel tijd). Van belang is te weten hoeveel afstand op een hoofdweg (B-C) is gereden – dat heeft een andere prijs dan een provinciale weg (A-B plus C-D). De bepaling gaat in een aantal stappen: locatiebepaling (waypoints GNSS), bepalen route en dan categorie weg, afleiden afstand per categorie, totaliseren per categorie. De vier varianten verschillen in de manier en plaats van verwerking: in het voertuig of centraal.

De ritinformatie wordt bepaald aan de hand van satellietinformatie. Met behulp van een GNSS-signaal[6] worden zogenaamde *waypoints*, referentiepunten, bepaald. Deze worden op een routekaart met wegen vergeleken en de route wordt vastgesteld (zie Figuur 1). De digitale kaart heeft vervolgens alle informatie over beprijzing en de prijzen voor de verschillende wegsegmenten: in het voorbeeld het stuk op de A28 en separaat de afstanden op de provinciale wegen. De informatie over het gebruik van een wegsegment wordt opgeteld per prijscategorie. Daarna worden de categorieën opgeteld. Het prijsplan verschilt per voertuig. Bij de bepaling van het wegsegment wordt de prijstabel van de weg toegepast, en worden de prijzen van speciale objecten berekend (zoals privaat gefinancierde tunnels of wegen). Maandelijks wordt afgerekend, bijvoorbeeld: 250 km snelweg à 5 cent/km plus 1000 km provinciale weg à 2 cent/km plus 4 keer Coentunnel à € 1 komt op een totaal van € 36,50. Een centrale administratie verzorgt facturering, inning en afhandeling. De gedetailleerde gegevens zijn beschikbaar om de opbrengsten te verdelen naar partijen, zoals de Rijksoverheid, Provincies, Waterschappen of private wegbeheerders en exploitanten.

De scenario's verschillen in de mate waarin deze stappen in de OBE of in een *back-office* worden uitgevoerd Een back-office is een centrale administratie, bijvoorbeeld bij de overheid, waar de gegevens worden verwerkt en de facturering afgehandeld.[7] Naarmate in de OBE meer stappen worden uitgevoerd, dient deze met meer functies te worden uitgerust. De scenario's worden aangeduid aan de hand van de hoeveelheid functies die de OBE moet hebben. De *Thin OBE* verzamelt alleen maar gegevens, de *Slim OBE* verfijnt ook gegevens, de *Smart OBE* aggregeert de ritgegevens naar kostensoort en de *Thick OBE* berekent zelfs de kilometerprijs. Op dit moment gaat de voorkeur van de overheid uit naar de Smart OBE.

3.1. Overzicht van de vier scenario's

Scenario 1: Thin OBE
De Thin (dunne) OBE bevat alleen een functie om de plaatsbepaling te doen en een elektronische identiteit. De waypoints, referentiepunten voor de plaatsbepaling, worden bij voorkeur versleuteld (encrypted) samen met de versleutelde identiteit van het voertuig (het elektronische kenteken) overgedragen naar de centrale administratie. Centraal wordt voor alle voertuigen een zelfde kaart gebruikt.[8] Alleen voor de beprijzing wordt de informatie uitgepakt en verwerkt. De wegsegmenten worden met de prijstabel in de centrale administratie beprijsd en vervolgens per categorie geaggregeerd. De prijstabellen staan centraal, en zijn gemakkelijk voor alle berijders tegelijk te wijzigen.

Scenario 2: Slim OBE
De Slim OBE verzamelt series van positiebepalingen en aggregeert die tot een route aan de hand van een digitale routekaart. In plaats van 25 afzonderlijke waypoints op de route van Den Haag naar Amsterdam, concludeert de OBE dat de A4 is afgelegd tussen een begin- en eindpunt. Daarmee wordt de hoeveelheid informatie die moet worden verstuurd aanzienlijk verkleind. De 'route-informatie' wordt samen met de versleutelde identiteit van het voertuig (het elektronische kenteken) overgedragen naar de centrale administratie; dit gebeurt na afloop van een rit of periodiek (maandelijks). De wegsegmenten worden in de centrale administratie geaggregeerd en beprijsd. Omdat de Slim OBE een commercieel voorstel is, is de precieze technische werking onbekend.

