*B.F.E. Bosch en prof. dr. N.A.N.M. van Eijk**

Wifi-tracking in de winkel(straat): inbreuk op de privacy?

251

Trefwoorden:
retailtracking, wifi-tracking, Bluetrace, Nomi

Tegenwoordig wordt de consument op steeds grotere schaal gevolgd via de wifi-signalen die smartphones uitzenden. Inzicht in hoe consumenten zich gedragen in een winkel levert commerciële voordelen op voor de winkeliers, maar ook risico's voor de persoonlijke levenssfeer. Onder de Wet bescherming persoonsgegevens is gegevensverwerking via wifi-tracking toegestaan, mits wordt voldaan aan de strenge eisen die de wet stelt. Ter vergelijking wordt gekeken naar de regulering van wifi-tracking in de Verenigde Staten.

1 Inleiding

'We know where people go', zo adverteert het Amsterdamse bedrijf Citytraffic haar wifi-trackingtechnologie op de website.[1] Winkeliers krijgen graag inzicht in het gedrag van consumenten om zo de winst te kunnen optimaliseren. Momenteel wint wifi-tracking als nieuwe retailtrackingtechnologie snel terrein, terwijl de consument zich zorgen maakt over de impact van deze nieuwe technologie op zijn/haar privacy.[2] Uit recent onderzoek blijkt dat 57% van de Nederlanders 'niet' of 'zeker niet' persoonlijke informatie met winkeliers wenst te delen.[3] De meeste consumenten zijn zich er echter niet van bewust dat hun verplaatsingsgedrag wordt geregistreerd door winkeliers. Ondanks de grootschalige toepassing in Nederland is de vraag in hoeverre deze nieuwe technologie überhaupt is toegestaan. Dit artikel beoogt de juridische kwalificatie van wifi-tracking inzichtelijk te maken. Daartoe wordt allereerst de technologie besproken en de voor- en nadelen hiervan. Het juridisch kader wordt uiteengezet evenals de *leading case* van de Autoriteit Persoonsgegevens (AP) op dit gebied: Bluetrace BV (Bluetrace). Vervolgens wordt ingegaan op het Amerikaanse wettelijk kader en de leading case aldaar (Nomi). In de analyse vindt een vergelijking plaats tussen beide landen en tot slot worden twee knelpunten gesignaleerd die verdere aandacht behoeven.

2 Retailtracking

2.1 *Het fenomeen*

Retailtracking is het fenomeen waarbij winkeliers het gedrag van consumenten in de winkel(straat) registreren en analyseren met als doel bedrijfseconomische inzichten te verwerven. De winkelier kan bezoekersaantallen, bezoekersstromen en het koopgedrag van consumenten analyseren en aan de hand daarvan de winst optimaliseren. Aan de hand van deze analyse kunnen de winkelindeling en het aanbod worden aangepast aan het winkelgedrag van de consument. Het in kaart brengen van consumentengedrag neemt explosief toe:[4] van handmatige tellingen, consumentenenquêtes, gedragsobservatie in de winkel, analyse van camerabeelden, naar het gebruik van de smartphone als uniek identificatiemiddel om consumentengedrag te registreren en analyseren. Wifi-tracking is daarbij een veelgebruikte technologie[5] en het focuspunt van dit artikel, maar ook vergelijkbare bluetooth-trackingtechnologie is populair.

2.2 *Wifi-trackingtechnologie*

Mobiele apparaten bevatten meerdere antennes om verbinding te kunnen maken met een mobiele aanbieder of wifi-hotspot, waaronder een wifi-antenne. Het apparaat zendt automatisch wifi-signalen uit als de wifi-functionaliteit is ingeschakeld om verbinding te kunnen maken met een wifi-netwerk. Deze signalen kunnen worden opgevangen door een wifi-hotspotaanbieder (actief monitoren) of door een derde (passief monitoren).[6] Dit laatste is het geval bij wifi-tracking. Voor wifi-tracking zijn in de winkel een of meerdere wifi-trackingsensoren geïnstalleerd. Deze sensoren vangen de wifi-signalen op die de mobiele apparaten uitzenden. Deze wifi-signalen bevatten een Media Access Control-adres (MAC-adres) dat uniek is voor elk apparaat. De sensoren registreren ook de signaalsterkte, tijd en datum. De geregistreerde gegevens worden vervolgens naar de cloud

