Gemeente Amsterdam

Retouradres: Postbus 94652, 1090 GR Amsterdam

Gemeente Amsterdam
Commissie Persoonsgegevens

Aan de Directeur Verkeer & Openbare Ruimte,
mevrouw E. Schieven
Manager IV Ruimte & Economie, de heer 5.1 5.1, 2, e
C.C.: Stedelijk directeur Ruimte & Economie,
de heer L. Loeven
CIO, de heer J. Flippo
Privacy officer Ruimte & Economie,
mevrouw mr. 5.1, 2, e 5.1, 2, e

Datum	23 oktober 2017
Ons kenmerk	U17074
Behandeld door	Mw. 5.1, 2, e
Doorkiesnummer	5.1, 2, e
Faxnummer	nvt
E-mail	5.1, 2, e @amsterdam.nl
Bijlage	1
Onderwerp	Advies Commissie Persoonsgegevens Amsterdam over Wifi-tracking

Geachte mevrouw 5.1, 2, e en heer 5.1, 2, e,

Op de vergadering van de Commissie Persoonsgegevens Amsterdam (CPA) van 28 september 2017 waren namens de gemeente Amsterdam aanwezig: mevrouw mr. 5.1, 2, e 5.1, 2, e (privacy officer Ruimte & Economie), de heer 5.1, 2, e en de heer 5.1, 2, e (Verkeer & Openbare Ruimte).

Bij het agendapunt "Wifi-tracking" is het volgende besproken.

U hebt de CPA geïnformeerd over de pilots op de Wallen en in de Kalverstraat die gestart zijn rondom crowd monitoring en het gebruik van wifi-tracking. De naam die het project draagt is Crowd Monitoring Systeem Amsterdam (CMSA).

De CPA is daarbij om advies gevraagd over het beleid inzake wifi-tracking en de hierbij te nemen privacybeschermende maatregelen, om te komen tot een aangescherpt protocol dat ook geschikt is voor de realisatie van CMSA.
U hebt daarbij gewezen op de brief van de Autoriteit Persoonsgegevens d.d. 15 juni 2016 inzake wifi-tracking.

De AP stelt in zijn brief d.d. 15 juni 2016 op (pagina . 5): *"Daarom geldt voor wifi-tracking op de openbare weg dat er meer waarborgen nodig zijn voor de persoonlijke levenssfeer dan voor wifi-tracking binnen (in) de ruimte van een organisatie. Een belangrijke waarborg in dit verband is het onmiddellijk en onomkeerbaar anonimiseren van gegevens, zodra deze door sensoren of andere meetinstrumenten worden vastgelegd."*

U hebt betoogd dat de gemeente Amsterdam eerder heeft getracht uitvoering te geven aan de richtlijnen in de brief van de AP, door middel van het Concept-protocol voetgangersonderzoek wifi-tracking gemeente Amsterdam", waarbij sprake is van dubbel pseudonimiseren, met gebruik van een Trusted Third Party (TTP), zodat de gemeente Amsterdam geen toegang heeft tot naar personen herleidbare gegevens, zoals Mac-adressen, tijdstippen en locatiegegevens.

Deze werkwijze is door een aanpassing in de techniek verder aangescherpt.
Daarbij wordt een onmiddellijke en onomkeerbare versleuteling direct op de sensor toegepast, waarbij -dit is nieuw- een deel van de code van het MAC-adres wordt afgekapt en weggegooid. Door deze ruistoevoeging zou het originele MAC-adres niet meer zijn te achterhalen.
Het afgekapte ('truncated') MAC-adres wordt vervolgens elke 24 uur nogmaals gehashed. Daardoor is een reispatroon na 24 uur niet meer te koppelen aan een nieuw patroon.
U stelt dat het gebruik van een TTP met bovenstaande technologie geen meerwaarde meer heeft. De aanwezigheid van een TTP zorgt voor tijdsvertraging die real-time crowd monitoring bemoeilijken.

Advies
De CPA stelt vast dat ruistoevoeging door het afkappen van het MAC-adres het minder makkelijk maakt om het MAC-adres terug te herleiden naar een geïdentificeerde of identificeerbare natuurlijke persoon. Na het rehashen blijft binnen 24 uur alleen het reispatroon over. Dit veronderstelt uiteraard wel dat de gegevens die zijn verkregen na de eerste versleuteling ook daadwerkelijk zijn vernietigd.

Een onafhankelijke technische test kan uitwijzen of de ruistoevoeging, onomkeerbare versleuteling op de sensor en rehash binnen 24 uur inderdaad een techniek is die de betrokkene onherroepelijk niet-identificeerbaar maakt. Het gaat daarbij niet alleen om de herleidbaarheid, maar ook om de koppelbaarheid en deduceerbaarheid van de overblijvende informatie. Daarbij dient onder meer gekeken te worden naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is dan wel door enige andere derde in te zetten zijn om een persoon te identificeren.

