D.R. Borghuis ook genaamd op de Borg
XXXXXXXXXXX
XXXXXXXXXX
Mobiel : XXXXXXXXX
Email : dave@daveborghuis.nl

Aan:
Gemeente Enschede
Postbus 20
7500 AA Enschede

10 November 2017

Betreft: Klacht wifi tracking door Gemeente Enschede

Geachte heer, geachte mevrouw,

Hierbij wil ik een klacht indienen bij Gemeente Enschede.

In brief van 5 September 2017 (kenmerk 1700087255) geeft de Gemeente Enschede aan dat door middel van WiFi tracking wordt uitgevoerd ten bate van bijhgouden bezoekers-aantallen en stromingen.

In brief van Autoriteit Persoonsgegevens aan VNG op 15 Juni 2017 (kenmerk z2016-00087) worden alle Nederlandse Gemeentes gewezen op de regels omtrent wifi tracking voor/van het winkelend publiek. Hierbij wordt aangegeven dat :

1) "In de openbare ruimte moeten mensen zich onbespied kunnen bewegen, zonder dat hun bewegingen in kaart worden gebracht."

Door al het winkelend publiek 24/7 ongevraagd te volgen wordt deze aanbeveling zeer duidelijk overtreden, Wifi tacking valt niet in beginsel proportionaliteit/subsidiariteit.

2) "Uit het genoemde onderzoek blijkt overigens dat het toepassen van een (vast) hashing algoritme op de verzamelde unieke identifiers niet altijd leidt tot anonimiseren (dus onveilig)."

Afgezien van de gekozen methode van hashing, je vervangt het ene nummer (MAC) naar een ander nummer (hash of versleuteling van MAC), zoals AP zelf ook aangeeft, is dit nog geen garantie voor anonimiteit.

City Traffic heeft in het overleg van 19 oktober 2017 aangegeven dat men voor de versleuteling een eigen ontwikkelde geheime methode gebruikt gebaseerd op SHA-256. Normaal in de wetenschappelijke wereld van versleuteling is de methode publiek en een gebruikte sleutel geheim. Dat bij City Traffic de methode zelf ook geheim is wil zeggen maakt dat deze niet te controleren valt door een deskundige en er ook geen oordeel kan worden gegeven hoe (on)veilig de gebruikte methode is (validiteit/betrouwbaarheid). Mede omdat het inmiddels bewezen is dat een "eigen ontwikkelde" methode in de regel onveiliger is dan het adopteren/hanteren van wereldwijde standaarden.

3) "Voorafgaande toestemming van de betrokkenen ...."
Het eerste onderdeel van de Wbp mbt toelaatbare gronden (grondslag voor verwerking, naast de doelbinding) voor gegevensverwerking stelt dat er sprake dient te zijn van ondubbelzinnige en

vrije/aantoonbare toestemming. Hiervan zal in beginsel geen sprake zijn. Het winkelend publiek heeft voor het verzamelen van wifi-gegevens immers geen toestemming gegeven, en is ook niet geïnformeerd (informatieplicht) / gewaarschuwd (recht op informatie en inzage).
De opt-out mogelijkheid op de website van City Traffic valt hierdoor niet onder de noemer "ondubbelzinnige toestemming", de bezoeker verricht namelijk geen actieve handeling om toestemming te geven op het moment hij/zij de binnenstad betreedt.
Tevens draagt het plaatsen van enkele stickers, voorzien van summiere teksten, weinig bij aan het feit dat een bezoeker (goed) geïnformeerd moet zijn voor een "ondubbelzinnige toestemming". Dat zou dan een 'OptIn' regeling betreffen.

4) "Het afbakenen van gebieden en periodes waarbinnen gemeten wordt is een voorbeeld van een waarborg op het gebied van proportionaliteit."
I.c.m. doel waarvoor het nodig is (doelbinding) Het monitoren van een (groot deel) van de binnenstad gedurende 24/7 is niet proportioneel. Immers bestrijken de winkeltijden slechts een klein deel van de uren waarop een bezoeker de binnenstad kan betreden. Doel/belang voor gemeente dus ook nog steeds niet helder.

5) Rechtmatigheid/Grondslag
De gegevensverwerking is ook niet noodzakelijk voor de nakoming van een wettelijke verplichting, noch is het een onderdeel van een (primaire) taak van de gemeente.

6) art. 8 sub f Wbp
Deze bepaling eist dat de gegevensverwerking noodzakelijk moet zijn voor de behartiging van het gerechtvaardigde belang van de commerciële activiteiten in de binnenstad, tenzij het belang of de fundamentele rechten en vrijheden van het winkelend publiek prevaleert. Het verzamelen en opslaan van wifi-gegevens is niet noodzakelijk voor het verrichten van reguliere bedrijfsactiviteiten in de binnenstad. Deze afweging behoort ook vastgelegd te zijn in de doelbinding/grondslag van betreffende verwerking.

7) Privacy by Design en Privacy by default
Op dit moment bevinden we ons in de overgangsfase naar de AVG, die op 25 mei 2018 de Wbp vervangt. In deze overgangsfase heeft de gemeente de tijd om zaken hierop in te richten.
De AVG bevat passages rondom Privacy by Design en Privacy by Default. Ook deze bepalingen stellen dat bij het ontwerp en bij instellingen van het '(meet-)systeem' een goede afweging genomen gemaakt moet worden of het verzamelen van persoonsgegevens nodig is en op welke wijze in te regelen (design/default). Tevens dient de standaard inrichting uit te gaan van privacy-vriendelijkheid / -bescherming (default).

In het overleg van 19 oktober jl. wordt door gemeente Enschede nogmaals benadrukt dat men alleen telt. Dit geldt inderdaad voor de totaal resultaten die de Gemeente krijgt, echter om deze te krijgen moeten door City Traffic zelf wel wifi tracking plaatsvinden en is e.e.a. herleidbaar tot natuurlijke personen en dus inbreuk privacy van het winkelend publiek.

Hierbij zou ik gemeente Enschede willen verzoeken te stoppen met het tracken van het winkelend publiek in Enschede. De wifi tracking is zoals dat momenteel voordoet volgens de Wbp niet toegestaan en onrechtmatig en betreft het een niet proportionele wijze van vergaren persoonsgegevens die een inbreuk op de privacy van de burgers in en bezoekers van Enschede betekeken.