Rapport

Bètawetenschappen

Ontwerp voor privacy-vriendelijk kentekenparkeer-systeem

U202009270/HJO

van: Hugo Jonker

Open Universiteit
www.ou.nl

Inhoud

Managementsamenvatting

Dit rapport is het tweede deelrapport in een onderzoek in opdracht van de gemeente Haarlem naar privacyvriendelijk kentekenparkeren. In het eerste deelrapport zijn de juridische achtergronden en de diverse datastromen van het huidige systeem in kaart gebracht. In dit rapport wordt de balans tussen privacy, efficiëntie en gebruikersgemak voor betaald parkeren op conceptueel niveau behandeld.

Hierbij wordt allereerst verschillende systeemconcepten voor betaald parkeren besproken en de inherente balans tussen privacy, efficiëntie van controle en gebruikersgemak op hoofdlijnen weergegeven. Vervolgens worden de privacyaspecten van het huidige systeem geanalyseerd, aan de hand van de resultaten van het eerste deelrapport.

Dit geeft aanleiding tot de wens tot een privacyvriendelijker systeem voor parkeren. Aangezien de opdrachtgever al had gekozen voor kentekenparkeren, wordt vervolgens een systeemontwerp voor privacyvriendelijker kentekenparkeren gepresenteerd. Dit systeemontwerp is in cocreatie met de gemeente Haarlem tot stand gekomen. Het maakt gebruik van zogenaamde Bloom filters. Deze filters maken het mogelijk te toetsen of een kenteken parkeerrechten heeft, zonder de verzameling van alle kentekens met parkeerrechten beschikbaar te hebben.

Tot slot wordt ingezoomd op de privacy-problematiek rondom bezoekersparkeren voor mantelzorgontvangers. Op basis van een medische indicatie ontvangen deze personen ruimere mogelijkheden voor bezoekersparkeren. Echter, de consequentie hiervan is dat in het parkeersysteem is na te zoeken wie ruimere rechten heeft gebruikt – en daarmee dus een medische indicatie heeft. Er worden een aantal beleidsmatige alsmede een praktische oplossing voorgesteld om dit privacyprobleem te voorkomen.

1 Inleiding

De gemeente Haarlem heeft het PI.lab (een samenwerking tussen TNO, Radboud Universiteit Nijmegen en TILT, Universiteit van Tilburg) gevraagd om onderzoek te doen naar de huidige privacyvraagstukken rond kentekenparkeren en naar mogelijke oplossingsrichtingen. Voor deze opdracht zal TNO als penvoerder optreden.

De werkzaamheden behelzen twee taken:

- een desk study o.b.v. openbare bronnen over de huidige praktijk van kentekenparkeren en de daaraan verbonden privacyrisico's en
- de co-creatie van een meer privacyvriendelijke architectuur en -ontwerp voor kentekenparkeren met de gemeente Haarlem.

Onder kentekenparkeren wordt verstaan het gebruik van een digitale registratie van kentekens, eventueel in combinatie met andere gegevens, om het gebruik van parkeervergunningen en betaald parkeren te faciliteren.

Het gebruik van kentekenparkeren kan voordelen leveren maar roept ook vragen op t.a.v. de privacy van de parkerende automobilist. Dit onderzoek dient voor de gemeente Haarlem als ondersteuning om een privacyvriendelijke oplossing voor kentekenparkeren verder te ontwikkelen.

1.1. Probleemstelling

Het onderzoek in zijn geheel beoogt de volgende twee hoofdvragen te beantwoorden:

A. Welke privacy-gerelateerde risico’s bestaan er in hoofdlijnen in de huidige praktijk van kentekenparkeren in de gemeente Haarlem?
B. Wat zijn mogelijke privacyvriendelijke oplossingsrichtingen die door de gemeente Haarlem gebruikt kunnen worden om haar dienstverlening richting burgers te verbeteren in het kader van privacy?

Dit rapport behandelt uitsluitend de tweede hoofdvraag. In samenspraak met de opdrachtgever is besloten om deze vraag te beantwoorden door middel van ontwerp op hoofdlijnen. In het bijzonder splits deze vraag zich uit naar de volgende delen:

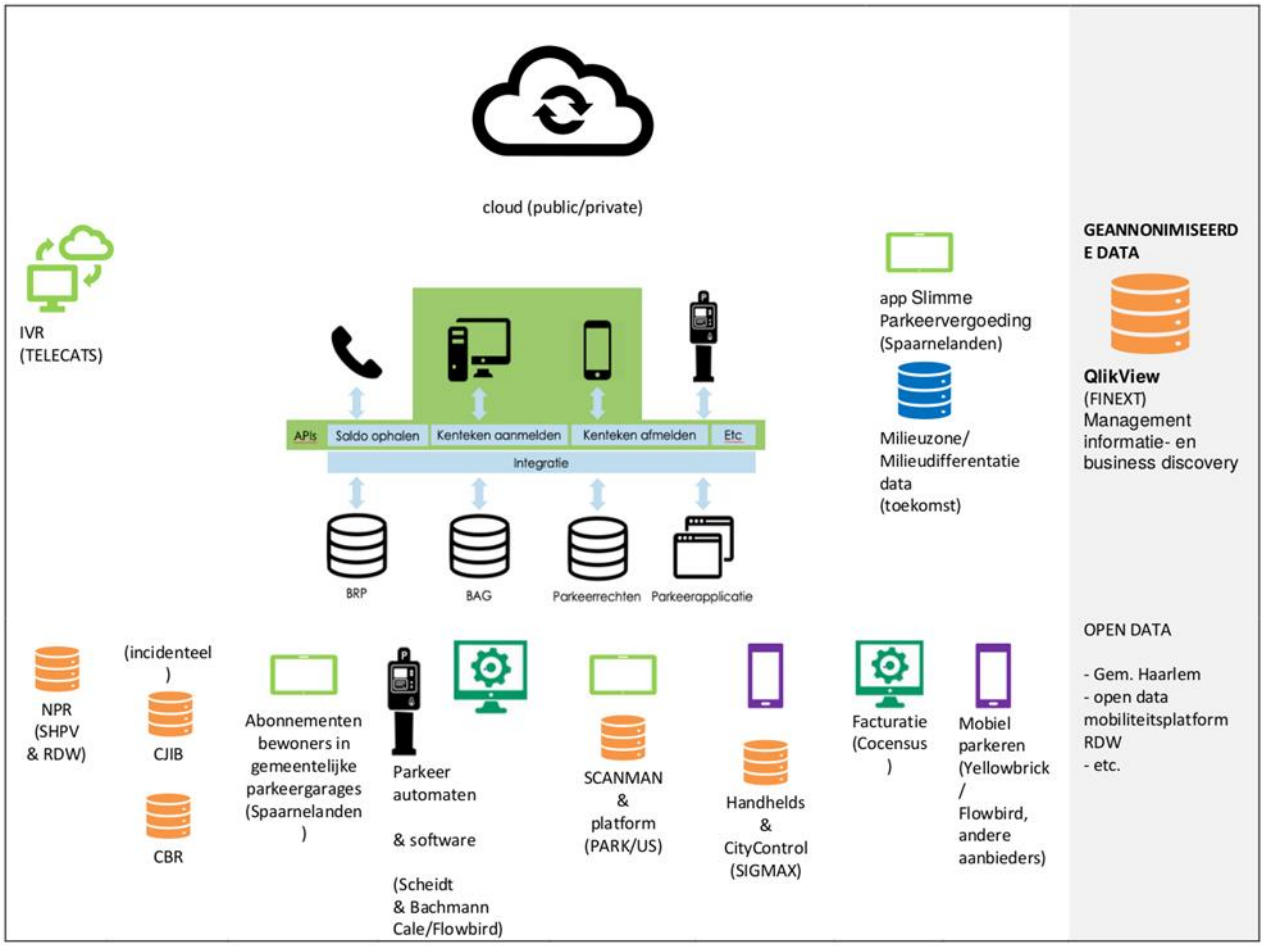
1. Een analyse van de privacy aspecten van het huidige systeem;
2. Een overzicht van de inherente balans tussen privacy en andere wenselijke eigenschappen van verschillende systeemconcepten voor betaald parkeren;
3. Een ontwerp op hoofdlijnen van een privacyvriendelijke kentekenparkeersysteem;
4. Het aandragen van oplossingsrichtingen voor bezoekersparkeren zodanig dat medische gegevens (in het bijzonder: gerelateerd aan mantelzorg) niet uit de parkeergegevens afgeleid kunnen worden.

Voor het systeemontwerp en de oplossingsrichtingen voor bezoekersparkeren wordt gezocht naar een oplossing die aansluit bij de huidige praktijk in de gemeente Haarlem in co-creatie met medewerkers van de gemeente Haarlem.

1.2 Korte samenvatting relevante aspecten eerste rapport

In het eerste deelrapport is onderzocht hoe de parkeerketen in Haarlem is ingericht, welke externe partners erbij betrokken zijn, welke gegevens onderling worden uitgewisseld, wat de juridische verankering is en welke privacy-gerelateerde zaken er een (juridische) rol spelen in de huidige situatie.

In figuur 1 (uit [TNO19]) wordt de parkeerketen op hoofdlijnen weergegeven, met daaromheen de verschillende partijen die hierop aangrijpen. Het groene gedeelte is in eigen beheer ontwikkeld door de gemeente, de overige stukken koppelen aan bestaande applicaties (waaronder die van derden).



