WRR

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID

# *Privacy en vormen van 'intelligente' mobiliteit*

## DE IMPACT VAN ICT-APPLICATIES VOOR DE WEG EN HET SPOOR

*Henk Griffioen*

AMSTERDAM UNIVERSITY PRESS

*Privacy en vormen van 'intelligente' mobiliteit*

De serie Webpublicaties omvat studies die in het kader van de werkzaamheden van de WRR tot stand zijn gekomen. De verantwoordelijkheid voor de inhoud en de ingenomen standpunten berust bij de auteurs. Een overzicht van alle webpublicaties is te vinden op de website van de WRR (www.wrr.nl).

Wetenschappelijke Raad voor het Regeringsbeleid
De WRR is gevestigd:
Lange Vijverberg 4-5
Postbus 20004
2500 EA 's-Gravenhage
Telefoon 070-356 46 00
Telefax 070-356 46 85
E-mail info@wrr.nl
Website http://www.wrr.nl

WRR

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID

# *Privacy en vormen van 'intelligente' mobiliteit*

## DE IMPACT VAN ICT-APPLICATIES VOOR DE WEG EN HET SPOOR

*Henk Griffioen*

Amsterdam University Press, Amsterdam 2011

Omslagontwerp en vormgeving binnenwerk: Studio Daniëls, Den Haag

ISBN 978 90 8964 416 9
E-ISBN 978 90 4851 602 5 (pdf)
E-ISBN 978 90 4851 603 2 (ePub)
NUR 754 / 759

# INHOUDSOPGAVE

# TEN GELEIDE

De voorliggende studie is opgesteld in opdracht van de Wetenschappelijke Raad voor het Regeringsbeleid, meer specifiek de projectgroep Beleid, Informatie en Technologie (BIT). Dit project heeft in maart 2011 het rapport iOverheid opgeleverd.

Het vertrekpunt van het WRR-onderzoek dat voor dit project is uitgevoerd, is de zoektocht naar de rol en verantwoordelijkheid van de overheid bij de inzet van ICT. Daarbij richtte het project zich meer in het bijzonder op een tweetal vragen: 1) wat zijn de consequenties van de inzet van ICT voor de relatie overheid-burger en welke tendensen zijn daarin zichtbaar? 2) wat is de betekenis van deze consequenties vanuit de verantwoordelijkheid van de overheid wanneer ze ICT inzet in bedrijfsvoering, beleid en beleidsuitvoering? Om meer inzicht te verwerven in de dynamiek rondom de ontwikkeling, invoering en het gebruik van ICT in de relatie overheid-burger heeft de projectgroep BIT een aantal empirische studies uitgezet.

Deze studies zijn deels beschikbaar als webpublicatie op de site van de WRR, deels als bijdragen aan de verkenning De staat van informatie die is verschenen in maart 2011, samen met het rapport iOverheid.

André Knottnerus
Voorzitter WRR

# 1 'ONDERWEG': EEN URGENTE MAAR VLUCHTIGE DIMENSIE VAN PRIVACY

## 1.1 INLEIDING

De auto is als cultureel symbool en als min of meer afgesloten fysieke ruimte een soort *home away from home*. Een levenssfeer die toch persoonlijk is, hoewel men zich voortbeweegt op de openbare weg. De opkomst van tal van ICT-applicaties – van automatische kentekenherkenning tot de OV-chipkaart – leidt op uiteenlopende manieren tot digitalisering van die levenssfeer 'onderweg', of dat nu de auto is, of het openbaar vervoer via de weg of het spoor. Dergelijke applicaties maken dat de bewegingen van mensen meer traceerbaar worden. Dat is vanuit het oogpunt van privacy een belangwekkende ontwikkeling. Maar ondanks dat traceerbaarheid maatschappelijk de nodige beroering wekt, is de digitalisering van de openbare ruimte nog niet neergedaald in de kaders en beschermingsconstructies die met privacy te maken hebben. De toenemende inzichtelijkheid van onze *whereabouts* is echter een urgente kwestie, die vraagt om aanpassingen in het denken over privacy in relatie tot digitale informatie. Dergelijke aanpassingen komen niet vanzelf tot stand.

In dit essay staat de invloed centraal van digitalisering op de levenssfeer van het onderweg zijn, op de mobiliteit. Onderzocht zal worden welke implicaties dit heeft voor de relatie overheid-burger.[1] De notie en het belang van privacy – dat eigenlijk niet sterk is toegesneden op locatie-informatie – wordt naast de verschillende ICT-ontwikkelingen op mobiliteitsgebied gelegd. Na een bespreking van de betekenis van locatie-informatie binnen de privacybescherming in dit hoofdstuk, geeft het tweede hoofdstuk daarom de meest relevante applicaties kort weer: *real-time*-verkeersinformatie in de auto, de OV-chipkaart, de kilometerprijsregistratie, en automatische kentekenherkenning. Ook politiek-bestuurlijk gezien 'kleinere' toepassingen als eCall worden daarbij aangestipt. Wat alle applicaties gemeenschappelijk hebben, is dat ze mensen meer traceerbaar maken dan in het verleden het geval was. Om de implicaties daarvan op waarde te schatten is kennis nodig van de technieken in kwestie, van de manier waarop zij het fenomeen mobiliteit 'programmeren'[2], en van de beleidsterreinen waarin ze figureren of de publieke belangen waaraan zij raken. Hoofdstuk 3 analyseert daarom hoe het bij deze applicaties staat met verschillende factoren – zoals *accountability* en technologische betrouwbaarheid – die de sterkte of zwakte van de bescherming van de persoonlijke levenssfeer in een digitale setting bepalen. Hoofdstuk 4 biedt enkele conclusies.

De beschreven applicaties hebben alle een (meer of minder dominante) bestuurlijke component – in de zin van inmenging van de overheid. Maar ook op het puur commerciële vlak is locatie-informatie een heet hangijzer geworden. Dat komt in dit essay zijdelings aan de orde. Enerzijds laat 'de' overheid zich op dat terrein nog nauwelijks horen. Maar anderzijds kan het toch niet onbesproken blijven; voor (inter-, supra-)nationale overheden is het ongetwijfeld slechts een kwestie van tijd voordat ze zich nadrukkelijker (moeten) gaan bemoeien met de locatie-informatie van burgers die in handen is van commerciële dienstverleners. Traceerbaarheid van burgers is ook in de context van commerciële dienstverlening een thema dat steeds meer aandacht zal vergen.

## 1.2 LOCATIE-INFORMATIE ALS DIMENSIE VAN PRIVACY

Een van de vele manieren om na te denken over privacy, ofwel het recht op een persoonlijke levenssfeer, is in termen van *selective disclosure*.[3] De gedachte achter *selective disclosure* is dat mensen een basale behoefte hebben om zelf te bepalen op welke manier en in welke mate ze zich blootgeven aan anderen. Zelfs voor de meest intieme relaties geldt dat menselijke interactie evenzeer wordt gekenmerkt door 'reserveren' als door 'delen' van informatie.[4] Dit maakt controle over de manier waarop en de mate waarin men zichzelf blootgeeft tot een belangrijk bezit. Het gaat om het prijsgeven van informatie, of dat nu visueel is – gezien worden – anderszins zintuiglijk of in taal (lexicaal).

Het concept privacy gaat over dit bezit. Het gaat bij privacy dus niet alleen om een 'officieel' recht, maar evengoed om een belangrijk sociaal en filosofisch ijkpunt. Welke plaats heeft het element *locatie* (locatie-informatie) hierin, als toespitsing van privacy? Hoe wordt de controle over zelfopenbaring geraakt door het ontstaan van een 'digitale fysieke ruimte',[5] in haar vele verschijningsvormen? Er zijn tekenen te over dat de controle die mensen hebben over 'hun' informatie ten aanzien van bewegingen in de openbare ruimte, serieus onder druk staat. Die controle over informatie is dus problematisch geworden. Maar raakt bij het spreken over privacy in termen van controle niet een meer intrinsieke betekenis van het begrip onderbelicht? Die onderliggende vraag of privacy door ontwikkelingen op mobiliteitsgebied ook geraakt wordt op een andere wijze dan door verlies van controle komt in dit essay ook aan de orde.

*Locatie-informatie lijkt triviaal*

Het verhaal van de opkomst van 'locatie' als toespitsing van privacy laat zich redelijk goed vertellen, hoewel de ontknoping nog ontbreekt. De categorie van informa-

tie over de plek waar iemand zich op een bepaald moment bevindt, bleef voorheen in wezen buiten het privacybewustzijn, omdat er met dit soort informatie niet zoveel aan de hand was. Deze informatiecategorie kenmerkt zich immers door een zekere trivialiteit: wie ligt er wakker van het bekend zijn van de informatie dat hij of zij zich op moment *t* bevond (c.q. bewoog) ter hoogte van *P* rijdend in het voertuig met het kenteken *X*? Een en ander drukt bepaald geen wezenlijk aspect van de persoonlijkheid uit, en behelst daarmee eigenlijk al geen gevoelige informatie.

Een kanttekening daarbij is dat locatie-informatie onder zekere omstandigheden allesbehalve triviaal is. Bijvoorbeeld als iemand verdacht wordt van een misdrijf dat even voor tijdstip *t* nabij plaats *P* is begaan. Dat gegeven is echter niet erg relevant: het maakt de informatiesoort zelf er nog niet anders op. Ook naar het oordeel van het Europees Hof voor de Rechten van de Mens is locatie-informatie naar haar aard een relatief weinig ingrijpende informatiesoort, zelfs al kan de vergaarde informatie doorslaggevend zijn voor een strafzaak, en de verdachte voor lange tijd in de gevangenis doen belanden. Dat blijkt uit de zaak-*Uzun* over GPS-tracering in een strafrechtelijk onderzoek.[6] Wat dit soort informatie relatief onschuldig maakt, is vooral het feit dat de locaties van mensen altijd al met het blote oog en in het openbaar konden worden vastgesteld, zonder dat hier 'regels' voor golden. Waarnemen staat vrij,[7] en de openbare ruimte heet niet voor niets openbaar. Of, zoals het Amerikaanse *Supreme Court* het in de *Knotts*-zaak uitdrukte:

> "A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When Petchen [zie hierna] travelled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from the public roads onto private property."[8]

Het citaat uit *Knotts* (en de uitspraak als geheel) illustreert het stempel dat openbaarheid drukt op locatie-informatie. Tegelijkertijd belichaamt het in optima forma een riskante, bestudeerd naïeve benaderingswijze ten aanzien van 'privacy in het openbaar'. Privacy wordt in dit citaat als belang nagenoeg geheel buitenspel gezet in zaken die de openbare ruimte betreffen. Dit standpunt kan zich wreken op het moment dat die ruimte revolutionair van karakter verandert doordat zij digitaal (verder) ontsloten wordt.
Om dit te doen beseffen moet aan het onschuldig ogende citaat de volgende achtergrondinformatie worden toegevoegd. Petchen, die tevoren niet in beeld was bij de politie, had nietsvermoedend een fles op zichzelf legale chemicaliën opgepikt.

Maar doordat de politie een elektronisch *tracking device* in die fles had verstopt, konden opsporingsambtenaren de weg vinden naar een drugslaboratorium. Door de openbaarheid van de levenssfeer 'onderweg' zo te benadrukken als de uitspraak in *Knotts*, wordt de ingrijpendheid van (in dit geval) een elektronisch opsporingsinstrument helemaal weg geïnterpreteerd. Het mag duidelijk zijn dat iedereen in het openbaar met het blote oog geobserveerd *kan* worden, maar uit dit triviale gegeven moet niet teveel worden afgeleid. Met alleen menselijke waarneming komt de politie natuurlijk nooit op deze eenvoudige manier bij een drugslaboratorium uit. De 'zichtbaarheid' die hier door een elektronisch hulpmiddel wordt bewerkstelligd, is alleen in metaforische zin verwant aan de zintuiglijke waarneming. De openbare weg wordt in het citaat voorgesteld als een stelsel van verbindingen tussen ontelbare particuliere opritten, een netwerk waarin de persoonlijke levenssfeer niet aan de orde is. Dat is een opvatting met verstrekkende consequenties.

Deze lijn in de rechtspraak heeft in de VS veel kritiek geoogst.[9] In Europa neemt de diskwalificatie van privacy in de openbare ruimte daarentegen minder absolute vormen aan.[10] Niettemin fungeert de waarneming die men met het blote oog in het openbaar kan doen ook in Europa en specifiek in Nederland als bliksemafleider, zoals de discussie over automatische kentekenherkenning (hierna ook: ANPR – *Automatic Number Plate Recognition*) laat zien.[11] Intussen is er wel degelijk iets aan de hand met locatie-informatie, ook al wordt die doorgaans op de openbare weg gegenereerd. De mengelmoes van locatietechnologieën en applicaties, en daarbij gevoegd hun commerciële en bestuurlijke populariteit, heeft het nadenken over *location based privacy* absoluut noodzakelijk gemaakt. Traceerbaarheid betekent dat de gangen van mensen *ex post* nagegaan worden, waardoor zich een nieuw spanningsveld ontvouwt.[12] Het stelt beheerders van locatie-data (publiek of privaat) in staat om op grote schaal leefpatronen van mensen te registreren, voor welk toekomstig gebruik dan ook. Eigenlijk is het pas nu noodzakelijk om voor dit aspect van privacy beschermingsmechanismen in het leven te roepen.[13]

*Steeds meer technologische toepassingen geven locatie-informatie prijs*
In het commerciële spectrum zijn steeds meer technologische toepassingen beschikbaar die de gebruiker oproepen om de eigen locatie prijs te geven voor een bepaalde vorm van dienstverlening. De meest in het oog springende voorbeelden zijn de vele *apps* die *location based services* laten draaien op de *smart phone*. Het prijsgeven van locatie-informatie is dan (meestal[14]) een integraal onderdeel van de functionaliteit. Deze toepassingen ontsluiten als het ware de fysieke ruimte, maar hebben daar wel informatie voor nodig.
Kijken we vervolgens naar het meer publieke spectrum, dan zijn de toepassingen van locatietechnologie legio, en qua bestuurlijk enthousiasme sterk in opkomst.

Het is niet eenvoudig om lijnen te trekken door deze veelheid van bestuurlijke toepassingen. Enerzijds zijn er applicaties in de sfeer van *surveillance* (zoals ANPR), anderzijds zijn er veel inspanningen in de sfeer van dienstverlening (zoals bij verkeersmanagement). Enerzijds zijn er systemen die van top tot teen een publiek karakter hebben, zoals belastingheffing via de kilometerprijs,[15] anderzijds zijn er gevallen waarin publieke actoren 'meeliften' met puur commerciële applicaties, zoals de locatiebepaling van mobiele telefoons. Deze leveren een schat aan gegevens die de politie in het kader van de opsporing kan opvragen. Er zijn ook verschillen tussen de technologieën die gebruikt worden: toepassingen als GPS of de triangulatie van mobiele telefoons peilen in principe voortdurend de locatie, terwijl in andere gevallen, zoals bij de OV-chipkaart of ANPR, sprake is van een vaste infrastructuur die passages vastlegt.

# 2 ENKELE PUBLIEKE EN HYBRIDE TOEPASSINGEN

Dit essay zal geen eenduidig of sluitend beeld schetsen van de digitalisering van de openbare ruimte. Wel is de vraag aan de orde wat er met privacy gebeurt in deze ontwikkeling. In dit hoofdstuk komen de applicaties aan bod die hieraan de meest markante bijdrage hebben geleverd. Daarbij blijven applicaties die geen bestuurlijke component bezitten grotendeels buiten beschouwing. Dit zijn commerciële applicaties waarbij ofwel geen publieke belangen in het spel zijn, ofwel – meer prangend – de overheid die belangen nog niet consistent gedefinieerd heeft.[16] Omdat het in dit essay om de *bewegingen* van mensen gaat, blijven ook applicaties als digitaal cameratoezicht buiten beschouwing, hoewel dit fenomeen het nodige bijdraagt aan de digitalisering van de openbare ruimte. Toch resteert nog een rijk scala aan applicaties, die stuk voor stuk worden gekenmerkt door complexe samenwerkingsvormen en vermengingen van publiek en privaat.

## 2.1 TECHNOLOGISCHE EN BESTUURLIJKE DRUKTE ROND DE 'INTELLIGENTE AUTO'

### 2.1.1 'INTELLIGENTE TRANSPORTSYSTEMEN': TECHNOLOGISCHE GRABBELTON

Veel veranderingen in de mobiliteitssector die zich onder invloed van ICT voltrekken, kunnen worden geschaard onder de noemer van 'intelligente transportsystemen' oftewel ITS. Wat de veelkleurige technologieën die hier onder vallen gemeenschappelijk hebben, is dat ze van 'de weg' een communicerend informatiesysteem maken, met onroerende elementen (informatie-infrastructuren aan de 'wegkant') en roerende elementen (de auto als zender en als bedieningspaneel). Systemen die auto's een veilige afstand tot elkaar laten behouden, systemen die automatisch 112 bellen als er een crash is (eCall[17]), maar ook navigatiesystemen zoals TomTom: deze voorbeelden zijn slechts een greep uit de technologische grabbelton die ITS heet.[18]

ITS wordt ook wel gerelateerd aan de opkomst van de 'intelligente auto': de auto die ons in de toekomst veel uit handen zal nemen – zowel controle als zorgen – doordat hij voortdurend communiceert met andere auto's en met de vaste infrastructuur om een veilige en qua duur optimale gang van A naar B te bewerkstelligen.[19] Ook andere vervoersmodaliteiten dan de auto zullen in dit toekomstbeeld op het infor-

mationele vlak geheel gekoppeld zijn aan het 'autosysteem'. Op deze manier kan de reiziger zijn optimale actuele vervoerswijze bepalen. Dit technologische plaatje heeft ook een sociologische component: de auto zal waarschijnlijk iets van zijn individualistische glans verliezen, doordat *toegang* tot mobiliteit belangrijker zal worden dan *bezit* van een (auto)mobiel.[20] De mogelijkheden die ITS biedt, zijn voor een groot deel weliswaar technologische toekomstmuziek – veel daarvan is immers nog niet gerealiseerd – maar sporen zijn er al wel: sommige duurdere automodellen bezitten bijvoorbeeld al ITS-applicaties die de verkeersveiligheid vergroten (door in gevaarlijke situaties de 'zeggenschap' van de bestuurder te verkleinen), en er zijn zelfs verzekeraars die ITS-producten aanbieden.[21] Natuurlijk is ook de routenavigatie, een applicatie die in de duurdere varianten echt interactief (communicatief) is, al een wijdverbreid gegeven.

Of en hoe de mogelijkheden van ITS zullen worden gerealiseerd, is niet in de laatste plaats een publieke of zelfs politieke zaak. Deze bestuurlijke aspecten (en het denken daarover) zijn echter nog verre van uitgekristalliseerd. Ze hebben zowel te maken met de adoptie van technologieën *door* het bestuur als met de verantwoordelijkheid *van* het bestuur voor het geleiden van de verdere ontwikkelingen. De directe implicaties voor de persoonlijke levenssfeer, die in het volgende hoofdstuk aan bod komen, lijken beduidend minder verstrekkend dan die van applicaties in het kader van de handhaving (automatische kentekenherkenning e.d.). Maar de maalstroom van informatie rond de 'intelligente auto' is niet minder typerend voor het gegeven dat de levenssfeer 'onderweg' nu al en in de toekomst nog verder zal worden opgenomen in het digitale tijdperk. ITS betreft een omvangrijke en complexe materie, waarvan de bestuurlijke implicaties nog amper in kaart gebracht zijn. Om die reden volsta ik hier met een schets op hoofdlijnen. De nadruk ligt daarbij op *realtime*-reis- en verkeersinformatie, een applicatie die naar het zich laat aanzien de verschillende aspecten van het mobiliteitsbeleid zal gaan verbinden.

### 2.1.2 AANTREKKINGSKRACHT OP HET OPENBAAR BESTUUR

Wereldwijd wordt veel verwacht van de mogelijkheden op ITS-gebied. Toch lijken in de meeste landen de enorme investeringen die nodig zijn om ITS-producten in de markt te zetten, achter te blijven bij de verwachtingen; alleen Japan vormt hierop wellicht een uitzondering.[22] Op diverse punten lijkt een impasse te zijn ontstaan. Overheden (Europese ambten, nationale en regionale wegbeheerders) en bedrijven kijken naar elkaar als het erom gaat wie de investering zal doen om een bepaalde applicatie (eCall bijvoorbeeld[23]) over het dode punt te helpen en haar een gezonde winstgevendheid te laten bereiken die een nieuwe technologie in het begin meestal niet heeft. Om met het *Beleidskader Benutten* van het (toenmalige) ministerie van

Verkeer & Waterstaat te spreken: "De overheid kan een belangrijke aanjaagfunctie hebben om deze patstelling te doorbreken."[24] Wat overheden in deze context te doen staat, is vooral een economische opdracht. Immers, bij de belofte van ITS op macroniveau gaat het vooral om een commerciële impuls en een potentiële productiviteitsimpuls. Deze economische opdracht is naar de aard van de zaak niet de primaire focus van dit essay over privacy 'onderweg', maar bepaalt wel degelijk de drijvende kracht achter de ontwikkelingen op ITS-gebied.

Ondanks het langzame verloop blijven de verwachtingen van ITS hooggespannen. Dat blijkt uit, maar wordt ook gevoed door, een veelheid aan goed geëquipeerde onderzoeksprojecten, gefinancierd met Europees en nationaal, publiek en privaat geld.[25] Ook de Europese Unie maakt zich namelijk op om de slapende prinses wakker te kussen. De indruk bestaat dat de belemmeringen voor ITS – dat als veld van onderzoek en expertise al vrij lang bestaat[26] – niet technisch maar organisatorisch-bestuurlijk van aard zijn.[27] Zo zou volgens de Digitale Agenda van de EU, het strategiedocument van de Europese Commissie (hierna: Commissie) voor de digitale toekomst,[28] ITS een krachtige *tool* zijn om de uitstoot van schadelijke stoffen tegen te gaan, en het milieu aanmerkelijk te verbeteren. Een onderbouwing van deze verwachting ontbreekt echter. Op een soortgelijke wijze meldt de minister van Infrastructuur en Milieu aan de Tweede Kamer over *realtime*-verkeersinformatie: "De verwachting is dat hierdoor reistijden met 5 tot 10% kunnen verminderen (KiM, 2011)."[29] Echter, niet alleen wordt de betreffende studie van het Kennisinstituut voor Mobiliteitsbeleid (KiM) in deze verkeerd geparafraseerd, ook wordt verzwegen dat de studie expliciet aangeeft dat die percentages uit het jaarverslag van TomTom komen[30] (waar ze evenmin onderbouwd zijn[31]). En als we het toch over getallen hebben: de minister laat onvermeld dat het KiM ook wijst op een omslagpunt (van 30% marktpenetratie) waarboven *realtime*-verkeersinformatie contraproductief zou gaan werken. Dit omslagpunt ontstaat door de bekende ironie dat meer informatiegestuurde mobiliteitskeuzes tot opstoppingen kunnen leiden op de alternatieve routes – lees: rustige, meanderende wegen door een gemoedelijk landschap – omdat de verkeersinformatie die routes aan iedereen aanbeveelt.[32] Er zijn dus grenzen aan het nut van de instrumenten die de overheid zo enthousiast heeft onthaald.

