Notitie ten behoeve van de Landelijke ITS Ronde Tafel Juridische aspecten van Smart Mobility

VRIJDAG 25 SEPTEMBER 2015

Marcel Otto - Wouter van Haaften
DITCM INNOVATIONS | WWW.DITCM.EU
25-9-2015

Notitie ten behoeve van de Landelijke ITS Ronde Tafel Juridische aspecten van Smart Mobility

Inleiding

De omarming van ITS (*Intelligent Transport Systems*) neemt internationaal een grote vlucht. Binnen Europa is het Platform C-ITS de plaats waar beleidsvoorbereiders, auto-industrie, ICT producenten en dienstverleners als infrastructuurbeheerders zich gezamenlijk buigen over de voorwaarden voor toepassing van C-ITS. Nederland wil binnen de EU, maar ook wereldwijd een voorlopers rol vervullen bij de ontwikkeling van ITS. Dat betekent dat de ontwikkelingen in Nederland zullen moeten passen in deze internationale context. De beoogde coöperatieve systemen zullen niet stoppen aan de grens. Op langere termijn zal een gestandaardiseerde EU brede uitrol noodzakelijk zijn. Voor het goed kunnen benutten van de technische ontwikkelingen, de beleidsontwikkelingen en de business ontwikkelingen is het van belang de juridische kaders in kaart te brengen en deze te confronteren met de bovengenoemde ontwikkelingen.

Juridische inbedding van C-ITS

Als het gaat om de vraag naar de juridische inbedding van C-ITS dan kun je onderscheid maken in twee soorten wetgeving. De eerste is de ordeningswetgeving waarin regels worden gesteld voor voertuigen en voor het verkeer. Deze regels zullen ongetwijfeld aan de veranderingen in de techniek, zoals zelfsturend en coöperatief rijden moeten worden aangepast. Deze uitdaging wordt op wereld schaal opgepakt in de vorm van aanpassing van het Verdrag van Wenen. Dat geldt minder voor de algemene rechtsgebieden die in het kader van C-ITS van belang zijn, zoals aansprakelijkheid, data-protectie en data-zeggenschap. Deze kennen hun eigen regels die niet zo snel aan een nieuw technisch en maatschappelijk fenomeen als C-ITC zullen worden aangepast. Een uitzondering vormt op termijn wellicht de aansprakelijkheid, die door de komst van zelfsturend en coöperatief rijden aanleiding kan geven tot de keuze in te grijpen in het wettelijk kader. Als je een jurist echter vraagt of zelfsturend of coöperatief rijden in de praktijk een juridische regeling vergt ten aanzien van dataprotectie of datazeggenschap, zal het antwoord al snel ontkennend luiden. Zolang je je aan de regels houdt kan er weinig misgaan, en ook als je je niet aan de regels houdt dan is altijd een gang naar de rechter mogelijk, die vervolgens een uitspraak doet en daarmee de zaak beslecht. Kortom juridisch is de wereld geregeld en nieuwe fenomenen krijgen, met uitzondering van zeer specifieke wetgeving, vanzelf een plaats in het bestaande recht, totdat blijkt dat de gang naar de rechter niet leidt tot een bevredigende uitkomst, of dat rechters een zodanig eenduidige lijn volgen in hun uitspraken dat overwogen moet worden deze in de wet op te nemen.

Toch is het goed om goed te kijken naar de algemene juridische aspecten van C-ITS. In de eerste plaats om het voor ontwikkelaars en dienstverleners mogelijk te maken rekening te houden met het juridisch kader door een brug te slaan tussen techniek en dienstverlening aan de ene kant en het juridisch kader aan de andere kant. Daarnaast is een belangrijke reden het verkrijgen van een zo groot mogelijke mate van rechtszekerheid. Partijen die veel geld investeren in de ontwikkeling van C-ITS kunnen het zich niet veroorloven achteraf te worden verrast door een uitspraak van de rechter over bijvoorbeeld hun aansprakelijkheid bij schade of bij schending van de privacy of het datarecht.

De juridische inbedding van C-ITS is dus vooral een kwestie van samen optrekken en voorkomen dat juridische issues onnodig showstoppers kunnen worden. Het bereiken van zoveel mogelijk rechtszekerheid is daarbij een belangrijke doelstelling.