Scenario 3: Smart OBE
In deze variant verwijst de naam naar het 'knap' omgaan met de informatie. Het concept is gebaseerd op een plaatsbepaling in de OBE met ook verwerking van een serie van positiebepalingen tot een route. De Smart OBE heeft een digitale routekaart aan boord. Het weggebruik per wegcategorie wordt opgeteld en deze 'gebruiksinformatie' wordt samen met de identiteit van het voertuig (het elektronische kente-

6. GNSS staat voor Global Navigation Satellite System en is een algemene term voor satelliet navigatiesystemen: het omvat zowel GPS als Galileo.
7. Overheidsorganisaties zoals de Belastingdienst en het Centraal Justitieel Incassobureau (CJIB) worden vaker genoemd als mogelijke uitvoeringsorganisaties. Daarnaast wordt overwogen om de afhandeling uit te besteden aan een of meer private partijen.
8. De centrale kaart kan niettemin doelgroepafhankelijk zijn, bijvoorbeeld voor vrachtwagens. Zware vrachtwagens betalen binnen het verdrag van het Eurovignet alleen op de hoofdwegen.

ken) overgedragen naar de centrale administratie. De beprijzing en inning vinden plaats in een centrale administratie.

Scenario 4: Thick OBE
Deze OBE heeft alle functies van de gehele keten in zich, beginnend met een plaatsbepaling, daarna verwerking van een serie van positiebepalingen tot een route en ten slotte een prijsberekening. Daartoe heeft de Thick OBE een digitale routekaart aan boord. De kaart bevat prijsgegevens en van elke rit wordt de prijs bepaald door wegsegmenten per prijscategorie op te tellen.
Het belangrijkste verschil met de Smart OBE is dat de Thick OBE ook een betaalfunctie heeft. Er is een 'digitale portemonnee' aan boord, met een saldo waarvan wordt afgeschreven. Regelmatig zorgt de berijder dat het saldo op de kaart wordt opgewaardeerd of dat het betreffende geld wordt afgerekend.

4. Privacyafwegingen

Privacy is een lastig te omschrijven begrip en de meningen zijn verdeeld over wat privacy precies inhoudt. Het moderne begrip privacy is voor het eerst gebruikt aan het eind van de 19e eeuw door Warren en Brandeis die privacy omschreven als het 'recht om met rust gelaten te worden'.[9] In 1967 beschreef Westin privacy als het recht om zelf te beslissen wanneer, hoe en in hoeverre informatie over jezelf wordt gecommuniceerd naar anderen.[10] Deze omschrijving, meer gericht op informatie, wordt nog steeds veel gebruikt en ligt aan de basis van de huidige privacywetgeving.
De huidige privacywetgeving in Nederland is vastgelegd in de Wet Bescherming Persoonsgegevens (WBP)[11] en is gebaseerd op een Europese richtlijn. Daarmee is de wetgeving op het gebied van privacy in alle EU-landen vergelijkbaar. De belangrijkste voorwaarden voor de rechtmatigheid van de verwerking van persoonsgegevens zijn:
- *Transparantie* – Voor de betrokkenen moet duidelijk zijn wie welke informatie van de ritten verwerkt en waarvoor;
- *Rechtmatige grondslag* – Voor de verwerking van de persoonsgegevens (bijvoorbeeld factuurgegevens) moet een rechtmatige grondslag bestaan. Dat kan door toestemming van de betrokkene, maar dat kan ook in de opzet van de nieuwe wet geregeld worden;
- *Doelbinding* – Voor elke vorm van gegevensverwerking moet het doel duidelijk worden omschreven. Bij het verzamelen van verplaatsingsgegevens moet terughoudendheid worden betracht en de gegevens mogen niet na verloop van tijd voor andere doeleinden worden gebruikt, zoals marketing, reisadviezen of opsporing;
- *Kwaliteit van de gegevens* – De gegevens moeten voldoende nauwkeurig zijn en zonodig worden bijgewerkt. Onnauwkeurige of onvolledige gegevens moeten worden gewist of gecorrigeerd;
- *Rechten van betrokkenen* – Voor betrokkenen moet inzage in en correctie van de (basis-)gegevens eenvoudig mogelijk zijn;
- *Beveiliging* – Er moet worden gezorgd voor een toereikende beveiliging, zodat verlies, verminking of onbevoegde toegang tot de ritgegevens wordt voorkomen.