De getalsmatige onderbouwing laat misschien nog te wensen over, maar een kwalitatief exposé over de impact van ITS op het beleid is wel te geven. Die onderbouwing gaat over de implicaties van ICT voor de samenhangende beleidsterreinen[33] van verkeersinformatie, verkeersmanagement en verkeersveiligheid. De belangrijkste tendens is dat de technologie een samenhang aanbrengt in wat anderszins onderscheiden taken en bevoegdheden zijn. De verspreiding van verkeersinformatie is weliswaar een publiek belang, maar de overheid (zeker in Nederland) drukte er

nooit een zwaar stempel op. Verkeersmanagement, de verzamelterm voor zaken als het geleiden van verkeersstromen, 'incidentmanagement' en dergelijke, is daarentegen een exclusieve overheidstaak. En verkeersveiligheid[34] moet als publiek belang gestalte krijgen in de samenwerking van de Europese overheid en de automobielindustrie (voor zover het over de veiligheid van de vervoersmiddelen gaat en niet over verkeerswetgeving e.d.).

### 2.1.3 *REALTIME*-VERKEERSINFORMATIE ALS SPIL

Verkeersinformatie, verkeersmanagement en verkeersveiligheid schuiven gaandeweg in elkaar. Verkeersinformatie wordt namelijk niet alleen de centrale schakel van het beleid, maar ook het zenuwstelsel van de verbonden technologische systemen zelf. Het gaat hierbij met name om *realtime*-verkeersinformatie. Het kunnen genereren van dit soort informatie (en vervolgens aanbieden/verkopen) is het summum van technologisch kunnen op dit gebied, en ondenkbaar in het tijdperk van de menselijke waarneming (of van de low-tech 'waarneming').

De nieuwe mogelijkheden voor verkeersinformatie zetten oude beleidsproblemen in een ander daglicht. Neem de congestie op de wegen. Voor een dichtbevolkt land als Nederland is dit een onvervalst 'wicked problem',[35] waarop de afgelopen decennia heel wat beleid is losgelaten, van volumebeleid (terugdringen van de mobiliteitsvraag) tot modaal beleid (stimuleren van alternatief vervoer);[36] beleid waarvan de doelstelling wisselde tussen het economisch belang van bereikbaarheid en het milieubelang van duurzaamheid.[37] En daarbij komt nog het beleid – of de 'must' – om steeds meer en steeds bredere wegen aan te leggen, in aansluiting op een vraag naar mobiliteit die steeds toeneemt – beleid of geen beleid. Beleidswetenschappers signaleren immers al lange tijd dat de effecten van de publieke inspanningen tegenvallen, gezien de nog steeds groeiende vraag naar mobiliteit en groeiende verstopping van de fysieke infrastructuur.[38] De komst van ICT-toepassingen voor mobiliteit steekt tegen deze achtergrond bijzonder rooskleurig af: dit instrumentarium heeft niets te maken met 'asfalt' of met kwetsbare pogingen tot gedragsbeïnvloeding, maar verandert het 'onderweg zijn' als het ware van binnenuit. Een applicatie als *realtime*-verkeersinformatie voor de individuele bestuurder – in de ogen van overheden zonder twijfel de belangrijkste toepassing in het ITS-domein[39] – maakt dat weggebruikers verstoppingen kunnen vermijden, prudente keuzes kunnen maken tussen verschillende vervoersmodaliteiten, enzovoorts. Kortom, er ligt een betere benutting van de bestaande infrastructuur in het verschiet. Vanuit het perspectief van de overheid tekent zich een vrolijk stemmend scenario af waarin het lanceren van nieuwe ICT-toepassingen geheel op eigen kracht, dus ogenschijnlijk zonder verliezers, tot een efficiëntere benutting van de gegeven capaciteit moet leiden. Niet

voor niets noemt het eerdergenoemde *Beleidskader Benutten* informatietechnologie als het middel om bij gelijkblijvende wegcapaciteit de fileproblematiek toch te kunnen aanpakken.[40] Wel signaleert het toenmalige ministerie van Verkeer en Waterstaat daarbij dat de rol van de overheid en haar instrumenten op dit gebied beperkt zijn. De nieuwe mogelijkheden zijn immers een direct gevolg van technologische innovaties die door hun commerciële succes gedragen worden en dus niet echt tot het overheidsinstrumentarium behoren. Sterker nog, het beleidsperspectief is gebouwd op een luxeversie van routenavigatie, die vergeleken met meer basale navigatiesystemen slechts een klein marktaandeel heeft.[41] Van *realtime*-verkeersinformatie is immers alleen sprake bij duurdere abonnementen.[42] In Nederland voorziet TomTom deze abonnementshouders van actuele informatie met behulp van geaggregeerde gsm-data van Vodafone,[43] aangevuld met meer statische (minder actuele) informatie die klanten leveren door hun navigatiesysteem te synchroniseren met hun computer.[44] De banden tussen de overheid en het geschetste instrumentarium van het mobiliteitsbeleid van de toekomst zijn dus tamelijk dun. Zeker als men bedenkt dat niet alleen de applicatie privaat bezit is, maar ook de informatie waarop die applicatie draait. Simpel gezegd is de informatie die *realtime*-diensten mogelijk maakt niet van de overheid, maar van TomTom, evenzeer als het platform waarop de communicatie met de automobilist plaatsvindt.

Dat de overheid *realtime*-verkeersinformatie tot de spil van haar beleid wil maken, betekent niet dat zij ernaar streeft om iedereen een duur routenavigatiesysteem te laten aanschaffen en gebruiken. Al klinkt die boodschap impliciet misschien door,[45] er zijn nóg twee desiderata die voor deze beleidslijn onmisbaar zijn. In de eerste plaats is de overheid geïnteresseerd in de data zelf, om haar eigen operationele besluitvorming mede[46] daarop te kunnen baseren. In de tweede plaats is de overheid geïnteresseerd in het platform voor communicatie met de automobilist, om daarop haar eigen boodschappen in te kunnen voegen: boodschappen over files, incidenten, adviesroutes enzovoorts. Het gaat met andere woorden niet slechts om de heilzame effecten voor de doorstroming die de applicatie *realtime*-verkeersinformatie van zichzelf al heeft (gesteld dat genoeg mensen die applicatie gebruiken[47]); het gaat ook om de instrumentele, actieve mogelijkheden die zij de overheid zou kunnen bieden. Deze twee desiderata zorgen tezamen voor het ineenschuiven van overheidsbeleid (zie hieronder).

Naast deze instrumentele kant heeft de overheid ook een meer algemene verantwoordelijkheid om zicht te houden op de ontwikkelingen op dit gebied. Dergelijke *floating car data* waar het om draait – een verzamelterm voor de gegevens die door meer of minder 'intelligente auto's' wordt gegenereerd – leveren weliswaar een schat aan nuttige informatie op, maar betekenen tegelijkertijd dat automobilisten

meer traceerbaar zijn, met alle privacy-implicaties van dien. Op dit moment gaat het om informatie voortgebracht voor (en deels door) *realtime*-routenavigatie, maar op termijn komt wellicht ook informatie beschikbaar uit andersoortige ITS-systemen in de auto. Het maakt voor het 'losmaken' van deze informatierijkdom immers niets uit of de auto voor de ene of de andere applicatie als zender functioneert, *als* de auto maar als zender functioneert. De invoering van de applicatie eCall, om een onschuldig voorbeeld te noemen, betekent dat alle auto's gaandeweg uitgerust zullen zijn met een zender die de locatie doorgeeft in het geval van een ongeluk, maar die (technisch gezien) natuurlijk met hetzelfde gemak voortdurend de locatie kan doorgeven. Voor eCall is 'permanent zenden' expliciet uitgesloten,[48] omdat deze applicatie een publiek karakter heeft en naar verwachting dwingend door overheden zal worden doorgevoerd. Hierdoor verkeren publieke autoriteiten in een goede positie om de voorwaarden voor te schrijven. Bij commercieel geïntroduceerde applicaties echter (bijvoorbeeld 'automatisch afstand bewaren', een applicatie die individuele autofabrikanten uit eigen beweging inbouwen) zal een dergelijke inmenging minder vanzelfsprekend zijn, zodat de kans dat auto's permanent op zenden staan, toeneemt. Althans indien de overheid daartegen niets doet.

### 2.1.4 DOOR ICT GEDREVEN BELEIDSTEKTONIEK

De mogelijkheden die ICT mobiliteitsvragen te bieden heeft, leiden tot een soort 'tektoniek' van beleid: overheidstaken, maar ook de publieke en private sfeer, schuiven in elkaar. Er zijn, zoals gezegd, twee motieven die tot deze tendens leiden: de aantrekkelijkheid van de door willekeurige automobilisten voortgebrachte informatie, en de aantrekkelijkheid van het communicatieplatform in de auto, dat op dit moment nog slechts geboden wordt door de *realtime*-routenavigatie.

Van de drie onderdelen van het mobiliteitsbeleid – verkeersinformatie, verkeersmanagement en verkeersveiligheid – staat de verkeersveiligheid (meer bepaald de veiligheid van voertuigen) het meest op zichzelf. Op dit vlak wordt vooral nagedacht over manieren om de marktpenetratie van de rijtaakondersteunende systemen te verhogen.[49] Dit zijn systemen als *Automatic Lane Assist* of *Advanced Cruise Control*, die het rijden op uiteenlopende manieren veiliger proberen te maken door de bestuurder in gevaarlijke situaties zeggenschap uit handen te nemen. Ook bij dergelijke systemen heeft communicatietechnologie alleen maar zin als er genoeg auto's zijn die 'meedoen'. Zelfs als in de toekomst een significant aandeel auto's voorzien zou zijn van deze rijtaakondersteunende systemen,[50] dan nog zal het door elkaar heen rijden – of het op elkaar botsen – van 'slimme' en 'minder slimme' auto's de overheid voor een lastig vraagstuk blijven plaatsen: welke regels te stellen rond aansprakelijkheid en, in het verlengde daarvan, verzekerbaarheid?[51] De rij-

taakondersteunende systemen bevinden zich op een glijdende schaal van het louter informeren/waarschuwen van de bestuurder tot het geautomatiseerd ingrijpen. De laatste soort systemen wordt echter nog vrijwel niet toegepast, omdat zij nopen tot een fundamentele heroriëntatie op de autonomie van de bestuurder,[52] en de culturele symboliek van de auto als bevrijdende egocapsule grotendeels tenietdoen.[53] Ook eCall, dat niet echt een rijtaakondersteunend systeem is, hoort thuis in de categorie verkeersveiligheid. Deze applicatie illustreert dat de overheid (Europees dan wel nationaal) wel degelijk de weg van dwingende, publieke regulering kan bewandelen. Dat lijkt bij de rijtaakondersteunende systemen op geen enkele manier aan de orde te zijn, omdat de ontwikkeling of het afblazen daarvan aan de autoindustrie zelf wordt overgelaten.

Applicaties voor de verkeersveiligheid kunnen, omdat ze de auto tot zender kunnen maken, opgenomen worden in de maalstroom van verkeersinformatie waarvan de combinatie TomTom/Vodafone voorlopig de vaandeldrager is. Dat verkeersmanagement en verkeersinformatie met elkaar versmelten is echter nog veel evidenter, en veel meer in beeld bij de actoren in kwestie. TomTom stelt het zelfs al als een voldongen feit dat "traffic managers use our vast knowledge to improve their work".[54] Gezien de ophef die in april 2011 ontstond over het feit dat de politie informatie afkomstig van TomTom gebruikte om geschikte plaatsen voor flitspalen te bepalen,[55] zit daar misschien ook wel een kern van waarheid in. Toch loopt deze constatering grotendeels op de zaken vooruit. De politie is niet primair verantwoordelijk voor het verkeersmanagement, een activiteit die bovendien heel wat fijnmaziger informatie vereist dan de plaatsing van flitspalen. De schok die de 'samenwerking'[56] tussen TomTom en de politie maatschappelijk teweegbracht, illustreert wel de weinig transparante manier waarop ontwikkelingen op dit gebied gestalte krijgen. Het is niet eenvoudig om vast te stellen hoe het er voor staat met privacy op de snelweg.

In de eerste plaats vervloeit het onderscheid tussen publiek en privaat gegenereerde informatie. De aard van de verkeersdata verandert 'van binnenuit' door de mogelijkheid om *floating car data* te registreren, te bewerken en daar prognoses op te baseren. Dit laat publieke verkeersmanagers niet koud. De operationele beslissingen die wegbeheerders als Rijkswaterstaat moeten nemen, vereisen zeer goede en zeer actuele informatie. De instrumenten die daarvoor in het predigitale tijdperk volstonden, zoals de zogenaamde lussen in de weg of de waarnemingen van beambten, komen in een heel ander licht te staan als alle auto's – of in ieder geval een wezenlijk deel daarvan – zenders van informatie worden. De traditionele informatiebronnen van de overheid benutten deze potentie niet, terwijl de samenwerking tussen TomTom en Vodafone er juist op drijft. Door de geaggregeerde maar niet-

temin bijna *realtime*-informatie van de locaties van mobiele telefoons kunnen verkeersstromen en -opstoppingen in beeld worden gebracht, waarmee de individuele automobilist zijn keuze voor een bepaalde route kan bepalen. De aldus ontsloten rijkdom aan verkeersdata is waarschijnlijk een voorbode van het feit dat de overheid hier haar feitelijke monopolie op het inwinnen van hoogwaardige informatie gaat verliezen. Dit ondanks de investeringen in de Nationale Databank Wegverkeersgegevens (NDW) om de verschillende bronnen van publieke mobiliteitsinformatie samen te brengen (ook geen eenvoudige klus, in een drukbevolkt bestuurlijk landschap van wegbeheerders). De arbeidsdeling die in Nederland is gegroeid,[57] met een overheid die als informatiereservoir functioneert maar het aan marktpartijen overlaat om met deze informatie meerwaarde te creëren, zou wel eens op haar kop kunnen worden gezet. Maar het is nog afwachten of de kwaliteit van privaat gegenereerde informatie hoogwaardig genoeg zal worden bevonden om er het hele scala aan publieke besluitvorming op te baseren.[58]

Toch zal de overheid waarschijnlijk geleidelijk aan accepteren dat informatievergaring op de weg onder invloed van ICT alomtegenwoordig wordt. Dat wil zeggen: als er miljoenen zenders van digitale informatie rondrijden, wie zou dan durven nalaten die informatie te gebruiken? In dat scenario zullen wegbeheerders hun besluiten in de toekomst toch nemen op basis van eenzelfde mengeling van publiek en privaat verkregen data waarvan ook particulieren via commerciële diensten gebruikmaken. Mogelijk zullen overheden zich dan ook meer gaan bemoeien met de voorwaarden waaronder die informatie gegenereerd mag worden; op dit moment bestaan daarvoor nog amper kaders. Het begin van de omschakeling naar één publiek-private informatie*pool* is al te herkennen.[59] Onlangs is het Besluit Personenvervoer zodanig aangepast dat alle vervoerders verplicht zijn om *actuele* informatie over hun vervoerssysteem te verstrekken aan derden die daaruit verkeersinformatie willen destilleren (die verkocht kan worden).[60] Ze moeten dat doen tegen "redelijke en objectief gerechtvaardigde voorwaarden",[61] wat waarschijnlijk neerkomt op kostprijs. Deze verplichting geldt niet voor TomTom/Vodafone e.d., maar slechts voor het openbaar vervoer. De overheid plukt nog even de vruchten van het feit dat ze nog het nodige te zeggen heeft over de openbaarvervoersbedrijven.

In de tweede plaats betekent het feit dat de Nederlandse overheid vol inzet op de ordenende werking van *realtime*-verkeersinformatie dat zij zich ook zal gaan interesseren voor het communicatieplatform in de auto. Waarschijnlijk – overheidspublicaties bieden daar al voorproefjes van[62] – zal zich een ontwikkeling aftekenen waarin maatregelen om de doorstroming van het verkeer te bevorderen steeds meer zullen worden vormgegeven over de band van de informatievoorziening voor

de individuele weggebruiker. Het idee is dat het bieden van *realtime* multimodale reisinformatie – een commerciële dienst waarvoor de overheid zekere randvoorwaarden moet veiligstellen – en het meer of minder dwingend geleiden van verkeersstromen – uiteraard een overheidsprerogatief – zullen gaan geschieden via hetzelfde *in-car*-platform. Hierdoor zullen weggebruikers in staat zijn rationele keuzes te maken over de af te leggen weg. Daarvoor is een huwelijk nodig tussen het informerend geleiden van verkeersstromen (routenavigatie) en het dwingend geleiden daarvan (verkeersmanagement), oftewel een innig verbond tussen publiek en privaat. Minister Schultz van Haegen van Infrastructuur en Milieu heeft al aangegeven dat de – vooralsnog alleen met publieke informatie gevoede – Nationale Databank Wegverkeersgegevens een rol kan spelen in deze "marktbenadering".[63] De neiging tot versmelting van informatie, en versmelting van (beleids)domeinen *door* informatie, krijgt zodoende ook letterlijk, in termen van hardware, vorm.

### 2.1.5 OPEN PLATFORMEN

Dit sluit naadloos aan op een andere ontwikkeling op het gebied van ITS die hier van belang is, namelijk de tendens naar 'open platformen'. Een voorbeeld zijn de genoemde ideeën voor een privaat-publiek platform in de auto (op dit moment belichaamd door routenavigatieapparatuur), met op de achtergrond een publiek-private database (de NDW). Deze vervlechting van publiek en privaat is te zien als een 'opschaling' van commerciële applicaties, die zich door hun succes aan de aandacht van de overheid opdringen en die haar wil tot daadkracht prikkelen. Een dergelijke opschaling brengt een nieuw fenomeen met zich mee, namelijk een overheid die data opkoopt in plaats van deze ('slechts') te vorderen (met wettelijke instrumenten). Een soortgelijk *level playing field* zal mogelijk ook ontstaan met betrekking tot de gebruikersinterface, oftewel het platform en medium van communicatie tussen dienstverlener en automobilist. Op het moment dat de overheid haar eigen boodschappen kwijt wil over zaken als wegafsluitingen – en dit zal zeker nodig zijn om verkeersinformatie tot een succesvol beleidsinstrument te maken – spreekt die overheid via het beeldscherm van de routenavigator of van een apparaat waarop meer dan één ITS-applicatie draait.

Deze ontwikkeling naar open platformen zal aanleiding geven tot een aanzienlijk aantal complexe organisatorische en aansprakelijkheidsvragen. Hoewel het enthousiasme van de overheid duidelijk te herkennen is, kristalliseert de nieuwe rolverdeling publiek-privaat zich nog niet echt uit, en spreekt de overheid ook niet met één stem. Immers, ook het hierna (§2.3) te bespreken programma Anders Betalen voor Mobiliteit had technologisch gezien uitstekend in deze convergerende tendensen kunnen passen, maar is daar om bestuurlijk-politieke redenen van weggehou-

den. Technisch en commercieel gezien had het 'kastje' bij voorkeur een zo open mogelijke architectuur moeten hebben, waardoor het zou kunnen functioneren als knooppunt van allerhande (voortdurend evoluerende) dienstverlening én overheidsregulering.[64] Elders is die 'open-platform'-gedachte wél duidelijk te bespeuren. Zo wordt op verschillende niveaus (Europees, nationaal) voorzichtig verkend wat de mogelijkheden zijn om alle aspecten van ITS te laten samenkomen[65], zowel voor overheidsapplicaties – kilometerprijs, incidentmanagement, eCall enzovoorts – als voor commerciële diensten. Zowel Eurocommissaris Kroes als het ministerie van Economische Zaken, Landbouw & Innovatie (EL&I) blijken expliciet voor de stimulering van dergelijke open platformen te zijn.[66]

Om open platformen te bewerkstelligen is het niet alleen nodig dat het platform zelf een open architectuur heeft[67], het vergt ook een totale compatibiliteit (interoperabiliteit) van alle systemen, en daarmee de standaardisatie van een groot aantal technische specificaties. Een dergelijke ontwikkeling zou de *business case* van afzonderlijke applicaties (ook voor de overheid zelf) aanmerkelijk rooskleuriger maken. Zonder overheidsinmenging is dit echter niet te realiseren, terwijl de overheid tot op heden juist de neiging heeft om technologische applicaties op het gebied van mobiliteit zo *dedicated* (d.w.z. gesloten, unifunctioneel; maar ook: veilig, betrouwbaar, controleerbaar) mogelijk te maken.

Als een onontwarbare verknoping van publiek en privaat de weg vooruit is, is het goed te leren van het ITS-dossier in de Europese rechtsvorming. Daar zorgt publiek-private samenwerking voor moeilijk te traceren processen, die tegelijk de kracht ('dingen voor elkaar krijgen') als de zwakte ('oncontroleerbaar') van zo'n samenwerking illustreren. De applicatie eCall is een goed voorbeeld van een besluitvormingsproces waarbij de Europese overheid aanvankelijk een 'extreme' versie van het fenomeen *level playing field* ontwierp.[68] De Commissie zette het proces van regulering zélf horizontaal op, volledig gebaseerd op consensus. Een speciaal geformeerde groep van meer dan 144 stakeholders (automobielindustrie, telecom, wegbeheerders enz.) presteerde het om een plan voor eCall overeen te komen, met daarin allerlei uitgewerkte specificaties, ook op het gebied van privacy.[69] Een ieder die het aanging – bij wijze van spreken de belangenvereniging voor Noord-Europese Fiat-dealers zij aan zij met lidstaten van de EU – kon zich vervolgens binden aan dit plan. De lidstaten, die bij ondertekening wel degelijk een en ander dwingend moesten regelen binnen hun eigen territoir,[70] committeerden zich echter niet unaniem. De Commissie schakelde om die reden over op het 'traditionele' instrument wetgeving. Intussen is de applicatie eCall onder de paraplu van de zogenaamde ITS-richtlijn gebracht.[71] Dit stelt de Commissie in staat om deze applicatie middels een gedelegeerde wetgevingshandeling (lees: zelf) verplicht te stellen.[72] Deze kapstok-Richtlijn

kreeg in de ontwerpfase kritiek van de European Data Protection Supervisor[73] en ook, in ongebruikelijk klare taal, van de Nederlandse regering.[74] De ontwerprichtlijn was in feite een blanco cheque voor de Commissie om zaken te kunnen regelen die onder de brede noemer ITS vallen. Kennelijk was de Commissie niet in staat of bereid vooraf een inhoudelijke koers uit te zetten. De kritiek heeft ertoe geleid dat de ITS-richtlijn uiteindelijk meer een keuzemenu is geworden, met een grote afwijkingsbevoegdheid van de lidstaten maar nog steeds zonder noemenswaardige inhoudelijke koers.

Zonder inhoudelijke aangrijpingspunten voor ITS – toch al een vage verzameling technologieën – is *function creep* (de geleidelijke overschrijding van oorspronkelijke functies) welhaast een zekerheid. Of moeten we spreken van 'cultivated spill-over',[75] oftewel bij voorbaat doorlatende afbakeningen? ITS komt met andere woorden als een technocratisch onderwerp naar voren, en niet als iets waarmee politiek bedreven kan worden. Daarmee zijn we terug waar we begonnen: de omvangrijke en complexe implicaties van ITS voor het openbaar bestuur zijn nog amper in kaart gebracht.