* **Berber Bosch is masterstudent Informatierecht. Nico van Eijk is als hoogleraar Informatierecht verbonden aan het Instituut voor Informatierecht (IViR, Universiteit van Amsterdam).**

1 citytraffic.nl/site/locaties.
2 Autoriteit Persoonsgegevens, *Wifi-tracking en de Wet bescherming persoonsgegevens*, brief aan Detailhandel Nederland, 15 juni 2016 (hierna: Brief Detailhandel Nederland AP), p. 1.
3 ABN AMRO, *Big data in de retail bezien vanuit een klantenperspectief*, rapport, februari 2016 (hierna: ABN AMRO), p. 6.
4 P. Underhill, *Why we buy, the science of shopping* (Simon & Schuster paperbacks), januari 2009.
5 Brief Detailhandel Nederland AP, p. 1.
6 A. Soltani, *Privacy trade-offs in retail tracking*, FTC blog 30 april 2015, www.ftc.gov/news-events/blogs/techftc/2015/04/privacy-trade-offs-retail-tracking (hierna: Soltani).

of server gestuurd en opgeslagen. Het systeem verwerkt en analyseert de gegevens tot geaggregeerde informatie. De winkelier krijgt hierna toegang tot de verzamelde gegevens en statistieken. Bluetooth-trackingtechnologie werkt op overeenkomstige wijze, maar dan met registratie van het bluetooth-MAC-adres.

2.3 *Voordelen*

Wifi-trackingtechnologie kan grote winst opleveren voor winkeliers. De combinatie van de verzamelde gegevens kan inzicht geven over de toeloop naar de winkel, gemiddelde duur van een winkelbezoek, de looproutes door de winkel, knelpunten, drukte en bezoekersfrequentie. De winkelier kan hierdoor het consumentengedrag en de consumentenvoorkeuren beter begrijpen. Deze kennis kan de winkelier vervolgens gebruiken om het productaanbod aan te passen aan de behoeftes van de klant, de winkelindeling te verbeteren, de personeelsplanning te optimaliseren en persoonlijke en locatiegebonden aanbiedingen te doen.[7] De consument kan eveneens voordeel beleven aan de toegenomen inzichten van de winkelier. De wachtrijen bij de kassa kunnen bijvoorbeeld verkort worden door een aangepaste personeelsplanning. Ook kan de consument mogelijk betere service en interessante gepersonaliseerde aanbiedingen ontvangen.

2.4 *Nadelen*

Het gebruik van wifi-trackingtechnologie brengt risico's mee voor de persoonlijke levenssfeer van de consument. Een mobiel apparaat is onlosmakelijk verbonden met een individu. De meeste mensen hebben hun telefoon naast het bed liggen, nemen het apparaat overal mee naar toe en lenen deze vrijwel nooit uit. De locatie van het apparaat geeft daarom een intieme kijk in het leven van de eigenaar. De combinatie van locatie, tijd, datum en MAC-adres maakt het eenvoudig mogelijk om te herleiden van wie het apparaat is.

De gemeten gegevens zijn ook te combineren met andere gegevens, zoals een bonuskaart, camerabeelden, sociale media, koopgeschiedenis en uiterlijke kenmerken.[8] Van de consument kan zo een zeer uitgebreid beeld worden gevormd en hieruit kunnen persoonlijke profielen worden opgesteld. Op basis daarvan kunnen gepersonaliseerde aanbiedingen worden gedaan, maar het is ook denkbaar dat deze profielen gebruikt worden voor bijvoorbeeld prijsdiscriminatie.[9]