Omdat privacy een belang is dat moet worden afgewogen tegen andere belangen, zullen hier ook andere belangen worden meegenomen, waartegen het privacybelang kan worden afgezet. De belangrijkste zijn:
- *Doeltreffendheid* – Het systeem moet leiden tot een eerlijke(re) beprijzing;
- *Kosten* – Het systeem mag niet te duur worden;
- *Handhaving* – Het systeem moet voldoende bestand zijn tegen fraude;
- *Klantvriendelijkheid* – De gebruiker moet het systeem zo min mogelijk als hinderlijk ervaren.

Deze afwegingen worden meegenomen als randvoorwaarden. Dat wil zeggen dat ze hieronder niet expliciet worden besproken, tenzij er niet aan voldaan is. Voor het overige wordt aangenomen dat alle scenario's voldoen aan deze criteria. Uitgangspunt voor de bespreking is doelmatigheid: de detailgegevens willen we niet beschikbaar hebben voor derden. Maar er moet wel toegang toe zijn: zelf (eigen inzicht, klantvriendelijkheid), voor controle op het betalen (door een controlerende instantie) of voor het weerleggen van een boete. Dus ongeacht waar de gegevens zijn, moeten ze toegankelijk zijn voor dergelijke doeleinden.

4.1. Afweging van de privacy per scenario

Thin OBE
Alle gegevens worden direct na het verzamelen verstuurd naar de centrale administratie. De OBE dient als een black box; de gebruiker kan niet zien wat er met zijn gegevens gebeurt. Een mogelijke oplossing voor transparantie en inzage- en rectificatiemogelijkheden is dat de gebruiker via een website kan inloggen (met DIGID) en zijn ritgegevens kan raadplegen. Door de gebruiker zelf (laagdrempelig) te laten kijken naar de gegevens, gaat de kwaliteit ervan ook omhoog. In dit scenario worden heel veel gegevens van de OBE naar de centrale administratie verstuurd. De gedetailleerdheid van de verzameling waarnemingen die verstuurd wordt, zorgt voor zowel een privacy- als een beveiligingsprobleem. Het privacyprobleem ontstaat doordat veel gegevens bij elkaar een completer persoonsbeeld bieden en dus meer inzicht geven in het leven van de betrokkene. Een oplossing hiervoor is om de gegevens te versleutelen en medewerkers van de back-office alleen toegang te geven tot de gegevens die ze voor hun taak nodig hebben (zogenoemde *role-based access*). Het beveiligingsprobleem ontstaat doordat veel informatie bij elkaar waarde creëert en daarmee aantrekkelijker wordt om te kraken, bijvoorbeeld voor identiteitsfraude. Hier helpen cryptografie en compartimentering (opdeling zodat een succesvolle hacker slechts een betekenisloos deel van de gegevens in handen krijgt).

Slim OBE
In de meeste opzichten verschilt de Slim OBE nauwelijks van de Thin OBE. Een belangrijk verschil is echter dat er veel minder gegevens naar de back office worden gestuurd, waardoor de privacy- en beveiligingsproblemen beperkter zijn. Wel zal voor de handhaving de registratie van waypoints in de OBE opgeslagen moeten worden om controlevergelij-

9. S.D. Warren & L.D. Brandeis, 'The right to privacy; the implicit made explicit', *Harvard Law Review* 1890, p. 193-220.
10. A. Westin, *Privacy and Freedom*. London: Bodley Head 1967.
11. Zie: <http://wetten.overheid.nl/>.

kingen met de centrale registratie mogelijk te maken. Bij de Thin OBE is zulke controle ook gewenst, maar minder noodzakelijk omdat interpretatiefouten bij de centrale administratie plaatsvinden (en aldaar gecontroleerd kunnen worden) en niet in de Slim OBE.