## 2.2 DE OV-CHIPKAART

De introductie van de OV-chipkaart heeft vele jaren gekost, en op het moment van schrijven is het introductieproces nog niet helemaal afgerond. De OV-chipkaart is een ambitieus project dat vele hobbels onderweg heeft gekend, en waarover uitgebreide maatschappelijke en parlementaire discussies zijn gevoerd. Het is evident dat de OV-chipkaart van belang is uit het oogpunt van *location based privacy*. Doordat de kaart de passages van reizigers vastlegt, en bewaart, is immers na te gaan waar iemand zich op een bepaald tijdstip bevond. Al vroeg in het proces werd daarom het College bescherming persoonsgegevens (Cbp) betrokken bij de plannen. Tegelijkertijd speelt privacy een vreemde en ondergeschikte rol in de maatschappelijke beroering die de OV-chipkaart heeft losgemaakt.

*Vooral bestuurlijk-financiële argumenten achter OV-chipkaart*
In oorsprong heeft de OV-chipkaart weinig te maken met controle of met het willen weten waar mensen zich bevinden.[76] Toen de Nederlandse Spoorwegen (NS), Connexxion, Rotterdamse Elektrische Tram (RET), Haagsche Tramweg Maatschappij (HTM), en het Gemeentelijk Vervoerbedrijf Amsterdam (GVB) in 2001 Trans Link Systems B.V. oprichtten, ging het er vooral om een rationele en gemakkelijke wijze van betalen te ontwikkelen, zowel voor reizigers als voor vervoerders onderling. Vooral het laatste aspect, de verdeling van gelden tussen vervoerders, was beslissend voor het ontstaan van het initiatief voor de OV-chipkaart. Aan de basis stond

de beslissing in de Wet personenvervoer van 2000 om vervoerders tariefvrijheid te geven.[77] Een beslissing die was ingegeven door Europese rechtsontwikkelingen en door de marktgedachte dat vervoerders niet tot volle ontplooiing kunnen komen als zij de belangrijkste schakel van hun bedrijfsvoering, de prijs, niet in eigen hand hebben.[78] En een beslissing die moeilijk te verenigen viel met de uniformiteit in tarieven van het Nationaal Vervoersbewijs (NVB), oftewel de strippenkaart.

De reden om de OV-chipkaart dwingend te schrijven, beginnend met steden als Rotterdam en Amsterdam, is niet ingegeven door een technologische wensdroom, maar door bestuurlijk-financiële imperatieven. Met de afschaffing van het NVB zou namelijk de grond ontvallen aan een zeer log financieel verdeelinstrument. Om vervoerders hun deel van de opbrengsten van het openbaar vervoer – in feite de betaling voor hun diensten – te doen toekomen moest de Werkgroep Reizigers Omvang en Omvang Verkopen (WROOV) op landelijk niveau jaarlijks, onder regie van het ministerie van V&W, ramen (gissen) hoeveel mensen waar hadden gereisd. Met de OV-chipkaart zet de overheid in op het instandhouden van een landelijk dekkend betaalsysteem,[79] maar dan zonder de uniformiteit die bij gebonden tarifering van overheidswege hoort.[80] Een landelijk dekkend systeem levert immers vanzelfsprekend een schat aan managementinformatie op, zowel voor vervoerders als voor hen die toezicht houden.[81] Wel is dan vereist dat de strippenkaart geheel en al verdwijnt, want bij het behoud daarvan is ook het voortbestaan van de WROOV een gegeven. In dit (financiële) licht is het hoogst onfortuinlijk dat de OV-chipkaart op zoveel plaatsen veel langer dan gepland de strippenkaart naast zich heeft moeten dulden.[82]

Maar het is juist de gedwongen invoering van de OV-chipkaart die voor weerstand heeft gezorgd. Het gegeven dat ook abonnementhouders altijd[83] moeten in- en uitchecken riep een wrevel op die gerelateerd is aan het belang van autonomie (keuzevrijheid) en, in het verlengde daarvan, privacy. Het pijnpunt was (en is nog steeds) met name dat abonnementhouders niet over een anonieme chipkaart kunnen beschikken, en dus niet kunnen profiteren van de optionele anonimiteit waarvoor het Cbp zich vanaf het begin van het proces heeft ingezet.[84] Een ander discussiepunt, ook gerelateerd aan autonomie, was de mogelijkheid van *targeted advertising*: de mogelijkheid voor vervoerders om aan de hand van de door hun beheerde informatie doelgroepgerichte reclame te kunnen maken. Tot tevredenheid van het Cbp[85] heeft dit uiteindelijk geleid tot een autonomievriendelijk opt-in regime voor commerciële aanbiedingen.

*Privacy, een vreemd issue in de discussie over de OV-chipkaart*
Opmerkelijk genoeg bleek privacy een non-issue te zijn in het strijdgewoel van de

voor- en tegenstanders van de OV-chipkaart. Het overkoepelende bezwaar van het zich niet kunnen onttrekken aan de digitalisering van het openbaar vervoer is het enige noemenswaardige bezwaar tegen de OV-chipkaart dat direct aan privacy gerelateerd is dat in de maatschappelijke en politieke discussie is komen bovendrijven. De discussie ging vooral over de *kraakbaarheid* van de chip, en daarmee over de veiligheid en geloofwaardigheid van het systeem,[86] en over financiële tegenvallers van allerlei aard.[87] Hoewel technologische veiligheid in verband met privacy een belangrijke factor is (zie § 3.2), was de discussie over de kraakbaarheid van de chip toch niet de duiden als een discussie over privacy.[88] Illustratief is het feit dat de commissie-Meijdam (voorheen commissie-Leers), die was opgericht om de vele opstartproblemen met de OV-chipkaart tegen het licht te houden, in haar advies privacy weliswaar opsomt als een van de zaken waar een nieuw op te richten OV-autoriteit zich mee bezig moet houden, maar er verder geen woord aan vuil maakt.[89] Dit in tegenstelling tot Bart Jacobs, de leider van de onderzoeksgroep van de Radboud Universiteit[90] die, bij wijze van wetenschappelijke demonstratie, de betreffende chip (Mifare Classic[91]) kraakte. Hij noemt de kraakbaarheid een privacyprobleem van schokkende proporties, en spreekt van de chip als "open portemonnee"[92] en van databases waar de Stasi jaloers op zou zijn geweest.[93]

Een nadere blik op de informatiestromen die het OV-chipkaartsysteem creëert, leert dat de privacyrisico's neerkomen op 'gewone' databaserisico's. Niettemin acht Jacobs die risico's hoog genoeg om van een "privacy disaster" te spreken, met name gezien het feit dat kwaadwillende derden ongemerkt iemands kaart kunnen lezen.[94] Het moet gezegd – en dit is zeker geen triviaal gegeven – dat de risico's van identiteitsfraude in algemene zin altijd toenemen met de komst van elke nieuwe database,[95] evenzeer als de informatiemacht van politie en justitie toeneemt met elke nieuwe database (zie hierna).[96] Het systeem van de OV-chipkaart is in dat opzicht 'another brick in the wall' – om met Pink Floyd te spreken – en niet een steen in de vijver.

De rijkste informatiestroom, die uitvoerige persoonsgerelateerde informatie bevat, is aan de orde wanneer een houder van een persoonlijke, oftewel niet-anonieme, OV-chipkaart gebruikmaakt van de diensten van de vervoerder die hem of haar de betreffende kaart geleverd heeft. Het uitgangspunt van het systeem is namelijk dat alleen Trans Link Systems en de vervoerder waarbij de reiziger een abonnement houdt, de verplaatsingsgegevens van die persoon kunnen 'lezen'.[97] Trans Link Systems beschikt als enige over de volledige klantgegevens, maar deze worden operationeel gescheiden gehouden van de database met verplaatsingsgegevens.[98] Dit betekent – mits rigoureus doorgevoerd – dat dit bedrijf alleen adhoc-koppelingen kan maken tussen identiteiten en locatie-informatie,[99] en geen massale of systematische koppelingen. De vervoerder weet pas enige tijd na een verplaatsing[100] dat een

*bepaalde*, geïdentificeerde, klant op een *bepaald* tijdstip langs de RFID[101]-lezer op een *bepaalde* plaats kwam. Trans Link 'weet' dit pas weer enige tijd later; hoewel slechts latent, omdat de informatie wordt opgeslagen in een database die als het ware 'blind' is voor identiteiten.

De keuze voor een dergelijke identificatie door de vervoerder lijkt in het geval van abonnementhouders onvermijdelijk – er moet immers worden bepaald of iemand recht heeft op korting – maar is dat bij nadere beschouwing niet. In een recente publicatie betoogt het Rathenau Instituut dat het met een redelijk eenvoudige organisatorische faciliteit ook voor abonnementhouders mogelijk zou moeten zijn om anoniem te reizen.[102] Wat de meerkosten van zo'n oplossing zouden zijn, wordt niet vermeld. Ook Teepe en Jacobs wijzen er, op technologische gronden, op dat een betaalkaart zoals de OV-chipkaart niet noodzakelijkerwijs met identiteiten hoeft te werken (sterker: bij voorkeur niet). Tegelijkertijd merken ze op dat een alternatief technisch omslachtiger is, en bovendien nog in ontwikkeling.[103]

In ieder geval kunnen we constateren dat het gekozen systeem met verschillende 'informatieniveaus' werkt, waarbij het 'rijkste' hoogstpersoonlijk is en het 'armste' niet zonder meer te herleiden tot individuen; de centrale database vormt een soort middencategorie. De armste informatiestroom verloopt tussen de reiziger (via de incheckapparatuur) en een vervoerder waarmee de reiziger geen banden (abonnementen) heeft. In dat geval komt in het systeem van de vervoerder alleen de identiteit van de *kaart* voor (als substituut van volledige klantgegevens), in de vorm van een uniek nummer, en dus niet met een generieke en daarmee perfect koppelbare *identifier* als het BSN of iets dergelijks. Hetzelfde geldt in principe voor de overkoepelende database van Trans Link Systems, waarin uiteindelijk alle reisbewegingen terechtkomen.[104] Wel heeft dat bedrijf – overigens om begrijpelijke redenen[105] – ook een bestand met de naam, adres- en woonplaatsgegevens van alle houders; een bestand dat naast de database met reisbewegingen kan worden gelegd.[106]

Niettemin is een relativering van dit op zichzelf redelijk zorgvuldig opgezette arrangement op haar plaats. Dat alle overige informatie in principe armer is dan de informatie die de 'eigen' vervoerder verzamelt, is weliswaar relevant in het licht van privacy, maar niet doorslaggevend. Wie over voldoende doorzettingsvermogen beschikt, of in het geval van de overheid doorzettingsmacht, kan de ene database prima combineren met de andere. Niet voor niets vroeg het Openbaar Ministerie (OM) in het kader van een strafrechtelijk onderzoek bij Trans Link Systems pasfoto's op van mensen die zich op een bepaald tijdstip hadden opgehouden in een metrostation in Rotterdam, in een zaak die uiteindelijk tot aan de Hoge Raad voerde – en waarin het OM aan het kortste eind trok.[107]

Alles is uiteindelijk terug te vinden, gescheiden databases of niet. Ook met deze aanzienlijke relativering blijft het voor *location based privacy* echter relevant dat het OV-chipkaartsysteem waar mogelijk met redelijk arme[108] informatie werkt. Die relevantie komt met name naar voren als we kijken naar twee onderscheiden vormen van toegang tot databases (zie verder § 3.4): de gerichte variant van individueel uitvragen en de ongerichte, massale variant van datamining, waarbij wordt gezocht naar opvallende patronen in grote datasets. Met individueel uitvragen wordt hier bedoeld dat gericht wordt gezocht naar informatie over een bepaalde persoon. Dat is bij de OV-chipkaart onmiskenbaar aan de orde, onder alle voorwaarden en waarborgen die het recht daaraan stelt natuurlijk. Daartegenover staat dat het loslaten van massale datamining op combinaties van OV-databases niet snel zal worden geaccepteerd. Het wordt ook bemoeilijkt door de informatiearme aanpak, al is dit laatste uiteindelijk technisch te voorkomen.

Toch stelt de vordering van het OM in de Rotterdamse zaak ons hier enigszins voor een probleem. Het OM had namelijk geen verdachte in beeld, en vroeg zich juist daarom af welke personen zich op een bepaald tijdstip in metrostations Maashaven en Heemraadlaan hadden opgehouden. De vordering aan Trans Link Systems is voldoende bewijs dat gericht en ongericht zoeken in databases in elkaar overlopen. Het OM vroeg namelijk om een "lijst met daarop de barcodes [unieke kaartnummers, HMG] van de gebruikers van het tourniquetsysteem op de metrostations Maashaven en de Heemraadlaan in de nacht van 6 maart 2007 22:00 uur tot 7 maart 2007 00:00 uur, om te zetten in naam, adres, postcode, woonplaats en eventuele foto van deze gebruikers."[109]

*Privacy in OV vraagt om stevige publieke waarborgen*

Hoe dan ook: het is misschien maar goed dat privacy geen vooraanstaande rol speelt in de discussie over de OV-chipkaart. Het maatschappelijk vertrouwen in Trans Link Systems lijkt ook zonder die problematiek uitermate laag; een reden waarom de commissie-Meijdam heeft voorgesteld om alle beleidsbeslissingen bij het bedrijf weg te halen.

Gezien de vele manieren waarop publieke autoriteiten nog steeds zeggenschap hebben bij het openbaar vervoer, gaat het niet te ver om te stellen dat privacy in het openbaar vervoer vraagt om stevige, publieke waarborgen. De kaders waarbinnen Trans Link Systems functioneert geven echter geen enkele indicatie dat er publieke belangen in het spel zijn. Het enige dat de statuten van deze vennootschap melden op het inhoudelijke vlak, dus los van alle bedrijfsmatige regels, is het volgende (uit art. 2):

> "De vennootschap heeft ten doel het komen tot ontwikkeling en implementatie van het elektronische registratie- en betaalsysteem voor het openbaar vervoer in Nederland en al hetgeen tot het vorenstaande behoort of daaraan bevorderlijk kan zijn, een en ander in de ruimste zin des woords (...)"[110]

## 2.3 DE KILOMETERPRIJSREGISTRATIE

Net als de OV-chipkaart is de kilometerprijs een bestuurlijk en politiek pikant thema. Eveneens als bij de OV-chipkaart is de reden daarvoor niet primair gelegen in het privacyaspect van het dossier. In een overigens zeer kritisch advies over de Wet kilometerprijs besteedde de Raad van State bijvoorbeeld hoegenaamd geen aandacht aan privacy.[111] Niettemin is ook de kilometerprijsregistratie een markant voorbeeld van de digitalisering van de openbare ruimte. Dit onderwerp illustreert bovendien een geheel andere inzet van de overheid dan in het geval van de open platformen die hiervoor in het kader van de 'intelligente auto' zijn besproken.

Het stranden van deze laatste poging tot invoering van een gebruiksbelasting op 'automobiliteit', het programma Anders Betalen voor Mobiliteit en het wetsvoorstel voor de Wet kilometerprijs, past in een reeks van eerdere pogingen – over decennia – van de rijksoverheid, die eveneens in zwaar weer terechtkwamen en als het ware al buiten het parlement ten onder gingen. Een bekende eerdere aflevering uit deze saga betrof het concept MobiMiles, dat Roel Pieper in 2001 lanceerde, daartoe uitgenodigd door het toenmalige ministerie van V&W. Na een aanvankelijk positieve ontvangst sloeg de sfeer (in de media) binnen enkele dagen om, en verdween het idee stilletjes naar de coulissen.[112]

Het waren vooral maatschappelijke spelers die hierbij steeds een belangrijke rol hadden, zowel aan de vergadertafel als in het kanaliseren van het maatschappelijk sentiment. Zo kon het onderwerp kilometerbeprijzing, ondanks eerdere mislukkingen, onder de noemer Anders Betalen voor Mobiliteit opnieuw op de rol komen omdat de ANWB zich achter een eventueel nieuw initiatief had geschaard,[113] daartoe bewogen door de nieuwe technologische mogelijkheden. Zoals bekend is het wetsvoorstel toch gestrand. Hoewel het voorstel formeel tot in de demissionaire fase van het kabinet-Balkenende IV aangehouden is, was zijn lot al enige tijd eerder beslecht. De toenmalige minister van V&W, Eurlings, zag zich namelijk geconfronteerd met een toenemende weerstand tegen de kilometerbeprijzing. Hij bepaalde daarop dat een ledenraadpleging die de ANWB – intussen weer een kritische speler[114] – over het onderwerp wilde houden, de doorslag moest geven. Deze raadpleging pakte voor de kilometerprijs negatief uit.

*Twee sporen, verschillende technologieën*
Als het gaat om ICT en informatiestromen, was het plan Anders Betalen voor Mobiliteit nadrukkelijk tweeledig.[115] In principe zouden commerciële spelers een grote rol vervullen in het geheel en de overheid zou alleen op de achtergrond meekijken. Wel zou bij de introductie van de kilometerregistratie in eerste instantie een andere, behoedzamer opzet gelden, met een veel nadrukkelijker rol voor de overheid. De commerciële variant, het middellangetermijnperspectief, werd aangeduid als 'het hoofdspoor' en de behoedzame, door de overheid gegarandeerde, variant als 'het garantiespoor'.

De twee sporen behelzen verschillende technologieën. In het garantiespoor was sprake van een registratieapparaat (hierna: kastje) dat onder nauwlettend toezicht van de overheid zou worden geproduceerd en ingebouwd. Een wezenlijke karakteristiek van dit kastje was dat deze niet alleen verplaatsingen zou registreren, maar ook rekencapaciteit zou hebben.[116] Deze rekencapaciteit onderscheidde het garantiespoor van het hoofdspoor. De 'garantie' van dit arrangement zou er immers in bestaan dat de verplaatsingsgegevens te allen tijde in het kastje verborgen zouden blijven (voor derden[117]) zodat niemand kon nagaan waar een automobilist gereden had. Met andere woorden: het kastje was een zorgvuldig ontworpen black box met als output het aantal per tariefsoort gereden kilometers (spitstarief of normaal tarief; zie hierna). De verdere berekening, gelet op tarieven voor het tijdstip van rijden en voor de milieubelasting van de auto, zou plaatsvinden bij de RDW, waar de gegevens van alle kastjes zouden moeten binnenkomen. Het Centraal Justitieel Incassobureau zou de door de automobilist verschuldigde gelden vorderen. Over de hele linie zouden de respectievelijke verantwoordelijkheden van de diverse informatieverwerkers helder moeten worden gemarkeerd, geheel in de geest van de Wet bescherming persoonsgegevens (Wbp). Bij deze hele streng van informatiedoorgifte zou de locatie-informatie in het kastje besloten blijven, zo verzekerde de regering.[118]

Uiteindelijk genoot het (vooruitzicht van het) hoofdspoor toch de voorkeur van de regering.[119] Bij dit spoor gaat het om heel andere informatiestromen, en een ander financieel plaatje. Dienstverleners zouden op contractuele basis (direct met de automobilist) de registratie van de kilometerprijs op zich kunnen nemen. De mogelijkheden voor het delen van en handelen in informatie zouden hierdoor veel groter zijn dan in het garantiespoor. Dat is ook onvermijdelijk aangezien de bedrijven in kwestie, in feite *information brokers*, een verdienmodel nodig hebben om in zo'n avontuur te stappen. Voor de klant zijn het interactieve diensten, voor de provider gaat het om een schat aan informatie: het model is bekend. Locatiegegevens zouden optioneel kunnen worden gedeeld en commercieel aangewend, maar met de uitdrukkelijke 'mits' dat alle differentiatie in het productaanbod volgens de regering

– met wettelijke sanctie – moest berusten op de uitdrukkelijke toestemming van de automobilist. Een absolute primeur was het idee, met de nodige slagen om de arm, om de belastingheffing en -invordering op termijn eveneens langs private weg te organiseren.

*Een amorfe privacydiscussie*
Bij de maatschappelijke discussie die deze versie van een gebruiksbelasting op automobiliteit de kop kostte, werd privacy vaak genoemd, maar op een vrij amorfe manier. De voorzichtigheid waarmee het project was aangevat[120] en die ook in de technologie zelf (althans van het garantiespoor) belichaamd had moeten worden, beklijfde niet. Als we privacybescherming opvatten als een afweging tussen de maatschappelijke voordelen die met een bepaald plan zijn gemoeid en de individuele privacynadelen die daarvoor geïncasseerd moeten worden, dan ging de maatschappelijke discussie over de kilometerprijs vooral over de geloofwaardigheid van de voordelen die de regering had voorgespiegeld. Er waren veel bedenkingen bij de differentiatie van tarieven; het spitstarief werd al snel geassocieerd met 'betaald in de file staan'. Dit idee werd versterkt doordat er in de media twijfels werden geuit over de door de regering geschetste effecten voor de doorstroming.[121]

De *raison d'être* van een gebruiksbelasting is dat zij mensen bewuster maakt van hun mobiliteitskeuzes en dat die keuzes daardoor per saldo rationeler uitvallen. Of deze, op zichzelf logische, gedachte zich ook echt zou manifesteren, werd op een gegeven ogenblik openlijk betwijfeld. Wanneer een voorstel om medestanders verlegen zit, moet de 'doorberekening' van de beleidsdoelen vaak helpen overtuigen. Is er in zo'n geval twijfel over de cijfers, dan kan het hele construct gaan rammelen. In veel gevallen gebeurt dit niet bij ICT-projecten, omdat deze niet 'gepolitiseerd' worden, net zo min als publieke besluitvorming over verkeer en vervoer gepolitiseerd wordt.[122] De wegenbelasting is hierop echter de markante uitzondering die de regel bevestigt.

## 2.4 ANPR

Automatische kentekenherkenning (ANPR) is in zekere zin een lot uit de loterij. Voor de handhaving van allerlei regels, of die nu tot het strafrecht, belastingrecht of sociaal recht behoren, is ANPR een uitzonderlijke steun in de rug. De techniek kan gebruikt worden om mensen (die daar aanleiding toe geven) stante pede uit het verkeer te lichten met behulp van een mobiele brigade. Of zij kan zich later terugverdienen doordat de kennis van de locatie waarop iemand zich op een bepaald tijdstip bevindt, onderdeel gaat uitmaken van een dossier, van belastend bewijs van overtreding van een wettelijke norm. ANPR biedt twee toepassingen die zorgvuldig moeten

worden onderscheiden, omdat ze rechtsstatelijk gezien zeer verschillend zijn terwijl ze technologisch hand in hand gaan.[123] Ten eerste onderscheiden we gerichte kentekenherkenning. Aan de hand van een tevoren opgestelde lijst met kentekens (het 'vergelijkingsbestand') kan volautomatisch nagegaan worden welke personen (kentekens) van die lijst een bepaalde camera passeren; zo kan hun locatie geverifieerd worden. De lijsten in kwestie zijn potentieel enorme databases waarin iedereen kan zijn opgenomen die ergens geregistreerd staat, of dat nu is omdat hij of zij een boete niet betaald heeft of rijdt in een leaseauto waarvoor in bepaalde omstandigheden belastingvoordeel wordt genoten. Met technologisch gezien bijna evenveel gemak (gelet op de lage kosten van dataopslag) kan sprake zijn van een tweede toepassing van ANPR: ongerichte kentekenherkenning. Hierbij worden *alle* passerende kentekens geregistreerd en opgeslagen, voor toekomstige opsporingen. Technologisch gezien is het verschil tussen beide toepassingen triviaal: in de eerste variant worden alleen de zogenaamde 'hits' bewaard,[124] in de tweede ook de 'no-hits'.[125]

ANPR is geen toekomstmuziek, maar een toepassing die al op grote schaal in werking is gesteld. Momenteel tellen de Nederlandse[126] wegen,[127] afgaande op de spaarzame parlementaire stukken over het onderwerp, minstens honderd installaties;[128] het is echter denkbaar dat er op termijn duizenden ANPR-camera's zullen hangen/staan. Lange tijd werd de technologie zelfs gebruikt terwijl een wettelijke grondslag of een publieke discussie van enigerlei soort ontbrak. Sinds begin 2010 is de ongerichte kentekenherkenning opgeschort, in afwachting van een wet die intussen in concept is gepubliceerd.[129] Deze wet moet alsnog een grondslag bieden voor ongerichte kentekenherkenning met als doel opsporing en vervolging van personen.