Winkels en wifi-trackingaanbieders communiceren weinig of niet met het publiek over de technologie, haar toepassing en de gevolgen. Dit gebrek aan transparantie heeft tot gevolg dat het publiek veelal geen idee heeft dat wifi-tracking plaatsvindt. Het is voor de consument moeilijk om zich aan wifi-tracking te onttrekken, omdat het een actieve handeling vraagt, namelijk het uitschakelen van de wifi-functionaliteit of het geheel uitzetten van de telefoon.[10]

Bovendien wordt er steeds meer trackingtechnologie ingezet, in winkels en in steden, waardoor er een samenleving ontstaat waarin men in toenemende mate traceerbaar is. Gewenst of ongewenst worden burgers aldus continu gevolgd zonder dat op het aanstaan van deze sensoren enige invloed kan worden uitgeoefend. Wifi-tracking strekt zich ook uit tot buiten de winkelmuren. Vaak wordt met een straal om de winkel heen gemeten met als doel de verhouding tussen voorbijgangers en winkelbezoekers te registreren. Dit heeft tot gevolg dat het verplaatsingsgedrag van willekeurige voorbijgangers en omwonenden wordt geregistreerd zonder dat zij hier invloed op kunnen uitoefenen.

Eenmaal verzameld kunnen de gegevens ook voor andere doeleinden worden gebruikt dan het registreren van bezoekersstromen en drukte. Zo kunnen ze worden gebruikt om whitelists en blacklists van gewenste en ongewenste klanten op te stellen.[11] De politie en veiligheidsdiensten kunnen de gegevens opvragen en gebruiken voor onderzoek of bewijsmateriaal en dit gebeurt ook in de praktijk.[12] Hackers kunnen de gegevens buitmaken in geval van een slechte netwerkbeveiliging of bij een datalek.

3 Toepasselijk juridisch kader

In Nederland is de Wet bescherming persoonsgegevens (Wbp), als implementatie van de Privacyrichtlijn 95/49/EG, van toepassing op elke verwerking van persoonsgegevens en vormt daarmee het juridisch kader voor wifi-tracking. De volgende vijf aspecten van de Wbp zijn bij wifi-tracking in het bijzonder van belang en worden nader geanalyseerd.

Persoonsgegevens

Persoonsgegevens zijn 'elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon' (artikel 1 onderdeel a Wbp). Wifi-trackingtechnologie registreert het MAC-adres van het mobiele apparaat als identificatiemiddel. Daarbij kan het de datum, tijd, sig-

7 ABN AMRO, p. 17; Soltani.

8 International Working Group on Data Protection in Telecommunications, *Working Paper on Location Tracking from Communications of Mobiles Services*, 58th meeting, Berlijn, Duitsland, 13-14 oktober 2015 (hierna: International Working Group on Data Protection in Telecommunications), p. 4, paragraaf 16e.

9 F.J. Zuiderveen Borgesius, *Online Price Discrimination and Data Protection Law*, 28 augustus 2015, Amsterdam Law School Research Paper No. 2015-32, Institute for Information Law Research Paper No. 2015-02.

10 L. Sweeney, *How retailers use smartphones to track shoppers in the store*, 16 juni 2014, www.npr.org/2014/06/16/322597862/how-retailers-use-smartphones-to-track-shoppers-in-the-store.

11 International Working Group on Data Protection in Telecommunications, p. 4, paragraaf 16j.

12 Autoriteit Persoonsgegevens, *Wifi-tracking van mobiele apparaten in en rond winkels door Bluetrace*, Rapport definitieve bevindingen, 13 oktober 2015 (hierna: Bluetrace-rapport), p. 31-32.

naalsterkte en het sensornummer (van het apparaat dat de signalen waarneemt) registreren. Een MAC-adres in combinatie met de locatie van het apparaat is door de Artikel 29-werkgroep aangemerkt als een persoonsgegeven, omdat deze gegevens tezamen te herleiden zijn tot de individuele eigenaar van het apparaat.[13]

Verantwoordelijke

De verantwoordelijke voor de gegevensverwerking is degene die formeel-juridisch het doel en de middelen vaststelt waarbij tevens in acht wordt genomen wat er feitelijk tussen partijen gebeurt (artikel 1 onderdeel d Wbp):[14] wie de verantwoordelijke is kan per wifi-trackingaanbieder en winkelier verschillen.