Smart OBE
Vanuit privacy- en beveiligingsperspectief is dit scenario om een aantal redenen erg gunstig. Ten eerste zijn de locatiegegevens niet centraal beschikbaar.[12] Dit voorkomt het opbouwen van een integraal beeld van iemands gangen en ook het gebruik voor oneigenlijke doeleinden, zoals grasduinen in de gegevens naar patronen is niet mogelijk. Uiteraard kan dit ook meteen een nadeel zijn, omdat allerlei beleidsmatige doelstellingen niet of nauwelijks gerealiseerd kunnen worden, zoals bijvoorbeeld filevoorspellingen, informatie voor wegbeheerders, quotering van milieuvervuiling op bepaalde locaties of grootschalig strafrechtelijk onderzoek.
De klantvriendelijkheid neemt mogelijk ook af, omdat bij fouten de centrale administratie niet meteen kan helpen. Alle gegevens zitten immers in de OBE, dus zal een bezoek met de auto naar een servicepunt nodig zijn.
In dit scenario wordt ook de invoering van een *Multi-Service Provider* (MSP) model overwogen. In dit model bieden private partijen de MSP's naast back-office functionaliteit ook OBE's aan. Wanneer elke MSP zijn eigen technologie gebruikt voor de digitale kaart en het algoritme voor de routebepaling (meestal een eigen, gepatenteerd concept), kunnen onderlinge afwijkingen ontstaan.

Thick OBE
Net als bij de Smart OBE, zijn ook bij de Thick OBE de locatiegegevens niet centraal beschikbaar, met dezelfde consequenties voor privacy, beveiliging, doeltreffendheid en handhaving. Bij de Thick OBE is er een betaalfunctie aan boord en dat geeft de gebruiker mogelijk een gevoel van privacy, omdat hij zelf het afrekenen in de gaten kan houden. Dit komt het dichtst in de buurt van Westin's bovengenoemde begrip van privacy. Uiteraard veronderstelt dit wel dat de OBE zodanig is opgezet dat de gebruiker ermee kan communiceren.
Tegelijkertijd is er echter een probleem met de handhaving, aangezien deze OBE extra fraudegevoelig is. Tot nu toe hebben aanbieders van mobiele telefonie nooit bereken- en betaalfuncties op de mobiele telefoons gezet, omdat de beveiliging lastig te regelen is.

5. Oplossingen

Uit het bovenstaande blijkt wel dat alle scenario's in eerste instantie op een of meerdere punten tekortschieten op het gebied van privacy en beveiliging. Toch zijn er verschillende (deel)oplossingen die kunnen zorgen dat aan bovengenoemde voorwaarden op het gebied van privacy en beveiliging (beter) wordt voldaan. Deze oplossingen zijn in alle beschreven scenario's in meer of mindere mate toepasbaar. Onderstaande lijst is niet compleet, maar slechts bedoeld om een beeld te geven van de mogelijke instrumenten voor privacyvriendelijke oplossingen.[13]

5.1. Technische oplossingen

5.1.1. Anonimiseren
Een van de belangrijkste *privacy enhancing technologies* is het anonimiseren van gegevens. Gegevens van meneer X zijn een stuk minder privacygevoelig dan gegevens van koningin Beatrix. Veel doelen van ABvM, waaronder filebestrijding, kunnen ook met anonieme gegevens bereikt worden. Beprijzing is nooit anoniem, omdat aan een individu gefactureerd moet worden. Toch kan ook bij beprijzing in delen van het proces anoniem gewerkt worden. Voor anonieme gegevens is de Wet Bescherming Persoonsgegevens niet van toepassing. Dat schept veel vrijheden voor het verzamelen en verwerken van gegevens. Voor de betrokkenen is er dan wel minder rechtsbescherming.

