Smart Mobility Ronde Tafels Security en Juridisch

Verslag workshop Privacy by Design
Datum: 17 maart 2017 van 13.30 tot 16.30 uur
Lokatie: RWS/ LEF Westraven CLC

Facilitators:

- Gilles Ampt — voorzitter ronde tafel Security van Smart Mobility
- Wouter van Haaften — voorzitter ronde tafel Juridische aspecten Smart Mobility
- Marc van Lieshout — directeur Privacy en Identity Lab

Deelnemers:

- Laurens Schrijnen — RWS strategie adviseur Smart Mobility
- Marcel Otto — I&M/ Connecting Mobility
- Tiffany Vlemmings — NDW
- Pierre v.d. Stokker — Beijer Automotive
- Eric v.d. Ster — RWS/ CIV-strategie en beleid
- Patrick Dersjant — RWS/ CIV-security en privacy officer
- Melle Vroom — I&M/ DGB
- Theo Arts — RWS/ Groepsondernemingsraad
- Yvonne Dierikx — RWS/ CIV/ C-ITS corridor
- Peter Hoernig — Innovatiecentrale
- Nelleke Groen — RWS/ Corporate Dienst/ juridische zaken
- Tjeerd Tuitel — Pon/ Mind Mobility

1. Doelstelling van de workshop

Het doel van de workshop is om deelnemers inzicht te geven in de relevante privacy ontwerp-mogelijkheden bij ITS (smart mobility) projecten. Dit is van belang bij de opschaling van kleinere pilots naar grotere ITS projecten.

De uitkomst van de workshop zal zijn een eerste outline van deze ontwerp-mogelijkheden en het handelingsperspectief voor alle betrokken partijen bij ITS.

Daarnaast willen we met elkaar vaststellen of de gebruikte methode en benadering van Privacy voor herhaling vatbaar is voor andere (smart mobility) toepassingen dan vanmiddag.

Het is geen juridische workshop.

2. Discussie over privacy-uitgangspunten Smart Mobility

Niettemin zijn discussies over de juridische status van de voertuigdata nooit ver weg. Zo wordt gesproken over het criterium wanneer gegevens afkomstig uit een voertuig in juridische zin beschouwd moeten worden als persoonsgegevens. De minimale use case is het geven van één enkele melding aan de omgeving dat de mistlamp is aangegaan.

Er is een partij die zegt in de praktijk altijd te zorgen voor een goede verwerkingsgrondslag als ware de verwerkte voertuiggegevens persoonsgegevens. Duidelijk is ook dat zo min mogelijk persoonsgegevens moeten worden verwerkt.

Hoeveel gegevens zijn nodig voor het (verkeerskundige) doel? Het benodigde marktaandeel van voertuigen als databron is wellicht veel hoger buiten de Randstad en in 'dunne' uren dan binnen drukke gebieden en drukke perioden.

Naast de juridische legitimatie van de verwerking van persoonsgegevens voor een specifiek doel het vertrouwen van de automobilist (data subject) van groot belang. Dit komt later aan bod bij het RESPECT 4U framework.

Hoe om te gaan met platforms zoals HERE die alerts verkopen als dienst of als abonnement? Als je die wilt inkopen, wat betekent dat voor het privacy-verhaal?

Dit brengt ons op het secundaire gebruik van data. De casus van TomTom is bekend dat zij data (van gereden snelheden) wilden gaan verkopen aan de politie. Dit waren geaggregeerde gegevens, geen persoonsgegevens, er was geen privacy issue, maar het waren wel gegevens waar de klanten van TomTom aan hadden bijgedragen. Dit was niet acceptabel voor de klanten waarna TomTom het contract met de politie direct heeft ontbonden.