Verwerkingsgrondslag

Elke verwerking van persoonsgegevens dient gebaseerd te zijn op een geldige grondslag (artikel 8 Wbp). In het kader van wifi-tracking zijn er meerdere grondslagen mogelijk, maar in de praktijk zal meestal alleen een gerechtvaardigd belang in aanmerking komen als geldige grondslag. Geëvalueerd dient te worden of de verantwoordelijke een gerechtvaardigd belang heeft, of de gegevensverwerking noodzakelijk is om het nagestreefde belang te bereiken en of het gerechtvaardigd belang in de belangenafweging met de rechten van de betrokkenen meer gewicht toegekend dient te worden. Het belang van de retailtrackingaanbieder of winkelier om bedrijfseconomische inzichten te verwerven met het meten van het verplaatsingsgedrag van de consument dient daarbij te worden afgewogen ten opzichte van het belang van de consument om niet aangetast te worden in zijn/haar persoonlijke levenssfeer.

Bewaartermijn

De gegevens mogen niet langer worden bewaard in een vorm die het mogelijk maakt om de betrokkene(n) te identificeren dan noodzakelijk is voor de verwerkelijking van de doeleinden van wifi-tracking (artikel 10 Wbp). Een MAC-adres in combinatie met locatiegegevens mogen maximaal 24 uur worden bewaard wanneer dit noodzakelijk is voor de dienst.[15]

Informatieplicht

Op de verantwoordelijke rust de plicht om de betrokkene(n) te informeren over de gegevensverwerking (artikel 33 en 34 Wbp). De verantwoordelijke dient de betrokkene op de hoogte te stellen over onder andere wie de wifi-trackingmetingen verricht, welke gegevens worden gemeten en met welke doeleinden.

4 Case: Bluetrace

De Autoriteit Persoonsgegevens (AP) heeft, als toezichthouder op naleving van de Wbp, ambtshalve onderzoek ingesteld naar de retailtrackingaanbieder Bluetrace.[16] Het bedrijf biedt zowel wifi-tracking als bluetooth-trackingtechnologie aan. De AP legt in het onderzoek de focus op wifi-tracking aangezien dit het overgrote deel van de metingen van het bedrijf betreft. De zaak kan gezien worden als de *leading case* op het gebied van wifi-tracking, aangezien het de eerste keer is dat de AP de vereisten onder de Wbp in het kader van wifi-tracking toetst.

4.1 *Onderzoeksrapport*

Op 1 december 2015, na ruim een jaar onderzoek, heeft de AP haar rapport over de werkwijze van Bluetrace gepubliceerd.[17] De AP geeft aan dat zij de activiteiten van de retailtrackingaanbieder heeft onderzocht, omdat wifi-tracking een betrekkelijk nieuw fenomeen is. Consumenten zijn zich doorgaans niet bewust van de registratie van hun verplaatsingsgedrag en de risico's voor de persoonlijke levenssfeer, aldus de AP.[18]

Bluetrace past de wifi-trackingtechnologie toe zoals hierboven in paragraaf 2.2 beschreven. Het bedrijf meet daarbij de ruwe gegevens: het MAC-adres van de (mobiele) apparaten, signaalsterkte van het geregistreerde wifi-signaal van de apparaten, het serienummer van de sensor en de datum en het tijdstip van de meting. De analyse van deze gegevens levert de volgende informatie op:

- tellingen: aantal unieke apparaten binnen sensorbereik;
- mobiliteit: bewegingsgedrag van de apparaten, waaronder stilstaan, versnellen, vastlopen en het onderscheid tussen voorbijgangers en winkelbezoekers; en
- bezoekfrequentie: verhouding tussen aantal unieke en terugkerende apparaten.