Waar willen we naartoe

In het komende halfjaar is het streven erop gericht om de belangrijkste juridische issues in C-ITS te benoemen, te agenderen en in gesprek met de stakeholders oplossingen te formuleren ten behoeve van de ontwikkeling van C-ITS. Het gaat er in het komende halfjaar om:

- Meer kennis en bewustzijn bij NL belanghebbenden over mogelijke juridische problemen en oplossingen op het terrein van C-ITS.
- Gecoördineerde en gedragen activiteiten vanuit NL partijen passend bij de ambities om koploper te zijn.
- het samen inventariseren, analyseren en prioriteren van risico's en beheersmaatregelen bij een aantal beeldbepalende en concrete use cases voor de toepassing van C-ITS. het opstellen en bijhouden van handreikingen (per onderdeel), met best practices en een overzicht van relevante publicaties , spelers en FAQ&A's.

Waar staan we nu

Recent is een aantal ontwikkelingen in gang gezet om beter zicht te krijgen op de juridische implicaties van zelfsturende auto's en ook van C-ITS op een drietal meest betrokken rechtsgebieden: Dataprotectie, Datazeggenschap en Aansprakelijkheid.

Bij de onderstaande paragrafen zijn vragen geformuleerd voor de discussie aan de juridische tafel C-ITS van 11 juni 2015.

Data protectie.

De regels rond dataprotectie vloeien voort uit EU richtlijnen, die in Nederland zijn opgenomen in de Wet bescherming persoonsgegeven, terwijl de voor C-ITS relevante bijzondere dataprotectieregels voor de telecommunicatiesector zijn opgenomen in de Telecommunicatiewet. Daarnaast zijn ook andere wetten relevant, zoals blijkt uit het volgende voorbeeld.

Recent speelde bijvoorbeeld dat de Belastingdienst parkeergegevens op kenteken opvroeg bij een parkeergarage. Na aanvankelijke weigering op grond van privacyoverwegingen bij het parkeerbedrijf bepaalde de rechter dat de gegevens aan de Belastingdienst moesten worden overgedragen. Daarmee werd de privacy van de klanten niet geschonden, de Belastingdienst heeft immers geheimhoudingsplicht. Het informatierecht van de fiscus ging in dit geval voor, en aangezien dit informatierecht niet snel zal worden beperkt is het goed om hiermee bij het opzetten van C-ITS diensten en het communiceren daarover rekening te houden.

Met de stakeholders is afgesproken om zowel naar coöperatieve als connected toepassingen te kijken. Het wettelijk kader ligt vast, en dus zullen de activiteiten worden gericht op het toelichten van de wettelijke regeling in relatie tot ontwikkelingen in het veld, zoals privacyverklaringen van voertuigfabrikanten. Daarbij wordt gestreefd naar het praktisch hanteerbaar maken van het kader door de stakeholders, bijvoorbeeld door het ontwikkelen van concrete handreikingen. Een nauwkeurige beschrijving van de werking van de C-ITS toepassing is van groot belang als startpunt van zo'n handreiking, aangezien de wijze van inrichting daarvan kan bepalen of wel of niet aan de wettelijke verplichtingen kan worden voldaan. Doelbinding, transparantie en accountability zijn hierbij de sleutelbegrippen. Om meer zicht te krijgen op de mogelijke privacy risico's binnen de verschillende C-ITS ontwikkelingen is een risico analyse dataprotectie uitgevoerd. Daarbij kwam de vraag aan de orde wat nu precies de privacy risico's zijn van C-ITS diensten en hoe de privacy van de gebruikers het beste kan worden beschermd. Ook werd al in de aanloop naar de sessie de vraag gesteld in welke mate anonimiseren van data mogelijk is en of dit een afdoende bijdrage kan leveren aan het behouden van de privacy van de gebruiker.

Risico-analyse

Samenvatting

Op 3 september werd de risico-analysesessie dataprotectie gehouden aan de hand van de vier geselecteerde use cases: Road works warning, Spookfiles, Floating car data en Verkeerslicht beïnvloeding. Tijdens de sessie is de indeling in use cases losgelaten. Deels omdat de use cases waar het om privacy ging nogal overlapten, maar ook omdat tijdens de bijeenkomst bleek dat behandeling per use case met name voor de externe dataprotectie deskundigen een meer gedetailleerde voorbereiding vergen. Ondanks, of misschien wel dankzij, deze aanpassing is een groot aantal zeer uiteenlopende risico's benoemd. Om de risico's zinvol te kunnen analyseren, prioriteren en van maatregelen te voorzien zijn ze onder verdeeld in hoofd- en subgroepen. De hoofdgroepen zijn:

- Beleidsmatige risico's
- Operationele risico's

Na deze indeling bleef nog een zeer kleine restgroep over. De beleidsmatige risico's zijn onder te verdelen in verschillende groepen. Ten eerste de politieke risico's. Die liggen met name op het vlak van negatieve beeldvorming (zie KM heffing), ongeacht of deze op feiten is gebaseerd of niet. Ook een mogelijke of gepercipieerde bedreiging van de keuzevrijheid van de bestuurder om zijn route zelf te kiezen valt daaronder. Vervolgens kunnen problemen optreden bij de doelbinding. Hier gaat het om of de doelen helder genoeg zijn, of het doel niet wordt opgerekt of dat het onderscheid tussen doelen waarmee is ingestemd en wettelijke doelen zoals opsporing en –fiscale- controle wel helder genoeg is. Een andere groep risico's heeft betrekking op de grondslag van de verwerking van persoonsgegevens. Daarbij kan worden gedacht aan het doorleveren van gegevens zonder voldoende wettelijke grondslag, en tot het combineren van allerlei op zich legitiem verkregen persoonsgegevens tot een ongewenst persoonsbeeld (profiling). Het gebruik door bestuursorganen van hun wettelijke bevoegdheden tot het opvragen van gegevens is gebaseerd op een separate rechtsgrondslag. Onvoldoende besef van deze wettelijke bevoegdheden bij de gebruikers kan hier tot problemen leiden als deze niet vooraf worden gewezen op het feit dat de dienstverlener geen zeggenschap heeft over het gebruik van wettelijke bevoegdheden bij opsporing, staatsveiligheid en belastingcontroles.

Ook internationaal kan het nodige misgaan. Zo bestaan er, ondanks de zelfde wettelijke basis in de Privacy Richtlijn, aanzienlijke verschillen tussen de wetgevingen van de West-Europese landen. Ook van de kant van de OEM's komt een bedreiging voor zover zij bijvoorbeeld onvoldoende samenwerken. Dat laatste lijkt overigens niet het geval gelet op het gemeenschappelijk protocol dat de Europese OEM's recent hebben uitgebracht. Ook werd een teveel aan dataprotectiemaatregelen als een risico gezien.

Bij de operationele risico's was er vooral zorg over externe inbreuken, waarbij een gebrek aan (fysiek) toezicht als reëel risico werd gezien. Dit zou kunnen leiden tot onbevoegd volgen van voertuigen en sabotage van het C-ITS systeem. Ook de niet-naleving van de wettelijke bepalingen werd als risico aangemerkt. Daarbij gaat het om het niet in acht nemen van bewaar- en vernietigingstermijnen, het op de juiste wijze invullen van de rol van de verantwoordelijke en bijvoorbeeld snelheidshandhaving door gebruik te maken van de C-ITS voorziening. Function creep behoort ook tot deze categorie. In de restcategorie kwam nog naar voren dat de privacy belangen heel goed op gespannen voet kunnen komen te staan met de commerciële belangen van dienstverleners en OEM's.

Als voorlopige conclusie kan worden vastgesteld dat anonimiseren van persoonsgegevens in een zo vroeg mogelijk stadium plaats moet vinden voor een optimale dataprotectie. Niettemin zullen privacy by design en privacy by default nooit alleen tot een goed resultaat kunnen leiden. Ook de verantwoordelijkheden voor data controller en data processor zullen goed moeten worden belegd voor de C-ITS en Connected toepassingen. Het ontwikkelen van privacy bewustzijn bij alle betrokkenen is een belangrijke voorwaarde voor succes. Dataprotectie is voor C-ITS toepassingen een license to operate. Zonder adequate dataprotectie is er voor de meeste C-ITS toepassingen geen bestaansrecht, laat staan een business case.

Documenten:

- NL-Wetgeving en toelichtingen
- Onderzoek juridische aspecten Spookfiles A58
- Data Protection Principles For Connected Vehicles (Verband Der Automobilindustrie-VDA, 3 november 2014)