Figuur 1. *Ecosysteem van kentekenparkeren in Haarlem* het kentekenparkeren-ecosysteem met centraal de hoofdlijnen parkeerketen gemeente Haarlem (bron: [TN019]).

De belangrijkste conclusies van het eerste deelrapport zijn:

1. Het doel en de noodzaak van gegevensverwerking door de (als “relatief veel” bestempelde) externe partijen zijn niet altijd evident.
2. Er worden verschillende bewaartermijnen gehanteerd door verschillende categorieën actoren. Dit maakt het ondoorzichtig waar en hoe lang persoonsgegevens zijn opgeslagen.
3. Er worden verschillende interpretaties m.b.t. anonimiseren, verwijderen, vernietigen en versleutelen van gegevens gehanteerd door de verschillende betrokken partijen.
4. Hoe persoonsgegevens technisch en organisatorisch beschermd worden, is slechts beperkt duidelijk geworden.

Merk op dat deze opmerkingen niet inherent aan het fenomeen kentekenparkeren lijken, maar veeleer van het ecosysteem.

1.3 Uitgangspunten en afbakening

Het doel van dit rapport is om de afwegingen tussen efficiëntie van controle, gebruiksgemak voor parkeerders en privacy van parkeerders inzichtelijk te maken. Een belangrijk aspect van privacy is helder te maken ten opzichte van wie de privacy vereist is. Ook dit aspect wordt in het voorliggend rapport besproken.

Het eerste uitgangspunt van het project is dat er een theoretisch ontwerp wordt geconstrueerd in cocreatie met de gemeente Haarlem, **aansluitend bij de huidige parkeersystematiek van de gemeente Haarlem**. Hierbij wordt benadrukt dat vanuit de opdrachtgever expliciet is verzocht om een ontwerp dat de huidige praktijk als uitgangspunt neemt en door ingrepen daarin tot een systeemontwerp komt dat privacy beter borgt. Het gevraagde doel is dus niet het ontwerp van een zo privacy-vriendelijk mogelijk theoretisch systeem, maar van een systeem dat, voor zover mogelijk, privacywaarborgen introduceert en verankerd binnen de bestaande praktijk.

De relevante bestaande praktijk wordt in het volgende hoofdstuk beschreven. Meest relevante inperking is dat het huidige systeem uitgaat van kentekenparkeren, en dat parkeren op basis van kenteken expliciet een uitgangspunt is van dit rapport.

De zeven uitgangspunten van privacy by design[1] zijn (kort samengevat) de volgende:

1. **Proactief, niet reactief.**
   Dit impliceert dat privacy-risico’s vóóraf worden voorkomen (preventie) in plaats van achteraf herstelacties te plegen.
2. **Privacy als standaard uitgangspunt.**
   Standaard uitgangspunt is privacy: als een gebruiker geen actie onderneemt, dan waarborgt het systeem zijn/haar privacy
3. **Privacy is ingebed in het systeemontwerp.**
   Het systeem wordt vanaf het begin ontworpen met inachtneming van privacy. Privacy wordt niet later alsnog toegevoegd.
4. **Volledige functionaliteit (positive-sum, niet zero-sum).**
   Soms wordt privacy als tegenhanger van andere functionaliteit beschouwd (bijv. security). Uitgangspunt is dat alle beoogde functionaliteit – zowel privacy-gerelateerd als anders – in samenhang gerealiseerd kan worden.

1 Zie bijv. https://en.wikipedia.org/wiki/Privacy_by_design#Foundational_principles_in_detail

5. **Sterke securitymaatregelen tijdens de gehele levenscyclus.**
   De security van het systeem (in het bijzonder: data) wordt door sterke maatregelen geborgd: end-to-end security. Dit geldt voor de gehele levenscyclus van het systeem, dus met inachtneming van onderhoud, uitbreiding en uitfasering van het systeem.
6. **Transparantie.**
   De correcte werking van het systeem kan door externe partijen onafhankelijk geverifieerd worden.
7. **Stel gebruiker centraal.**
   Dit principe omvat, maar gaat verder dan, de uitgangspunten *toestemming*, *accuraatheid*, *toegang*, *compliance*.

Merk op dat deze uitgangspunten de uitgangspunten van wettelijke regelingen zoals de AVG (GDPR op Europees niveau) bevatten, maar nog verder gaan.

We gebruiken deze uitgangspunten als inspiratie. Hierbij plaatsen we de kanttekening dat een uitgangspunt van het project is om een ontwerp te maken voor een privacyvriendelijker kentekenparkeersysteem dat nauw aansluit bij de huidige praktijk. Dat leidt ertoe dat het beoogde ontwerp niet een geheel onafhankelijk nieuw ontwerp is, maar veel meer een aanpassing van het bestaande ontwerp. Daardoor kunnen de uitgangspunten van privacy by design niet zonder meer rechtstreeks gehanteerd worden.

1.4 Structuur rapport

De verdere structuur van het rapport is als volgt.
In hoofdstuk 2 volgt een schets van het huidige systeem voor betaald parkeren in de gemeente Haarlem. Dit wordt gevolgd op privacy aspecten van de gegevensverwerking van dit systeem (hoofdstuk 3). Daarna volgt een beschouwing van privacy- en efficiency-aspecten van bestaande concepten van parkeersystemen, waaronder kentekenparkeren. Deze vormen de aanleiding in hoofdstuk 5 voor een theoretisch ontwerp op hoofdlijnen van een nieuw systeem voor betaald parkeren, dat nauw aansluit bij de huidige praktijk. In hoofdstuk 6 wordt vervolgens verschillende oplossingsrichtingen voor de privacyproblematiek rondom mantelzorgindicaties die zichtbaar zijn in de parkeerrechtendatabase besproken Tot slot volgt in hoofdstuk 7 de conclusie.

2. Schets huidig systeem betaald parkeren Haarlem

In het eerste deelrapport [TNO19] wordt in hoofdstuk 3 het systeem van kentekenparkeren in Haarlem en de daaraan gerelateerde datastromen (voor zover te achterhalen) beschreven. In dit hoofdstuk worden de relevante punten van hoofdstuk 3 van het eerste deelrapport kort herhaald danwel samengevat.

Overzicht betaald parkeren in Haarlem
In de gemeente Haarlem zijn een aantal gebieden waar betaald parkeren is ingevoerd. In deze gebieden kan de parkeerbelasting voldaan worden door middel van parkeerautomaten en via aaneengesloten belparkeerproviders. Verworven parkeerrechten worden op kenteken opgeslagen in een lokale parkeerrechtendatabase. Handhaving geschiedt in twee fases: allereerst een scanauto die kentekens scant en een eerste controle op parkeerrechten uitvoert. Indien er geen parkeerrechten worden gevonden voor een kenteken, dan wordt dit gecommuniceerd naar een handhaver die ter plekke het kenteken nogmaals controleert en tevens controleert of er geen sprake is van overige parkeerrechten (zoals tijdelijke vergunning of Europese gehandicaptenparkeerkaart). Zo nee, legt de handhaver een naheffingsaanslag op.

Naast dit hoofdoverzicht zijn er een aantal speciale situaties:

- **bewonersparkeren (parkeervergunningen):**
  Parkeervergunningen worden uitgegeven op adres en kenteken; het kenteken wordt geregistreerd in de parkeerrechtendatabase. Deze kentekens worden dus automatisch door het systeem herkend als beschikkend over een geldig parkeerrecht.
- **Bezoekersregeling:**
  Bewoners van bepaalde zones kunnen een bezoekersregeling aanvragen. Hierdoor krijgen zij de mogelijkheid (concreet: een maximum saldo) om bezoek tegen een sterk gereduceerd parkeertarief te laten parkeren. De bewoner meldt hiervoor het kenteken van de bezoeker aan bij het systeem. Hiermee verkrijgt het kenteken een parkeerrecht voor de duur van het bezoek. Facturatie geschiedt achteraf aan de bewoner, voor het verbruikte saldo.
- **Hulpverleningsvergunning:**
  Bedoeld voor professionele hulpverlenersorganisaties. Deze kunnen een parkeervergunning aanvragen om tegen gereduceerd tarief te parkeren bij cliënten
- **mantelzorgregeling:**
  Om mantelzorgers van bewoners met speciale zorgbehoefte te ontzien, is er een speciale mantelzorgregeling. Bewoners met een indicatie in het kader van Wet Maatschappelijke Ondersteuning (WMO), Wet Langdurige Zorg (WLZ) of Jeugdzorg kunnen deze regeling aanvragen. Bij deze regeling wordt er een bepaald bedrag (momenteel €60,-) extra saldo toegevoegd aan de bezoekersregeling. Dit bedrag wordt niet gefactureerd (gratis parkeertegoed).

3. Privacyaspecten huidige gegevensopslag en verwerking

In dit hoofdstuk wordt de privacygevoeligheid besproken van de data die wordt uitgewisseld en/of opgeslagen, zoals achterhaald in het TNO-rapport [TNO19, hoofdstuk 3]. Hierbij wordt de volgorde van de bespreking in dat rapport gehanteerd. De onderhavige tabellen worden genoemd maar niet in hun geheel herhaald – daarvoor verwijzen we naar het TNO-rapport.

Doel van dit hoofdstuk is inzicht te krijgen in waar beveiligingsmaatregelen nodig zijn, niet om specifieke aanvallen op de privacy van een parkeerder te beschrijven. Algemeen uitgangspunt is toetsen aan dataminimalisatie: verwerving / communicatie van data is alleen toegestaan, indien die data die strikt noodzakelijk is om een bepaalde functionaliteit te realiseren.