In het onderzoeksrapport werd vastgesteld dat Bluetrace deze metingen 24 uur per dag, zeven dagen per week verricht. Bluetrace voorzag de consument niet van informatie in de winkels of op haar website. Het bedrijf had geen bewaartermijnen ingesteld, maar verving de gemeten gegevens na maximaal drie weken met gehashte waarden. Hashen is een wiskundige bewerking die de informatie omzet in een hashwaarde. Het is afhankelijk van de omstandigheden of dit tot pseudonimisering (Wbp van toepassing) of anonimisering (Wbp niet van toepassing) leidt.

13 Artikel 29-werkgroep, *Advies 13/2011 over geolocatiediensten op slimme mobiele apparaten*, WP 185, 16 mei 2011 (hierna: WP29 Geolocatiediensten 13/2011), p. 10 -11.
14 *Kamerstukken II* 1997/98, 25892, 3, p. 55, onderdeel d; zie ook: Artikel 29-werkgroep, *Advies 1/2010 over de begrippen verantwoordelijke en bewerker*, WP 169, 16 februari 2010, p. 8-9.
15 WP29 Geolocatiediensten 13/2011, p. 18 en 20.
16 www.bluetrace.eu.
17 Bluetrace-rapport.
18 Bluetrace-rapport, p. 4.

In haar onderzoeksrapport concludeert de AP dat Bluetrace met haar werkwijze in strijd handelt met artikel 8, 10, 34 in samenhang met artikel 6 Wbp.

Persoonsgegevens

Allereerst stelt de AP vast dat de Wbp van toepassing is op wifi-trackingtechnologie, omdat er persoonsgegevens in de zin van artikel 1 onderdeel a Wbp worden verwerkt. De combinatie van het MAC-adres en de locatie van het apparaat maakt identificatie van de eigenaar van het apparaat mogelijk.[19] Dit blijkt ook onder meer uit het feit dat Bluetrace in het verleden meetgegevens aan de opsporingsdiensten heeft gegeven en in de rechtspraak dit soort gegevens zijn gebruikt als bewijs.[20] De hashingmethode van Bluetrace leidt niet tot anonimisering van de gegevens nu de mogelijkheid tot identificatie van de betrokkenen niet onherroepelijk is uitgesloten.[21] Het bedrijf heeft namelijk zelf de hashing-algoritmen in bezit die gebruikt worden voor het hashen.[22]

Verantwoordelijke

De AP merkt Bluetrace als (mede)verantwoordelijke aan voor de gegevensverwerking. Alhoewel het bedrijf de gegevens verwerkt als uitvloeisel van de dienst die zij aan haar klanten aanbiedt, bepaalt zij zelf welk soort gegevens zij verwerkt, hoe lang en met welke middelen (artikel 1 onderdeel d Wbp).

Geldige grondslag

Het ontbreekt Bluetrace aan een geldige grondslag op grond van artikel 8 Wbp voor de verwerking van de persoonsgegevens in de winkels en buiten de winkels. Op zichzelf kan het verzamelen van informatie over bezoekersaantallen, drukte en looproutes door een winkel, door middel van wifi-tracking, een gerechtvaardigd belang zijn voor de gegevensverwerking *in* de winkel voor Bluetrace en de winkeliers. De AP is echter van mening dat de verwerkingen niet noodzakelijk zijn voor de verwerkelijking van dit nagestreefde belang. Het meten van de bezoekersaantallen en verblijftijden kan namelijk op een minder ingrijpende wijze plaatsvinden door de metingen te beperken in tijd en ruimte. Een beperking van de bewaartermijnen en het voorzien van de consument van informatie over de metingen zijn daarvoor vereiste waarborgen.

Ten aanzien van de metingen *buiten* de winkels zijn de eisen voor de bescherming van de belangen van de betrokkenen strenger. Wifi-tracking op de openbare weg heeft namelijk een grotere impact op de persoonlijke levenssfeer van de consument. Bluetrace verwerkt meer gegevens dan noodzakelijk en zou ook op een andere, minder ingrijpende, wijze voorbijgangers kunnen tellen. Daarnaast dient Bluetrace een effectieve opt-out aan te bieden aan omwonenden en hen gericht en actief te informeren.