De dataprotectieverklaring van de Europese autofabrikanten heeft ten doel aan te geven dat de fabrikanten privacy aandacht geven bij hun ontwerpen (Privacy by design) maar ook om de klanten te wijzen op hun eigen verantwoordelijkheid ten aanzien van dataprotectie. Hoewel met geen woord wordt gerept over de in de EU vigerende wetgeving, komt deze wel op verschillende plaatsen impliciet terug, in de vorm van tegemoetkoming aan de klant in plaats van een harde verplichting. In die zin zijn de principes wat misleidend. De scope van de verklaring is met name de innovaties in connected en vernetwerkte voertuigen. Onder de kop transparantie verwijst de verklaring naar het streven van de leveranciers naar adequate informatievoorziening omtrent de data in de voertuigen en het gebruik van deze data. Daarbij worden 6 categorieën data onderscheiden. Deze categorieën komen ten dele overeen met de categorieën uit de EU Richtlijn, maar het lijkt erop dat de autofabrikanten de privacy aspecten verbinden aan de zeggenschap over de data. Met name de technische en service data lijken op die manier minder bescherming te genieten omdat zij 'van de fabrikant zijn'. Daar is juridisch geen grond voor, privacy wordt altijd beschermd, ongeacht wie de beschikking of de zeggenschap over de data heeft, en daarbij is de aard van de data bepalend. In lijn met de Richtlijn wordt het informed consent opgevoerd als middel om de data met toestemming van de klant te kunnen gebruiken. Daarbij gaat het echter over data in het kader van services die door de klant separaat worden afgenomen. Technische data en service data van het voertuig lijken daar niet onder te worden begrepen. De VDA streeft naar de implementatie van dezelfde sterke veiligheidscultuur in het connected voertuig, als ook in de industrie gebruikelijk is. Daarbij zal gebruik worden gemaakt proactief ontwikkelde beveiligingsmaatregelen om de data in het voertuig te beschermen, inclusief cryptografische maatregelen. Deze maatregelen betreffen zowel technische als persoonsgebonden data. Het stuk vermijdt iedere verwijzing naar de van toepassing zijn de wetgeving, volgens welke de fabrikanten verantwoordelijk zijn voor de bescherming van de door hen verzamelde persoonsgegevens, hetzij als verantwoordelijke hetzij als verwerker van persoonsgegevens.

- Consumer Privacy Protection Principles (Alliance of Automobile Manufacturers INC., Association of Global Automakers INC., 12 november 2015)

Deze dataprotectieverklaring van de wereldwijde auto-industrie onderkent de gevoeligheid van lokatiegegevens als gevoelige gegevens (covered information). Verder worden dezelfde issues benoemd als in de geldende EU Richtlijnen, zij het wat minder strak geformuleerd. Het heeft een beperkte juridische waarde, aangezien de wetgeving van de staten waar de dienst wordt verleend doorslaggevend is. De verklaring geeft aan dat de autofabrikanten zich bewust zijn van de privacy issues en dat ze van plan daar zorgvuldig mee om te gaan.

- Voorstel voor een nieuwe data protectie verordening (nog in wording)

- *Navraag bij het Ministerie van V&J levert op dat de huidige tekst van het voorstel zeer sterk afwijkt van het oorspronkelijk ontwerp van 2012, maar dat de wijzigingen ten opzichte van de huidige Richtlijn veelal beperkt zullen blijven tot aanscherpingen van het toezicht en de handhaving. Gezien de vele onzekerheden in de discussie hierover is een beoordeling voor het doel van de juridische tafel op dit moment minder zinvol. Inmiddels is de EU Raad van Ministers het eens geworden over een ontwerp tekst. Over de verschillende teksten zal in het komend halfjaar worden onderhandeld tussen de EU Raad, het EU Parlement en de EU Commissie. Als er eind 2015 een Verordening is kan deze in 2018 in werking treden. De directie HBJZ van IenM zal in juli een impactanalyse te maken van de verordening voor ons beleidsterrein. In augustus gevolgd door een analyse van de wettelijke grondslag voor de uitgebreide dataverzameling met C-ITS. Daarbij zullen zij onder meer het advies van WRR van ca. twee jaar geleden, diverse adviezen Rathenau en de kamerbrief van de Minister van EZ van nov. 2014 over bi data, dataprofiling en privacy betrekken.*

    - Stukken van WG4 (9 juni 2015) System's Governance & Privacy onder het Europese C-ITS Platform. (zie bijlage 2)

Datazeggenschap.

Coöperatieve ITS, waarbij voertuigen onderling en voertuigen en wegkant doorlopend met elkaar in verbinding staan, betekent dat grote hoeveelheden data van en naar voertuigen worden gezonden. In feite worden voertuigen rijdende zendmasten. De zeggenschap over de uitgezonden en ontvangen data is in principe een kwestie van bilaterale overeenkomsten tussen de verschillende betrokken partijen. Bij onderling dataverkeer tussen weggebruikers ligt een dergelijke overeenkomst niet voor de hand en zal moeten worden gekeken naar alternatieve rechtsvormen. Het overzicht dat ten behoeve van de Werkgroep 4 van het EU C-ITS platform is gemaakt biedt een basis voor de discussie. In het document worden de verschillende wijzen waarop door stakeholders met de data wordt omgegaan geïnventariseerd. Daarbij wordt sterk vanuit de positie van de fabrikanten en dienstverleners gedacht, en minder vanuit de consument en de wegbeheerder.

Bij het maken van een goede belangenafweging moet zeker de positie van de eindgebruiker worden betrokken. Tevens moet worden gezorgd voor transparantie en accountability met betrekking tot doel van en werkwijze bij de overdracht van data. Aan de hand van de uitkomsten van de risicoanalyse kan met alle betrokkenen worden gezocht naar een evenwichtig gemeenschappelijk model waarin alle partijen zich kunnen vinden. Daarbij zal met name de positie van de eindgebruiker als relatief zwakke partij moeten worden bewaakt.