3.1 Inherente privacyrisico's

Inherent aan kentekenparkeren is dat het kenteken alsmede aanvangstijd en duur danwel eindtijd gecommuniceerd dienen te worden. De privacy impact van deze gegevens bespreken we daarom voorafgaand aan de specifieke analyses.
Daarnaast is inherent aan betaald parkeren dat er een betalingsactie plaatsvindt. Ook dit levert privacyrisico's op en wordt voorafgaand besproken.

Van kentekenparkeren
De voor kentekenparkeren noodzakelijke gegevens (w.o. kenteken) koppelen een parkeeractie (aanvang + duur) aan een specifiek, tot een persoon herleidbaar gegeven (het kenteken).
Dat wil zeggen dat bij kentekenparkeren in het algemeen maatregelen nodig zijn om de privacy van parkeerders voldoende te borgen.

Van traceerbare betalingsmethoden
Bij betaald parkeren hoort betalen. Als dit gebeurt met contant geld, dan is de betaling niet rechtstreeks[2] te koppelen aan een persoon. Echter, tegenwoordig wordt vaak betaald via andere mogelijkheden, zoals een PIN betaling, een credit card betaling, of via een mobiel (Goole Pay, Apple Pay). Bij dit soort betalingen is er een tussenpartij die als dienst de verwerking van een betaling aanbiedt. Daartoe heeft de parkeerder een rekening bij de tussenpartij.

Bij betaling via een tussenpartij leert de ontvangende partij:

- Dat de parkeerder een rekening heeft bij tussenpartij
- De identiteit van de tussenpartij
- Een identifier van de rekening bij de tussenpartij (bankrekening nummer, credit card nummer, etc.)

Deze informatie is inherent gekoppeld aan de parkeeractie, oftewel aan aanvangstijd, duur of vertrektijd en (in geval van kentekenparkeren) het kenteken.
Merk op dat de identiteit van de tussenpartij onbedoeld informatie over de persoon kan lekken. Zo zal iemand die voor parkeren betaald met een buitenlandse rekening waarschijnlijk geen inwoner van Nederland zijn. Individueel genomen zijn zulke afgeleide gegevens niet per se herleidbare

2 Als er een camera in de betaalautomaat zit, kan de betaling indirect wel koppelbaar zijn.

persoonsgegevens, maar als er meerdere van zulke gegevens gecombineerd worden, is het vaak toch te herleiden tot een uniek persoon.

3.2 Privacy-aspecten van digitale bezoekersregeling [TNO19, tabel 1]

Voor het bezoekersparkeren worden de volgende persoonsgegevens verwerkt door de gemeente:

- Bij initiële aanvraag:
  - DigID
  - Burgerservicenummer
  - Huisnummer+toevoeging
  - Aanmeldcode (ten behoeve van pseudonimisering bij aan/afmelden)
  - optioneel: emailadres
- Bij aanmelden bezoeker[3]:
  - bron (website, app of automaat)
  - standaard gegevens (kenteken, aanvang, eind)
  - lokatie/zone

Daarnaast worden verschillende gegevens gecommuniceerd met externe dienstverlener Cocensus ten behoeve van facturatie. Deze externe partij wordt in paragraaf 4.6 behandeld.

Van andere externe partijen die betrokken kunnen zijn, is uit tabel 1 niet duidelijk welke data zij verkrijgen. Genoemd worden: IVR (Telecats), parkeerautomaten (Scheidt & Bachmann, Cate / Flowbird), handhaving met scanauto's en handhelds (Parkius & Sigmax), parkeergarages (Spaarnelanden), software leveranciers, etc.

Privacy aspecten
Wat opvalt:

- Gebruik van zowel DigID als burgerservicenummer lijkt dubbelop.
- Gegevens voor aanmelden zijn (i.h.a.) al beschikbaar voor de gemeente vanuit bestaande administraties (GBA, BAG). Het is niet duidelijk uit de beschikbare data of deze gegevens slechts ter verificatie aan deze administraties worden getoetst, of dat de gegevens ook daadwerkelijk in het parkeersysteem worden ingevoerd. Dat laatste is in ieder geval niet noodzakelijk en daarmee vanuit privacy oogpunt niet wenselijk.
- Voor mantelzorgontvangers wordt het feit dat zij een medische indicatie hebben, zichtbaar in het parkeersysteem, door het feit dat voor hun een hoger maximum aan bezoekersuren geldt dan voor inwoners zonder zorgindicatie.
  NB: Dit privacy probleem is bekend bij opdrachtgever en een oplossing hiervoor is expliciet onderdeel van de huidige opdracht.
- Het is onduidelijk waarom informatie zowel in de bezoekersparkerendatabase als in de parkeerrechtendatabase wordt opgeslagen. Zowel vanuit algemene ontwerpprincipes (*avoid duplication of (volatile) information*) als vanuit privacy oogpunt is het advies om het systeemontwerp op dit punt te herzien.
- In hoeverre de bewaartermijnen redelijk zijn is niet te evalueren zonder te weten welk doel bewaren dient, alsmede de periode waarin dat doel relevant is.
  Zo lijkt een bewaartermijn van 15 maanden erg lang voor bezoekersparkeren. Dit blijkt ter

3 Volgens [TNO19, Tabel 1] worden deze gegevens in 2 databases opgeslagen: de PRDB en de bezoekersparkerendatabase.

facturatie en bezwaartermijn daartegen. De aanbeveling is om te kijken of dit te reduceren is.

- Externe dienstverlener Cocensus:
  In het rapport is de rol van Cocensus in de bezoekersparkerenregeling wellicht niet geheel duidelijk. Bij navraag bleek, dat Cocensus jaarlijks de gemeentelijke belastingen int. Hieronder valt ook de facturatie (achteraf) van parkeervergunning en gebruikte uren bezoekersparkeren.

3.3 Dataverwerking aan-/afmelden via telefoon – Telecats [TNO19, tabel 2]

Externe partij Telecats biedt telefonische parkeerrechtenverwerving door middel van spraakherkenning aan voor bezoekersparkeren. Hiertoe wordt in ieder geval het kenteken ingesproken. Daardoor beschikt Telecats over in ieder geval de volgende gegevens:

- Ingesproken kenteken
- Belgegevens (zoals telefoonnummer beller)
- Datum + tijdstip aanmelding / afmelding

In de eerste fase van dit project is niet alles rondom aan-/afmelden via telefoon duidelijk geworden. Zo is bijvoorbeeld niet duidelijk, hoe een telefonische aanmelding aan een specifieke bewoner gekoppeld wordt – of door welke partij dit gebeurt.

Daarnaast merken we op dat Telecats aan haar klanten optionele tools aanbiedt, waaronder real-time spraakanalyse en detectie van emoties in spraak. De door de gemeente Haarlem afgenomen diensten zouden expliciet van dit soort analyses uitgesloten moeten worden – ook als het gaat om puur intern gebruik (zoals het trainen van emotieherkenningssoftware).

3.4 Aanmelden via parkeerautomaat – Scheidt & Bachmann [TNO19, tabel 3]

Beheer van de parkeerautomaten in Haarlem zijn uitbesteed aan Scheidt & Bachmann. Deze automaten bieden een mogelijkheid tot ter plaatse betalen voor een parkeerrecht. Scheidt & Bachman ontvangt aangemelde kentekens en biedt betaling via PIN of creditcard. Ook voor deze categorie heeft het eerste deelonderzoek geen compleet beeld opgeleverd. We behandelen hier enkel de gegevens die ondubbelzinnig gebruikt worden. Dit zijn:

- kenteken
- datum/tijd van handeling
- maximale duur van de parkeerrechten

Uit het TNO-rapport is het niet duidelijk of Scheidt & Bachmann ook betaalgegevens (kaartnummer, rekeningnummer, etc.) ontvangt. Vanuit point-of-sale regelgeving van de betaalaanbieders zou dit niet mogen gebeuren; echter het rekeningnummer zal zichtbaar zijn in de overschrijving en dus via die route alsnog bekend worden.

De lijst gegevens zoals hier beschrijven zijn de minimale gegevens nodig voor het registreren en verwerken van een parkeerrecht in een kentekenparkeersysteem. Deze zijn dan ook noodzakelijk. Het is wel onduidelijk in hoeverre deze gegevens met derden gedeeld worden. Dat is een punt van aandacht.

3.5 Handhaving met scanautos – PARK/US & Sigmax [geen gegevens beschikbaar]

Handhaving geschiedt als volgt: een scanauto rijdt rond en matcht gescande kentekens tegen de parkeerrechtendatabase. Vervolgens worden individuele handhavers via handhelds gedirigeerd naar voertuigen van welke de gescande kentekens niet in de parkeerrechtendatabase voorkomen. De scanauto is een service geleverd door externe partij PARK/US. De handhelds worden geleverd door Sigmax.

In de eerste fase van dit project is niet inzichtelijk geworden welke data hier verzameld danwel gecommuniceerd werd.
Met betrekking tot deze externe partij kan dus geen gericht privacyadvies geformuleerd worden. Bij een nieuwe aanbesteding is het advies hier aandacht aan te besteden, bijvoorbeeld in de DPIA.

3.6 Facturatie – Cocensus [TNO19, tabel 1 en tabel 4]

Cocensus is een uitvoeringsorganisatie opgericht door samenwerkende gemeentes. In opdracht van de gemeente Haarlem verzorgt Cocensus de uitvoering van gemeentelijke belastingen en belastingaanslagen. Zij innen dan ook de gemeentelijke parkeerbelastingen. Dit gebeurt achteraf, op basis van nacalculatie.

