PRIVACY FIRST

Postbus 16799
1001 GR Amsterdam
Tel. 020 - 8100279

Aan:
Tweede Kamer der Staten-Generaal
Vaste commissie voor Infrastructuur en Waterstaat
Per email: cie.iw@tweedekamer.nl

Uw ref.	:	
Onze ref.	:	SPF20190905
Datum	:	5 september 2019
Betreft	:	Position paper t.b.v. rondetafelgesprek toegang tot OV-data 10 september 2019

Geachte Kamerleden,

Dank voor uw uitnodiging om deel te nemen aan het rondetafelgesprek inzake toegang tot OV-data. Hieronder zal Stichting Privacy First haar voornaamste standpunten in dit verband kort uiteenzetten.

1. Recht op anonimiteit in het openbaar vervoer

Iedere reiziger dient het openbaar vervoer desgewenst volstrekt anoniem te kunnen gebruiken. Iedere burger heeft immers recht op anonimiteit in de openbare ruimte, waaronder het openbaar vervoer. Dit vloeit voort uit de combinatie van twee klassieke mensenrechten: het recht op privacy in combinatie met het recht op vrijheid van beweging. Anonimiteit in het openbaar vervoer is tevens een voorwaarde voor de uitoefening van diverse andere klassieke burgerrechten, waaronder de vrijheid van demonstratie en (daarmee) meningsuiting.[1] Ook de journalistieke bronbescherming en persvrijheid zijn hiermee gediend. In bredere zin is anoniem openbaar vervoer dus een kernaspect van een vrije democratische rechtsstaat.

Voor een actuele rechtszaak waarin het recht op anonimiteit in het openbaar vervoer centraal staat verwijst Privacy First graag naar de zaak van Michiel Jonker vs. Autoriteit Persoonsgegevens aangaande de “anonieme” OV-chipkaart; zie https://www.privacyfirst.nl/aandachtsvelden/mobiliteit/item/1155-rechtszaak-over-privacy-anonieme-ov-chipkaart.html.[2]

2. Alleen geanonimiseerde, geaggregeerde data delen, met strikte waarborgen

Omdat mobiliteit in de openbare ruimte onlosmakelijk verbonden is met menselijk gedrag mag dit niet belast worden met monitoring en surveillance. Tegelijk kunnen OV-bedrijven behoefte hebben aan data om hun diensten te leveren. Slechts geanonimiseerde, geaggregeerde reizigersstatistieken op macroniveau zouden door OV-bedrijven met derde partijen gedeeld mogen worden. Dergelijke data mogen in geen enkel geval tot individuele reizigers herleidbaar zijn. Er zou een limitatieve lijst moeten komen van duidelijk omschreven

[1] Een voorbeeld waarbij openbaar vervoerbewegingen gebruikt worden om vrijheid van meningsuiting en het recht op demonstratie te hinderen is momenteel in Hong Kong te zien. Uit angst voor digitale sporen kopen demonstranten losse treinkaartjes.

[2] In algemene zin heeft Stichting Privacy First de heer Jonker tevens gemachtigd om namens Privacy First (en desgewenst ook op individuele titel) het woord te voeren bij het rondetafelgesprek over de toegang tot OV-data op 10 september as.

data die mogen worden gedeeld. Alles wat niet op die lijst staat, mag niet worden gedeeld. Er zouden waarborgen moeten zijn dat er, ten behoeve van aggregatie, geen persoonlijke reisgegevens worden verzameld. De geaggregeerde data zouden dus niet gebaseerd moeten zijn op een compilatie van geregistreerde individuele reisbewegingen, maar alleen op waarnemingen van aantallen reizigers in het OV.

3. **Geen massa-surveillance van overheidswege in het openbaar vervoer**

Er mag geen sprake zijn van directe, heimelijke toegang door inlichtingendiensten tot de databanken van OV-bedrijven. Van bulk-data *hacking* in dergelijke OV-databanken door overheidsdiensten mag evenmin sprake zijn. Dit vergt aanscherping van de nieuwe Wet op de inlichtingen- en veiligheidsdiensten. Tevens dienen OV-bedrijven niet te fungeren als verlengstuk van politie en justitie; opsporing en vervolging is een taak van de overheid, niet van OV-bedrijven.

4. **Transparantie bij privacy-inbreuken**

OV-bedrijven dienen transparant te zijn over het vorderen van OV-data door overheidsdiensten, bijvoorbeeld middels jaarlijkse openbare statistische rapportages. Tevens dient de bestaande notificatieplicht na dergelijke vorderingen door overheidsdiensten tegenover de betreffende reizigers tijdig en actief te worden gehandhaafd.

5. **Privacy-waarborgen bij reizigersonderzoek**

Reizigers dienen actief geïnformeerd te worden dat zij nimmer verplicht zijn om mee te werken aan OV-onderzoeken, bijvoorbeeld voorafgaand aan dergelijk onderzoek in de trein. Het registreren van individuele reisbewegingen zou bovendien alleen mogelijk moeten zijn in de vorm van duidelijk in tijd en omvang begrensde onderzoeksprojecten waar beperkte groepen reizigers zich vrijwillig voor zouden kunnen aanmelden, met een bovengrens van (bijvoorbeeld) 5000 reizigers in heel Nederland tegelijk op enig tijdstip.

6. **Aantoonbaar gebruik van *privacy by design***

OV-bedrijven dienen aantoonbaar gebruiken te maken van *privacy by design* (art. 25 AVG). Overwogen kan worden de gebruikte software en algoritmes te openbaren zodat deze onafhankelijk beoordeeld kunnen worden. Instandhouding van de OV-chipkaart vergt bovendien een geheel nieuwe, decentrale architectuur met actieve implementatie van – bijvoorbeeld – zero-knowledge chiptechnologie.[3]

Voor nadere informatie of vragen met betrekking tot bovenstaande punten is Privacy First te allen tijde bereikbaar op telefoonnummer 020-8100279 of per email: info@privacyfirst.nl.

Hoogachtend,

Stichting Privacy First

mr. Vincent A. Böhre, CIPP/E
directeur

[3] Zie bijvoorbeeld ook de beschreven oplossingen van Jaap-Henk Hoepman op https://blog.xot.nl/2019/08/29/privacy-friendly-public-transport-ticketing/ , 29 augustus 2019.