Een bijzonder plaats als het gaat om datazeggenschap wordt ingenomen door de data die moet worden verstrekt aan officiële instanties, bijvoorbeeld met het oog op toelating van een voertuig, of bij het organiseren van dealer-onafhankelijk onderhoud. Hierbij kunnen zeggenschapskwesties gemakkelijk tot maatschappelijk ongewenste effecten leiden, zoals inperking van concurrentie tussen onderhoudsbedrijven en een gebrek aan adequate informatie met betrekking tot toelating van een voertuig, omdat de software van de systemen in de auto op elk moment kan worden gewijzigd. Een van de vragen die het meest urgent lijkt binnen het datazeggenschapsdomein is hoe datazeggenschap op een evenwichtige manier moeten worden verdeeld tussen de verschillende stakeholders, van autofabrikant tot en met eindgebruiker.

Risicoanalyse

Samenvatting

Op 10 september werd de risico-analysesessie datazeggenschap gehouden aan de hand van de vier geselecteerde use cases: Road works warning, Spookfiles, Floating car data en Verkeerslichtbeïnvloeding. Bij Roadworks warning liggen de risico's vooral bij het ontbreken van consensus over de zeggenschapsverdeling, waardoor mogelijk bepaalde data misschien niet meer beschikbaar zijn in bepaalde gevallen. Hetzelfde risico kan zich voordoen bij Spookfiles. Het datazeggenschapsrisico bij Floating Car Data is vooral dat de zeggenschap niet goed geregeld is tussen de verschillende partijen, gebruikers, OEM's/SP's en wegbeheerder, terwijl deze data wel de basisgrondstof vormen voor veel C-ITS toepassingen. Ook belemmerende of uiteenlopende voorwaarden die OEM's stellen aan de levering van data zijn alleen met heldere afspraken over de datazeggenschap het hoofd te bieden. Bij de verkeerslicht beïnvloeding kan de datazeggenschap in relatie tot de prioritering bij de verkeerslichten tot onduidelijkheid leiden. Ook de zeggenschap over eventueel opgebouwde intelligentie in het systeem zal goed moeten worden geregeld.

<u>Documenten:</u>

- Relevante NL wetgeving
- Onderzoek juridische aspecten Spookfiles A58
- Access to vehicle resources and data (summary for the C-ITS Platform WP 6, nieuwe versie op komst). (nb. Dit document richt zich vooral op technische mogelijkheden en niet de principiële uitgangsgpunten).

Aansprakelijkheid

Recent onderzoek van de VU naar de aansprakelijkheid in relatie tot zelfrijdende auto's, levert veel inzichten voor belanghebbenden. Ook fabrikanten van voertuigen en systemen alsmede verzekeraars lijken zich al tamelijk goed voor te bereiden op de mogelijke aansprakelijkheidskwesties, zoals onder meer blijkt uit het AON-rapport 'Als de auto autonoom wordt'. Om de ontwikkelingen goed te volgen en daarop zo nodig te anticiperen zal AON aan de juridische tafel worden uitgenodigd. In het rapport wordt bijvoorbeeld ten aanzien van de bewijslast nadrukkelijk gesproken over de mogelijkheid om een zogenoemde Event-data-recorder (EDR) in coöperatieve voertuigen te installeren, om zo de bewijsvoering bij ongevallen te vergemakkelijken. Een dergelijke voorziening zal wel onmiddellijk nieuwe dataprotectie- en datazeggenschapsvragen met zich brengen. Welke vragen en eisen dan vooral van toepassing zijn op C-ITS kan wel nader in beeld worden gebracht. Enkele van deze vragen werden al in de aanloop naar de risicoanalysesessies geformuleerd, zoals de vraag welke juridische issues de installatie van een EDR met zich mee kan brengen. En hoe te komen tot een afweging tussen belangen van voor o.a. gebruikers, fabrikanten en overheden. Ook de vraag naar de verdeling van de aansprakelijkheidsrisico's over partijen en de rol van de verzekeraars hierbij zal moeten worden beantwoord.