Cocensus verkrijgt de volgende informatie:

- Tabel 1 (bezoekersparkeren)
    - Facturatiebestand: BSN, factuurbedrag, periode, omschrijving
    - Naam, adres, woonplaatsgegevens
    - Toegang tot BRP
    - Naam en kenteken
- Tabel 4 (facturatie)
    - Uit BRP: BSN, naam, adres, woonplaats, geboortedatum, geslacht, burgerlijke staat
    - Via burger: telefoonnummer, email adres, IBAN-nummer
    - Uit onbekende bron:
        - Voor behandeling van kwijtscheldingsverzoeken en dwanginvordering: informatie over financiële situatie, w.o. inkomsten en schulden
        - Om fraude te bestrijden en aan wettelijke verplichtingen te voldoen: andere categorieën persoonsgegevens

Merk op dat de dienstverlening van Cocensus verder gaat dan enkel innen van parkeergelden in het kader van een bezoekersparkeerregeling. Het is in de eerste fase niet duidelijk geworden of het overzicht van door Cocensus ontvangen gegevens enkel die gegevens behelst, die voor bezoekersparkeren relevant zijn. Ook bestaat er onduidelijkheid omtrent de bewaartermijnen.

Duidelijk is in ieder geval dat Cocensus veel meer persoonsgegevens ontvangt dan noodzakelijk voor facturering van een bezoekersparkeerregeling. Gegevens als geboortedatum, geslacht, burgerservicenummer of burgerlijke staat zijn compleet irrelevant in dit proces. Het advies is dan ook grondig te analyseren welke gegevens in het kader van (bezoekers)parkeren worden gedeeld met Cocensus, en dit te minimaliseren tot de strikt benodigde gegevens (bijv.: naam, adres, woonplaats, totaalbedrag factuur).

3.7 Mobiel parkeren – Yellowbrick [TNO19, tabel 5]

De gemeente Haarlem werkt samen met verschillende commerciële aanbieders van mobiel parkeren (parkeren met parkeerapp). Zoals opgemerkt in het TNO rapport hanteren de verschillende aanbieders verschillende regels rondom verwerking van persoonsgegevens. Het TNO-rapport biedt inzage in de verwerking door aanbieder Yellowbrick. Daarom wordt hier enkel deze verwerker verder behandeld.

Yellowbrick verkrijgt de volgende informatie bij mobiel parkeren:

- In het kader van factureren:
    - Parkeerlokatie (straat en stad)
    - Geografische locatie (vereist gebruikerstoestemming)
    - Kenteken
    - Email adres
    - Telefoonnummer
    - Naam, adres, woonplaatsgegevens
    - Geslacht
    - Geboortedatum
    - Klantnummer
- In het kader van een parkeeractie:
    - device fingerprint (o.a. MAC adres, IP adres, device ID, OS details, browsertype, etc.)
    - device contents (o.a. locatiegeschiedenis)
    - loginformatie (o.a. website-bezoeken aan Yellowbricks, details over gebruik app, etc.)

De bewaartermijn van gegevens is enkel als bovengrens gegeven (18 maanden), wat royaal is. Daarnaast is in de eerste fase van dit project achterhaald dat persoonsgegevens worden gedeeld met FBTO en ANWB voor een marketingdatabank.

Hoewel het niet in het TNO-rapport bekend is, welke data andere mobiel parkeren providers verzamelen, is bovenstaande lijst reden tot zorg. Net als bij Cocensus worden er gegevens gedeeld die niet ter zake doen voor facturatie. Het advies is om dit in te perken en voor de overige providers na te gaan en, waar nodig, in te perken.
Daarnaast wordt bij het parkeren veel gegevens van een telefoon opgevraagd die overbodig zijn om de parkeeractie te verwerken, maar typerend zijn voor *device fingerprinting*. Device fingerprinting is het identificeren van een apparaat aan de hand van een verzameling attributen (IP adres, versie OS, geïnstalleerde software, telecomprovider, etc.). Aangezien bij mobiel parkeren de parkeerder een account heeft bij de aanbieder van mobiel parkeren, zijn dit soort fratsen geheel overbodig.

3.8 Conclusie

Zoals opgemerkt in het TNO-rapport: het doel en de noodzaak van gegevens die gedeeld worden met derden is niet altijd evident. Het is daarmee niet duidelijk geworden of de gemeente Haarlem zich aan haar verplichtingen jegens burgers kan houden, wat betreft omgang met de data van burgers.

4. Privacy/efficiency van systemen voor betaald parkeren

Dit hoofdstuk beschouwt principes van bestaande systemen voor betaald parkeren, met een focus op afwegingen tussen gebruiksgemak (incl. aansluiting op abonnementsparkeren), efficiency, privacy en kosten. Bij de efficiency ligt de focus op efficiëntie van het controleren van parkeerrechten. De bespreking is op principieel niveau; er is geen concrete instantie van een systeem bedoeld. Iedere bespreking wordt afgesloten met een kort overzicht van de afwegingen. Dit overzicht is relatief: het plaatst het besproken systeem wat betreft de afwegingen ten opzichte van de reeds eerder besproken systemen.

Met betrekking tot privacy merken we op dat hier in beginsel privacy ten opzichte van de systeemeigenaar (typisch: de gemeente) wordt beschouwd. Waar een systeem betaling via tussenpartijen eenvoudig mogelijk maakt, wordt privacy ten opzichte van die tussenpartijen ook beschouwd.

4.1. Onbetaald parkeren

Niet betalen voor parkeren levert weliswaar geen inkomsten op, maar controle valt ook geheel weg. Dit levert een optimaal systeem op wat betreft gebruikersgemak, efficiency, privacy en kosten van het systeem.
Ter volledigheid merken we op, dat onbetaald parkeren ook nadelen heeft, die niet privacy-technisch en niet kosten-technisch van aard zijn. In het bijzonder kan de parkeerdruk op gewilde parkeerplaatsen (bv. nabij winkelcentra) zodanig toenemen, dat omwonenden niet meer in hun eigen buurt kunnen parkeren.

Afwegingen:

- **Gebruikersgemak**
  - **Om parkeerrechten te verwerven**: optimaal.
    - **Aansluiting abonnement**: overbodig.
- **Efficiency van handhaving**: optimaal: geen controle nodig.
- **Privacy**: perfect: geen data-opslag noch verwerking betekent ook geen privacy-risico's.
- **Kosten**:
  - Installatiekosten: gratis.
  - Operationele kosten: gratis

4.2. Individuele meter per parkeerplaats

Een reeds bestaand concept is het idee van één parkeermeter per parkeerplaats. Het voordeel van dit systeem is dat handhaving vrij recht-toe-recht-aan is: men dient enkel de parkeermeter te controleren – die op een toegankelijke, goed zichtbare plek staat.

Echter, er kleven enkele nadelen aan dit systeem. Zo wordt iedere parkeermeter maar voor één parkeerplaats gebruikt. Daarnaast moet iedere parkeermeter in staat zijn, een betaaltransactie te verwerken – ofwel met muntgeld, ofwel elektronisch. Beide vereisen extra mechanismen in de parkeermeter, waardoor deze duurder wordt. Een uitvoering die muntgeld accepteert, heeft daarnaast het risico dat criminelen de meter openbreken om het muntgeld te krijgen. Een uitvoering die elektronische betaling accepteert, zal moeten kunnen communiceren met een betaalsysteem om de betaling te verwerken – wat het systeem nog duurder maakt.

Afwegingen:

- **Gebruikersgemak**: redelijk.
  Betalen kan direct op de parkeerplaats, maar vereist wel dat de parkeerder over een geschikt betaalmiddel (muntgeld / elektronisch betaalmiddel) beschikt.
  - **Aansluiting abonnement**: onmogelijk binnen systeem.
- **Efficiency van handhaving**: inefficiënt.
  Controle is bewerkelijk. Er is één meter per parkeerplaats, dus moet er per parkeerplaats één meter visueel gecontroleerd worden.
- **Privacy**: redelijk tot goed.
  De betaling zou traceerbaar kunnen zijn (bij elektronische betaling) naar de parkeerder. Afgezien daarvan wordt er geen data over de parkeerder of diens voertuig uberhaupt opgenomen in het systeem.
- **Kosten**:
  - Installatie: duur.
    Hoewel de individuele meters simpel kunnen zijn en daardoor relatief goedkoop, is er één meter per parkeerplaats nodig.
  - Operationeel: redelijk / duur
    - Elektronische betalingen: redelijk.
      Hoofdzakelijk repareren van defecte meters – wat met veel meters regelmatig nodig zal zijn.
    - Contante betalingen: duur.
      De meters zullen allen regelmatig geleegd moeten worden.

4.3. Papieren parkeerbewijs

Het ligt voor de hand om één parkeermeter voor meerdere parkeerplaatsen te gebruiken. Een manier om dit te bewerkstelligen is om de parkeermeter een parkeerrechtbewijs uit te laten geven, dat de automobilist vervolgens achter de voorruit legt.

Dit systeem biedt als voordeel dat een parkeermeter voor meerdere parkeerplaatsen tegelijk kan worden gebruikt. Het nadeel is dat controle meer handelingen vereist: er moet bij iedere auto visueel gezocht worden naar een parkeerbewijs.