5.1.2. Versleutelen
Door middel van *cryptografie* kunnen de verzamelde gegevens versleuteld worden. Zo kan worden voorkomen dat gegevens snel weglekken. Iemand die zich fysiek toegang verschaft tot de bestanden krijgt alleen abracadabra te zien.

5.1.3. Secret sharing
Dit is een versleutelvariant waarbij de sleutel als het ware in meerdere stukjes onder verschillende mensen wordt verdeeld.[14] Vervolgens kunnen alleen twee mensen samen de sleutel gebruiken om bij de gegevens te komen.[15] Wanneer een sleutel verdeeld wordt tussen de gegevensbeheerder en het data subject dan biedt dit extra mogelijkheden voor transparantie, inzage en correctie. Een sleutel verdelen tussen meerdere databeheerders biedt extra beveiliging tegen medewerkers die hun buurman of een bekende Nederlander willen opzoeken in de bestanden.

5.1.4. Role-based access
Bij deze oplossing krijgt een gebruiker niet toegang tot alle gegevens in de databank, maar alleen tot de gegevens die hij uit hoofde van zijn rol of taak nodig heeft. Dit principe staat bekend als *need-to-know*. Een medewerker die moet factureren krijgt wel het aantal gereden kilometers te zien, maar niet de locaties van het voertuig. Een data subject krijgt wel inzage in zijn eigen gegevens (op basis van DigiD), maar niet in die van zijn buurman.

5.2. Juridische oplossingen

5.2.1. Grondslagen vastleggen
Op dit moment is de wet- en regelgeving op bepaalde punten onduidelijk over wanneer gegevens mogen worden verzameld en verwerkt. Daarin kan op meerdere manieren verheldering

12. De gegevens in de OBE moeten wel extern in te zien zijn voor handhaving, maar inzage per OBE is een decentrale oplossing.
13. Voor een uitgebreidere bespreking, zie ook B.H.M. Custers, *The Power of Knowledge*, Tilburg: Wolf Legal Publisher 2004. Zie ook J.J. Borking & C.D. Raab, 'Laws, PETs and other Technologies for Privacy Protection', *Journal of Information, Law & Technology* (JILT) 2001, Vol. 1, No. 1.
14. Om precies te zijn gaat het niet om stukjes van de sleutel zelf, maar om stukjes informatie die tot de sleutel leiden. Als de PIN-code 8706 is, krijgt niet de ene gebruiker 87 en de andere 06. De ene gebruiker krijgt 2145 en de ander 6561, waardoor de ene helft niets zegt over de totale sleutel.
15. Dit kan ook bewerkt worden naar toegang met bijvoorbeeld minimaal 'drie van de vier personen' of toegang met 'twee agenten in combinatie met hetzij een officier van justitie hetzij betrokkene'.

worden gebracht. Als eenmaal duidelijk is welke gegevens nodig zijn, moet daarvoor een goede grondslag gezocht worden. Toestemming van de betrokkene is een mogelijke grondslag, maar niet aannemelijk, tenzij de betrokkene er financieel op vooruitgaat (bijvoorbeeld wanneer kilometerbeprijzing goedkoper is dan de af te schaffen wegenbelasting en BPM). De nieuwe Wet op ABvM moet dus aangeven welke gegevens worden verzameld en verwerkt, door wie en hoe dat gebeurt en welke bewaartermijnen er van kracht zijn.[16] Daarnaast is er ook de mogelijkheid om tussen verschillende betrokken organisaties *convenanten* op te stellen waarin wordt geëxpliciteerd welke gegevens waarvoor worden uitgewisseld.[17]