3. Use case Mist-waarschuwing

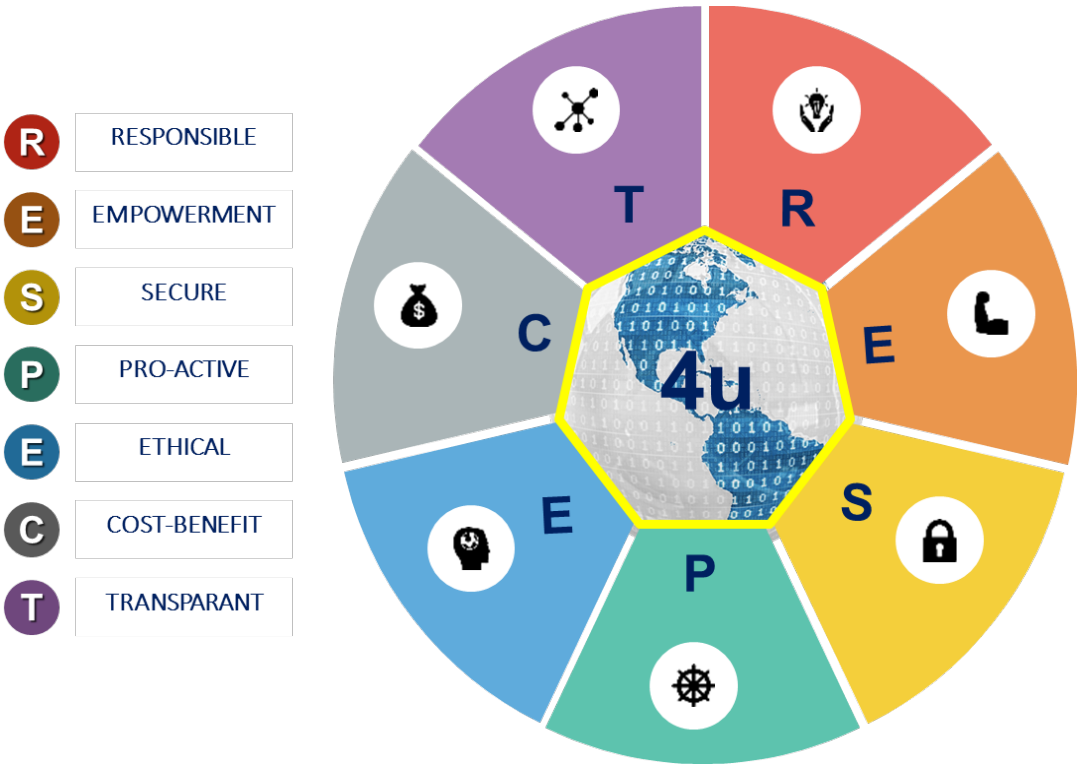
De casus is dat een voertuigsensor mist detecteert en dit gegeven (plaats, tijd) aan derden kan leveren die (al dan niet direct of via een keten) andere weggebruikers actief waarschuwt.

Voor het vervolg van de workshop beschouwen we dit als de verwerking van persoonsgegevens, in ieder geval aan de kant van de bron van de informatieketen.

De vraag wordt opgeworpen of het project wel tot een casus kan worden beperkt, en of er niet meer sprake is van een netwerk dan van een keten.

4. RESPECT 4 U oefening

Het R-E-S-P-E-C-T 4 U privacy framework is door de deelnemers doorlopen voor de use case van de mist-alert. De resultaten zijn ten dele plenair besproken. Het onderstaande verslag is een weergave van het besprokene en de input van de deelnemers.



- Responsible = verantwoordelijkheden van de data controller, maar ook verantwoordelijkheid voor bijv. een data gedragscode of data zeggenschap, niet alleen privacy gerelateerd.
    - veel vragen over verantwoordelijke, doel en doelbinding
    - wie beschikt (al) over welke gegevens? (zie ook Transparantie)
    - legitieme grondslag kan per controller in de informatieketen verschillend zijn.
    - toets de compatibiliteit van de doelen van de gegevensverwerking ook in de keten. Kijk uit voor 'function creep'.
    - als een partij meer gegevens ontvangt dan noodzakelijk hoef je die niet te gebruiken.
    - informed consent lijkt niet geschikt als grondslag voor veiligheid gerelateerde toepassingen. Sterker, daar lijkt een wettelijke grondslag meer toepasselijk (vgl. seat belts).
    - er is al een wet over het verplicht delen van verkeersveiligheidsinformatie tussen partijen, t.w. verordening 886/2013/EU [1] .