Risico-analyse

Samenvatting

Op 10 september werd de risico-analysesessie aansprakelijkheid gehouden aan de hand van de vier geselecteerde use cases: Road works warning, Spookfiles, Floating car data en Verkeerslichtbeïnvloeding. Vooropgesteld kan worden dat de wettelijke bescherming van het slachtoffer niet verandert doordat de bestuurder slechts van advies wordt voorzien. Dus als het gaat

om aansprakelijkheid bij Road works warning dan zal deze vooralsnog niet erg veranderen zolang het om adviezen gaat en niet om technische ingrepen in het voertuig. Wel zal de aansprakelijkheidsverdeling tussen wegbeheerder, in-car dienstverlener en bestuurder afhankelijk van de omstandigheden en de aard van de dienst onduidelijker kunnen worden. Bij Spookfiles speelt ook een adviessituatie en kan mogelijk dezelfde onduidelijkheid ontstaan. Wat gebeurt er als een aanrijding plaatsvindt terwijl de bestuurder het advies opvolgt? Of juist negeert? Dezelfde onduidelijkheid kan op den duur ontstaan bij het gebruik van Floating car data. Bij de verkeerslichtbeïnvloeding kan het falen van het systeem, waarbij beide rijrichtingen 'groen licht' hebben wellicht kunnen leiden tot een meer gedeelde aansprakelijkheid tussen de wegbeheerder en de verantwoordelijke voor het systeem. Daarbij komt nog het risico van samenloop en cumulatie van toepassingen die tot een exponentiele toename van de complexiteit kan leiden, met alle gevolgen voor de aansprakelijkheidsverdeling van dien.

Documenten:

- Relevante NL wetgeving
- Onderzoeksrapporten in opdracht van het Ministerie van I&M
  - Zelfrijdende auto's en het Verdrag van Wenen inzake het wegverkeer (I&M-VU 2015)
  - Aansprakelijkheidsaspecten van zelfrijdende auto's (I&M-VU 2015)
- Als de auto autonoom wordt (AON, april 2015)
- Onderzoek juridische aspecten Spookfiles A58

Aanpak Connecting Mobility en Ditcm na de kick-off meeting

In de eerste juridische tafelsessie is in samenspraak met de aanwezige stakeholders de nodige richting gegeven aan de aanpak voor de voorziene tafelperiode, tot en met oktober 2015. Afgesproken is om op basis van de lijst van use cases die ook bij de tafels 'Dutch Profiles' en 'Architectuur' worden gebruikt een viertal use cases te selecteren voor nadere analyse. De doelstelling is om binnen de afgesproken format te komen tot een samenhangend inzicht waardoor juridische issues kunnen worden gedetecteerd en zo nodig opgelost. De eerste fase is de voorbereiding van de workshops rond de verschillende rechtsgebieden. Deze zal met de meest betrokken tafelgenoten worden gedaan. Uitkomst van deze verkenning is een overzicht van gedetecteerde juridische issues. Deze zullen in verschillende workshops worden gehanteerd bij de risicoanalyse van de geselecteerde use cases.

Bijlage 1

Use Cases

Tijdens de tafelbijeenkomst van 6 juni is een viertal use cases geselecteerd om nader te onderwerpen aan een juridische risico-analyse die in de eerste helft van september zal plaatsvinden. Vastgesteld is dat de beschrijvingen van de use cases nog niet scherp genoeg zijn voor een dergelijke analyse. De desbetreffende tafel verwacht begin september de use cases voldoende scherp te hebben gedefinieerd. Het gaat om de volgende use cases:

Snelheidsadviesdienst

Bij deze dienst grijpt het coöperatieve systeem niet rechtstreeks in in de techniek van het voertuig, maar voorziet een display in de auto in adviezen ten aanzien van de snelheid of rijbaan, vooralsnog alleen op snelwegen. De bestuurder blijft dus in control van het voertuig. Voorbeeld: Spookfiledienst A58.

Floating vehicle data

Floating vehicle data zijn verkeersgegevens die doorlopend worden verzameld van GSM en GPS systemen die weggebruikers aan hebben staan, zoals bijvoorbeeld reistijden. Bij deze use case spelen zowel de herleidbaarheid van de gegevens tot een concrete weggebruiker, de zeggenschap over deze gegevens, die immers een commerciële waarde vertegenwoordigen en de aansprakelijkheid bij het gebruik van de gegevens een rol.

Road works warning

Floating vehicle data zijn verkeersgegevens die doorlopend worden verzameld van GSM en GPS systemen die weggebruikers aan hebben staan, zoals bijvoorbeeld reistijden. Bij deze use case spelen In het kader van Road Works Warning (RWW) ontvangt het naderende verkeer bij wegwerkzaamheden waarschuwingen en beperkingen van bijvoorbeeld snelheid of inhaalmogelijkheden. De juridische aspecten zitten hier met name in de dataprotectie bij het gebruik van de floating car data en de aansprakelijkheid door eventuele fouten die tot schade leiden.