De wijze waarop ANPR geïntroduceerd is, inclusief het conceptwetsvoorstel, roept een beeld op van een rechtsculturele niche waarin 'buitenwettelijk pionieren' bijzonder mild wordt beoordeeld. Zowel regionale spelers, zoals politiekorpsen, als nationale spelers, zoals de Belastingdienst en inspecties, zagen vrij snel het enorme potentieel dat ANPR biedt voor kostenefficiënte handhaving van strafrechtelijke, bestuursrechtelijke en fiscale voorschriften.[130] Deze als het ware 'automatische herkenning' van handhavingskansen kon zonder gemor leiden tot een al even automatische benutting van die kansen. Van Ooijen constateert op basis van sociaalwetenschappelijk onderzoek bij een politiekorps dat de gebruikers van ANPR nogal pragmatisch aankijken tegen de juridische randvoorwaarden en grenzen aan de technologie; zij zien in juridische discussies vooral een gevaar voor de ongehinderde doorgang van de ontplooide initiatieven.[131]

De voorgeschiedenis van het voorliggende (concept)wetsvoorstel valt in hetzelfde licht te bezien. Pas toen het Cbp in januari 2010 voor de tweede keer aangaf dat

de ongerichte kentekenherkenning niet zonder speciale wettelijke grondslag kon plaatsvinden,[132] riep de regering die praktijk een halt toe. Waarbij zij direct aangaf zo snel mogelijk alsnog in die grondslag te willen voorzien.[133] Daaraan voorafgaand had ook de commissie-Brouwer-Korf, die uitdrukkelijk was gevraagd zich mede over ANPR te buigen, slechts in het voorbijgaan opgemerkt dat de wettelijke basis van de technologie "dun" was.[134] Gezien deze coulance was te verwachten dat het conceptwetsvoorstel niet in het teken staat van de innerlijke noodzaak van wettelijke verankering en inkadering van een ingrijpend opsporingsmiddel. Eerder is sprake van het overwinnen van een hindernis waarachter dit felbegeerde instrument was blijven haken. In het concept voor de memorie van toelichting worden vonnissen geanalyseerd van strafrechters die met de oorspronkelijke waarborgloze toestand geworsteld hebben, omdat ze voor de lastige vraag stonden of het bewijs verkregen uit ANPR kon worden toegelaten; het resultaat van hun worsteling liep uiteen.[135] De toelichting op het conceptwetsvoorstel haalt deze zaken puur aan ter illustratie van de rijkdom aan informatie die met ANPR kan worden opgediept, ter adstructie van de door niemand weersproken stelling dat ANPR veel nut heeft voor opsporing en vervolging. Ook de ervaring die is opgedaan met toenmalige "illegale" ANPR-praktijken wordt zo als waardevolle input opgevoerd. We lijken hier te maken te hebben met de experimentele overheid in optima forma.

Een ander probleem is het feit dat de praktijk van gerichte kentekenherkenning, aangezien die in het conceptwetsvoorstel buiten beschouwing blijft. De toelichting beredeneert waarom hiervoor geen regeling nodig zou zijn: gerichte ANPR is een *common sense*-onderdeel van het politiewerk. De algemene politietaak (in de zin van de Politiewet) zou – onder fiat van het Cbp[136] – een voldoende grondslag zijn om met ANPR een 'digitale zeef' door al het autoverkeer te halen, zo is de aanname. Hoe ingrijpend deze technologie kan zijn – van een gemiddelde automobilist worden in de toekomst dagelijks misschien tientallen locaties bewaard – lijkt niet te zijn doorgedrongen tot de 'powers that be', en evenmin tot de meeste burgers. Er is over ANPR maar af en toe iets in de media te lezen.[137] Een verklaring hiervoor is misschien dat de opstelling van minister Opstelten van Veiligheid & Justitie stilzwijgend op massale instemming kan rekenen. Opstelten merkte over ANPR op: "Is het nu een raar idee dat de techniek zijn gang kan gaan?"[138] En hij karakteriseerde zijn eigen ethos als "een bewindspersoon die strak, maar wel zorgvuldig de grenzen opzoekt om het opsporingsbelang te dienen".[139] De schriftelijke vragen over ANPR van het Kamerlid Çörüz illustreren bovendien dat als de Tweede Kamer digitale *surveillance* aan de kaak stelt, dit evengoed kan zijn ingegeven door de opvatting dat de techniek nog niet genoeg 'zijn gang kan gaan'.[140]

# 3 FACTOREN VOOR *LOCATION BASED PRIVACY*

De in het vorige hoofdstuk beschreven toepassingen van ICT voor de mobiliteitssector bieden een breed palet aan technologieën en bestuurlijke contexten. Hoewel al veel punten zijn aangestipt die van belang zijn uit het oogpunt van de persoonlijke levenssfeer, is er meer nodig om mobiliteitsapplicaties vanuit privacyperspectief de maat te nemen. Zo is het vruchtbaar om privacy in dit kader te begrijpen als (de mogelijkheid van) *selective disclosure*, hier specifiek de selectieve ontsluiting van locatie-informatie. Maar wat bepaalt nu de kracht of zwakte van het bouwwerk van privacy? In dit hoofdstuk zal ik alle applicaties spiegelen aan een aantal factoren die bepalen hoe geloofwaardig privacy(bescherming) is, zoals veiligheid van de technologie, secundair gebruik van informatie enzovoorts. Dit is de eigenlijke analyse, die ons in staat moet stellen een eindoordeel te vellen over de stand van 'privacy onderweg'.

## 3.1 GEVOELIGHEID VAN INFORMATIE

Locatie-informatie is zoals gezegd als zodanig geen bijzonder gevoelige categorie van informatie. De gevoeligheid van informatie, zoals dat criterium ook in de Wbp tot uitdrukking komt, wordt bepaald door de mate waarin zij iets over de persoonlijkheid zegt. Locatie-informatie is naar haar aard uitwendig en zakelijk. Een persoon die 'gepeild' wordt, wordt vastgepind op een bepaalde coördinaat en een bepaald tijdstip. We hebben het dan bij uitstek over wetenschappelijke ruimte en wetenschappelijke tijd,[141] oftewel over onvermurwbare feitelijkheden. Wel is duidelijk dat het bij locatie-informatie ook om persoonsinformatie gaat. Informatie over de plek waar iemand (of iemands voertuig) zich op een bepaald moment bevond, is in principe herleidbaar tot die persoon.[142] Dus meestal levert deze data persoonsinformatie op. Dat is ook het geval als voor het 'herleiden tot een bepaalde persoon' enige moeite moet worden gedaan, zoals bij ANPR, waar met kentekens in plaats van met namen wordt gewerkt.[143] Dit is alleen anders wanneer de informatie volstrekt geanonimiseerd is, bijvoorbeeld voor analysedoeleinden. Zulke anonieme, geaggregeerde informatie is in mobiliteitsland voor veel partijen waardevol. Maar met de aantrekkelijkheid van geaggregeerde informatie – een in principe onschuldige informatiesoort – komt het des te meer aan op de (technische, bestuurlijke) garanties dat hetgeen als geanonimiseerd te boek staat niet door een soort *reverse engineering* weer tot personen te herleiden is. Op deze verhoogde inzet voor het technisch (en organisatorisch) ontwerp ga ik de volgende paragraaf nader in.

Overigens blijkt uit de recente mediastorm over de (indirecte) verkoop van geaggregeerde snelheidsinformatie van de openbare weg door TomTom aan de politie, en de geschrokken reactie van TomTom zelf op alle ophef,[144] dat veel mensen ook geanonimiseerde en geaggregeerde informatie als gevoelig beschouwen.[145] Of de ophef betekent dat het publiek niet doorhad dat het om anonieme, geaggregeerde informatie ging.

Bij locatie-informatie spreken we dus over een (*an sich*) relatief weinig ingrijpende informatiesoort die niettemin het beschermen waard is. Die bescherming is vervat in de Wbp, met zijn welbekende speerpunten van doelbinding en dataminimalisatie, en de centrale plaats voor toestemming van de persoon om wie het gaat. Deze uitgangspunten zijn uiteraard van groot belang voor allerlei commerciële en bestuurlijke initiatieven op mobiliteitsgebied. Doelbinding zal hierna aan de orde komen in relatie tot het secundair gebruik van informatie (§ 3.4), en dataminimalisatie in relatie tot *accountability* (§ 3.6). Evenzeer als deze uitgangspunten gemeengoed zijn, is het bijna een open deur om te zeggen dat ze dikwijls onder druk komen te staan – ook met betrekking tot het onderhavige onderwerp, en om uiteenlopende redenen.

In relatie tot de aard van de informatie en het beschermingsniveau dat daarbij hoort, zijn de uitgangspunten van de Wbp om nog twee redenen te relativeren. In de eerste plaats komt deze wet in vergelijking tot andere wetten geen bijzondere rang toe. De bescherming van persoonsgegevens is geen constitutionele of fundamentele aangelegenheid,[146] dit in tegenstelling tot het grondrecht op privacy waar het weliswaar veel mee te maken heeft, maar niet mee samenvalt.[147] Zodra de introductie van een technologische applicatie gepaard gaat met een speciale wettelijke regeling (die daarmee 'voor gaat' op de Wbp), is het dus heel goed mogelijk dat uitgangspunten van de Wbp op het tweede plan komen. In deze studie is in twee gevallen een wettelijke regeling voorzien: het (gestrande) wetsvoorstel voor de kilometerprijs en het conceptwetsvoorstel om het gebruik van ANPR in de strafvordering te regelen.

Een tweede relativering betreft een beperking die het kijken door de lens van de bescherming van persoonsgegevens met zich meebrengt. Hoe waardevol de uitgangspunten van de Wbp (die overigens al heel lang mee gaan, binnen en buiten Nederland[148]) ook zijn, ze laten toch een deel van de risico's van het hedendaags 'genetwerkt' informatiegebruik buiten beeld. Die risico's betreffen vooral interpretatiefouten bij 'gestapeld' informatiegebruik, in combinatie met de veranderde ambities die men met informatie heeft, met name de praktijk van prognosticeren via profielen. Wie die risico's onderkent, richt de kritische aandacht meer op de *processen* van informatiegebruik, zoals het samenvoegen van informatiebronnen en

het maken van profielen, dan op de *aard* van de informatie.[149] Mobiliteitsinformatie wordt bij uitstek gebruikt voor het herkennen van gedragspatronen, en kan zo een grotere impact hebben dan de propositie 'persoon P was op tijdstip t op locatie x, y' doet vermoeden. Op het moment dat een individueel[150] gedragspatroon wordt opgetekend, verschuift de onvermurwbare feitelijkheid van locatie-informatie een stuk in de richting van het persoonlijke of zelfs existentiële. Ook de Europese 'Artikel 29 Werkgroep' (het netwerk van nationale privacytoezichthouders) signaleert dat "the movement patterns of the [smartphone] devices provide a very intimate insight into the private life of the owners".[151] Als iemand een profiel van je maakt, dan voelt dat aanmatigend, ook (of juist) als dat profiel (b)lijkt te kloppen.

Bij ANPR doet zich een specifieke praktijk ten aanzien van profielen voor. Bij de gerichte variant van kentekenherkenning worden vergelijkingsbestanden opgesteld die in feite bepalen wie – wat voor 'soort mensen' – er uit de verkeersstroom gelicht wordt. Het samenstellen van die bestanden is daarmee nogal gevoelig, terwijl er geen enkele specifieke wettelijke regeling voor is opgesteld. Het ligt voor de hand dat de vergelijkingsbestanden worden opgesteld met behulp van profielen: in het kader van *preventive policing* gaat het er om mensen in beeld te hebben nog voordat zij in strafrechtelijke termen in beeld (kunnen) zijn. Dat betekent dat die mensen uit de massa gelicht worden die daar op basis van hun profiel aanleiding toe geven. Het gevaar ligt al snel op de loer dat de profielen in kwestie discriminatoir of stigmatiserend zijn. Een paradoxaal gegeven dat uit het Europese Schengen-recht voortvloeit, is dat het politieoptreden rond de landsgrenzen (waarbij ANPR intensief gebruikt wordt) eigenlijk zo discriminatoir mogelijk moet zijn – gericht op het onderscheppen van illegalen, drugsrunners enzovoorts.[152] ANPR van het profilerende soort kan bij deze Europese opdracht een belangrijke steun in de rug zijn.

## 3.2 TECHNOLOGISCHE BETROUWBAARHEID

Bij de toepassingen die in dit essay worden besproken, komt veel aan op het technisch ontwerp en de organisatorische inbedding van dat ontwerp. Technische betrouwbaarheid is duidelijk een factor van privacy. Veel van de geboden garanties – bijvoorbeeld dat verschillende soorten informatie niet met elkaar vermengd worden, dat bepaalde informatie niet gedeeld wordt enzovoorts – staan of vallen bij de kwaliteit en betrouwbaarheid van de techniek, in combinatie met de wijze waarop organisaties zijn ingericht (door middel van autorisatie van personen e.d.) met betrekking tot die techniek. De kilometerprijsregistratie kan als voorbeeld dienen voor garanties die niet anders dan technisch kunnen worden vormgegeven. De Memorie van Toelichting bij de Wet kilometerprijs verzekerde dat het 'kastje' de gegevens over de locaties – alle individuele ritgegevens dus – angstvallig bij zich zou houden, en deze

niet zou delen met de inningsorganisatie[153] noch met de tussenpersoon.[154] Het kastje zou zelf berekenen hoeveel kilometers er tegen welk tarief gereden waren, en alleen die verwerkte informatie delen. Dit gegeven was de spil van de Wet kilometerprijs, en de oplossing die ervoor moest zorgen dat het project Anders Betalen voor Mobiliteit wél de eindstreep zou halen, in tegenstelling tot eerdere pogingen.

De techniek moest bij de kilometerprijsregistratie de privacybelofte waarmaken. Daar is op zichzelf niets mis mee. Maar informatietechnologie staat niet voor niets bekend als 'verbinder'; het vergt veel om die karakteristiek te onderdrukken. Hoe zorgvuldig men ook is geweest en hoe terughoudend de opzet van het systeem voor kilometerbeprijzing ook was, een vraag blijft hangen die kenmerkend is voor het digitale tijdperk: hoe kan de gebruiker zekerheid krijgen dat het kastje de informatie die het verzamelt, echt niet deelt? De ritgegevens moeten immers in het apparaat worden opgeslagen om er een berekening op uit te kunnen voeren, en het kastje is hoe dan ook een zender. Het antwoord op deze vraag luidt dat dat niet met zekerheid te zeggen is, maar dat de initiatiefnemers (in dit geval de overheid) ons verzekeren dat het *niet* gebeurt. De situatie is niet fundamenteel anders dan bij een recente internationale rel rond de iPhone van Apple. Deze apparaten blijken permanent locatiegegevens in hun geheugen op te slaan.[155] Ook hier moeten we het met de verzekering doen dat het apparaat deze informatie niet verzendt.[156] Maar zelfs als een apparaat (of dat nu een kilometerprijs-kastje of een iPhone is) de opgeslagen informatie niet verzendt, kan deze informatie nog steeds uit het apparaat zelf worden uitgelezen, en zo soms voor rare verrassingen zorgen. Dit is bijvoorbeeld het geval bij de zogenaamde *On Board Diagnostics* van veel auto's. Dit systeem ziet in principe toe op het technisch functioneren van de motor, maar kan ook dienen als 'geheugen van de auto' en kan de politie zodoende informatie verschaffen over het rijgedrag.[157]

Er zijn nog tal van voorbeelden te noemen waarin de voorgeschotelde technische afscherming van (locatiegerelateerde) informatie uiteindelijk op vertrouwen berust. Bij de totstandkoming van de toepassing eCall is bijvoorbeeld verzekerd dat de zender in de slaapstand staat zolang er geen beroep op wordt gedaan.[158] Met andere woorden: de GPS-informatie die voortdurend wordt gegenereerd, blijft in de auto. En, om het belangrijke onderwerp van anonieme, geaggregeerde data weer op te pakken, in het kader van de inzet van ANPR voor (verkeerskundige) analysedoeleinden moet men er op kunnen vertrouwen dat geanonimiseerde data niet weer kunnen worden ontsleuteld tot persoonlijke data.[159] Voor gebruik van geanonimiseerde data gelden (met reden) aanmerkelijk minder hoge drempels dan voor niet-geanonimiseerde data, maar dan moet het geanonimiseerde karakter wel helemaal vaststaan. Exact dezelfde vertrouwenskwestie speelt bij de samenwerking tussen TomTom en Vodafone.[160]

Alle applicaties waar de digitale overheid op draait zijn op de tekentafel begonnen. De consultants en ICT'ers die een applicatie ontwerpen, doen dat om begrijpelijke redenen bij voorkeur modulair: door verschillende onderdelen van applicaties als een soort *prefab*-bouwstenen in te richten kan het totale ontwerp eenvoudig aangepast worden aan de (veranderende) wensen van de klant. Als die klant de overheid is, dan valt te verwachten dat er een bovengemiddelde aandacht voor 'technische schotten' wordt gevraagd, maar evenzeer dat de vereisten bij gewijzigd politiek inzicht gaandeweg kunnen worden aangepast. Daarom worden de schotten zo ingericht dat zij redelijk eenvoudig te verwijderen of te versterken zijn.[161] Deze praktische aanpak mag bedrijfsmatig gezien heel goed voorstelbaar zijn, het maakt de integriteit van de technische schotten, waar zoveel van afhangt, er niet sterker op.

Technologische betrouwbaarheid heeft, zoals gezegd, ook een organisatiecomponent. Die is duidelijk verankerd in de Wbp, met zijn regels over beveiliging van en toegang tot persoonsgegevens. Op dit punt tikt het Cbp bedrijven en overheidsorganisaties regelmatig op de vingers. Onlangs nog stelde het vast dat het systeem van autorisaties met betrekking tot het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) niet deugde, vooral bij de politiekorpsen. Het CIOT is een database die permanent wordt ververst met de 'verkeersgegevens' van de klanten van telecomaanbieders; het is ingericht voor de strafvorderlijke bevoegdheden van opsporingsambtenaren. Zo kunnen bevoegde instanties toegang krijgen tot de telecomgegevens van alle mensen die zich in Nederland bevinden, inclusief de locatiegegevens van hun mobiele telefoons. Er is het nodige te doen geweest over de miljoenen keren per jaar dat Nederlandse overheidsorganisaties dergelijke gegevens uit het CIOT opvragen. Een van de onderliggende redenen achter dit extreem hoge aantal is dat politiekorpsen te coulant omspringen met autorisaties, door die vaak ofwel niet te regelen ofwel niet te handhaven.[162] Het doet denken aan het verhaal van enkele jaren geleden, dat een groot aantal onbevoegde politieambtenaren uit nieuwsgierigheid het strafdossier hadden ingekeken van de voetballer Van Persie, die in verband was gebracht met een zedenzaak. Men kan zich afvragen of tegen een dergelijke cultuur van nonchalance over autorisaties veel te doen valt. Op papier mag een systeem van autorisaties een mooie constructie zijn, op de werkvloer is de situatie beduidend ambivalenter.[163] Onbedoeld echter komt met deze nonchalance wel een van de pijlers van technologische betrouwbaarheid op losse schroeven te staan. Dit klemt temeer omdat toch al vrij veel functionarissen bij de betreffende informatie kunnen komen, of dat nu bevoegde opsporingsambtenaren zijn of particuliere *controllers*.[164]

## 3.3 HOUDBAARHEID

Nadenken over de implicaties van informatietechnologie in allerlei contexten komt vaak neer op nadenken over de implicaties van een revolutionair toegenomen *opslagcapaciteit*. Het thema 'bewaren' – de houdbaarheid van informatie – vormt ook in de context van dit essay een waterscheiding tussen het pre-ICT-tijdperk en de situatie waarin we ons nu bevinden. De in de inleiding genoemde trivialisering die volgt uit het feit dat iedereen in het openbaar met het blote oog geobserveerd kan worden, vormt met name een drogreden omdat het de impact van technologische opslagcapaciteit miskent. De ongeclausuleerde lancering van ANPR vormt hiervan een treffende illustratie.

Natuurlijk is het zo dat iedereen altijd al kon worden waargenomen op de openbare weg. Maar deze niet-ondersteunde waarneming 'van weleer' was vele malen vluchtiger dan de door de technologie ondersteunde waarneming, die vaak nog slechts op een metaforische manier lijkt op de zintuiglijke (vooral visuele) waarneming waar zij mee geassocieerd wordt.[165] In het Amerikaanse privacydebat wordt dit verschil in zichtbaarheid tussen 'toen' en 'nu' soms aangeduid met behulp van de term *practical obscurity*.[166] Hier bedoelt men het volgende mee: *in praktische zin* was iedereen in het verleden veel onzichtbaarder, ook als men zich bijvoorbeeld op de openbare weg in het volle zicht bewoog. Dus de persoonlijke levenssfeer werd weliswaar niet principieel maar wel feitelijk gewaarborgd door de beperkingen van het waarnemingsvermogen en van het geheugen, en de implicaties van fysieke afstand.

Intussen kan die praktische onzichtbaarheid potentieel voor een groot deel ongedaan worden gemaakt door de rijkdom aan informatie die door ICT wordt gegenereerd en voor toekomstig (her)gebruik wordt opgeslagen. Dat potentieel wordt in toenemende mate aangeboord door commerciële en bestuurlijke toepassingen van locatietechnologie. Opvallend in dit kader is dat ook de toelichting op het conceptwetsvoorstel ANPR deze omslag van zintuiglijke naar technologisch ondersteunde waarneming trivialiseert. Hierbij leunt men sterk op de deels expliciet gemaakte stelling dat het waarnemingsvermogen van politieagenten zich niet wezenlijk onderscheidt van technologisch waarnemingsvermogen. De techniek is niets meer dan een 'extension of man', om een woord van Marshall McLuhan te gebruiken. Literatuur over digitale *surveillance* laat doorgaans echter een ander beeld zien: technologische waarneming is oneindig veel indringender, blijvender en onverbiddelijker.[167] Echt curieus wordt het als in de toelichting de EHRM-uitspraak *Peck-Verenigd Koninkrijk*[168] wordt aangehaald ter ondersteuning van de stelling dat gerichte kentekenherkenning onvoldoende ingrijpend is om als inbreuk op een grondrecht te kunnen gelden. Maar dat arrest benadrukt nu juist dat de kwalitatieve sprong van

menselijke waarneming naar technologische waarneming om een nieuw 'mensenrechtelijk' perspectief vraagt.