De CPA acht het in het kader van de goede vervulling van een publiekrechtelijke taak in de zin van artikel 8 onder e Wet bescherming persoonsgegevens én binnen de voorwaarden die de AP in de brief d.d. 15 juni 2016 stelt mogelijk om wifi-tracking toe te passen.

Het algemeen belang dat wordt gediend met de wifi-tracking moet worden afgewogen tegen het uitgangspunt dat burgers zich in beginsel onbespied in de openbare ruimte moeten kunnen bewegen, zoals de AP aangeeft in voornoemde brief. Als de uitkomst hiervan is dat wifi-tracking kan worden toegepast, kan de CPA zich vinden in de voorgestelde techniek, waarbij onmiddellijk en direct op de sensor wordt versleuteld en binnen 24 uur definitieve onomkeerbaarheid van het MAC-adres wordt bewerkstelligd. De CPA gaat er daarbij vanuit dat het MAC-adres met locatiegegevens en tijd het enige persoonsgegeven is dat verwerkt wordt.

De CPA kan uw stelling volgen dat onder omstandigheden bij dit proces geen TTP hoeft te worden betrokken. Dit is naar het oordeel van de CPA echter sterk afhankelijk van de gebruikte techniek en de vraag wie -en voor hoelang- de beschikking heeft over de sleutel en zal per situatie moeten worden beoordeeld.

Over het vervolg zijn volgende afspraken met u gemaakt die zijn genoemd in de zakelijke samenvatting van hetgeen op de vergadering is besproken.

Ik vertrouw er op u aldus voldoende geïnformeerd te hebben.

5.1, 2, e

Hoogachtend,

5.1, 2, e

De heer mr. dr. U van de Pol
Voorzitter Commissie Persoonsgegevens Amsterdam

5.1, 2, e

Commissie Persoonsgegevens Amsterdam
Uittreksel van het concept-verslag van de openbare vergadering op donderdag 28 september 2017

5. Wifitracking (Ruimte & Economie)

Er wordt een presentatie gegeven over het project CMSA (Crowd Monitoring Systeem Amsterdam). Na proeven bij evenementen als Sail wil Amsterdam het instrument om via het versleutelde MAC-adres van mobiele telefoons bewegingen van grote massa's voetgangers te volgen en in banen te leiden, nu ook structureel gaan toepassen. Daarvoor lopen nu proefprojecten in de Kalverstraat en op de Wallen. Er wordt gewerkt met simulatiemodellen om te bepalen op welke momenten men moet ingrijpen met het oog op de veiligheid. Zo is in beeld gebracht hoeveel gewicht een brug kan dragen of wat de capaciteit is van een route. De potentiële knelpunten zijn in kaart gebracht en crowdmanagers krijgen de gegevens vertaald in een dashboard voor zich op een scherm zodat ze kunnen anticiperen en tijdig maatregelen kunnen treffen om de menigte om te leiden voordat zich werkelijk een probleem bij een van die knelpunten voordoet.
Voor dat doel worden wifisensoren en tel-camera's aangebracht. De AP heeft gesteld dat ter bescherming van de privacy de gesignaleerde MAC-adressen onmiddellijk geanonimiseerd moeten worden. Maar als men dat doet, kan men geen beleidsinformatie genereren over voetgangersstromen gedurende een bepaalde periode. In het eerder toegestuurde protocol wordt uitgegaan van dubbel pseudonimiseren met gebruik van een TTP. Dat wil men nu aanscherpen door als directe versleuteling direct op de sensor een deel van het MAC-adres af te knippen en weg te gooien, waardoor het resultaat onherroepelijk niet meer is terug te voeren naar dat MAC-adres. Het versleutelde adres kan men vervolgens 24 uur blijven volgen. Na elke 24 uur wordt het afgekapte adres dan weer opnieuw gehashed. Het inzetten van een TTP heeft met deze techniek geen meerwaarde meer, maar levert alleen nog maar extra kosten en vertraging op in het real time volgen van de stromen. In het analyseplatform en in het dashboard komen alleen geaggregeerde gegevens terecht.
De projectleiders denken daarom dat het zinnig is nog eens naar het protocol te kijken in het licht van deze nieuwe techniek. Daar komt bij dat de partner in het project, de TU Delft, het idee heeft om de geëncrypteerde adressen zeven dagen in het monitorgebied te volgen om meer inzicht te krijgen in patronen per week. Bij Sail werden alle adressen 's avonds uit de bestanden verwijderd.
Het is de bedoeling te komen tot een Programma van Eisen van het project. Op het gebied van privacy moet daar onder meer in komen te staan hoe de voorlichting aan het publiek geregeld wordt over deze aanpak, het doel en de plekken van de monitoring. Daarvoor is een communicatieplan naar bewoners en bij de camera's komen stickers en informatieborden. Het moet duidelijk zijn of er alleen getallen doorgegeven worden of ook beelden.
De vraag aan de commissie is ook of de encryptie van de MAC-adressen nu afdoende is. Ook over de opslaglocatie en -termijn moet duidelijkheid zijn. Voorts moeten regels vastgesteld worden over de toegang tot de gegevens.