Afwegingen:

- **Gebruikersgemak**: redelijk.
  De parkeerder kan niet direct bij de parkeerplaats betalen, maar moet heen en weer lopen naar een centrale meter. Anderzijds kan de meter meerdere betaalmethodes ondersteunen, wat het gebruikersgemak vergroot.
  - **Aansluiting abonnementsparkeren**: prima.
    Het abonnement kan simpelweg op de plaats van het papieren parkeerbewijs gelegd worden.
- **Efficiency**: slecht.
  Controle moet bij ieder voertuig kijken, of er een geldig parkeerbewijs ligt. In vergelijking met één meter per parkeerplaats zelfs een achteruitgang: de plaatsing van het betaalbewijs kan van voertuig tot voertuig variëren.
- **Privacy**: redelijk / goed.
  Afgezien van de traceerbaarheid van de betaalmethode, wordt er geen data over de parkeerder opgeslagen.

- **Kosten**:
  - Installatie: vrij duur:
    Deze parkeermeters zijn complexer (elektronisch ipv mechanisch) dan de meter-per-parkeerplaats en daardoor duurder. Anderzijds zijn er fors minder nodig.
  - Operationeel: redelijk.
    Sowieso zullen de papieren tickets en de printer regelmatig aangevuld moeten worden. Indien de meters ook contante betalingen verwerken, zullen ze regelmatig leeggehaald moeten worden. Omdat er significant minder meters zijn, is dit veel minder bewerkelijk dan bij de meter-per-parkeerplaats.

4.4. Parkeren op vaknummer

Een systeem dat controle versimpelt, is parkeren op vaknummer. In dit systeem krijgt iedere parkeerplaats zijn eigen vaknummer. In de parkeermeter wordt dan voor een specifiek vaknummer betaalt. Controle is nu simpel: de controleur vraagt eenvoudigweg op, voor welke parkeerplaatsen niet betaald is en kijkt of daar voertuigen staan. Zo ja, worden deze beboet.

Een ander voordeel van dit systeem is dat het privacy-vriendelijk is. Controle is gebaseerd op het nummer van de parkeerplaats: een statisch, niet-persoonsgebonden gegeven. Enkel op het moment dat er beboet wordt, wordt het kenteken (een persoonsgebonden gegeven) genoteerd. Dat is in dat geval ook noodzakelijk, waarmee dit systeem inherent al principes zoals doelbinding, gegevensbeperking en bewaarbeperking deels goed bewaakt. Tot slot is parkeren op vaknummer ook te combineren met abonnementen / bezoekersparkeersystemen: via de app van het bezoekersparkeersysteem kan het vaknummer worden doorgegeven.

Er kleven echter ook nadelen aan dit systeem. Allereerst zijn er, voor zover bekend, geen apps die parkeren op vaknummer ondersteunen (hoewel dit technisch prima mogelijk is). Een dergelijke app zou het gebruikersgemak vergroten.
Daarnaast vereist parkeren op vaknummer een aanpassing van de bestaande infrastructuur: iedere parkeerplaats moet een duidelijk herkenbaar nummer krijgen en de bestaande betaal-infrastructuur moet omgeschakeld worden naar parkeren op vaknummer.
Tot slot is volledige automatisering van de handhaving uitdagend. Controle moet noodzakelijkerwijs plaats vinden op het niveau van parkeervakken. Een automatisch controlesysteem zal dus de parkeervakken moet herkennen. Visuele herkenning is hiervoor ontoereikend, aangezien het (in het algemeen) openbare ruimte betreft, waarvan het visuele uiterlijk niet statisch is (graffiti, fiets, vuilniszak, ...). Dat betekent dat er initiële stap benodigd is om herkenning op niet-visuele gronden mogelijk te maken. Voorbeelden hiervan zijn exacte GPS inmeting van ieder afzonderlijk vak, of inbedding van camera's of RFID tags in ieder afzonderlijk parkeervak.

Afwegingen:

- **Gebruikersgemak**: vergelijkbaar met "papieren bewijs".
  De parkeerder kan niet direct bij de parkeerplaats betalen, maar moet naar een centrale meter lopen. Daarnaast is de betaalhandeling bewerkelijker dan bij een papieren bewijs: het vaknummer moet (correct) ingegeven worden. Anderzijds hoeft de parkeerder niet terug te lopen en kan de meter meerdere betaalmethodes ondersteunen, wat het gebruikersgemak vergroot.
  - **Aansluiting abonnementsparkeren**: redelijk.
    Dit vereist een (gemeentelijke) parkeerapp om een vaknummer door te geven.
- **Efficiency**: goed.
  De controleur hoeft slechts een overzicht te hebben van de parkeerplaatsen binnen een zone waar niet voor is betaald, om vervolgens enkel die plaatsen af te gaan. Als daar een

voertuig staat, kan dat meteen beboet worden.
NB: volledige automatisering van de controle is niet triviaal.

- **Privacy**: redelijk (traceerbare betaling) / goed (contante betaling).
  Afgezien van de traceerbaarheid van de betaalmethode, wordt er geen data over de parkeerder opgeslagen.
- **Kosten**:
  - Installatie: duurder dan “papieren parkeerbewijs”.
    De bestaande infrastructuur moet aangepast worden (toevoegen vaknummers). Ook zal er per zone danwel centraal een systeem om parkeerrechten te beheren moeten worden opgetuigd en worden ingericht voor de specifieke situatie (o.a. de vaknummers van specifieke zones).
  - Operationeel: laag.
    Er worden geen *consumables* verbruikt voor parkeren. Controle kan eventueel wat data verbruiken (communicatie lijst vaknummers). Verder zal de hoofdmoot van de te verwachten kosten bestaan uit reparatie (defecte meter / vernielde vaknummers).

4.5. Kentekenparkeren

Bij kentekenparkeren wordt het parkeerrecht gekoppeld aan een specifiek voertuig door middel van het kenteken. De gebruiker kan de betaling via verschillende kanalen realiseren, zoals via een centrale parkeermeter, via een tussenpartij zoals een parkeerapp, SMS parkeren, of zelfs een partij voor telefonische aan- en afmelding. Welke kanalen ondersteunt worden, varieert per systeem. De verschillende kanalen vergroten het gebruikersgemak.

Merk op dat gebruik van een parkeerapp van een tussenpartij een nieuw privacy-probleem introduceert: niet alleen beschikt een tussenpartij over parkeerdata, maar de app kan allerlei irrelevante data van de smartphone opvragen. Zo vraagt de huidige ParkMobile app[4,5] onder meer toegang tot een overzicht van draaiende apps op, alsmede uitgebreide toegang tot Bluetooth data. Een overzicht van draaiende apps heeft uiteraard niets te maken heeft met parkeren, maar kan wel gebruikt worden om een gebruikersprofiel op te stellen. De uitgebreide toegang tot Bluetooth maakt het opstellen van een gebruikersprofiel op Bluetooth-niveau triviaal.

Kentekenparkeren maakt automatisering van de controle relatief simpel: een scanauto scant de geparkeerde voertuigen in het voorbijgaan. Dit kan eventueel (zoals in Haarlem) met opvolging door handhavers waar nodig, waardoor de personele inzet gefocust wordt waar nodig. Anderzijds is het technisch mogelijk om direct over te gaan tot beboeting op basis van de scan door de scanauto.
Voor dit parkeersysteem is geen specifieke aanpassing voor nodig: scanauto’s die kentekens kunnen herkennen worden reeds door externe partijen aangeboden.

Afwegingen:

- **Gebruikersgemak**: prima.
  - **Aansluiting abonnementsparkeren**: vergelijkbaar met “parkeren op vaknummer”.

Efficiency: uitstekend.
Met behulp van een scanauto kan automatisch bepaald worden welke kentekens parkeergelden

4 ParkMobile is hier als willekeurig voorbeeld gekozen, andere aanbieders zijn niet geëvalueerd.

5 Er is ***niet*** onderzocht of de ParkMobile app deze toegangspermissies ook daadwerkelijk gebruikt. Sowieso impliceert het verzamelen van deze data niet per se, dat er een profiel wordt opgesteld. Echter, het feit dat ze gevraagd worden, terwijl ze niet nodig zijn voor parkeren, is zorgelijk.

- verschuldigd zijn. Beboeting kan geschieden door menselijke opvolging, maar technisch gezien hoeft dit niet; de scanauto zou zelfs deze taak over kunnen nemen.
- **Privacy**: zeer slecht.
  - Het parkeersysteem zelf ontvangt gegevens herleidbaar tot een persoon (kenteken). Dit betekent dat de toegang tot deze gegevens technisch en organisatorisch zoveel mogelijk beperkt moet worden.
  - Bij gebruik van betaling via tussenpartijen wordt deze informatie ook met de tussenpartijen gedeeld.
  - Tot slot stimuleert deze vorm het gebruik van apps van tussenpartijen, waarvan het niet duidelijk is welke irrelevante data zij van smartphones trekken.
- **Kosten:**
  - Installatie: in basisuitvoering, goedkoper dan “parkeren op vaknummer”.
    De infrastructuur hoeft niet te worden aangepast. Plaatsing van meters en optuigen van een systeem om de parkeerrechten centraal te beheren blijft noodzakelijk.
    NB: het aanbieden van betalingskanalen van tussenpartijen kan extra kosten met zich meebrengen.
  - Operationeel: laag.
    Er worden geen *consumables* verbruikt voor parkeren. Controle zal data verbruiken (communicatie lijst kentekens). Verder zal de hoofdmoot van de te verwachten kosten bestaan uit reparatie (defecte meter / vernielde vaknummers).