5.2.2. Privacybescherming uitbreiden

Op sommige momenten is onduidelijk of de gegevens die verwerkt worden persoonsgegevens zijn en daarmee onder de WBP vallen. Anonieme gegevens bijvoorbeeld vallen niet onder de WBP en kentekengegevens alleen dan wanneer ze herleidbaar zijn tot een persoon. Daarmee ontbreekt een stuk rechtsbescherming voor de betrokkenen, want alleen als de WBP van toepassing is, is er recht op bijvoorbeeld inzage. Door de rechtsbescherming duidelijk aan te geven en op enkele punten uit te breiden, groeit zeer waarschijnlijk het draagvlak onder burgers. Door een versleuteld elektronisch kenteken te hanteren aan de bron en in de afhandeling wordt het probleem technisch opgelost.

5.2.3. Strenge handhaving bij fraude

De heffing van de variabele kilometerbeprijzing bedraagt ongeveer € 6 miljard per jaar, afgezien van aanloopeffecten. Met een dergelijk omvang is het denkbeeldig dat er een 'fraude-industrie' ontstaat. Handhaven gaat in eerste instantie met waarnemingen (cameraobservatie, kentekenherleiding) die ter plekke of achteraf vergeleken worden met de ritgegevens. De privacy staat op gespannen voet met deze vergelijking: er moet immers in een administratie worden gekeken. De belastingdienst zal dergelijke registratieapparatuur hetzelfde beschouwen als een boekhouding. Bij verdenking van fraude volgt opsporing. In geval van opsporing (dus geen controle!) zal de houder inzage moeten verschaffen. De vraag is natuurlijk wie er dan in de gegevens mag kijken en wanneer. Hiervoor zijn voor de Belastingdienst geen speciale bevoegdheden noodzakelijk. Die bevoegdheden zijn nu ook op een abstractieniveau beschreven in de Algemene Wet Rijksbelastingen. Voor andere opsporingsdiensten zal dat anders liggen. Het meest voor de hand liggend lijkt te zijn dat de officier van justitie of de rechter-commissaris daarvoor toestemming moet geven. Die kan dan een zorgvuldige belangenafweging maken tussen enerzijds het privacybelang en anderzijds het opsporingsbelang. Hiervoor moet een heldere en eenduidige procedure worden opgesteld.

5.2.4. Strenge handhaving van privacy

Ook op de privacy moet worden toegezien. Het College Bescherming Persoonsgegevens (CBP) is op dit moment verantwoordelijk voor het toezicht op de privacy. Omdat er nog geen sprake was van een goed functionerend toezicht, heeft het CBP in het jaarplan van 2008 een nieuwe koers ingezet ter versterking van de handhaving.[18] Naar verwachting zal het CBP dan net als toezichthouders in andere sectoren strenger gaan handhaven. Het gebruik van sancties als boetes en bestuursdwang staan het CBP daarbij ter beschikking.

5.2.5. Inzage en rectificatie aanbieden voor gebruikers

Voor de betrokkenen moet duidelijk zijn wie welke informatie verwerkt en waarvoor. Deze transparantie kan verschaft worden door middel van mogelijkheden tot inzage. Te denken valt aan een website waar een gebruiker met een persoonlijke code kan inloggen of aan een helpdesk waarnaar een gebruiker kan bellen. Als de gegevens onjuist of onvolledig zijn, bieden rectificatiemogelijkheden ook een manier om de datakwaliteit te verbeteren. Uiteraard moet daarbij wel gecontroleerd worden of bij het wijzigen niet wordt gefraudeerd. Mogelijkheden tot inzage en rectificatie zijn niet alleen verplicht, ze kunnen ook bijdragen aan het draagvlak onder burgers. Anderzijds wordt met het opnemen van de Wet Mulder in de Wet ABvM juist getracht lange, kostbare en zinloze administratieve bezwaarprocedures tegen te gaan.