De CPA wil graag een nadere toelichting van de TU Delft op de motieven om de adressen zeven dagen te monitoren.

Als de adressen elke 24 uur versleuteld worden, lijkt dat de CPA niet mogelijk dus is het de vraag hoe men dat denkt op te lossen of dat men nu ook dezelfde encryptie zeven dagen lang wil gebruiken. Dat kan in ieder geval niet met geanonimiseerde data. De vraag is echter vooral wat men met die extra dagen volgtijd denkt toe te voegen aan het inzicht in de drukte en de bewegingen. Ook wijst men op het risico dat gegevens gekoppeld gaan worden aan die van andere monitorgebieden in de stad. Als er dan gepseudonimiseerde MAC-adressen bewaard zijn, kan men de bewegingen van de betreffende persoon gedurende een hele week volgen en dat lijkt op een nachtmerriescenario. Door die gegevens dan ook nog slim te koppelen is het zelfs mogelijk de betreffende persoon te achterhalen en verbanden te leggen met andere profielen in andere bestanden. Dat zou in potentie allemaal mogelijk zijn met deze technologie. Dat alles pleit voor een kortere bewaartermijn.
De CPA merkt op dat in de meegestuurde bewerkersovereenkomst een bewaartermijn van drie weken genoemd staat. Verder is de CPA wat er gebeurt met de MAC-adressen van bewoners waarvan signalen opgevangen worden door de sensoren. Ook is men benieuwd hoe men zeker kan weten dat het voor de technische kant ingeschakelde bedrijf Blip Systems via de sensoren niet ook meteen andere gegevens uitleest.

De projectleiders zullen de vraag over die verlenging van de bewaartermijn tot een week doorgeven aan de TU Delft. Als het erom gaat te achterhalen hoeveel mensen meer dan een dag in het gebied komen, zijn daar ook andere middelen voor, bijvoorbeeld een statistische enquête. Bewoners van het gebied die een sensor passeren, tellen gewoon mee in de voetgangersstroom. De bewerkersovereenkomst hoort nog bij het protocol dat hier enkele maanden geleden is besproken. Dat sluit echter niet meer aan bij het huidige project met zijn andere technologie zonder TTP en zal dus moeten worden aangepast. Daarom komen zij nu ook advies vragen aan de CPA. In theorie zou men na de eerste encryptie die direct op de sensor gebeurt, nog het MAC-adres kunnen terughalen als men in het bezit is van de sleutel die de sensor op het betreffende moment hanteert. Die sleutel wordt bij elke sensor om de zeven dagen gewijzigd. Na de tweede rehash is er sprake van volledige anonimiteit en is het betreffende item alleen nog bekend als behorende tot een bepaalde categorie. Anders dan bij kentekens is er nergens een register met tenaamstellingen van MAC-adressen. De koppeling van de opgeslagen data aan persoonsprofielen gebeurt dus niet.
Het is niet mogelijk andere gegevens dan het MAC-adres van een telefoon op te vangen met de sensoren, tenzij de telefoonbezitter op dat moment actief ingelogd heeft op dat netwerk, wat zo goed als uitgesloten is. Het bedrijf is gevestigd in Denemarken, maar levert deze diensten in veel landen. De sensoren zelf komen uit Zwitserland.

De CPA en de indieners komen tot de conclusie dat het nodig is nog een keer bij de commissie langs te komen met een concept voor het Programma van Eisen, waarin dan antwoorden op de openstaande vragen verwerkt zijn. De volgende punten zijn dan van belang:

- Een goede toelichting van de TU Delft op de wens om de bewaartermijn te verlengen tot een week en de wijze waarop men dan de genoemde privacy-risico's wil voorkomen.
- Het standpunt van de projectleiders zelf over die bewaartermijn.
- De regels rond de toegang van de gegevens voor verschillende belanghebbenden of gebruikers.
- Aanpassingen aan het protocol.

- Een goed onderscheid tussen echte passanten en de bijvangst van bewoners die hun telefoon of ander wifi-apparaat in huis hebben aan staan.
- Opnemen dat men in de voorlichting ook moet vermelden dat men zich aan de monitoring kan onttrekken door de telefoon uit te schakelen.

De voorzitter stelt voor het project in december of januari weer hier aan de orde te stellen. Hij adviseert de projectleiders daarover tijdig afspraken te maken met het secretariaat.