4.6. Conclusie

Link parkeerrecht aan voertuig
Een parkeerrecht is het recht om een voertuig ergens (op één lokatie of binnen een zone) te parkeren. Om controle mogelijk te maken, dient het parkeerrecht direct of indirect verbonden te kunnen worden met het onderhavige voertuig. Er zijn in het algemeen slechts 3 opties waarmee het parkeerrecht verbonden kan worden:

- **voertuig**
  Bijvoorbeeld het kenteken of het Voertuig-Identificatie-Nummer.
  De koppeling is tussen parkeerrecht en voertuig is rechtstreeks.
- **lokatie**
  Bijvoorbeeld het nummer van het parkeervak waarin is geparkeerd.
  De koppeling tussen parkeerrecht en voertuig gaat via de lokatie waar het voertuig gestald is.
- **bewijs aan toonder**
  Bijvoorbeeld een papieren parkeerbewijs achter de voorruit.
  De koppeling tussen parkeerrecht en voertuig wordt volbracht doordat het bewijs in het voertuig getoond wordt.

In huidige in gebruik zijnde systemen in Nederland, zoals in dit hoofdstuk beschreven, komen alle drie de varianten voor. Merk tot slot op dat vanuit Privacy by Design oogpunt een directe koppeling tussen parkeerrecht en voertuig onwenselijk is. Directe koppeling heeft als inherent voordeel dat controle zich rechtstreeks kan richten op het herkennen van voertuigen – iets wat te automatiseren is. Dit kan ook bij lokatie-gebonden parkeerrechten: in dit geval dienen enkel lokaties waarvoor geen parkeerrechten staan geregistreerd, geïdentificeerd te worden. Ook dit valt, eventueel met aanpassingen in de openbare ruimte, te automatiseren. Voor parkeren met bewijs aan toonder zou voor automatisering gedacht kunnen worden aan RFID tags in nummerborden of ingebed in papieren tickets. Dit zal echter meer onderzoek vergen.

Betalingsmechanismes
Merk op dat in bovenstaande bespreking het aspect betaling buiten beschouwing is gelaten. De focus ligt op het verkrijgen en controleren van bewijs van parkeerrecht. De systemen zelf zijn onafhankelijk van het betalingsmechanisme. Het betalingsmechanisme kan echter nog impact op de privacy hebben: betalen met geld aan toonder (cash) is niet eenvoudig herleidbaar tot een persoon, maar bij betalingen via een tussenpartij (zoals pin-betaling, of betaling met mobiel) wel. In dit geval is er namelijk een koppeling tussen de identiteit van het betalende object (pinpas, app, mobiele telefoon) en een rekening van de betaler (bankrekening, app-account, Apple/Google Pay rekening). Daarbovenop komt dat parkeer-apps geïnstalleerd moeten worden op een smartphone – een hoogst persoonlijk apparaat – en daar, theoretisch gezien, allerlei data ongerelateerd aan parkeren zouden kunnen verzamelen.
Vanuit privacy-oogpunt verdienen algemene betaalmiddelen (contant, pinnen, mobile pay) de voorkeur boven toepassingsspecifieke betaalmiddelen. Zelfs voor betalen per app is de voorkeur voor een algemene betalingsapp (bijv. Tikkie) boven een parkeergerichte app. Die laatste wordt immers alleen gebruikt om te parkeren – wat valt af te leiden aan de servers waar data naar werd verstuurd, onafhankelijk van encryptie van de data.

Mate van privacy en mate van efficiency
De verschillende bestaande systemen bieden verschillende mates van privacy en van efficiency van controle. Sommigen leveren specifiek uitdagingen op voor efficiency van automatische controle. Kentekenparkeren is het meest efficiënt voor automatische controle: de controle kan door middel van een scanauto snel en doelmatig plaatsvinden. Voor parkeren op vaknummer is het wellicht mogelijk een automatisch controle-systeem te ontwikkelen, maar dit zal waarschijnlijk (significante) aanpassingen aan de openbare ruimte (parkeerlokaties) vereisen.

Anderzijds is privacy bij parkeren op vaknummer inherent geborgd, doordat geen tot personen herleidbare gegevens moeten worden opgeslagen. Bij kentekenparkeren is dit niet inherent het geval. Borging van de privacy vereist daar extra functionaliteit in het systeem.

Interessant genoeg zijn deze twee systemen (kentekenparkeren en parkeren op vaknummer) enigszins vergelijkbaar: ze borgen één aspect fundamenteel (privacy danwel efficiency), wat ertoe leidt dat er investeringen nodig zijn om het andere aspect goed te bewerkstelligen.

- parkeren op vaknummer (sterk punt: privacy): investeringen in de fysieke infrastructuur om automatische herkenning van de individuele parkeervakken mogelijk te maken, alsmede een significante aanpassing van het bestaande parkeersysteem. Daardoor kan parkeren op vaknummer niet voldoen aan de eis van een systeem dat nauw aansluit bij de huidige parkeersystematiek.
- Kentekenparkeren (sterk punt: efficiency van controle): investeringen in afspraken met externe partijen om de benodigde data te minimaliseren en privacy door de gehele keten te borgen.

Focus voor ontwerp
Bij het verwerven van parkeerrechten kunnen meerdere externe partijen een rol spelen (leverancier parkeerautomaat, leverancier mobiel parkeren-app, etc.). Veranderingen aan het verwerven van parkeerrechten moeten met al deze partijen afgestemd worden en kunnen niet eenzijdig worden doorgevoerd. Daardoor vallen aanpassingen aan dit onderdeel buiten het kader van “een systeem dat nauw aansluit bij de bestaande praktijk”, het uitgangspunt van deze ontwerpopdracht. In concreto betekent dit dat het te ontwerpen systeem een variant van kentekenparkeren zal zijn, dat betere privacy biedt dan het huidige systeem. Specifieker richt het ontwerp in het volgende hoofdstuk zich, vanuit bovenstaande focus, op de controle-fase. Deze wordt in het huidige systeem

uitgevoerd door BOA's in dienst van de gemeente, waardoor de gemeente Haarlem een grote mate van controle heeft over de uitvoering van deze fase.

Waarschuwing voor glijdende schaal

Tot slot plaatsen we hier de algemene kanttekening dat overwegingen als bovenstaande focus voor ontwerp een glijdende schaal bewerkstelligen: het zal altijd makkelijker zijn om kleine aanpassingen aan het bestaande systeem door te voeren, dan het systeem ingrijpend te wijzigen. Echter, soms kunnen zulke ingrijpende wijzigingen nodig zijn om de verschillende belangen terug in balans te brengen.

5. Ontwerp privacy-vriendelijk kentekenparkeersysteem

Een parkeersysteem omvat twee fases:

1. een deelsysteem voor *verwerving en opslag* van parkeerrechten;
2. een deelsysteem voor de *controle* van parkeerrechten.

Zoals reeds eerder opgemerkt, zijn bij de eerste fase (verwerving parkeerrechten) diverse externe partijen betrokken. Het doorvoeren van technische veranderingen is daardoor complex. Daarnaast borgen de juridische kaders hieromtrent de toegang tot en verzamelen van data (zie ook eerste deelrapport). Daardoor zijn privacy-eisen in deze fase op systeemniveau niet technisch, maar wel juridisch geborgd. Aangezien privacy al juridisch geborgd is en de coördinatie van technische aanpassingen aan deze fase complex is, richt het ontwerp zich op de controle-fase.

De opdracht is een ontwerp te maken dat nauw aansluit bij de bestaande situatie. Dat laat weinig ontwerpruimte. Ter herinnering de schematische weergave van de huidige controle-fase:

Een match op kenteken (tweede stap) is noodzakelijk in het geval van kentekenparkeren – een uitgangspunt van dit project. In dit ontwerp wordt deze stap opgevolgd door fysieke controle door een bevoegd controleur. Het uitdelen van naheffingen (parkeerboetes) gebeurt dus niet automatisch. De fysieke controle door handhavers zorgt voor een menselijke controle op het goed functioneren van het systeem. In overleg in het kader van cocreatie werd hieraan ook door de opdrachtgever belang gehecht. Dat betekent dat ook de derde stap (concrete informatie aanbieden aan handhavers) noodzakelijk is.
Dit betekent dat in zowel het huidige systeem als in het nieuwe ontwerp het kenteken noodzakelijk bij de scanauto bekend wordt (om de match te maken) en bij de controleur (die ter plaatse de naheffing uitschrijft).

Waar nog ontwerpruimte zit, is in hoe de matching plaatsvindt. Specifiek zijn er twee aspecten relevant voor privacy:

1. hoe recent de gegevens zijn waarmee de scanauto de match maakt, en
2. in welke vorm deze gegevens worden aangeleverd aan de scanauto t.b.v. matching.

Merk op dat vanuit privacy-oogpunt, de matching ook het interessantst is. In andere stappen wordt alleen informatie verzameld in de publieke ruimte, maar bij de matching wordt deze informatie gecombineerd met informatie uit de parkeerrechtenadministratie. Informatie uit de parkeerrechtenadministratie is niet publiek toegankelijk. Daarnaast is de privacy-gevoelige informatie in stappen één en drie enkel beschikbaar op het moment van parkeren voor partijen die fysiek aanwezig zijn. Een parkeerrechtenadministratie zou (in algemene zin) gegevens kunnen bewaren en dus achteraf inzichtelijk maken, ook voor partijen die niet aanwezig zijn.