Discussies over het bewaren van gegevens worden wel gevoerd met betrekking tot individuele applicaties. Het meest uitgebreid was de discussie over het bewaren van de verkeersgegevens van telefonie, waaronder de locatie-informatie die door mobiele telefoons wordt voortgebracht. Op Europees niveau was er een felle discussie over de zogenaamde Dataretentierichtlijn.[169] Hoewel velen vermoedden dat deze Richtlijn de privacybepaling (art. 8) van het Europees Verdrag voor de Rechten van de Mens (EVRM) schond, vanwege de disproportionaliteit van het ingezette middel, kwam deze er uiteindelijk wel.[170] Vervolgens ontstond in Nederland een langlopende discussie over de manier waarop deze Richtlijn geïmplementeerd diende te worden. Eerst de Tweede Kamer en vervolgens de Eerste Kamer bedong daarbij een verkorting van de door de regering voorziene bewaartermijn.[171] Ook de bewaartermijn van het conceptwetsvoorstel ANPR geeft aanleiding tot discussie,[172] en recent heeft het Cbp zich ingespannen om de bewaartermijnen van verschillende spelers rond de OV-chipkaart te bekorten.[173] Steeds moet de afweging gemaakt worden tussen enerzijds het (privacy)belang van 'vergeten' en anderzijds het maatschappelijk nut dat in de toekomst kan voortvloeien uit de bewaarde informatie, met name doordat criminelen in de kraag kunnen worden gegrepen. Dat is geen sinecure: het eerste belang (vergeten) is vaag, en het tweede (nut in de toekomst) is speculatief.

Er worden dus deeldiscussies gevoerd over en deelafwegingen gemaakt voor het belang van bewaren versus vergeten. Maar daarmee is de erosie van de *practical obscurity* nog niet in beeld, omdat dit plaatje wordt bepaald door de opstapeling van verschillende technologieën en applicaties die tegelijkertijd de openbare ruimte bevolken. Bovendien herbergt het dilemma bewaren versus vergeten een nogal taaie praktische problematiek, die met het keurig afspreken van termijnen niet is opgelost. Het blijkt namelijk maar al te vaak dat de bewaartermijnen bijvoorbeeld door politie en justitie niet worden nageleefd.[174] Zoals we hierboven ook al vaststelden met betrekking tot autorisaties: er zit een forse ('bedrijfs')culturele component in deze problematiek.

## 3.4 SECUNDAIR GEBRUIK

Secundair gebruik van informatie is tegelijkertijd een van de drijvende krachten achter het succes van ICT en een van de meest spanningsvolle aspecten van ICT voor de persoonlijke levenssfeer. Secundair gebruik kan worden gedefinieerd als gebruik dat niet voorzien werd op het moment dat de data vergaard werden, en/of niet past bij het doel waarvoor de data oorspronkelijk vergaard werden. Het impliceert bijna

per definitie dat informatie uit de oorspronkelijke (informationele) context wordt gehaald, en in een nieuwe wordt ingepast.

Secundair gebruik van informatie heeft doorgaans een sterke *business case*, maar evenzeer een sterke *regulatory case*. Wat het verkopen van informatie is voor commerciële dienstverleners, is het koppelen van informatiebestanden voor het openbaar bestuur. Wat productinnovatie is voor de een, is – veelal evenzeer bewuste – *function creep* voor de ander. Bovendien is het openbaar bestuur ook niet wars van onvervalste *business cases*. In de eerste plaats – overheidsintern gezien – omdat er meer wordt gestuurd op kostenefficiënt beleid. In de tweede plaats omdat ICT-innovatie een belangrijke economische kracht is die de welvaart van een land bevordert.

Secundair gebruik kent twee soorten dilemma's die de overheid bij het ontwerp van een applicatie tegenkomt. Enerzijds is er de vraag welk secundair gebruik van informatie zij zichzelf wil toestaan. Bijvoorbeeld: moet zij toestaan dat databases met locatie-informatie verkregen uit ANPR worden gekoppeld aan databases uit de sociale zekerheid, om na te gaan of mensen zich qua gedragspatroon wel manifesteren als bijstandsgerechtigde? Of is zo'n koppeling te ingrijpend? Anderzijds is er de vraag wat de overheid aan commerciële of semipublieke dienstverleners wil toestaan, als het gaat om het verwerken van – en verdienen aan – locatie-informatie. Moet zij toestaan dat de OV-bedrijven de informatie die zij door de OV-chipkaart bezitten, aanwenden voor *targeted advertising*?

Het bedrijfsmatige model dat zo innig verbonden is met de opkomst van informatietechnologie laat ook de overheid niet onberoerd. Dit is het model waarbij het verbinden van functionaliteiten en het vernetwerken van informatie meerwaarde oplevert. De spanning tussen dit model enerzijds en de meer klassieke taken van de overheid anderzijds komt sterk terug bij de ICT-applicaties op mobiliteitsgebied. De Memorie van Toelichting bij de Wet kilometerprijs flirtte bijvoorbeeld voorzichtig met de open-platformgedachte, terwijl de kaarten uiteindelijk werden gezet op een *dedicated* (dichtgetimmerd) systeem.[175] Enerzijds werd het 'kastje' neergezet als een interessant knooppunt voor allerlei aanvullende diensten, anderzijds durfde men het om privacyredenen niet aan dat knooppuntkarakter van meet af aan te ontsluiten. Andere beleidsbeslissingen daarentegen zijn al eerder in de technologische ontsluitingsmodus gezet. Zo is al geruime tijd geleden besloten de ruwe publieke verkeersdata (met name verzameld door Rijkswaterstaat) gratis ter beschikking te stellen van bedrijven die er informatieproducten op willen baseren.[176] Het heeft weliswaar een paar rechtszaken gekost om deze rolverdeling helemaal te doen uitkristalliseren, maar intussen is het een vaststaand uitgangspunt. De OV-informatie

van 9292ov.nl geeft recentelijk aanleiding tot eenzelfde strijd. Op Europees niveau is men over het algemeen minder terughoudend in het schetsen van verreikende ICT-perspectieven (misschien omdat de beleidsplannen minder concreet hoeven te worden), en voert de open-platformgedachte de boventoon. Dit is, zoals gezegd, terug te zien in de beleidsdocumenten over de ontsluiting van de mogelijkheden van ITS.

Een dergelijke ambiguïteit van commerciële c.q. economisch gedreven rolpatronen tegenover publieke c.q. ordenende rolpatronen is in de mobiliteitssector veelal te verklaren uit de enormiteit van de investeringen die bijvoorbeeld ITS-applicaties vragen, en het feit dat deze investeringen vooral door grote industrieën (*automotive*) en/of grote dienstverleningssectoren (mobiele telefonie) moeten worden gedragen. De overheid kan simpelweg niet pretenderen hier alles te kunnen bepalen. Bij een initiatief als eCall is de betrokkenheid van bedrijven/bedrijfsorganisaties daarom vanaf het begin dominant geweest. Een dergelijke rolverdeling, waarin de overheid zich slechts opwerpt als facilitator van het proces om belangen bijeen te brengen, kan niet anders dan consequenties hebben voor de omgang met persoonsgegevens. Niettemin toont het dossier eCall dat er toch redelijk secuur over privacy is nagedacht[177] – ook bedrijven hebben hier een belang bij. Misschien is dat juist de reden dat de 'uitrol' van deze applicatie zeer vertraagd is: er is niet echt sprake van vernetwerking en het bijbehorende verdienmodel.

Bij secundair gebruik in een publieke context hebben we het over het koppelen van informatiebestanden, een wezenlijk onderwerp vanuit de privacyoptiek. Al zijn bij de verschillende initiatieven die in deze studie de revue passeren nog betrekkelijk weinig koppelingen bediscussieerd of gemaakt, dat betekent geenszins dat zij niet in het vat zitten. Er moet een onderscheid worden gemaakt tussen een volledige koppeling van informatiebestanden enerzijds en individuele 'uitvraging' van gegevens anderzijds. Bij een volledige en zogezegd massale koppeling kunnen er correlaties van gegevens worden gezocht die dwars door alle geregistreerde data (van soms miljoenen mensen) heengaan. Daarentegen gaat het bij individuele uitvraging om het lichten van één brokje informatie over een persoon die anderszins al de aandacht had getrokken.

Een volledige koppeling van bijvoorbeeld de database van Trans Link Systems (OV-chipkaart) aan een of meerdere overheidsdatabases is, zoals in het vorige hoofdstuk al is gesteld, moeilijk voorstelbaar. Niet omdat de overheid er geen 'baat' bij zou hebben, maar omdat dit maatschappelijk als veel te ingrijpend zou worden gezien. Daar komt bij dat de OV-bedrijven (in ieder geval naar de vorm[178]) geprivatiseerd zijn, zodat de overheid niet zonder meer kan pretenderen dat reis-

gegevens afkomstig van de OV-chipkaart 'haar' informatie zijn. Daarentegen lijkt de informatie verkregen uit gerichte kentekenherkenning als vogelvrij beschouwd te worden: de overheid kan naar hartenlust op zoek naar correlaties met andere bestanden.

Individueel uitvragen is een heel ander verhaal. Hoewel het vorderen van gegevens wel degelijk een ingrijpende bevoegdheid is, en steeds ingrijpender wordt naarmate er meer databases komen, wordt daarbij geen gebruik gemaakt van ingrijpende technieken, zoals datamining en profiling. Een voor de hand liggende vraag die in discussies rond de lancering van een nieuwe applicatie vaak opkomt, is of de informatie gedeeld wordt met politie en justitie. Bij volledige koppeling blijft die vraag klemmend, maar bij individuele uitvraging is dit eigenlijk een gepasseerd station – hetgeen weinigen beseffen. De Wet bevoegdheden vorderen gegevens[179] biedt namelijk een generieke mogelijkheid tot individueel uitvragen – natuurlijk met alle waarborgen die daarbij horen. Elke nieuwe database is per definitie een nieuwe bron van informatie voor politie en justitie. Tussen de categorieën volledige koppeling en individueel uitvragen bevindt zich nog een schemergebied. Dit schemergebied is aan de orde wanneer een instantie bijvoorbeeld de gegevens opvraagt van alle mensen die zich op een bepaald tijdstip op een bepaalde plaats ophielden ('metrostation Weesperplein, 21.35 uur'). Dit was aan de orde bij de zaak waarin het OM OV-chipkaartgegevens opvroeg, welke uiteindelijk tot aan de Hoge Raad leidde.

Een bijzondere vorm van secundair gebruik is de benutting van dataverzamelingen als bron voor managementinformatie. Bijvoorbeeld wanneer de organisatie die de ICT draait zelf lering wil trekken uit de registraties, of wanneer een toezichthoudende organisatie de prestaties van een ander wil controleren. Dit managementaspect is wezenlijk voor het 'slimme' imago van ICT: de gegenereerde informatie biedt veelal een terugkoppeling over de prestaties van de eigenaar van de toepassing. Ook bij mobiliteitstoepassingen treft men dit veelal aan. Verkeersinformatie is weliswaar informatie voor automobilisten, maar vanuit een ander perspectief ook managementinformatie voor wegbeheerders. De kilometerprijsregistratie is natuurlijk een belastingmaatregel, maar ook een instrument voor de overheid om te bepalen welk mobiliteitsbeleid (tarifering) werkt, in de zin dat het de doorstroming bevordert, en welk niet. En bij de OV-chipkaart was managementinformatie al bij aanvang een zeer belangrijk motief. Het hele vervoerssysteem zou slimmer worden door een betere kennis van het reisgedrag van mensen, en de mogelijkheid om op die kennis in te springen. Opmerkelijk genoeg zijn er juist op dit overkoepelende niveau van het vervoerssysteem een aantal kinken in de kabel gekomen. Hierdoor zijn de data uit de OV-chipkaart eigenlijk ongeschikt als basis voor beleid. In de eerste plaats 'klopt' de informatie pas als iedereen met de chip reist, en dat laat veel langer op zich wachten

dan gepland,[180] vooral omdat de chip veel gevoeliger blijkt te liggen dan gedacht. In de tweede plaats blijkt de opbrengst van de terugkoppeling die de kaart mogelijk maakt, namelijk de mogelijkheid om het productaanbod te differentiëren of zelfs te personaliseren, veel gevoeliger te liggen dan gedacht. Misschien wordt het tijd om te bedenken dat secundair gebruik altijd gevoeliger ligt dan men denkt.

## 3.5 TRANSPARANTIE

Privacybescherming heeft ook een procesmatige kant.[181] Er moeten immers afdoende mogelijkheden zijn om de op papier geboden bescherming af te dwingen. De belangrijkste procesmatige noties zijn transparantie en *accountability*.[182] Het spreekt voor zich dat transparantie een eerste vereiste is: wie geen inzicht heeft in de eigen situatie kan aan die situatie weinig veranderen. Transparantie is op die manier een voorportaal van de rechtsbescherming. Naast deze individuele dimensie is transparantie ook nodig op een meer geaggregeerd, beleidsmatig niveau. De politieke en beleidsmatige afwegingen, ook in het domein van mobiliteit, moeten inzichtelijk zijn om op legitimiteit te kunnen hopen.

De inzichtelijkheid van de eigen situatie van het individu is in relatie tot ICT-toepassingen op mobiliteitsgebied niet altijd even makkelijk te waarborgen.[183] De reiziger kan niet goed nagaan wat voor informatie in de databases is achtergebleven. Een Nationale Database (!) Openbaar Vervoersgegevens zou aan deze behoefte aan meer inzicht tegemoet moeten komen,[184] maar die laat nog op zich wachten. Bovendien is het de vraag of deze database die functie wel zal krijgen.[185] En hoewel het conceptwetsvoorstel ANPR belooft dat de automobilist wordt 'gewaarschuwd' voor een ANPR-installatie,[186] weet je uiteindelijk pas echt waar je aan toe bent als je door toedoen van ANPR ergens voor wordt 'gepakt', of dat nu is een uitstaande boete, een onjuiste belastingopgaaf (in verband met leaseauto's) of iets ergers.[187] De waarschuwingen voor ANPR-installaties langs de weg zullen gaandeweg inhoudsloos worden op het moment dat er – niet geheel denkbeeldig – duizenden ANPR-punten in Nederland zijn. Voor vrijwel iedereen geldt immers: er is geen ontkomen aan het zich begeven op de openbare weg.

Een centrale gedachte achter het bieden van transparantie is dat dit mensen in staat stelt zich te beraden op gedragsalternatieven.[188] Maar als er een fijn maaswerk van digitale surveillance over de openbare weg wordt gespannen, zijn die alternatieven op een gegeven moment niet echt meer voorhanden. Op het moment dat niet goed (meer) is na te gaan wat de overheid precies doet, neigt de technologie naar heimelijke observatie. Het EHRM heeft in een lange reeks uitspraken, beginnend met *Klass* t. *Duitsland*[189] in de jaren zeventig, geëist dat er extra zware procedure-eisen gelden

voor vormen van observatie waarvan het lijdend voorwerp niet op de hoogte kan zijn. Deze eisen moeten burgers – potentieel onderworpen aan observatie – in staat stellen te beoordelen hoe ver de bevoegdheden strekken en onder welke omstandigheden ze kunnen worden uitgeoefend. Aan dergelijke procedure-eisen wordt, zoals het zich nu laat aanzien, niet voldaan: voor 'ongerichte' ANPR is een schamele wettelijke grondslag voorzien, en voor 'gerichte' ANPR nagenoeg[190] geen. Heel anders is de situatie in Duitsland, waar het Constitutionele Hof (*Bundesverfassungsgericht*) een deelstaatwet heeft geannuleerd die nota bene voorzag in een grondslag voor gerichte kentekenherkenning (hetgeen in Nederland wordt geacht onder de algemene politietaak te vallen). Vanwege de ingrijpendheid van de techniek oordeelde het Hof dat de wet in strijd was met het *lex-certa*-beginsel[191] en het proportionaliteitsbeginsel.[192] In Nederland is veel minder goed na te gaan wat kan en mag; een nonchalante houding ten aanzien van digitale surveillance-innovaties ligt hieraan ten grondslag. Zo is de politie ook al geruime tijd bezig met 'stealth sms', een techniek die het mogelijk maakt de *realtime*-locatie van de ontvanger te bepalen zonder dat die persoon dit weet. De politie wordt daarin vooralsnog niet gehinderd door enige bevoegdheidsomschrijving – en verrassenderwijs ook niet door de rechter.[193]

Bij applicaties waar geen speciale wettelijke regeling aan voorafgaat, is de kans groot dat er ook geen parlementair debat wordt gevoerd over de merites van het initiatief. In die gevallen staat de beleidsmatige en politieke transparantie – de inzichtelijkheid van de beweegredenen en de afwegingen die achter het initiatief steken – direct op achterstand. Dit is evident het geval bij 'gerichte' ANPR. Met de OV-chipkaart is iets heel anders aan de hand. Doordat de overheid slechts zijdelings bij dat initiatief betrokken is, hebben de parlementaire debatten, hoe uitvoerig ook, eenzelfde zijdelings en onwezenlijk karakter gekregen.[194]

## 3.6 ACCOUNTABILITY

Net als transparantie is de notie van *accountability* op twee niveaus van belang, namelijk de individuele rechtsbescherming en het politiek-beleidsmatig debat. Bij de applicaties die in dit essay aan de orde zijn, is aan de individuele rechtsbescherming weinig aandacht geschonken. Het blijkt bijvoorbeeld lastig om papieren regelingen op het punt van bewaartermijnen en autorisaties echt operationeel te maken. Die aspecten (bewaartermijnen en autorisaties) zullen ook grotendeels aan het zicht van de burger onttrokken zijn, hoewel ze wel degelijk voor zijn bescherming in het leven geroepen zijn. Bovendien ontbreken, zoals hierboven betoogd, echte kaders voor de besproken mobiliteitstoepassingen bijna geheel. Hierdoor komt het qua rechtsbescherming aan op de algemene regeling vervat in de Wbp, eventueel aangevuld met algemene voorwaarden van commerciële dienstverleners. Ten slotte is

al vaak vastgesteld dat de informatierechten tot inzage en correctie die in dergelijke algemene regels vervat zijn, een sluimerend bestaan leiden.[195] Burgers weten niet gemakkelijk de weg naar de rechter te vinden als het geschil 'slechts' om informatie draait, en niet om iets tastbaars. Het is in het complexe landschap van de mobiliteitsinformatie ook niet eenvoudig om de bal aan het rollen te brengen. Illustratief hiervoor is de hoeveelheid energie die het een bovengemiddeld geïnformeerde activist kostte om simpelweg de van hem bekende locatiegegevens op te vragen bij zijn provider.[196] En als de burger dan toch ergens een voet tussen de deur heeft kunnen krijgen, bestaat het risico dat het antwoord op zijn of haar verzoek een variant zal zijn op de *Little Britain* sketch 'computer says no'.[197]

Bij *accountability* op het hogere abstractieniveau van politiek en beleid is het beeld wisselend. Enerzijds is er het dossier kilometerprijs, dat vrij zorgvuldig was opgezet en toch ten prooi viel aan electorale weerstand. Anderzijds is er het dossier ANPR, dat ingrijpende gevolgen heeft maar desondanks op weinig aandacht of zorgvuldigheid kan rekenen. En dan zijn er nog onderwerpen die een minder duidelijk publiek stempel dragen, zoals eCall en *realtime*-verkeersinformatie. Vanwege de verstrengeling van publieke en private actoren volgen deze onderwerpen een weinig inzichtelijk proces, waaruit ook niet duidelijk wordt wie waarvoor verantwoordelijk zullen zijn.

Het voorstel voor de Wet kilometerprijs (althans het garantiespoor daarvan) is een voorbeeld van een zorgvuldige publieke afweging en een zeldzaam secure verdeling van verantwoordelijkheden ten aanzien van de informatiestromen die met de applicatie in het leven geroepen zouden zijn.[198] Van Nederlanders wordt doorgaans gezegd dat zij weinig privacybewust zijn. Toch bleek het kastje dat de kilometerprijs moest gaan berekenen, als een rode lap op tal van critici te werken. Hierdoor heeft de toenmalige minister Eurlings op een gegeven moment het lot van het initiatief in handen gelegd van een ad-hocraadpleging door de ANWB, met een ongunstig resultaat. Op deze ANWB-raadpleging was methodologisch van alles af te dingen.[199] Bovendien is dit in een representatieve democratie natuurlijk een vreemde constructie.[200] Kennelijk durfde het kabinet dan wel de minister niet te vertrouwen op de afwegingen die onder eigen verantwoordelijkheid waren gemaakt. Het is nooit te zeggen wat de meeste tegenstand opriep: het idee van een belasting op het weggebruik of de privacyaspecten van het voorstel. Hoogstwaarschijnlijk moet de uitkomst grotendeels op het conto van de eerste factor worden geschreven, gezien de voorgeschiedenis van Anders Betalen voor Mobiliteit. Desondanks is het stranden van dit voorstel, bezien door de lens van (een zorgvuldige omgang met) privacy, nogal een paradox.

Ook de vele discussies over de OV-chipkaart zijn, zij het op een wat andere manier, een voorbeeld van het niet durven staan voor de eigen afwegingen. Hier gaat het niet primair om de afwegingen van de wetgever of de rijksoverheid, maar om die van de samenwerkende geprivatiseerde OV-bedrijven die Trans Link Systems hebben opgericht en de OV-chipkaart hebben ontwikkeld. Wat zij steeds hebben miskend, is dat ook het risico dat iets misgaat deel uitmaakt – of zou moeten uitmaken – van de afweging die bij aanvang wordt gemaakt. De eindeloze discussies die dit onderwerp in de media en in het parlement hebben opgeroepen draaiden vrijwel zonder uitzondering om de technische veiligheid van de chip, of om de klantvriendelijkheid van het systeem in termen van reiskosten. Na een bewerkelijke kraak van de Radboud Universiteit Nijmegen en uiteindelijk een laagdrempelige kraak van (tal van) anonieme hackers bleek de veiligheid van de chip inderdaad niet waterdicht te zijn. Realistisch gezien hadden de partijen betrokken bij Trans Link Systems de kraakbaarheid van de chip – van welke chip dan ook – moeten incalculeren. Vervolgens zou het voor de overheid geen ongewone vraag moeten zijn hoe om te gaan met frauderende reizigers.

Van Eeten (2011) stelt het contrast centraal tussen de lage risicotolerantie die kennelijk geldt voor een (semi)overheidsproject als de OV-chipkaart en de kalme berekening die ervoor zorgt dat de creditcard nog steeds zonder noemenswaardige problemen als mondiaal betaalmiddel op internet kan fungeren, ondanks de notoire technische onveiligheid van dat systeem.[201]

De strubbelingen rond de OV-chipkaart hebben amper iets met privacy te maken. Het probleem van frauderende reizigers is vooral een handhavings- en financieel probleem. Oftewel: de (vele) kraken zijn geen *privacy breach* maar een (beheersbare[202]) *financial breach*. De alarmistische toon van de discussies zou anders doen vermoeden. De eerste, zogezegd wetenschappelijke, kraak gaf wel aanleiding tot een interessante kwestie over de vrijheid van meningsuiting, toen de fabrikant van de chip in een kort geding, tevergeefs, probeerde de publicatie van de wetenschappelijke bevindingen te onderdrukken.[203] Maar er zijn ook voorbeelden van applicaties waarbij publieke afwegingen (zo ze al zijn gemaakt) überhaupt amper in het volle licht komen, zodat aan een beoordeling daarvan niet wordt toegekomen. Zo is de democratische basis van ANPR, eufemistisch gesteld, nogal dun, in ieder geval bij aanvang.[204] Dan zijn de ietwat eigenaardige debatten over de OV-chipkaart of de eigenaardige dynamiek van de kilometerprijs te prefereren.