[1] GEDELEGEERDE VERORDENING (EU) Nr. 886/2013 VAN DE COMMISSIE van 15 mei 2013.

De Verordening heeft betrekking op gegevens en procedures voor het aanbieden, waar mogelijk, van minimale universele verkeersveiligheidsinformatie die kosteloos is voor de gebruikers. Het gaat om specifieke gevallen zoals: tijdelijk glad wegdek; dieren, mensen, obstakels en puin op de weg; onbeveiligde ongevalslocatie; kortstondige wegwerkzaamheden; verminderde zichtbaarheid; spookrijder; onbeheerde wegblokkade; uitzonderlijke weersomstandigheden. Het toepassingsgebied is beperkt tot door de lidstaten geselecteerde delen van het trans-Europees wegennet. De Verordening is in 2015 in werking getreden.

- toestemming vragen bij het delen van gegevens met een nieuwe partij, als principe, ook als het niet langer om persoonsgegevens gaat.
- proportionaliteit en subsidiariteit – in deze use case – afwegen tegen alternatieve bronnen, bijv. de beschikbare mistgegevens van het KNMI. Hier spelen de beoordeling van het kwalitatieve aspect en de resolutie/ fijnmazigheid van de gegevens een grote rol.

- Empowerment (van de data subject/ betrokkene/ automobilist) :
  - Over welke automobilist gaat het? De eigenaar van het voertuig, of de bestuurder, die al dan niet de vaste bestuurder is van het voertuig? Als je toestemming vraagt aan wie vraag je dat dan?
  - Bij poolauto's zoals bij RWS heeft de automobilist een andere positie dan een particulier. Er blijkt wat verwarring over het project in de zin dat het eerzijds gaat om een proef met RWS auto's en anderzijds wordt gesproken over opschaling.
  - Is er wel sprake van een relatie tussen verantwoordelijke en betrokkene bij een wettelijke bepaling als grondslag van de gegevensverwerking?
  - Hoe kun je de automobilist overtuigen van de meerwaarde?
  - Is opt out beter dan opt in? Vgl. het donorcodicil. Voor opt out is een wet nodig.
  - 3 fasen:
    - 1e fase is voorbereiding van de verwerking (o.a. PIA).
    - 2e fase is de verwerking zelf.
    - 3e fase is de afronding van de verwerking. Hierbij horen uitoefenen recht op inzage en recht op correctie en het naleven van bewaartermijnen.

- Secure = maatregelen voor de bescherming van persoonsgegevens, zoals anonimisering, pseudonimisering, toegangscontrole en versleuteling.
  - Zo vroeg mogelijk in de keten gegevens gaan anonimiseren zodat het geen persoonsgegevens meer zijn.
  - Wie houdt toezicht op anonimiseren van persoonsgegevens, bijv. kenteken-data? Is dat de afnemer in de keten die gegevens ontvangt/ bestelt?
  - Hoe bestendig is anonimiseren tegen de-anonimiseren? (casus in Tegenlicht van Smart City Amsterdam die geanonimiseerde gegevens levert aan Google).
  - In veel gevallen zal anonimiseren feitelijk neerkomen op pseudonimiseren omdat het proces toch omkeerbaar zal blijken.

- Pro-actief = ontwerpstrategieën die de privacy impact voor betrokkenen reduceren.
  - Legitiem doel staat voorop.
  - Meerwaarde van de data voor toepassing door de overheid moet duidelijk zijn.
  - Data-minimalisatie zo vroeg mogelijk in de keten toepassen, o.m. voor de gegevens die herleidbaarheid zijn naar een individu.
  - Niet alleen individuele use cases onderzoeken maar ook de samenhang van meerdere use cases tezamen.