5.1. Recentheid parkeerrechten voor matching

Omdat de scanauto in het ontwerp geen eindbeslissing neemt, is het dus ook niet noodzakelijk dat deze over de meest recente representatie van de parkeerrechten voor de huidige zone beschikt. Bij opvolging kan een eventuele false positive (onterechte veronderstelling van geen parkeerrechten) door de controleur ter plaatse worden opgemerkt. Dit levert inherent ook een kleine privacywinst: de scanauto weet nu niet zeker of kentekens, die niet gematcht worden, geen parkeerrechten hebben.

Vandaar wordt in dit ontwerp gekozen om de representatie van parkeerrechten voor een te scannen zone vóór aanvang van het scannen van die zone te downloaden. Hierdoor heeft de scanauto geen real-time versie van de parkeerrechten nodig. De controleur behoeft dit overigens ook niet: voor de controleur volstaat een check of het kenteken van het onderhavige voertuig op dat moment parkeerrechten heeft. Dit kan door middel van een query van de parkeerrechtendatabase worden voltooid.

Zoals opgemerkt levert de keuze om geen real-time data te gebruiken in de scanauto een kleine privacywinst op. Dit kan eventueel enkele false positives opleveren, wat een klein nadelig effect heeft op de efficiency van controle.

5.2. Representatie parkeerrechten t.b.v. matching

Merk op dat matching met parkeerrechten (stap 2) enkel hoeft te testen of een element in een lijst voorkomt. Er zijn verschillende manieren om dit te testen. Dit kan uiteraard direct, door de gehele lijst inzichtelijk te maken. Echter, het overzicht van alle parkeerrechten (van een bepaald gebied) is privacygevoelig. Bij voorkeur wordt dit dan ook niet met derden (zoals de scanauto) gedeeld.

Een alternatief is om de lijst abstract te representeren. Het moet nog steeds mogelijk zijn om te testen of een kenteken dan in zo'n abstracte representatie voorkomt, maar de volledige lijst met parkeerrechten is dan niet meer direct inzichtelijk.
Dit kan met behulp van Bloom filters (zie appendix A). Een Bloom filter is een abstracte representatie van een verzameling die specifiek gebruikt kan worden om te testen of een element (hier: een kenteken) in de lijst voorkomt.

Een abstracte representatie brengt concessies met zich mee. Bloom filters zijn zo ontworpen, dat negatieve antwoorden ("kenteken staat **niet** op de lijst") altijd terecht gegeven worden. Maar er is een kleine kans op een vergissing bij een positief antwoord ("kenteken staat **wel** op de lijst"). Dit biedt een privacy-voordeel: er komt een zeer kleine mate van onzekerheid in het systeem. Specifiek: een positief antwoord van een Bloom filter levert een bepaalde kans op dat een kenteken parkeerrechten had, maar niet 100% zekerheid hieromtrent.

Deze (geringe) mate van privacy wordt gebalanceerd door een kans op onterecht geen naheffing uitschrijven. Echter: voor een bestuurder valt daar zo goed als geen voordeel te behalen. De bestuurder kan dit namelijk niet sturen – hij/zij kan alleen zelf het Bloom filter namaken om te testen of dit toevalligerwijs op dit moment zo zou kunnen zijn. Daarvoor zou de bestuurder alle parkeerrechten binnen de parkeerzone moeten verzamelen. Maar die zijn niet publiek toegankelijk. Hooguit kan de bestuurder alle kentekens van geparkeerde voertuigen binnen de zone verzamelen, hopen dat ze allen nog langlopende rechten hebben, en hierop een Bloom filter construeren. In dat geval blijkt dat de kans dat zijn/haar specifieke kenteken afgedekt is door het Bloom filter, erg klein is. Kortom, dit biedt vrijwel geen enkele ruimte voor misbruik.

Kans op onterecht positief antwoord instellen

De kans op een onterecht positief antwoord door een Bloom filter kan bepaald worden door de parameters waarmee het Bloom filter geconstrueerd wordt, verstandig te kiezen. Dit betekent dat men ervoor kan kiezen om de kans op onterecht geen naheffing uitschrijven kan minimaliseren, maar ook dat men de privacy kan vergroten door de kans op één onterecht positief antwoord bijvoorbeeld op 5% te zetten. In Appendix A.2 wordt dit in meer detail besproken, met rekenvoorbeelden voor een pakkans van 99.95% en van 95%.

6. Voorkomen detecteerbaarheid medische indicaties in bezoekersregeling

De tweede deelvraag van dit rapport betreft het aandragen van oplossingsrichtingen voor bezoekersparkeren zodanig dat medische gegevens (in het bijzonder: gerelateerd aan mantelzorg) niet uit de parkeergegevens afgeleid kunnen worden. In dit hoofdstuk wordt deze deelvraag behandeld.

6.1. Probleemschets

In de huidige situatie kunnen bewoners parkeerrechten voor bezoekers verwerven. Dit geeft hen een bepaald aantal uren om te parkeren. Deze uren worden achteraf gefactureerd. De gemeente Haarlem heeft de politieke keuze gemaakt om voor inwoners met mantelzorgers een deel van de gebruikte parkeerrechten niet te factureren. Het privacyprobleem hierbij is dat het bepalen of een inwoner recht heeft op deze regeling, gebeurt op basis van medische indicaties (WMO en Wet Langdurige Zorg). Als een inwoner een dergelijke indicatie heeft, dan worden extra uren toegekend aan de standaard bezoekersregeling, welke niet gefactureerd worden.
Omdat deze extra uren anders niet toegekend worden, is het dus in de bezoekersregeling zichtbaar of een inwoner een dergelijke medische indicatie heeft en lekt dit goedbedoelde gebaar van de gemeente medische gegevens. Ook bij de facturering achteraf wordt dit zichtbaar, aangezien de extra uren niet gefactureerd worden.

Aangezien dit een beleidsmatige keuze is, zijn er niet alleen uitvoeringsgerichte oplossingsrichtingen mogelijk, maar ook beleidsmatige oplossingsrichtingen.

6.2. Beleidsmatige oplossingsrichtingen

De gemeente kan haar beleid aanpassen om dit privacy probleem te voorkomen.

1. Geheel theoretisch bezien zou de gemeente bijvoorbeeld de regeling kunnen afschaffen. Dan lekt er triviaal geen medische gegevens meer. Dit is uiteraard niet wenselijk, onder meer aangezien het zorgbehoevenden danwel hun zorgverleners op extra kosten jaagt.
2. Een andere beleidsmatige oplossing zou zijn om alle inwoners deze uren kado te doen. Ook in dit geval is er geen onderscheid tussen inwoners met en inwoners zonder zorgindicatie.
3. Via de WMO: de gemeente zou ervoor kunnen kiezen om inwoners die mantelzorg ontvangen en die bovendien in een vergunningengebied wonen op grond van de WMO een extra financiële bijdrage te verstrekken om de parkeerlasten te dragen. Daardoor blijft dit helemaal buiten het systeem van bezoekersparkeren; de registratie vindt plaats in het kader van de WMO. Dit zou kunnen op twee manieren:
    a. Er wordt een extra bedrag uitgekeerd. Dat kan natuurlijk ook voor andere doelen worden gebruikt, daar heeft de gemeente dan geen grip op. Het is de vraag of dat erg is.
    b. Er wordt een anonieme prepaidkaart verstrekt, waarmee de mantelzorger aan de betaalpaal kan betalen.

6.3. Oplossingsrichting binnen het bestaande systeem bezoekersparkeren

Een oplossing die facturering in stand houdt, is om alle inwoners de extra uren toe te kennen en de inwoners met indicatie op een andere wijze de financiële waarde van de toegekende uren doen toekomen. Dan zou het urenplafond voor alle inwoners hetzelfde zijn, en zouden alle inwoners ook op dezelfde wijze gefactureerd worden.

Een dergelijk systeem zou gerealiseerd kunnen worden door het uitgeven van een anonieme prepaid parkeerkaart aan inwoners met een zorgindicatie. Registratie van uitgifte van deze kaarten gebeurt in de WMO-registratie. Betaling van parkeergelden voor mantelzorgers geschiedt dan door middel van de kaart. Daarmee wordt het probleem van extra uren zichtbaar in de bezoekersregeling voorkomen. Omdat deze uren niet in de bezoekersregeling zichtbaar zijn, worden deze ook niet gefactureerd. Dus wordt hiermee ook het probleem van herkenning in de facturering voorkomen.

Om misbruik te voorkomen, zou de gemeente de geldigheid van zo'n prepaid-parkeerkaart kunnen beperken tot bijvoorbeeld een jaar.

7. Conclusies

Het systeem van kentekenparkeren heeft een inherente preferentie voor efficiency van controle ten koste van privacy. De samenwerking met derden verergert deze zorgen. In het bijzonder is bij de samenwerking met leveranciers van parkeerapps de gegevensverwerking door de app zelf ondoorzichtelijk en mogelijk privacy-technisch problematisch.

Er zijn verschillende opties voor een systeem voor betaald parkeren in de gemeente Haarlem. Afschaffing van betaald parkeren levert, ten opzichte van de eisen beschouwd in dit rapport, veruit de meeste winst. De alternatieven “parkeren op vaknummer” en “bewijs aan toonder” bieden een verbetering van de privacy, ten koste van efficiency van controle en van gebruikersgemak. Kentekenparkeren levert simpele mogelijkheden voor vergaande automatisering van de controle: er zijn meerdere dienstverleners die diensten hiervoor aanbieden. Ook gebruiksgemak van kentekenparkeren is groot: betalen kan onder andere via een app, de parkeerder hoeft niet meer naar een parkeermeter te lopen. Deze voordelen gaan ten koste van privacy: inherent wordt een parkeeraktie gekoppeld aan een kenteken, wat herleidbaar is naar een persoon. Daarnaast zijn er in het ecosysteem rondom kentekenparkeren veel externe dienstverleners aanwezig, waardoor er veel datastromen zijn waarin persoonsgegevens of tot personen herleidbare gegevens voorkomen.