# 4 CONCLUSIE

We staan waarschijnlijk nog maar aan het begin van de digitalisering van de openbare ruimte. En evenzeer staan we nog maar aan het begin van het denken over de manier waarop die ontwikkeling in goede banen kan worden geleid. Informatie komt steeds makkelijker boven water en maakt vervolgens bestuurlijk en maatschappelijk veel los. Het is daardoor niet eenvoudig om het nieuwe informatiedomein 'locatie' weer vast te pinnen. Het is dus zaak om in dit verband goed na te denken over privacybescherming, en daarvoor arrangementen in het leven te roepen. Daarbij mag uit het huidige betoog wel afgeleid worden dat *location based privacy* geen eenduidig geheel is, maar een complexe samenloop van meerdere factoren die de robuustheid van de beschermingsconstructies bepalen. *Location based privacy* is daarnaast ook een complexe samenloop van rolpatronen tussen publiek en privaat, betrouwbaarheid en winstgevendheid, technologische oplossingen en bestuurlijk-juridische oplossingen.

Toch is het goed om uit al die complexiteit het eenvoudige idee van *selective disclosure* naar voren te halen. Het gaat tenslotte om wat er *per saldo* overblijft van 'privacy in het openbaar', en niet, of niet slechts, om wat elke afzonderlijke applicatie in dit opzicht 'doet'. In hoeverre hebben burgers nog controle over informatie over waar ze zich ophouden? Uit de voorgaande beschrijvingen volgt het antwoord: 'niet veel'. Dan moet de vervolgvraag zijn hoeveel van die controle we burgers eigenlijk zouden willen gunnen, en of die controle niet min of meer per ongeluk is verdwenen. Is de situatie waarin *location based privacy* zich per saldo bevindt, niet veroorzaakt doordat we ICT meer als een instrument benaderen dan als een zelfstandig gegeven met wijde repercussies voor maatschappij en bestuur? Maar welke rol de overheid ook kiest, de digitalisering van de openbare ruimte zal ontegenzeggelijk doorgaan. De digitale sporen die mensen achterlaten, zullen nog talrijker en wellicht ook onuitwisbaarder worden. Dit roept de vraag op wat een privacybesef bij overheid en burgers en de daaruit voortvloeiende arrangementen überhaupt zouden kunnen uitrichten. Om die vraag te beantwoorden moet waarschijnlijk gekeken worden voorbij de *controle over* locatie-informatie, en meer worden nagedacht over de *toegang tot* die informatie. Oftewel: welke data moeten beschikbaar zijn voor wie?

Deze omslag in het denken is noodzakelijk om een aantal redenen. In de eerste plaats omdat er in praktische zin van uitgegaan kan (gaan) worden dat locatiedata van alle dagelijkse beslommeringen wel ergens zijn gegenereerd en opgeslagen. De

sensorische rijkdom die is aangeboord, kan niet zomaar weer worden afgedekt. Zo zal informatievergaring via *floating car data* waarschijnlijk sterk toenemen, en is nu al elke (ingeschakelde) mobiele telefoon door triangulatie van zendmastinformatie te traceren. De notie van controle over zelfopenbaring (*selective disclosure*) is in dat licht te optimistisch, aangezien zij suggereert dat iemand het vrijkomen van informatie kan tegengaan. Een benadering die de massale technologische ontsluiting van locatie-informatie (met gepaste tegenzin) voor lief neemt, is dan meer op haar plaats. Het is de 'Faustian bargain' waar de mobiliteitstheoreticus Urry het over heeft: gaan we voertuigen vernetwerken, dan gaan we ook mensen traceerbaar maken.[205] Deze berusting over het ontstaan ('loskomen') van gigantische hoeveelheden locatie-informatie impliceert wel dat er (veel) meer moet worden geïnvesteerd in de inkadering van het gebruik van die informatie.

Die omslag van controle naar toegang is in de tweede plaats nodig, omdat de notie van controle over zelfopenbaring er enigszins van uitgaat dat het individu zelf primair verantwoordelijk is voor het op orde hebben van zijn of haar digitale zaakjes. Dit is geen geschikt uitgangspunt, omdat het vertakte informatie-universum simpelweg te complex en ontransparant is om de bescherming van burgers geheel afhankelijk te maken van hun eigen kennis en actiebereidheid.

In de derde plaats is een nieuwe insteek nodig om enige mate van *practical obscurity* te herwinnen. Deze onzichtbaarheid was vroeger een natuurgegeven en niet zozeer een principiële inspanning. De stand van de techniek maakt haar inmiddels tot een principieel na te streven zaak, omdat de natuurlijke grenzen van openbaarheid enorm zijn afgenomen. Daarbij heeft het dus relatief weinig zin om de kaarten te zetten op het beheersen van het ontstaan van informatie. Veeleer moeten overheid en bedrijfsleven bewijzen dat de voorhanden zijnde informatierijkdom spaarzamer, zorgvuldiger en 'rechtmatiger' gebruikt kan worden. Er zou kortom moeten worden ingezet op de organisatorische en institutionele omlijsting van de technologie. Technologische en institutionele kwaliteit zijn twee kanten van dezelfde medaille; tijd dus om de achterzijde voorbij de fase van de ruwe schets te brengen.

# LITERATUUR

Adviescommissie Verkeersinformatie (Commissie Laan ii) (2009) *Eindrapport*, Den Haag.

Agre, P.E. (1994) 'Surveillance and capture: two models of privacy', *The Information Society*, 10, 101-127.

Alpert, S.A. (1995) 'Privacy and intelligent highways: finding the right of way', *Santa Clara Computer & High Technology Law Journal*, 97-118.

Article 29 Data Protection Working Party, *Opinion* 4/2007 on the concept of personal data; http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

Article 29 Data Protection Working Party, *Opinion* 13/2011 on Geolocation services on smart mobile devices, Brussel 16 mei 2011; www.cbpweb.nl/downloads_int/wp185_en.pdf.

Ashley, S. (2008) 'Driving toward crashless cars', *Scientific American*, 58-65.

Bonham, J. (2005) 'Transport: disciplining the body that travels', blz. 57-74 in S. Böhm et al. (red.), *Against Automobility*, Londen: Blackwell.

Bovend'Eert, P. et al. (red.) (2010) *Tekst en commentaar Nederlandse Grondwet*, Alphen aan den Rijn: Kluwer.

Boyd, D. (2010) 'Making sense of privacy and publicity', speech SXSW, Austin, Texas, 13 maart.

Bruinsma, F., J. van Dijk & C. Gorter (2002) 'Mobiliteit en beleid', blz. 1-6 in F. Bruinsma, J. van Dijk & C. Gorter (red.), *Mobiliteit en beleid*, Assen: Van Gorcum.

Buruma, Y. (2011) 'Het recht op vergetelheid. Politiële en justitiële gegevens in een digitale wereld', blz. 165-218 in D.W.J. Broeders, M.K.C. Cuijpers & J.E.J. Prins (red.), *De staat van informatie*, WRR Verkenningen nr. 25, Amsterdam: Amsterdam University Press.

College bescherming persoonsgegevens, Brief van 08-11-2008 aan staatssecretaris van V&W mw. J.C. Huizinga-Heringa; www.cbpweb.nl/downloads_pb/pb_20081111_brief_aan_staatssecretaris_huizinga_over_OV-chipkaart.pdf.

College bescherming persoonsgegevens (2009) Consultatiedocument *'Cbp Richtsnoeren ANPR'*, Den Haag, januari.

College bescherming persoonsgegevens (2010a) *Rapport van bevindingen: Verwerking van persoonsgegevens ten behoeve van de OV-chipkaart bij Trans Link Systems B.V.*, Den Haag, december.

College bescherming persoonsgegevens (2010b), *Rapportage 'ANPR Rotterdam-Rijnmond'*, Den Haag, januari.

College bescherming persoonsgegevens (2011) *Verslag over bevindingen bij CIOT, Politiekorps Haaglanden, Dienst Nationale Recherche*, Den Haag, 28 april; www.cbpweb.nl/Pages/pb_20110428_ciot.aspx.

Commissie Permanente Structuur en Dubbel Opstaptarief in de treinrailketen (commissie-Meijdam) (2011) *Het spoor naar slagkracht*, Den Haag.

Connekt (2011) *ITS in the Netherlands*, Den Haag.

Deny, M. (2005) '"Always crashing in the same car": a head-on collision with the technosphere', in: S. Böhm et al. (eds.), *Against Automobility*, London: Blackwell, 223-239.

Eeten, M. van (2010) *Techniek van de onmacht. Fatalisme in politiek en technologie*, oratie TU Delft, Delft.

Eeten, M. van (2011) 'Gedijen bij onveiligheid. Afwegingen rond de risico's van informatietechnologie', blz. 133-164 in D.W.J. Broeders, M.K.C. Cuijpers & J.E.J. Prins (red.), *De staat van informatie*, WRR Verkenningen nr. 25, Amsterdam: Amsterdam University Press.

eSafety Forum (eCall Driving Group) (2006) *Recommendations of the DG eCall for the introduction of the pan-European eCall*, Brussel; www.ecall.fi/Position_papers_DG_eCall_v2.pdf.

European Data Protection Supervisor (2009) *Opinion of the European data protection supervisor on the action plan and proposal for an ITS directive*, Brussel 22 juli.

Europese Commissie (2008) *Actieplan voor de invoering van intelligente voertuigsystemen in Europa*, COM 886 def.

Europese Commissie (2010) Mededeling *Een digitale agenda voor Europa*, COM (245) def./2.

Europese Commissie (2011) 'Digitale Agenda: de Commissie zet eerste stap om tegen 2015 een levensreddend noodoproepsysteem voor verkeersongevallen in te voeren', Persbericht 8 september 2011, IP/11/1010.

Fried, C. (1984), 'Privacy: a moral analysis', blz. 203-222 in F.D. Schoeman (ed.), *Philosophical Dimensions of Privacy: an anthology*, Cambridge: Cambridge University Press 1984.

Geuens, Ch., E. Kindt & J. Dumortier (2010) 'Anders betalen voor mobiliteit: is de privacy gewaarborgd?', *Computerrecht*, 5, 228-236.

Gifford, J.L., & V. Marchau (2007) 'U.S. and European responses to uncertainty about intelligent transportation systems: a comparative analysis', blz. 96-108 in P. Rietveld & R. Stough (red.), *Institutions and sustainable transport: regulatory reform in advanced economies*, Cheltenham, UK: Edward Elgar.

Griffioen, H.M. (2011) annotatie bij EHRM 14 december 2010, Ternovszky t. Hongarije, klachtnr. 67545/09, *European Human Rights Cases*, nr. 44.

Griffioen, H.M. (2011) 'Automatische kentekenherkenning: all systems are go?', *Nederlands Juristenblad*, 9, 550-554.

Groothuis, M.M. (2006) 'De bewaarplicht van verkeersgegevens bij Internet en telefonie en de verhouding tot het recht op eerbiediging van de persoonlijke levenssfeer', NJCM-*Bulletin*, 792-811.

Hafkamp, W.H. & H. Geerlings (2002) 'Mobiliteit en ruimte anders beschouwd; groei als kans voor vernieuwing', blz. 7-18 in F. Bruinsma, J. van Dijk & C. Gorter (red.), *Mobiliteit en beleid*, Assen: Van Gorcum.

Harms, L. (2008) *Overwegend onderweg. De leefsituatie en de mobiliteit van Nederlanders*, Den Haag: SCP.

Hert, P. de & S. Gutwirth (2006) 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power', blz. 61-104 in E. Claes et al. (red.), *Privacy and the Criminal Law*, Antwerpen.

Hoen, W. 't (2010) *Wisselende verwachtingen. Een onderzoek naar de oorzaken van veranderde verwachtingen van betrokken actoren binnen het OV-chipkaartproject en de invloed op de toekomst van het project*, Scriptie EUR: Rotterdam.

Hof, Ch. van 't (2010) 'Case 0001. Pasjes en poortjes', in: Ch. van 't Hof, R. van Est & F. Daemen, *Check In / Check Uit. De digitalisering van de openbare ruimte*, Rotterdam: Rathenau Instituut/NAi Uitgevers.

Hof, Ch. van 't, R. van Est & F. Daemen (2010) *Check In / Check Uit. De digitalisering van de openbare ruimte*, Rotterdam: Rathenau Instituut/NAi Uitgevers.

Jacobs, B., 'Architecture is politics: security and privacy issues in transport and beyond', blz. 289-299 in S. Gutwirth, Y. Poullet & P. de Hert (eds.) (2010), *Data Protection in a Profiled World*, Berlin: Springer.

Keizer, A.G. (2011) 'De digitale patiënt centraal. Medische informatie in een digitale wereld', blz. 345-390 in D.W.J. Broeders, M.K.C. Cuijpers & J.E.J. Prins (red.), *De staat van informatie*, WRR Verkenningen nr. 25, Amsterdam: Amsterdam University Press.

Kennisinstituut voor Mobiliteitsbeleid (2011) *Slim benutten: bereikbaarheidsmaatregelen op een rij*, Den Haag: Ministerie van Infrastructuur & Milieu, juni.

Latour, B. (1992) 'Where are the missing masses? The sociology of a few mundane artifacts', blz. 226-258 in W. Bijker & J. Law (red.), *Shaping technology/ building society*, Cambridge, Mass.: MIT Press.

Mayer-Schönberger, V. (2009) *Delete. The virtue of forgetting in the digital age*, Princeton: Princeton University Press.

Meijer, A. & M. Thaens (2009) 'Public information strategies: Making government information available to citizens', *Information Polity* 14, 31-45.

Ministerie van Economische Zaken, Landbouw & Innovatie (2011) *Digitale*

*Agenda.nl – ICT voor innovatie en economische groei*, Den Haag.

Ministerie van Veiligheid en Justitie, Conceptwetsvoorstel regeling van het vastleggen en bewaren van kentekengegevens door de politie, Den Haag 10 januari 2011; www.rijksoverheid.nl/documenten-en-publicaties/regelingen/2011/01/11/wetsvoorstel-regeling-van-het-vastleggen-en-bewaren-van-kentekengegevens-door-de-politie.html.

Ministerie van Verkeer en Waterstaat (2008) *Beleidskader Benutten. Eén van de pijlers voor betere bereikbaarheid*, Den Haag 4 januari.

Munnichs, G., M. Schuijff & M. Besters (red.) (2010) *Databases: over ICT-beloftes, informatiehonger en digitale autonomie*, Den Haag: Rathenau Instituut.

Ooijen, C. van & S. Nouwt (2009) 'Power and privacy: the use of LBS in Dutch public administration', blz. 75-87 in B. van Loenen, J.W.J. Besemer & J.A. Zevenbergen (red.), *SDI convergence: research, emerging trends, and critical assessment*, Delft: Netherlands Geodetic Commission.

Ooijen, C. van (2011) 'Legitimacy issues regarding citizen surveillance – the case of ANPR-technology in Dutch policing', blz. 197-216 in S. van der Hof & M.M. Groothuis (red.), *Innovating government. Normative, policy and technological dimensions of modern government*, The Hague: T.M.C. Asser Press.

Peters, P. & R. de Wilde (2004) 'De politiek van de straat. Een stijlvolle kijk op mobiliteit', *Krisis*, 38-51.

Peters, P.F. (2006) *Time, Innovation and Mobilities. Travel in technological cultures*, London: Routledge.

Potters, P. & M. de Vreeze (2010) *eCall Blackbox*, Webpublicatie nr. 48, Verkennende studie voor het WRR-rapport *iOverheid*, Den Haag (www.wrr.nl).

PriceWaterhouseCoopers (2011) *Toets rapportage TLS /vervoersbedrijven OV-chipkaart fraude*, 24 februari.

Reiman, J. (2004) 'Driving to the panopticon. A philosophical exploration of the risks to privacy posed by the information technology of the future', blz. 194-214 in B. Rössler (red.), *Privacies. Philosophical Evaluations*, Stanford: Stanford University Press.

Solove, D.J. (2008) *Understanding privacy*, Cambridge, Mass.: Harvard University Press.

Staatscommissie Grondwet (2010) *Rapport staatscommissie grondwet*, Den Haag.

Stephenson, P. (2010) 'Let's get physical: the European Commission and cultivated spillover in completing the single market's transport infrastructure', *Journal of Public Policy* 17: 7, 1039-1057.

Sussman, J.M. (2005) *Perspectives on intelligent transport systems*, New York: Springer.

Teepe, W. (2010) 'De OV-chipkaart en de kilometerheffing: een elektronisch enkelbandje voor reizigers?', blz. 30-41 in G. Munnichs, M. Schuijff & M. Besters (red.), *Databases: Over ICT-beloftes, informatiehonger en digitale autonomie*, Den Haag: Rathenau Instituut.

TomTom (2011) *Annual Report and Accounts 2010: Freedom to Move…*, zonder plaatsaanduiding.

Trans Link Systems BV (2008) Statutenwijziging per 21-01-2008, dossiernr. 30177126, Kamer van Koophandel Gooi-, Eem- en Flevoland.

Tweede Kamer (1997-1998), *Memorie van toelichting Wet bescherming persoonsgegevens,* Kamerstukken II, 25892, nr. 3, 46-47.

Tweede Kamer (2008-2009a), *Brief inzake Mobiliteitsbeleid*, Kamerstukken II, 31305, nr. 143.

Tweede Kamer (2008-2009b), *BNC-fiche inzake Actieplan en Richtlijn Intelligente vervoerssystemen*, Kamerstukken II, nr. 802.

Tweede Kamer (2008-2009c), *Vragen van Kamerleden Van Baalen, Griffith en Teeven*, Handelingen II, Aanhangsel, nr. 3264.

Tweede Kamer (2009-2010a), *Advies en Nader Rapport Wet kilometerprijs,* Kamerstukken II, 32216, nr. 4.

Tweede Kamer (2009-2010b), *Memorie van Toelichting bij de Wet kilometerprijs*, Kamerstukken II, 32216, nr. 3.

Tweede Kamer (2009-2010c), *Brief inzake onderzoek Cbp naar ANPR bij politie Rotterdam-Rijnmond en IJsselland*, Kamerstukken II, 31051, nr. 6.

Tweede Kamer (2010-2011a), *Update* Beter Benutten, Kamerstukken II, 32500 A, nr. 81.

Tweede Kamer (2010-2011b), *Instelling Commissie-Leers (later Meijdam),* Kamerstukken II, 23645, nr. 392.

Tweede Kamer (2010-2011c), *Algemeen Overleg over o.m. ANPR*, Kamerstukken II, 32500 VI, nr. 85.

Tweede Kamer (2010-2011d), *Vragen van Kamerlid Verhoeven*, Handelingen II, Aanhangsel, 2011Z11763.

Tweede Kamer (2011-2012), *Vragen van Kamerlid Çörüz (met antwoorden)*, Handelingen II, Aanhangsel, nr. 29.

Urry, J. (2007) *Mobilities*, Cambridge: Polity.

Urry, J. (2004) 'The "system" of automobility', *Theory, Culture & Society* 21, 25-39.

Vlek C.A.J. & E.M. Steg (2002) 'Mobiliteit en omgevingskwaliteit: naar een duurzaam verkeer en vervoer', blz. 19-38 in F. Bruinsma, J. van Dijk & C. Gorter (red.), *Mobiliteit en beleid*, Assen: Van Gorcum.

Wees, K.A.P.C. van (2004) *Intelligente voertuigen, veiligheidsregulering en aansprakelijkheid: een onderzoek naar juridische aspecten van Advanced Driver Assistance Systems in het wegverkeer*, Delft: TRAIL.

Weisberg, R. (1995) 'IVHS, Legal privacy, and the legacy of Dr. Faustus', *Santa Barbara Computer & High Technology Law Journal*, 75-96.

WRR (2000) *Het borgen van publiek belang*, WRR rapporten aan de regering nr. 56, Den Haag: SDU.

WRR (2011) *iOverheid*, WRR rapporten aan de regering nr. 86, Amsterdam: Amsterdam University Press.

Zimmer, M. (2005) 'Surveillance, privacy and the ethics of vehicle safety communication technologies', *Ethics and Information Society*, 7, 201-210.

# JURISPRUDENTIE

ABRVS, 28 december 2010, zaak 201010790/1/V3 (www.raadvanstate.nl).
BVerfG, 11 maart 2008, zaken 1 BvR 2074/05 & 1 BvR 1254/07 (www.bundesverfassungsgericht.de).
EHRM, 6 september 1978, *Klass* t. *Duitsland*, klachtnr. 5029/71 (www.echr.coe.int).
EHRM, 28 januari 2003, *Peck* t. *Verenigd Koninkrijk*, klachtnr. 44647/98 (www.echr.coe.int).
EHRM, 2 september 2010, *Uzun* t. *Duitsland*, *European Human Rights Cases* 2010/123 , annotatie De Hert en Van Caeneghem.
Gerechtshof 's Hertogenbosch 5 oktober 2010, 'Waakzaam II', LJN BN9352 (www.rechtspraak.nl).
HR, 9 januari 1987, *Nederlandse Jurisprudentie* 1987, nr. 928, annotatie Alkema.
HR, 23 maart 2010, LJN: BK6331 (www.rechtspraak.nl).
HvJ EU, 22 juni 2010, *Melki*, zaken C-188/10 en C-189/10 (www.curia.europa.eu).
Rechtbank Amsterdam, 31 mei 2011, LJN: BQ9049 (www.rechtspraak.nl).
Rechtbank Arnhem (Kort Geding), 18 juli 2008, LJN: BD7578 (www.rechtspraak.nl).
Supreme Court (VS), 2 maart 1983, *Knotts*; http://supreme.justia.com/us/460/276/case.html

# GEÏNTERVIEWDE PERSONEN

Drs. R. Adams, Rijkswaterstaat, december 2009.
Dr.ir. M. van Gelderen, ministerie van Verkeer en Waterstaat, november 2009.
Mr. S. Katus, NS, februari 2010.
Drs. B. Pel, Erasmus Universiteit Rotterdam, februari 2010.
Dr.ir. E.J. Sol, TNO, december 2009.

# NOTEN

1 Vervoerswijzen of sectoren die buiten beschouwing blijven zijn het wegtransport, de scheepvaart en de luchtvaart. Dit is niet omdat digitalisering op die terreinen geen invloed heeft – integendeel, de logistiek van het wegtransport was al vroeg een laboratorium voor ICT – maar omdat de implicaties daarvan niet primair burgers ('particulieren') in relatie tot de overheid aangaan.

2 Hier zijn programma's in de zin van Latour bedoeld: de technologie stuurt het gedrag op wijzen die vaak 'op de tekentafel' niet te voorzien zijn. B. Latour, 'Where are the missing masses? The sociology of a few mundane artifacts',blz. 226-258 in W. Bijker & J. Law (red.), Shaping technology/building society, Cambridge, Mass.: MIT Press 1992.

3 Volgens Solove, die dit kritisch bespreekt, is deze benadering van het begrip privacy de meest wijdverbreide; zie hoofdstuk 2 in D.J. Solove, *Understanding privacy*, Cambridge, Mass.: Harvard University Press 2008.

4 Vgl. C. Fried, 'Privacy: a moral analysis', blz. 203-222 in F.D. Schoeman (red.), *Philosophical dimensions of privacy: an anthology*, Cambridge: Cambridge University Press 1984.

5 Zie, algemeen, bijv. Ch. van 't Hof, R. van Est & F. Daemen, *Check in / Check uit. De digitalisering van de openbare ruimte*, Rotterdam: Rathenau Instituut/NAi Uitgevers 2010.