- Ethisch:
    - Spelen ethische vragen minder als het om verkeersveiligheid gaat?
    - Is het ethisch verantwoord om gegevens niet te verwerken als het gaat om verkeersveiligheid?
    - Wat is de relatie tussen de activatie van mistlampen en andere variabalen zoals snelheid en aansprakelijkheid?

- Kosten / baten:
    - Hoe ontwikkelen kosten en baten zich op korte termijn en lange termijn?
    - Hoe is de verhouding van kosten en baten bij ieder van de verschillende entiteiten in de keten?
    - Immateriële en materiële baten
    - Hoeveel wordt er bespaard op ongelukken en weegt dat op tegen de kosten?
    - Kunnen kosten/ baten worden bepaald in combinatie met andere toepassingen en andere gegevens?

- Transparantie (van doelen, middelen, verantwoordelijkheden, processen en data):
    - Bestaat volledige transparantie?
    - Hoe krijgt de automobilist inzicht in zijn gegevens en kan die bepalen of zijn gegevens correct zijn? Hoe wordt dan “de” automobilist gedefinieerd en afgebakend? (zie ook Empowerment)
    - Welke data wordt door wie verwerkt en met wie gedeeld?
    - Waar botst transparantie met bedrijfsgeheimen en competitieve posities in de markt?

5. Bevindingen en Conclusies

a. De term Privacy by Design (term uit de GDPR/ Algemene Gegevensverwerking Verordening) suggereert dat je één grand design kunt maken voor een bepaalde toepassing. Beseft moet worden dat dit ontwerp niet in één stap gemaakt kan worden. Vergelijk het met keuzes maken uit een buffet, er is niet recept of één menu. Het ontwerpen van de gegevensverwerking – volgende de noodzakelijke privacy principes – is een proces.
b. Een ontwerp, hoe goed afgewogen en zorgvuldig gemaakt, kan niet statisch blijven en onveranderd voor zeg de komende 10 jaar. De afweging van proportionaliteit en subsidiariteit kan enige jaren laten anders uitvallen door allerlei maatschappelijke, economische en/ of technische ontwikkelingen. Het ontwerp is dus dynamisch.
c. Het is voor een categorie van toepassingen ondoenlijk en zeker onwenselijk om elke toepassing apart te ontwerpen. Het is noodzakelijk over de toepassingen (use cases) heen te generaliseren. Bijv. t.a.v. de beslissing waar in de keten aggregatie en/of anonimisatie van gegevens wordt ingezet.
d. Voor de opschaling van toepassingen, waar van heel veel voertuigen brongegevens benodigd zijn, is er een grote rol voor autofabrikanten (OEM's). Deze opschaling kan niet enkel bereikt worden met retrofit devices en nomadische devices.
e. Het is de verwachting dat er als snel een markt van alert services zal ontstaan. Daar moeten partijen adequaat op inspelen.
f. Voor veiligheidsalerts is er een (EU) Verordening (zie 1e voetnoot) die alle betrokken partijen verplicht om bepaalde bij hen bekende veiligheidsinformatie te registreren bij een aangewezen nationaal toegangspunt en op verzoek ook om niet of tegen vertrekkingskosten, door te leveren aan partijen die daarom vragen. In Nederland is NDW het nationaal toegangspunt en ziet de RDW toe op de registratie en distributie.

6. Acties/ follow up

- Dit verslag is aangeboden aan de deelnemers van de workshop voor review op inhoud en anonimiteit van het besprokene.
- De eerste verspreiding van resultaten van deze workshop heeft plaatsgevonden tijdens de Automotive Week op 30 maart tijdens de privacy sessie voor wegbeheerders.
- Dit verslag zal worden uitgewerkt in een document met een aantal potentiële ontwerp richtlijnen.