Ten einde het privacy probleem van kentekenparkeren te verminderen, is een ontwerp gepresenteerd voor privacyvriendelijker kentekenparkeren. In dit ontwerp wordt privacy ten opzichte van de scanauto verbeterd. Merk op dat privacy ten opzicht van andere partijen (gemeente, dienstverleners) onveranderd blijft.

Tot slot wordt het probleem van bezoekersparkeren en medische indicaties besproken. Kern van het probleem is dat de gemeente een tegemoetkoming wil doen jegens inwoners met een medische indicatie inzake de parkeerkosten voor mantelzorg. De huidige oplossing, het vergroten van het maximum toegestane aantal uren bezoekersparkeren, heeft als nadeel dat hieruit valt af te leiden dat de inwoner een medische indicatie heeft. In andere gevallen wordt het maximum namelijk niet verhoogd.
Er zijn een aantal oplossingsrichtingen besproken, waaronder afschaffen van de tegemoetkoming, het direct storten van de tegemoetkoming op de rekening van de inwoner in het kader van de WMO en het verhogen van het maximum voor alle inwoners. Als laatste is een operationele ingreep besproken: het uitgeven van een pas met extra parkeertegoed aan inwoners met een medische indicatie. Deze uitgave zou ook in het kader van de WMO kunnen gebeuren, waarmee er geen medische informatie naar het parkeersysteem lekt.
Daaruit blijkt dat het mogelijk is om een tegemoetkoming wegens parkeren te realiseren, zonder dat uit het parkeerrechtensysteem informatie over een medische indicatie is af te leiden.

Referentie

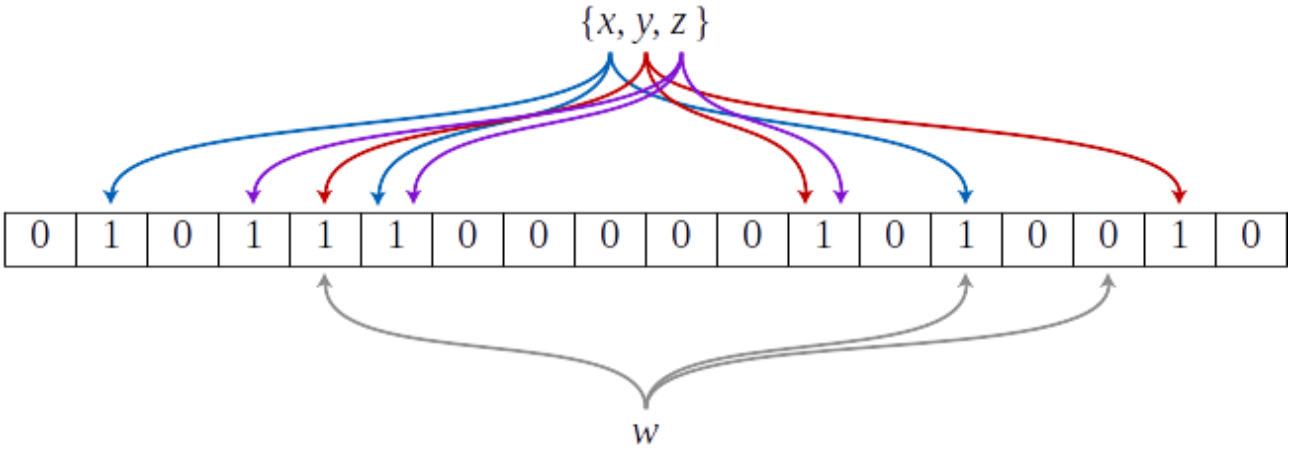
[TNO19] Gabriela Bodea, Francisca Grommé. Eindrapport Privacyvriendelijk kentekenparkeren. TNO en Privacy & Identity Lab, 10 december 2019.

Appendix A: Bloom filters

A.1. Werking Bloom filters

Technisch gezien is een Bloom filter een bitstring van m bits. Initiëel zijn alle bits op 0 gezet. Het vullen van het filter gebeurt door middel van k zogenaamde hashfuncties $h_i()$, voor $0 \leq i < k$. In de context van Bloom filters is een hashfunctie een functie die aan willekeurige invoer een index in de bitstring (een getal tussen de 0 en de $m - 1$) toekent.
Om een element X toe te voegen aan het Bloom filter (deel te maken van de verzameling), worden de k hashwaarden $h_i(X)$ berekend ($0 \leq i < k$). Iedere hasfunctie levert een index in de bitstring op, dit bit wordt op 1 gezet.

In Figuur 2 wordt een voorbeeld van een Bloom-filter weergegeven. Dit Bloom-filter gebruikt 3 hashfuncties en encodeert een verzameling van 3 elementen: x, y, en z. De pijlen tonen aan, welke indices in het Bloomfilter bij welk element horen. Ieder element wordt dus 1x met iedere hashfunctie gehashed, en de resulterende index in de lijst wordt op 1 gezet.
Merk op dat in Figuur 2 verschillende indices meerdere inkomende pijlen hebben. In dit geval zijn er dus verschillende combinaties van hashfuncties en elementen, die dezelfde index opleveren.



Figuur 2. *Een Bloomfilter voor de verzameling {x, y, z} m.b.v. 3 hashfuncties*

Om te testen of een element Q lid is van de verzameling, neemt men de k hashfuncties en past ze een voor een toe op Q. Voor iedere index wordt gechecked of het bit op 1 staat in het Bloom filter. Als het element toegevoegd zou zijn, dan worden al deze bits op 1 gezet – dus betekent een enkele 0 dat het element gegarandeerd niet voorkomt in de verzameling. Afhankelijk van het aantal elementen ingevoerd in het filter en het aantal gebruikte hashfuncties k kan er overlap ontstaan: een element Q is geen lid van de verzameling, maar in het Bloom filter zijn de k bits behorend bij Q toch allen 1.

In Figuur 2 wordt getoond hoe getest wordt, of ‘w’ een element is van de verzameling. Het kandidaat-element wordt met ieder van de drie hashfuncties gehashed. Vervolgens wordt gekeken of op ieder van de drie resulterende indices een 1 staat. Zo ja, dan lijkt w een element van de verzameling. In dit geval blijkt één index de waarde 0 te bevatten, dus is w zonder twijfel geen element van de verzameling.

A.2. Privacy versus gemiste inkomsten: keuze parameters Bloom filter

Bij het maken van een Bloom filter moeten een aantal parameters gekozen worden, afhankelijk van hoeveel elementen het Bloom filter moet kunnen weergeven en wat de gewenste kans op een false positive is. Voor dit ontwerp betekent dat: het verwachte maximum aantal geldende parkeerrechten per zone en de gewenste kans dat het filter ten onrechte denkt dat een bepaald kenteken geldige parkeerrechten heeft.
Ter herhaling: het Bloom filter kan zich alleen vergissen in false positives (onterecht parkeerrechten vermoeden), **niet** in false negatives (onterecht gebrek aan parkeerrecht vermoeden). Als de uitkomst van het Bloom filter stelt, dat het kenteken niet in de parkeerrechtendatabase voorkomt, dan is dat per constructie correct en kan het voertuig dus zonder twijfel beboet worden.

Een benadering van de foutkans (de kans dat één individuele test een false positive oplevert) wordt, voor een Bloomfilter met *k* hashfuncties, *n* elementen en een lengte van *m*, gegeven door de formule $(1 - e^{-k \cdot n / m})^k$. Het getal e in deze formule is een wiskundige constante met waarde ongeveer 2,71828.

Aan de hand van deze formule kan bepaald worden, of de kans op een false positive moet worden geminimaliseerd of juist niet. Minimaliseren van de kans op een false positive betekent dat illegale parkeerders hoogstwaarschijnlijk gedetecteerd zullen worden.
Aan de andere kant: een redelijke kans op een false positive heeft een klein positief effect op de privacy. Het betekent namelijk dat de scanauto niet zeker weet of een gescand kenteken ook daadwerkelijk parkeerrechten heeft, of dat dit een false positive is.
Merk hierbij op dat een parkeerder niet kan voorspellen of zijn/haar voertuig een false positive oplevert. Dit hangt namelijk onder meer af van de overige geparkeerde voertuigen.

Parameters voor 0.05% false positives (pakkans: 99.95%)
Uitgaande van een maximum van 1.000 geldige parkeerrechten binnen één zone, dan levert (volgens deze formule) de keuze voor 12 hashfuncties en een lijst van 15.859 bits een kans van 0,05% op een false positive. Deze kans lijkt voldoende gering om het parkeergedrag niet te beïnvloeden.

Parameters voor 5% false positives (pakkans: 95%)
Wederom uitgaande van een maximum van 1.000 geldige parkeerrechten binnen één zone, dan levert de keuze voor 3 hashfuncties en een lijst van 6.529 bits een kans van 5% op een false positive. Dit betekent dat een individuele parkeerder nog steeds een kans van 95% op een correct antwoord van het Bloom filter heeft. Dat lijkt voldoende om structureel misbruik af te schrikken. De kans om een boete te ontlopen doordat geen controle heeft plaatsgevonden, zal in veel gevallen groter zijn.