Compass4D verkeerslichten

Bij Compass4D zendt en ontvangt een voertuig via een on board unit doorstroom informatie. Hierdoor kunnen de verkeerslichten worden beïnvloed hetgeen de doorstroming bevorderd. Bijzondere voorrang kan worden gecreëerd voor bijvoorbeeld hulpdiensten en openbaar vervoer. Juridische vragen kunnen zich voordoen rond privacy en aansprakelijkheid.

Bijlage 2
EU C-ITS WG 4

Documenten

Ontwerp input CAM/DENM berichten derde meeting WG 4 Governance en Privacy
Het document is geschreven vanuit het ETSI perspectief met betrekking tot de security van Cam/Denm berichten. Een misvatting in het document lijkt dat met goede security ook de privacy beschermd is. Security is weliswaar een voorwaarde voor privacy, maar niet afdoende. Van groot belang bij privacy zijn niet alleen de externe- maar met name ook de interne bedreigingen. Wat gebeurt er met de verzamelde gegevens? Welke ketenpartners beschikken over persoonsgebonden lokatiegegevens?

In het stuk wordt gerefereerd aan 'services'. Niet duidelijk is welke services worden bedoeld. In de Richtlijn wordt onderscheid gemaakt in drie soorten diensten:

1. Telecommunicatiediensten, geleverd door de telecom serviceprovider, zoals bellen sms etc.
2. Diensten van de informatiemaatschappij, geleverd door webwinkels. De beperkingen hebben betrekking op het plaatsen van cookies. Deze dienst wordt in het stuk ten onrechte aangehaald.
3. Diensten met toegevoegde waarde. Hieronder vallen de C-ITS diensten. Deze diensten horen vanwege hun combinatie van persoonsgegevens en locatie in de hoogste beschermingscategorie. Dit punt is in het stuk gemist.

Ik zou de summary vervangen door:

1. CAM en DENM messages bevatten persoonsgegevens met extra bescherming vanwege de combinatie met locatiegegevens.
2. Het gebruik van CAM DENM berichten vraagt altijd een informed consent van de voertuigeigenaar/gebruiker. De bewijslast ten aanzien van het verkrijgen van het consent en ten aanzien van het verstrekt hebben van de relevante informatie ligt bij de dienstverlener.

Legal basis for processing personal data in C-ITS context 0.1 (30 March 2015, Kujala)
Dit document kiest weer een ander uitgangspunt, niet beveiliging, maar de ETSI definitie. Dat levert het probleem op dat daarin de value added services anders worden gedefinieerd. Alle drie ETSI categorieën vallen binnen de Richtlijn definitie van value added services.

In het document wordt gekeken naar art. 7 van de Richtlijn 95/46/EC terwijl de gedetailleerde regeling voor telecommunicatiediensten te vinden is in Richtlijn 2002/58. Daardoor is het document slechts beschrijving en deels interpretatie van de Richtlijn. Meer van belang is om te kijken naar wat er feitelijk gebeurt.

Gelet op de basisrichtlijn en de meer specifieke Richtlijn 2002/58 stelt het document dat twee grondslagen voor de verwerking van data in C-ITS het meest voor de hand liggen:

1. informed consent , een verzwaarde vorm van het genoemde consent uit Art. 7a
2. Verwerking in het kader van de C-ITS dienstverleningsovereenkomst

De overige gronden zijn niet goed voorstelbaar tenzij er een C-ITS wet komt met verplichte deelname(7c), bijvoorbeeld op termijn voorstelbaar bij full automated driving, of e-call ter bescherming van een vitaal belang van de betrokkene wordt aangemerkt (7d), of de verkeersveiligheid als noodzakelijk publiek belang wordt gedefinieerd dat een inbreuk op de privacy rechtvaardigt (7e). zal niet snel als grond worden aangemerkt, tenzij bijvoorbeeld bij e-call. Bij de gerechtvaardigde belangen (7f) wordt verwezen naar een stuk van WP29, (Privacy commissioners) van 2014 over dit artikel. Het stuk geeft handvatten om in concrete gevallen tot een juiste afweging van de 'legitimate interests' te komen, maar lijkt mij minder geschikt om in het algemeen een toepasbaarheid van het artikel bij C-ITS uit af te leiden.

De conclusie stelt terecht dat buiten art 7a (informed) consent, er geen artikel in de Richtlijn 95/46/EG is dat de juridische basis voor het gebruik van persoonsgegevens in algemene zin rechtvaardigt. Deze conclusie valt samen met het in dit kader van toepassing zijnde Artikel 9 en overweging 35 van de Richtlijn 2002/58/EG, waarin over de behandeling van locatiegegevens niet zijnde verkeersgegevens wordt vastgelegd dat deze uitsluitende met ondubbelzinnige toestemming van de betrokkene mag plaatsvinden.