5.3. Organisatorische oplossingen

5.3.1. Voorlichting

De meeste van de bovengenoemde technische en juridische oplossingen werken alleen als burgers zich voldoende bewust zijn van de mogelijke privacyproblemen die zich kunnen voordoen.[19] Voorlichting heeft zowel betrekking op de data subjecten als op de gegevensbeheerders. Voor beide groepen moet duidelijk zijn wat de spelregels zijn en wat de rechten en plichten zijn als die spelregels worden overtreden. Een burger kan echter alleen zijn beklag doen als hij weet wie zijn gegevens verwerkt (transparantie) en vervolgens wie hij daarop kan aanspreken (verantwoordelijkheid). Dat vereist nogal wat kennis en kunde van de burger en daarom is het redelijk dat de gegevensverwerker in heldere taal uitlegt hoe hij te werk gaat en wat de mogelijkheden zijn voor bezwaar en beroep.

5.3.2. Inzage en rectificatie

Hierboven zijn inzage en rectificatie al genoemd als een juridische oplossing. Hier zit echter ook een organisatorische component aan vast. Er moeten immers procedures komen hoe er omgegaan wordt met inzage en rectificatie. Daarover wordt in de huidige plannen voor ABvM nauwelijks gesproken. Daarnaast moet er bij rectificatie een toetsing komen over welke gegevens uiteindelijk de juiste zijn. Tenslotte moet ook gewerkt worden naar een algemene cultuur van openheid waarin niet voetstoots wordt aangenomen dat de informatiesystemen altijd gelijk hebben. Medewerkers dienen er reke-

16. De grondslag wordt daarmee afgedekt via artikel 8d (wettelijke verplichting) en/of artikel 8f (noodzakelijkheid voor publieke taakvervulling) van de WBP.
17. Voor de variant met een nieuwe wet die alle grondslagen voor gegevensverwerkingen en -verstrekkingen in de hele keten afdekt, kan geleerd worden van de Wet Suwi uit de keten werk & inkomen. Voor de variant met convenanten kan geleerd worden van de helpdesk privacy van het Ministerie van Justitie, die helpt bij het opstellen van convenanten voor onder meer de jeugdzorg en de aanpak van veelplegers.
18. Zie ook B.H.M. Custers, 'Bedrijven die privacy burgers schenden pakken we te slap aan', *Trouw*, 3 maart 2007, p. 14.
19. Voor een overzicht van de privacyproblemen bij ABvM, zie noot 4.

ning mee te houden dat wat ze op een computerscherm lezen niet altijd betrouwbare informatie is.[20]

6. Conclusies

De vraag is nu welk scenario de voorkeur heeft in het licht van bovenstaande beschouwing. Gesteld kan worden dat in beginsel alle scenario's mogelijk zijn, mits een selectie uit de bovengenoemde (deel)oplossingen wordt gebruikt. Vanwege hun decentrale aanpak hebben de Smart en de Thick OBE vanuit privacyoogpunt de voorkeur boven de Thin en de Slim OBE. De Slim OBE heeft weer de voorkeur boven de Thin OBE omdat er uiteindelijk minder gegevens verzameld en verwerkt worden. Maar als de in dit artikel genoemde oplossingen voor privacywaarborgen worden geïmplementeerd, kan de balans verschuiven naar een voordeel voor de twee 'dunne' varianten, waar een centrale administratie meer gemak geeft. Ook al zijn de verplaatsingsgegevens in een centrale administratie beschikbaar voor deelbewerkingen, een integraal beeld over een persoon is dan niet te verkrijgen.

Welk van de genoemde scenario's ook wordt gekozen, het is sterk aan te bevelen om de bovengenoemde (deel)oplossingen te verwerken in het gekozen scenario. Hoewel niet alle maatregelen strikt noodzakelijk zijn, bieden ze de beste garantie dat de voorwaarden op het gebied van privacy optimaal worden ingevuld. Op die manier kan worden voorkomen dat uw gegevens op straat komen te liggen.

20. Zie ook A. Vedder & R. Wachbroit, 'Reliability of Information on the internet: some distinctions', *Ethics and Information Technology* 2003, 5, p. 211-215.