6 *Uzun* t. *Duitsland*, EHRM, 2 september 2010, *European Human Rights Cases* 2010, nr. 123, annotatie De Hert en Van Caeneghem. Het Hof benadrukt dat het volgen van een verdachte door middel van een heimelijk geplaatste GPS-zender in de auto gunstig afsteekt op de meetlat van de subsidiariteit, omdat het minder ingrijpend is dan andere vormen van *surveillance*.

7 Illustratief is het feit dat het strafprocesrecht nagenoeg geen regels of voorwaarden stelt aan het toelaten van 'tips' – waarnemingen van buitenstaanders – in het strafproces, behalve dat de informatie in principe opnieuw present gesteld moet worden in de rechtszaal, door middel van het getuigenverhoor.

8 Rechter Rehnquist in *Knotts*, Supreme Court, 2 maart 1983, geciteerd in: R. Weisberg, 'IVHS, legal privacy, and the legacy of Dr. Faustus', *Santa Barbara Computer & High Technology Law Journal* 1995, 75-96, p. 96.

9 Vgl. Solove 2008 over wat hij noemt de "secrecy paradigm" (dat privacy alleen van toepassing is als iets geheim moet blijven), o.m. hoofdstuk 5. Verder, over privacy in het openbaar, D. Boyd, 'Making sense of privacy and publicity', speech SXSW, Austin, Texas, 13 maart 2010.

10 Zie bijvoorbeeld: *Tekst en Commentaar* bij de Nederlandse Grondwet (P. Bovend'Eert et al. (red.), Alphen aan den Rijn: Kluwer 2010), welke onder art. 10 (privacy) vermeldt dat bescherming in de openbaarheid niet is uitgesloten, en ter ondersteuning een bekende uitspraak van de Hoge Raad aanhaalt die bekend staat onder de titel 'Edamse bijstandsvrouw' (Hoge Raad, 9 januari 1987, *Nederlandse Jurisprudentie* 1987, nr. 928, annotatie Alkema).

11 Zie op dit punt kritisch over de Toelichting bij het conceptwetsvoorstel ANPR: H.M. Griffioen, 'Automatische kentekenherkenning: all systems are go?', *Nederlands Juristenblad* 2011, 9, 550-554.

12 Zie bijv. C. van Ooijen & S. Nouwt, 'Power and privacy: the use of LBS in Dutch public administration', in: B. van Loenen, J.W.J. Besemer & J.A. Zevenbergen (red.), *SDI convergence: research, emerging trends, and critical assessment*, Delft: Netherlands Geodetic Commission 2009, 75-87; M. Zimmer, 'Surveillance, privacy and the ethics of vehicle safety communication technologies', *Ethics and Information Society*, 7, 2005, 201-210.

13 Een vooruitziende blik levert het artikel van J. Reiman (oorspronkelijk gepubliceerd in 1995), 'Driving to the panopticon. A philosophical exploration of the risks to privacy posed by the information technology of the future', blz. 194-214 in B. Rössler (ed.), *Privacies. Philosophical Evaluations*, Stanford: Stanford University Press 2004.

14 Er wordt in sommige commerciële applicaties ook aan de gebruiker gevraagd om de locatie prijs te geven waar dit voor de functionaliteit niet noodzakelijk is. Zie *Wall Street Journal*, 17 december 2010, 'Your apps are watching you' voor een overzicht, waaruit bovendien blijkt dat (binnen de categorie *location based services* maar ook daarbuiten) er zelfs *apps* zijn die zonder toestemming van de gebruiker de locatie peilen én verzenden.

15 Overigens ruimde het voorstel voor een Wet kilometerprijs een belangrijke plaats in voor uitvoering van deelonderwerpen door commerciële dienstverleners.

16 Publieke belangen zijn belangen die de burger als burger raken, niet zozeer als klant. Voor een belangrijk deel is de aanduiding dat iets een publiek belang behelst, een politieke beslissing (vgl. WRR, *Het borgen van publiek belang*, WRR-rapporten aan de regering nr. 56, Den Haag: SDU 2000). Voordat echt sprake is van een dergelijke opwaardering – of, in marktperspectief, afwaardering – kan er een schemergebied zijn waarin bijvoorbeeld nu de overheidsbemoeienis (Nederland, EU) met sociale netwerksites zich bevindt.

17 Zie over eCall P. Potters & M. de Vreeze, *eCall Blackbox*, Webpublicatie nr. 48, Verkennende studie voor het WRR-rapport *iOverheid*, 2010 (www.wrr.nl).

18 Zie voor een overzicht Connekt, *ITS in the Netherlands*, in opdracht van het ministerie van Infrastructuur en Milieu, Den Haag 2011.

19 Zie bijv. S. Ashley, 'Driving toward crashless cars', *Scientific American* 2008, p. 58-65.

20 J. Urry, *Mobilities*, Cambridge: Polity 2007; J. Urry, 'The "System" of automobility', *Theory, Culture & Society* 21, 2004, p. 25-39.

21 http://www.unive.nl/e-support/veelgesteldevragen

22 J.M. Sussman, *Perspectives on intelligent transport systems*, New York: Springer 2005.

23 Deze dynamiek is duidelijk te herkennen in het dossier eCall, maar ook bij rijtaakondersteunende systemen. Niet echter bij routenavigatie; het verschil is dat routenavigatie in essentie geen communicatie tussen systemen bewerkstelligt – daarvan niet afhankelijk is – en andere systemen wel, waardoor zij alleen bij een zekere penetratiegraad zinvol zijn.

24 Ministerie van Verkeer en Waterstaat, *Beleidskader benutten. Eén van de pijlers voor betere bereikbaarheid*, Den Haag, 4 januari 2008, p. 46.

25 Van belang is de grote hoeveelheid onderzoeksgeld dat de EU onder het 6e Kaderprogramma heeft toegewezen aan (inmiddels afgeronde) ITS-projecten als CVIS, Coopers en Safespot, maar los daarvan ook de grote dynamiek die het entrepreneurschap rond ITS heeft, welke op evenementen als het ITS World Congress (in 2010 in Amsterdam) samenkomt. Vgl. de groots opgezette proefopstellingen die organisaties als TNO met communicerende (bestuurderloze) auto's maken.

26 Sussman 2005.

27 J.L. Gifford & V. Marchau, 'U.S. and European responses to uncertainty about intelligent transportation systems: a comparative analysis', blz. 96-108 in P. Rietveld & R. Stough (red.), *Institutions and sustainable transport: regulatory reform in advanced economies*, Cheltenham, UK: Edward Elgar, 2007; Sussman 2005.

28 Europese Commissie, Mededeling *Een digitale agenda voor Europa*, COM 2010 (245) def./2.

29 Tweede Kamer (2010-2011a), *Update* Beter Benutten, Kamerstukken II, 32500 A, nr. 81, p. 6.

30 Waar de studie wel over 5-10% spreekt, gaat het niet over *realtime*-verkeersinformatie per se, en waar het daar wel over gaat maakt de studie (met verwijzing naar TomTom) melding van 5% mobiliteitswinst, bij een penetratiegraad van 10% voor de applicatie. Kennisinstituut voor Mobiliteitsbeleid, *Slim benutten: bereikbaarheidsmaatregelen op een rij*, Den Haag: Ministerie van Infrastructuur & Milieu, juni 2011, p. 61.

31 De percentages zijn afkomstig uit TomTom's 'Traffic Manifesto', gepubliceerd als deel van het jaarverslag over 2010. TomTom, *Annual report and Accounts 2010: freedom to move…*, zonder plaatsaanduiding, 2011.

32 Adviescommissie Verkeersinformatie (Commissie Laan II), Eindrapport, Den Haag 2009; KiM 2011: 61.

33 Eigenlijk is het beter om hier van 'publieke goederen' (*public goods*) te spreken in plaats van beleidsterreinen, aangezien het feit dat commerciële initiatieven een belangrijke rol spelen (met

name bij verkeersinformatie) niets afdoet aan het publieke belang van deze zaken. 'Beleidsterrein' heeft de klank van een exclusieve overheidstaak, en dat is hier zeker niet het geval.

34 In dit essay wordt alleen over het aspect van verkeersveiligheid gesproken dat te maken heeft met veiligheid van de vervoersmiddelen zelf.

35 Vgl. L. Harms, *Overwegend onderweg. De leefsituatie en de mobiliteit van Nederlanders*, Den Haag: SCP 2008, p. 82-83 over de gordiaanse knoop van mobiliteitsaanbod (vgl. ook Urry 2007, p. 281): als de infrastructuur (aanbodzijde) verbeterd wordt, stijgt de vraag en blijft de doorstroming even slecht. Dit gaat ook op voor aan mobililteit gerelateerde ICT-onderwerpen. Eenzelfde boodschap heeft C.A.J. Vlek & E.M. Steg, 'Mobiliteit en omgevingskwaliteit: Naar een duurzaam verkeer en vervoer', blz. 19-38 in F. Bruinsma, J. van Dijk & C. Gorter (red.), *Mobiliteit en beleid*, Assen: Van Gorcum 2002.

36 Zie voor deze slingerbeweging F. Bruinsma, J. van Dijk & C. Gorter, 'Mobiliteit en beleid', blz. 1.6 in F. Bruinsma, J. van Dijk & C. Gorter (red.), Mobiliteit en beleid, Assen: Van Gorcum 2002.

37 Zie voor deze slingerbeweging: P.F. Peters, *Time, innovation and mobilities. Travel in technological cultures*, London: Routledge 2006, 157-175.

38 Zie bijvoorbeeld W.H. Hafkamp & H. Geerlings, 'Mobiliteit en ruimte anders beschouwd; groei als kans voor vernieuwing', blz. 7.18 in F. Bruinsma, J. van Dijk & C. Gorter (red.), *Mobiliteit en beleid*, Assen: Van Gorcum 2002.

39 Dit is ook waar het ITS-gidsland Japan in uitblinkt.

40 Ministerie van Verkeer en Waterstaat (2008).

41 In 2010 had ongeveer 3% van de klanten van TomTom de beschikking over *realtime*-diensten. Dit valt af te leiden uit TomTom (2011), p. 16.

42 Specifiek gaat het om het 'HD Traffic' pakket.

43 In andere landen werkt TomTom samen met andere telecombedrijven.

44 In 2010 deed ongeveer de helft van de klanten van TomTom dat (TomTom 2011, p. 16).

45 Het KiM (2011: 62) rekent voor wat een stimuleringsmaatregel van die strekking de overheid zou kosten.

46 De overheid heeft uiteraard ook haar eigen informatiebronnen; zie hierna.

47 Overigens voorspelt TomTom in zijn jaarverslag over 2010 (TomTom 2011, p. 13) dat bij een marktaandeel van slechts 10% voor *realtime*-routenavigatie, de reistijd voor *eenieder* met 5% zou afnemen.

48 Potters & De Vreeze 2010, p. 23: deze eis is afgedwongen door de Europese Art. 29 Werkgroep (het netwerk van nationale privacytoezichthouders), maar werd eerder in het proces ook al door telecom-aanbieders ingebracht (p. 20).

49 Europees onderzoeksprogramma Safespot; intussen afgerond (www.safespot-eu.org).

50 Het KiM voorspelt dat voor 2028 geen noemenswaardige effecten voor de doorstroming zullen optreden door deze technologieën (KiM 2011, p. 25).

51 Zie K.A.P.C. van Wees, *Intelligente voertuigen, veiligheidsregulering en aansprakelijkheid: Een onderzoek naar juridische aspecten van* Advanced Driver Assistance Systems *in het wegverkeer*, Delft: TRAIL, 2004.

52 Vgl. S.A. Alpert, 'Privacy and intelligent highways: finding the right of way', *Santa Clara Computer & High Technology Law Journal* 1995, 97-118.

53 Sociologische verhandelingen over 'automobiliteit' zijn uiteraard zeer divers, maar benadrukken wel allemaal de individualistische trek van de autocultuur. Zie bijvoorbeeld het werk van John Urry, zoals kort weergegeven in Urry 2004. Deze lijn wordt door sommigen zelfs doorgetrokken tot aan het auto-ongeval: M. Deny, '"Always crashing in the same car": a head-on collision with the technosphere', blz. 223-239 in S. Böhm et al. (red.), *Against Automobility*, London: Blackwell 2005.

54 TomTom 2011: 8.

55 O.a. *Algemeen Dagblad*, 27 april 2011, 'TomTom tipt politie over verkeersmisbruik'.

56 Er was – zoals TomTom later benadrukte – in feite niet echt sprake van samenwerking, want de politie had de informatie van een tussenpersoon gekocht.

57 Zie A. Meijer & M. Thaens, 'Public information strategies: making government information available to citizens', *Information Polity* (14) 2009, 31-45.

58 Zie brief inzake Mobiliteitsbeleid aan de Tweede Kamer (2008-2009a), Kamerstukken II, 31305, nr. 143. 4.

59 Die *pool* zal waarschijnlijk eerder vorm krijgen in de (toekomstige) Nationale Databank Openbaar Vervoersgegevens (NDOV) dan in de NDW, omdat het makkelijker/goedkoper is om actuele informatie van (openbaar) vervoerders los te krijgen dan van TomTom/Vodafone e.d.

60 Wijziging van art. 10 Besluit Personenvervoer 2000: *Staatsblad* 2010, nr. 695. Voorheen stond actuele informatie niet bij de categorieën van informatie die door vervoerders verstrekt moeten worden.

61 Art. 14, Wet personenvervoer 2000.

62 KiM 2011, p. 61 stelt het zo voor dat het vooral de commerciële dienstverleners zijn die zitten te springen om deze publieke informatie op hun platformen te kunnen draaien. Dat belang is onmiskenbaar, maar de omgekeerde relatie is ingewikkelder: de overheid zal een uitvoerig en buitengewoon streng eisenpakket hebben klaarliggen, mocht het zover komen dat verkeersmanagement via commerciële platformen plaatsvindt.

63 Tweede Kamer (2010-2011a), p. 6.

64 'Het' kastje had niet noodzakelijkerwijs 'het' platform hoeven worden, al lag dat wel voor de hand gezien de verplichting voor alle automobilisten om er een te hebben.

65 Europese Commissie, Actieplan voor de invoering van intelligente voertuigsystemen in Europa, COM (2008) 886 def., p. 11-12; Ministerie van V&W 2008, p. 35.

66 Neelie Kroes, Vice-president van de Europese Commissie, Speech van 8 september 2011 (http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/557&format=HTML&aged=0&language=EN&guiLanguage=en); Ministerie van EL&I, *Digitale Agenda.nl – ICT voor innovatie en economische groei*, Den Haag 2011. Dit is een uitwerking van de Digitale Agenda van de Europese Commissie.

67 Het is overigens denkbaar dat ook een dergelijk platform zelf door verschillende bedrijven wordt aangeboden, als de specificaties maar hetzelfde zijn.

68 Uitgebreider in Potters & De Vreeze 2010.

69 eSafety Forum (eCall Driving Group), Recommendations of the DG eCall for the introduction of the pan-European eCall, Brussel 2006 (www.ecall.fi/Position_papers_DG_eCall_v2.pdf).

70 Dit onderscheidt het proces zoals dat door de Commissie was opgezet van 'normale' zelfregulering door private partijen.

71 Richtlijn 2010/40/EU, *Pb* [2010] L 207/1.

72 Die wetgeving is intussen door de Commissie aangekondigd; Europese Commissie, Persbericht 8 september 2011, 'Digitale Agenda: de Commissie zet eerste stap om tegen 2015 een levensreddend noodoproepsysteem voor verkeersongevallen in te voeren', IP/11/1010.

73 Opinion of the European Data Protection Supervisor on the action plan and proposal for an ITS directive, Brussel, 22 juli 2009.

74 Tweede Kamer (2008-2009b), *BNC-fiche inzake Actieplan en richtlijn intelligente vervoerssystemen*, Kamerstukken II, 22112, nr. 802.

75 P. Stephenson, 'Let's get physical: the European Commission and cultivated spillover in completing the single market's transport infrastructure', *Journal of Public Policy* 17: 7, 1039-1057.

76 Het enige motief voor het opzetten van het OV-chipkaartsysteem dat direct met het verzamelen van locatie-informatie te maken heeft, is het marketingmotief: de wens van vervoerders om reisgerelateerde boodschappen en meer commercieel getinte aanbiedingen aan reizigers te kunnen sturen.

77 *Staatsblad* 2000, nr. 314.

78 Zo blijkt uit een rapport uit 1992 opgesteld door het kennisinstituut en bureau NEA (voor Vervoersbewijzen Nederland), welke organisatie een belangrijke rol heeft vervuld in het samenbrengen van partijen om de toekomst van de tarifering te bediscussiëren. Zie W. 't Hoen, *Wisselende verwachtingen. Een onderzoek naar de oorzaken van veranderde verwachtingen*

*van betrokken actoren binnen het OV-chipkaartproject en de invloed op de toekomst van het project*, Scriptie EUR: Rotterdam 2010.

79 Voor de NS gelden andere overwegingen. Dat bedrijf had al eerder tariefvrijheid, en viel ook niet onder het Nationaal Vervoersbewijs.

80 Zie uitgebreid het advies van de commissie-Meijdam (2011); 't Hoen 2010.

81 Voor toezichthouders en concessieverleners is die managementinformatie ook een instrument om de prestaties van vervoerders te controleren, hetgeen voor die laatsten in zekere zin natuurlijk 'minder gunstig' is.

82 Vgl. *NRC Handelsblad*, 14 juni 2011: 'Kamer vreest schadeclaims bij vertraging afschaffing strippenkaart'. De "schadeclaims" in kwestie zijn verzoeken van decentrale bestuursorganen aan het rijk om financiële compensatie voor de meerkosten van naast elkaar bestaande systemen.

83 Studenten hoeven bij vrij reizen formeel (nog) niet in en uit te checken bij de NS, maar zijn daar vaak niet van op de hoogte; zie de last onder dwangsom die het Cbp op 9 juni 2011 oplegde aan de NS, www.cbpweb.nl/Pages/pb_20110726_OV-chip_LOD.aspx.

84 Van 't Hof 2010.

85 Cbp, Brief van 8 november 2008 aan staatssecretaris van V&W mw. J.C. Huizinga-Heringa, www.cbpweb.nl/downloads_pb/pb_20081111_brief_aan_staatssecretaris_huizinga_over_OV-chipkaart.pdf.

86 Privacy is bijvoorbeeld niet aan de orde bij de opdracht aan de commissie-Leers (nu Meijdam) die door de minister van V&W (I&M) is ingesteld om onderzoek te doen naar het functioneren van de OV-chipkaart (Tweede Kamer (2010-2011b), Kamerstukken II, 23645, nr. 392). Ook bij de inbreng die consumentenorganisaties tijdens de totstandkoming van de OV-chipkaart hebben geleverd speelde privacy doorgaans geen rol van betekenis. Vgl. Ch. van 't Hof, 'Case 0001. Pasjes en poortjes', blz. 37-73 (47) in: Van 't Hof, Van Est & Daemen 2010, over de 11 eisen die consumentenorganisaties in 2005 inbrachten: "Zelfs punt 7, de privacy van de reiziger, gaat vooral over de financiële consequenties."

87 De commissie-Kist heeft onderzoek moeten doen naar kostenoverschrijdingen van het hele project, en geadviseerd over de verdeling daarvan over de verschillende actoren. Bovendien hebben reiskosten voor individuen steeds een prominente rol gespeeld in het proces. Zie Van 't Hof 2010.

88 Vgl. M. van Eeten, 'Gedijen bij onveiligheid. Afwegingen rond de risico's van informatietechnologie', blz. 133-164 in D.W.J. Broeders, M.K.C. Cuijpers & J.E.J. Prins (red.), *De staat van informatie*, WRR Verkenningen nr. 25, Amsterdam: Amsterdam University Press 2011.

89 Commissie Permanente Structuur en Dubbel Opstaptarief in de treinrailketen (commissie-Meijdam), *Het spoor naar slagkracht*, Den Haag 2011.

90 De bevindingen zijn gepubliceerd in verschillende wetenschappelijke tijdschriften. Zie voor verwijzingen: B. Jacobs, 'Architecture is politics: security and privacy issues in transport and beyond', blz. 289-299 in S. Gutwirth, Y. Poullet & P. De Hert (red.), *Data Protection in a Profiled World*, Berlin: Springer 2010.

91 Deze chip is algemeen verspreid in vooral beveiligingssystemen van gebouwen.

92 In een hoorzitting van de Tweede Kamer over de OV-chipkaart; geciteerd door W. Teepe, 'De OV-chipkaart en de kilometerheffing: een elektronisch enkelbandje voor reizigers?', blz. 30-41, aldaar 37 in G. Munnichs, M. Schuijff & M. Besters (red.), *Databases: Over ICT-beloftes, informatiehonger en digitale autonomie*, Den Haag: Rathenau Instituut 2010.

93 Jacobs 2010, p. 293. Met de *data security* van die organisatie zal overigens niets mis zijn geweest.

94 Jacobs 2010, p. 292.

95 Algemeen G. Munnichs, M. Schuijff & M. Besters (red.), *Databases: Over ICT-beloftes, informatiehonger en digitale autonomie*, Den Haag: Rathenau Instituut 2010.

96 Zie § 3.4.

97 Daarnaast bevat de kaart zelf de gegevens over de laatste tien transacties. Die zijn uiteraard tegen misbruik beveiligd, maar volgens de meeste experts is die beveiliging onvoldoende.

98 Zie Teepe 2010.

99 Cbp (2010a), *Rapport van bevindingen: Verwerking van persoonsgegevens ten behoeve van de*

*OV-chipkaart bij Trans Link Systems BV*, Den Haag, december 2010, p. 7.

100 Het OV-chipkaartsysteem levert geen *realtime*-informatie op, omdat de decentrale bestanden (op een bepaalde plaats) niet voortdurend worden gesynchroniseerd (gebufferd) met de centrale database van de vervoerder. Deze laatste database is op zijn beurt niet synchroon met (of identiek aan) de database van Trans Link Systems.

101 Radio Frequency Identification, de technologie waar de OV-chipkaart gebruik van maakt. Dit zijn op korte afstand uitleesbare chips.

102 Van 't Hof 2010, p. 69.

103 Teepe 2010, p. 40; Jacobs 2010, p. 294.

104 Zie de apologetische speech die de directeur van Trans Link Systems, de heer Nelemans, hield bij de uitreiking van de zogenaamde Big Brother Awards van 2011; www.TransLink.nl/media/bijlagen/nieuws/Speech_Big_Brother_Award.pdf.

105 Om een voorbeeld te noemen: Trans Link Systems is verantwoordelijk voor het verstrekken van de reisgeschiedenis aan de betrokkene zelf, als die daarom verzoekt ten behoeve van bijvoorbeeld een declaratie.

106 Zie bijvoorbeeld Cbp 2010a, p. 7.

107 Hoge Raad, 23 maart 2010, LJN: BK6331 (www.rechtspraak.nl).

108 Het had zoals gezegd technologisch gezien zeker nog armer gekund.

109 Zie § 2.2 van het Hoge Raad-arrest.

110 Trans Link Systems BV, Statutenwijziging per 21-01-2008, dossiernr. 30177126, Kamer van Koophandel Gooi-, Eem- en Flevoland.

111 Tweede Kamer (2009-2010a), *Advies en Nader Rapport Wet kilometerprijs,* Kamerstukken II, 32216, nr. 4. De Raad was vooral kritisch over het optimisme over de technische betrouwbaarheid van GPS en verder over de fiscaalrechtelijke inbedding van het voorstel. In zijn advies noemde de Raad de persoonlijke levenssfeer precies één keer, en wel op een ondergeschikt punt.