De vraag of de gebruikte data binnen C-ITS persoonsgegevens zijn wordt in een ander paper of hoofdstuk behandeld. (nog niet beschikbaar)

Navigating the C-ITS Data Protection Landscape

Dit verzameldocument omvat ook de voorgaande documenten als hoofdstukken. Data protectie wordt sterk benaderd vanuit de beveiliging. Het document heeft bovendien dataprotectie in de kop, maar lijkt breder door het toevoegen van governance, data-elementen en procesinformatie. Aan de andere kant moet het stuk specifiek handreikingen gaan bieden voor de omgang met data door zowel de overheid als belangstellende app-bouwers. Het belang van locatie als essentieel data-element wordt niet onderkent, behalve bij diensten als points of interest, parking app's en lokale e-commerce. De geschetste bedreigingen omvat niet alleen dataprotectie- maar ook andere bedreigingen, zoals gebrek aan controle over dataverkeer vanuit de auto, hergebruik, profiling, verlies van anonimiteit, verlies van vertrouwen in het ITS-systeem en misbruik. Aan de andere kant worden de mogelijkheden van ongewenste identificatie via CAM en DENM berichten met persoonsgegevens onderkent. Daarbij wordt steeds uitgegaan van een aanval van buitenaf, en niet ingegaan op interne bedreigingen in de informatieketen van verantwoordelijke dienstverleners en verwerkers. Op de externe bedreigingen worden maatregelen genomen (Guidance) die door de lid-staten kunnen worden gebruikt bij proeven en implementatie. Naast aanbevelingen zijn voorlopige conclusies getrokken op basis van wat tot nu toe in het rapport is opgenomen. De belangrijkste is dat de privacyrichtlijnen van toepassing zijn, maar bij de interpretatie daarvan lijken nog geen deskundigen op het gebied van dataprotectie te zijn betrokken. In de commentaren van WG-leden wordt nader verwezen naar de EU dataprotectie richtlijnen zonder dat daaraan concrete conclusies worden verbonden. De aanbevelingen komen neer op het advies je aan de (privacy) wetgeving te houden.

Report Osborne Clarke advocaten

In een rapportage van het advocatenkantoor van augustus 2014 wordt de regelgeving rond e-call en verzekeren met behulp van een EDR in de conceptfase weergegeven. Inmiddels is de Verordening e-call van kracht (Vo (EU) nr 305/2013), en de concept verordening dataprotectie kan eind 2015 gereed zijn.

Altijd aan de wet houden als het om dataprotectie gaat lijkt het devies, zowel uit juridisch als uit marketing oogpunt. Bij e-call is de dataprotectiewetgeving van toepassing. Er is dus geen sprake van een in te vullen juridisch tekort.

Het gaat ook hier vooral om een marketingafweging voor de verzekeraars zoals bijvoorbeeld: moet er een premiedifferentiatie komen naar mate van informatieverstrekking?

Bijlage 3

Definities van connected en coöperatief, zoals gebruikt door WG5 van EU C-ITS Platform:

Connected means that data/information will be sent to and from vehicles/drivers (or broader road users) by all communication means but mainly by cellular 3/4G/LTE (for information and advice) and for specific critical services by short range Wifi-p (warnings). The information received in the vehicle will be used by the drivers themselves.
Cooperative means that the data will be sent from roadside to and from the vehicles (V2I2V) and between vehicles (V2V) by all communication means but mainly by short/range Wifi-p (control and warnings) and less by cellular 3/4G/LTE (for less critical services). In the “cooperative” situation real coordination takes place between vehicles mutually and between vehicles and roadside. This coordination can take place by a driver action (max speed; initially during day one) or automatically by the vehicle systems themselves (eg CACC).

Bijlage 4

Bevindingen risico analyse C-ITS

Bijlage 5

Deelnemers risicoanalyse sessies

Dataprotectie, 3 september 2015

Gilles Ampt	
Tanja Braun	V-tron
Gerbrand Klijn	Grontmij
Marcel Otto	DGB
Mike Pinckaers	ANWB
Josee Sombekke	SIMS
Sussanne Strolenberg	RWS
Wim Vossebelt	V-Tron
Meine van Essen	RWS
Vincent Habers	IAM/pBB
Matilda Troost	RWS
Ernstjan van der Meer	AON
Martijn van der Veen	Privacy First
Wouter van Haaften	Universiteit van Amsterdam

Datazeggenschap en aansprakelijkheid, 10 september 2015

Tanja Braun	V-Tron
Marcel Otto	DGB
Mike Pinckaerts	ANWB
Josee Sombekke	SIMS
Joelle van den Broek	DITCM
Wouter van Haaften	Universiteit van Amsterdam
Steven Kuiper	SIMS