112 Zie voor een weergave van deze en andere 'afleveringen' Peters 2006, p. 157-175.

113 De ANWB maakte deel uit van het Platform Anders Betalen voor Mobiliteit, dat in 2007 de minister adviseerde om door te gaan met de omschakeling naar een gebruiksbelasting. Zie www.anwb.nl/verkeer/nieuws-en-tips/archief,/nederland/2008/01/Advies-platform--Anders-Betalen-voor-Mobiliteit-.html.

114 Eenzelfde patroon had zich voor en na lancering van het Mobimiles-concept van Roel Pieper voorgedaan; Peters 2006, p. 165.

115 Zie de Memorie van Toelichting bij de Wet kilometerprijs, Tweede Kamer (2009-2010b), Kamerstukken II, 32216, nr. 3; verder Ch. Geuens, E. Kindt & J. Dumortier, 'Anders Betalen voor Mobiliteit: Is de privacy gewaarborgd?', *Computerrecht* 2010, 5, 228-236.

116 Zie in het kort Jacobs (2010, p. 291) over de voordelen van zo'n "decentrale architectuur".

117 De gebruiker/belastingbetaler zelf zou de verplaatsingsgegevens wel kunnen uitlezen. (En daarmee ook overheidsinstanties met wettelijke vorderingsbevoegdheden.)

118 Dit is allemaal af te leiden uit de Memorie van Toelichting (Tweede Kamer 2009-2010b).

119 Zo blijkt duidelijk uit de Memorie van Toelichting (Tweede Kamer 2009-2010b) uit november 2009. Teepe (2010, p. 38 e.v.) schrijft desondanks ruim een jaar later nog dat er niets bekend is over de keuze tussen een "dikke" en een "dunne" variant van de kilometerprijsregistratie, maar dat de minister blijkens een interview uit januari 2008 een voorkeur heeft voor de "dikke variant" (i.e. het garantiespoor).

120 Vgl. Teepe 2010, p. 38-39.

121 Zie bijv. NRC *Handelsblad*, 17 november 2009, 'Rekentruc: elke auto goedkoper. Eurlings cijfert creatief om steun voor kilometerheffing te behouden'. In 1999 'bleek' overigens al uit een onderzoek van de ANWB dat 80% van de Nederlanders niet gelooft dat een gebruiksbelasting leidt tot minder files; Peters 2006, 161.

122 P. Peters & R. de Wilde, 'De politiek van de straat. Een stijlvolle kijk op mobiliteit', *Krisis* 2004, 38-51; J. Bonham, 'Transport: disciplining the body that travels', blz. 57-74 in: S. Böhm et al. (red.), *Against Automobility*, London: Blackwell 2005.

123 Dit onderscheid is verder uitgewerkt in Griffioen 2011, waar het hiernavolgende op gebaseerd is.
124 Een 'hit' is een 'match' (overeenkomstigheid) tussen een passerend kenteken en een kenteken dat vooraf in het zogenaamde vergelijkingsbestand was opgenomen.
125 Terminologisch: een installatie die is opgesteld om alleen aan ongerichte kentekenherkenning te doen, bewaart alles, zodat het eigenlijk vreemd is om van 'no-hits' te spreken. Maar in de discussie over ANPR heeft men het veelal over installaties die zowel voor gerichte als voor ongerichte kentekenherkenning dienen.
126 Het KLPD beschikt overigens ook over een ANPR-installatie in Spanje: Tweede Kamer (2008-2009c), Handelingen II, 2008-2009, Aanhangsel, nr. 3264.
127 Een soort ANPR in broekzakformaat wordt bijvoorbeeld ook door parkeerwachten gebruikt, maar daar zal verder niet op in worden gegaan.
128 De toelichting bij het conceptvoorstel voor een ANPR-wet (zie hierna) spreekt (§ 7) van "26 locaties met vaste camera's en 78 mobiele ANPR-camera's" die de politiekorpsen nu tot hun beschikking hebben. Maar het Cbp stelde eerder (begin 2010) vast dat alleen al het korps Rotterdam-Rijnmond over 68 vaste camera's beschikte (Cbp (2010b), Rapportage 'ANPR Rotterdam-Rijnmond', januari 2010, p. 6).
129 Ministerie van Veiligheid en Justitie, Conceptwetsvoorstel regeling van het vastleggen en bewaren van kentekengegevens door de politie, Den Haag 10 januari 2011; www.rijksoverheid.nl/documenten-en-publicaties/regelingen/2011/01/11/wetsvoorstel-regeling-van-het-vastleggen-en-bewaren-van-kentekengegevens-door-de-politie.html.
130 Zie bijv. www.rijksoverheid.nl/nieuws/2009/12/09/belastingdienst-int-openstaande-schulden.html.
131 C. van Ooijen, 'Legitimacy issues regarding citizen surveillance – The case of ANPR-technology in Dutch policing', blz. 197-216 in S. van der Hof & M.M. Groothuis (red.), *Innovating government. Normative, policy and technological dimensions of modern government*, The Hague: T.M.C. Asser Press 2011.
132 Cbp 2010b gaf de doorslag, maar ook in januari 2009 had het Cbp het bewaren van 'no-hits' al expliciet afgekeurd (Cbp, Consultatiedocument 'Cbp Richtsnoeren ANPR', januari 2009).
133 Tweede Kamer (2009-2010c), Brief inzake onderzoek Cbp naar ANPR bij politie Rotterdam-Rijnmond en IJsselland, Kamerstukken II, 31051, nr. 6.
134 Het betreffende rapport ('Gewoon doen') is opmerkelijk genoeg niet meer op internet te vinden.
135 Zie bijv. de uitspraak 'Waakzaam II', Gerechtshof 's Hertogenbosch, 5 oktober 2010, LJN BN9352 (www.rechtspraak.nl).
136 Zie bijv. Cbp 2009.
137 Zie bijv. M. van Doornik, 'Kentekenregistratie door camera's gaat mij veel te ver', NRC *Handelsblad* 29 september 20011.
138 Tweede Kamer (2010-2011c), *Algemeen Overleg over o.m. ANPR*, Kamerstukken II, 32500 VI, nr. 85, p. 14.
139 Idem.
140 Kamervragen van 17 augustus 2011, o.a.: "Bent u het met de politie en het CDA eens dat indien de beelden nu niet mogen worden opgeslagen dat dit wel zou moeten kunnen?" (http://www.cda.nl/coruz/Wat_doe_ik/Kamervragen/Schietincidenten_op_snelwegen_.aspx). In de parlementaire stukken luidt de vraag iets anders. Tweede Kamer (2011-2012), *Vragen van Kamerlid Çörüz (met antwoorden)*, Handelingen II, Aanhangsel, nr. 29.
141 In de filosofie wordt (bijv. bij Henri Bergson) wetenschappelijke tijd c.q. ruimte vaak gecontrasteerd aan een meer existentiële beleving daarvan. Die beleving lijkt niet aan de orde wanneer iemand bijvoorbeeld door een kentekenherkenningscamera 'gepeild' wordt.
142 Vgl. Article 29 Data protection working party, opinion 4/2007 on the concept of personal data, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf, 11.
143 De toelichting bij het conceptwetsvoorstel ANPR presenteerde het werken met kentekennummers in plaats van met namen als een beschermingsconstructie. Maar eigenlijk is dit verschil irrelevant, aangezien de autoriteiten, wanneer daar aanleiding voor is, al vrij snel van het kenteken bij de

naam uitkomen – wat toch ook de bedoeling zal zijn van deze handhavingstechniek; zie Griffioen 2011. Ook de memorie van toelichting van de Wbp laat aan duidelijkheid niets te wensen over: Tweede Kamer (1997-1998), Kamerstukken II, 25892, nr. 3, 46-47.

144 Zie http://weblogs.nrc.nl/hebben/2011/04/28/tomtom-zwicht-voor-flitsgevoelige-automobilist voor de e-mail die de CEO van TomTom de nacht volgend op de rel stuurde aan al zijn abonnees (geraadpleegd op 6 mei 2011).

145 Het pijnpunt lijkt te zijn geweest dat de politie deze informatie gebruikte om te bepalen waar flitspalen moesten worden geposteerd. Zie *Algemeen Dagblad*, 27 april 2011, 'TomTom tipt politie over verkeersmisbruik'.

146 De Staatscommissie Grondwet heeft er onlangs voor gepleit om de bescherming van persoonsgegevens deze rang wel te verlenen; Staatscommissie Grondwet, *Rapport Staatscommissie Grondwet*, Den Haag 2010. In bijvoorbeeld het recht van de Europese Unie daarentegen zijn de bescherming van persoonsgegevens enerzijds en privacy anderzijds constitutioneel gelijkwaardig.

147 Zie bijvoorbeeld P. De Hert & S. Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power', blz. 61-104 in E. Claes et al. (red.), *Privacy and the Criminal Law*, Antwerpen 2006, voor een uiteenzetting over de relatie tussen de twee noties.

148 De uitgangspunten van de Wbp zijn alle terug te vinden in een verdrag uit 1981: Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (Vastgesteld in Straatsburg, 28 januari 1981), Tractatenblad 1988, nr. 7.

149 Vgl. WRR, *iOverheid*, Rapporten aan de regering nr. 86, Amsterdam: Amsterdam University Press 2011, 214-226.

150 Het vormen van geaggregeerde gedragspatronen voor bijvoorbeeld verkeersmanagement vraagt om een geheel andere – minder strenge – afweging.

151 Article 29 data protection working party, opinion 13/2011 on geolocation services on smart mobile devices, Brussel 16 mei 2011 (www.cbpweb.nl/downloads_int/wp185_en.pdf).

152 Het handelen moet zo specifiek mogelijk gericht zijn op 'probleemgroepen', om maar geen gelijkenis te vertonen met de grenscontroles die door 'Schengen' zijn afgeschaft. Dit valt af te leiden uit het arrest *Melki* van het Hof van Justitie van de EU; HvJ, 22 juni 2010, zaken C-188/10 en C-189/10 (www.curia.europa.eu). De toepassing van *Melki* door de Nederlandse Raad van State is echter een andere; ABRvS, 28 december 2010, zaak 201010790/1/V3 (www.raadvanstate.nl).

153 In de publieke variant (het garantiespoor) was dit zoals gezegd het Centraal Justitieel Incassobureau (CJIB).

154 In de publieke variant (het garantiespoor) was dit zoals gezegd de Rijksdienst voor het Wegverkeer (RDW).

155 Het gaat niet om de plaatsbepaling die bij iedere mobiele telefoon mogelijk is, namelijk triangulatie ten opzichte van zendmasten. Die normale plaatsbepaling bij mobiele telefoons vindt buiten het apparaat plaats. Die informatie bevindt zich latent in de bestanden van de telecomaanbieder.

156 Zie bijv. *Webwereld*, 5 mei 2011, 'Apple-update verhelpt iPhone locatieopslag'. Inmiddels heeft Apple het besturingssysteem van de iPhone en iPad zodanig aangepast dat er minder informatie blijft hangen in het apparaat. Dit lost de vertrouwenskwestie echter niet principieel op.

157 WRR 2011, 133.

158 Potters & De Vreeze 2010, 23; nogmaals herhaald in Europese Commissie 2011.

159 Het ANPR-systeem @MIGO-BORAS van de Koninklijke Marechaussee brengt bijvoorbeeld een strikte scheiding aan tussen analyse en operationeel gebruik. Voor analysedoeleinden wordt ook gebruikgemaakt van 'ongerichte ANPR' – het opslaan van de gegevens van *alle* passages, in plaats van slechts van voertuigen die 'gezocht' worden.

160 Deze samenwerking stelt zoals gezegd TomTom in staat uit bergen locatie-informatie van Vodafone-abonnees een geloofwaardige *realtime*-dienst te destilleren voor verkeersinformatie (en advisering) aan haar (beter betalende) klanten. De samenwerking berust op de volstrekte anonimiteit van de Vodafone-gegevens.

161 Interview Nico Kaptein, CapGemini (citaat bij WRR 2011, 165).

162 Cbp, Verslag over bevindingen bij CIOT, Politiekorps Haaglanden, Dienst Nationale Recherche, Den Haag 28 april 2011; zie www.cbpweb.nl/Pages/pb_20110428_ciot.aspx.

163 Vgl. over het EPD A.G. Keizer, 'De digitale patiënt centraal. Medische informatie in een digitale wereld', blz. 345-390 in D.W.J. Broeders, M.K.C. Cuijpers & J.E.J. Prins (red.), *De staat van informatie*, WRR Verkenningen nr. 25, Amsterdam: Amsterdam University Press 2011, p. 345-390; en over politiegegevens Y. Buruma, 'Het recht op vergetelheid. Politiële en justitiële gegevens in een digitale wereld', in: D.W.J. Broeders, M.K.C. Cuijpers & J.E.J. Prins (red.), *De staat van informatie*, WRR Verkenningen nr. 25, Amsterdam: Amsterdam University Press 2011, p. 165- 218.

164 De 'Art. 29 Werkgroep' (2011) vraagt ook aandacht voor dit gegeven.

165 Vgl. de titel van een vrij willekeurig artikel in *Webwereld*, 12 mei 2011: 'KPN luistert abonnees af met Deep Packet Inspection'. In feite is 'afluisteren' hier een metafoor, want aan de orde is eerder een soort 'uitlezen' – net als bij ANPR overigens, waar volautomatisch visuele informatie in lexicale informatie wordt omgezet. Voor een boeiende verhandeling over de privacy-implicaties van *semantic capture*, zie P.E. Agre, 'Surveillance and capture: two models of privacy', *The Information Society*, 10, 1994, 101-127.

166 Vgl. bijvoorbeeld Solove 2008, p. 118 e.v. ten aanzien van de *Supreme Court*-uitspraak *Reporters Committee*. Deze notie wordt overigens niet specifiek toegepast op locatie-informatie, of zelfs op zintuiglijke informatie, maar zij leent zich daar wel erg goed voor.

167 Zie bijvoorbeeld Reiman 2004.

168 EHRM, 28 januari 2003, *Peck – United Kingdom*, klachtnr. 44647/98 (www.echr.coe.int).

169 Richtlijn 2006/24/EG.

170 M.M. Groothuis, 'De bewaarplicht van verkeersgegevens bij Internet en telefonie en de verhouding tot het recht op eerbiediging van de persoonlijke levenssfeer', NJCM-Bulletin 2006, 792-811.

171 De door de Eerste Kamer bedongen nadere verkorting is pas in 2011 tot stand gebracht.

172 Tweede Kamer (2010-2011c).

173 Dwangsombesluiten van 9 juni 2011 tegen NS, RET, GVB en Translink; zie www.cbpweb.nl/Pages/pb_20110726_OV-chip_LOD.aspx.

174 Buruma 2011.

175 Aan de 'dichtgetimmerde' optie kleefde wel een paradoxaal bezwaar vanuit het perspectief van de burger: er zou met geen mogelijkheid kunnen worden nagegaan of de geregistreerde hoeveelheid kilometers juist was, omdat het kastje ook voor de klant een black box was. Hieraan werd tegemoetgekomen door de mogelijkheid voor de automobilist om zelf zijn kastje 'uit te lezen' met een USB-stick – wat overigens weer andere risico's oplevert. Die mogelijkheid werd toegevoegd naar aanleiding van de kritiek van de Raad van State (zie Tweede Kamer (2009-2010a), p. 11).

176 Meijer & Thaens (2009).

177 Zie eSafety Forum (eCall Driving Group) 2006.

178 De aandelen van vervoersbedrijven zijn veelal in meerderheid in handen van overheidsorganisaties, zoals het ministerie van Financiën in het geval van Connexxion.

179 *Staatsblad* 2005, p. 390.

180 Diverse verschijnselen doen of deden af aan de sluitendheid van het OV-chipkaartsysteem: aanvankelijke weigerachtigheid van abonnementhouders om in te checken, het feit dat studenten dat nog steeds niet hoeven, de trage afschaffing van de strippenkaart, het onverplichte karakter van de chipkaart bij de NS. En getalsmatig het minst belangrijk: reizigers met gemanipuleerde kaarten.

181 Ook het Straatsburgse Europees Hof voor de Rechten van de Mens erkent en ijvert voor deze procedurele dimensie van afzonderlijke grondrechten, zoals het recht op leven (art. 2 EVRM) en de persoonlijke levenssfeer (art. 8 EVRM). Het Hof kiest ervoor deze procedurele dimensie als een integraal deel van die substantiële grondrechten zelf te zien, terwijl het verdrag ook afzonderlijke procedurele grondrechten bevat, zoals art. 6 en 13 EVRM (eerlijk proces resp. effectief rechtsmiddel).

182 Zie uitgebreid WRR 2011.

183 Vgl. 'Art. 29 Werkgroep' 2011 ten aanzien van *location based services*, met name voor wat betreft de vaagheid en verwarrendheid van de toestemming die *apps* vragen aan de klant – als ze die

toestemming al vragen.

184 Van 't Hof 2010, 63.

185 Er lijkt eerder sprake van een functie parallel aan die van de NDW, met *information brokers* en niet particulieren als afnemers. Zie het antwoord op de vragen van Kamerlid Verhoeven (Tweede Kamer (2010-2011d), Handelingen II (Aanhangsel), 2011Z11763), te vinden op www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2011/06/28/beantwoording-kamervragen-over-ov-data-en-9292.html.

186 Strikt genomen geldt deze belofte alleen voor (installaties voor) 'ongerichte' kentekenherkenning, omdat het conceptwetsvoorstel ook alleen daarover gaat.

187 Al gesteld dat automobilisten ook zullen worden gewaarschuwd voor 'gerichte' kentekenherkenning, zullen ze niet weten waar de politie met de betreffende installatie naar op zoek is. Dit is namelijk afhankelijk van het criterium dat leidend is geweest bij het opstellen van het vergelijkingsbestand.

188 Dit is een fundamenteel uitgangspunt van het staatsrecht, maar ook van het strafrecht: (kennis van) de wet stelt mensen in staat om hun gedragsalternatieven te bepalen. Zie bijvoorbeeld H.M. Griffioen, annotatie bij EHRM, 14 december 2010, Ternovszky t. Hongarije, klachtnr. 67545/09, *European Human Rights Cases* 2011, nr. 44.

189 EHRM, 6 september 1978, *Klass* t. *Duitsland*, klachtnr. 5029/71 (www.echr.coe.int). Zie voor een korte schets van deze lijn Griffioen 2011b.

190 Er is altijd de generieke bescherming van de wbp en de Wet politiegegevens, maar deze wetten vormen niet zozeer een grondslag voor een bevoegdheid, en als kader zijn ze ook niet zaligmakend. Er kan vanuit de wbp bijvoorbeeld weinig zinnigs worden gezegd over het opstellen van een vergelijkingsbestand voor een ANPR-operatie. Zie nader Griffioen 2011a.

191 Dit beginsel eist dat ingrijpende bevoegdheden van de overheid nauwkeurig beschreven moeten worden (in de wet). Het wordt ook wel het 'bepaaldheidsgebod' (*Bestimmtheitsgebot*) genoemd.

192 Bundesverfassungsgericht, 11 maart 2008, zaken 1 BvR 2074/05 & 1 BvR 1254/07 (www.bundesverfassungsgericht.de).

193 Rechtbank Amsterdam, 31 mei 2011, LJN: BQ9049.

194 Van Eeten 2011; verder M. van Eeten, *Techniek van de onmacht. Fatalisme in politiek en technologie*, oratie TU Delft, Delft 2010.

195 V. Mayer-Schönberger, *Delete. The virtue of forgetting in the digital age*, Princeton: Princeton University Press 2009, 138-139.

196 Zie www.rejo.zenger.nl.

197 Teepe (2010, p. 37) signaleert dit in het kader van de OV-chipkaart.

198 Geuens, Kindt & Dumortier 2010.

199 NRC *Handelsblad*, 25 januari 2010, 'ANWB-enquête over kilometerheffing niet waterdicht'.

200 Er kwam later nog een andere vreemde constructie aan het licht, die op een andere manier over representatie gaat: een milieuorganisatie bleek *tegen betaling* te hebben meegeschreven aan het voorstel. Zie *Webwereld*, 12 april 2011, 'Eurlings betaalde milieuclub voor lobbyactiviteiten'.

201 Overigens speelde in de beginfase van de OV-chipkaart het idee dat deze functionaliteit op de bankpas zou kunnen worden gezet, maar het bankwezen was in het geheel niet geneigd om daarmee in te stemmen. Een dergelijk semipubliek vehikel was waarschijnlijk niet welkom, omdat de banken nu geheel zelf het communicatie- en verwachtingenmanagement rond bijvoorbeeld het probleem van skimmen kunnen beheersen (en met succes).

202 Zie de doorlichting van de maatregelen genomen door Trans Link Systems na de laatste serie kraken, uitgevoerd door PriceWaterhouseCoopers: *Toets rapportage TLS/ vervoersbedrijven OV-chipkaart fraude*, 24 februari 2011. Het gaat om vrij onaanzienlijke bedragen aan gederfde inkomsten, bezien vanuit het totale reizigersvolume. Hier moet wel bij gezegd worden dat de inschattingen waar dit onderzoek op berust vrij provisorisch zijn.

203 Rechtbank Arnhem (Kort Geding), 18 juli 2008, LJN: BD7578 (www.rechtspraak.nl).

204 Te denken valt aan de wordingsgeschiedenis van (digitaal) cameratoezicht en van internetfilters.

205 Urry 2007, p. 289.

WRR WEBPUBLICATIES 59

# *Privacy en vormen van 'intelligente' mobiliteit*

De gangen van mensen worden steeds meer traceerbaar. Er is een bonte verzameling ICT-applicaties op het toneel van mobiliteit verschenen, waarmee informatie over de locatie wordt gegenereerd. Het denken over de persoonlijke levenssfeer en de bescherming van privacy loopt bij deze ontwikkelingen achterop. Dat komt omdat locatie-informatie op het eerste gezicht niet echt privé lijkt. Wie zich in het openbaar beweegt, kan immers door iedereen worden geobserveerd. Waarnemen staat vrij, en de openbare ruimte heet niet voor niets openbaar. Desondanks is er reden genoeg – vooral door het voortschrijden van de techniek – om locatie-informatie als een urgent onderdeel van het privacydebat aan te merken. De studie analyseert de meest markante ICT-applicaties die de overheid inzet om mobiliteitsvragen op te lossen. Dit zijn achtereenvolgens de verzamelcategorie 'intelligente transportsystemen' (ITS), de OV-chipkaart, de kilometerprijsregistratie en automatische kentekenherkenning (ANPR). Deze systemen dragen bij aan de digitalisering van de openbare ruimte en daarmee van de levenssfeer 'onderweg'. Hoe het met die levenssfeer is gesteld, hangt af van een aantal factoren die de kracht of zwakte van de constructie van privacybescherming bepalen, zoals technologische betrouwbaarheid, secundair gebruik van informatie en accountability. Dit mondt uit in de diagnose dat realistisch gezien steeds meer locatie-informatie zal worden gegenereerd. Maar daarom komt het er des te meer op aan dat de kwaliteit van de institutionele omlijsting van de gebruikte technologie verbeterd wordt, en er dus verder wordt gekeken dan naar technisch kunnen alleen.

*Henk Griffioen is staatsrechtjurist en rechtsfilosoof.*

ISBN 978 90 8964 416 9

9 789089 644169 >

WWW.AUP.NL