Bewaartermijn

De AP is van mening dat Bluetrace in overeenstemming met artikel 10 Wbp had moeten handelen door bewaartermijnen vast te stellen en de gegevens vervolgens volledig had moeten anonimiseren of verwijderen. Een maximale opslagtermijn van 24 uur acht de AP passend indien dit nodig is voor het functioneren van de trackingdienst en korter voor gerechtvaardigde bedrijfseconomische belangen.

Informatieverplichting

Tot slot meent de AP dat Bluetrace tekortschiet in haar informatieverplichting aan het publiek (artikel 34 in samenhang met artikel 6 Wbp). Zij stelt geen specifieke voorwaarden aan het voldoen aan de informatieplicht, maar geeft wel een aantal mogelijkheden weer, zoals informatiestickers, -borden en -brochures in de winkel en borden op de paden bij de ingangen van winkelcentra en openbare aanplakkingen buiten de winkels.[23] Door de betrokkenen niet voldoende te informeren over welke gegevens worden verwerkt, waar, waarom en wie voor de verwerkingen verantwoordelijk is, handelt het bedrijf in strijd met haar informatieplicht en het beginsel van 'fair processing'.

4.2 *Algemeen beleid AP inzake wifi-tracking*

Op 15 juni 2016 maakt de AP de eisen die de Wbp stelt aan de toepassing van wifi-trackingtechnologie algemeen bekend en waarschuwt dat het kan overgaan tot het opleggen van handhavende maatregelen. Dit gebeurt via brieven aan de Detailhandel Nederland[24] en de Vereniging Nederlandse Gemeenten en publicatie hiervan op de eigen website.[25]

4.3 *Last onder dwangsom Bluetrace*

Ondanks de maatregelen die Bluetrace naar aanleiding van het onderzoeksrapport heeft genomen (zie hierna), constateert de AP dat het bedrijf met haar werkwijze nog steeds in overtreding is met de Wbp. Op 1 september 2016 publiceert zij de last onder dwangsom waarmee zij handhavend optreedt tegen de werkwijze van Bluetrace.[26] De maatregelen die Bluetrace heeft genomen zijn deels in overeenstemming met de wensen van de AP en deels niet vergaand genoeg om de vastgestelde overtredingen

19 Bluetrace-rapport, p. 35.
20 Hof Arnhem-Leeuwarden 24 november 2014, ECLI:NL:GHARL:2014:9050 (*Medeplichtigheid aan moord op sportschoolhouder Almere*).
21 Artikel 29-werkgroep, *Advies 5/2014 over anonimiseringstechnieken*, WP 216, 10 april 2014.
22 Bluetrace-rapport, p. 33.
23 De vraag is in hoeverre de consument hier daadwerkelijk mee bereikt wordt. Zie ook: I. Westerman, 'Create with Context, We create the digital future', Workshop FTC on Mobile Device Tracking, Spring Privacy Series, 19 februari 2014 (hierna: Westerman).
24 Brief Detailhandel Nederland AP.
25 Autoriteit Persoonsgegevens, *Wifi-tracking en de Wet bescherming persoonsgegevens*, brief aan Vereniging Nederlandse Gemeenten, 15 juni 2016. Zie ook in dit kader de ontwikkeling van smart cities en de stad als 'living lab': *Stcrt.* 2016, 48889.
26 Autoriteit Persoonsgegevens, *Last onder dwangsom Bluetrace B.V.*, 1 september 2016.

van de Wbp weg te nemen. In de beoordeling in de last onder dwangsom stelt de AP wederom overtredingen vast aan de zijde van Bluetrace van artikel 8, 10 en 34 in samenhang met artikel 6 Wbp. Het bedrijf heeft zes maanden om aan de last te voldoen. Bij niet naleven van de last is Bluetrace een bedrag van € 5000 per week of een gedeelte daarvan verschuldigd met een maximum van € 100 000.

Persoonsgegevens en verantwoordelijke

In overeenstemming met hetgeen de AP in haar onderzoeksrapport heeft vastgesteld, stelt de AP vast dat Bluetrace met haar wifi-trackingactiviteiten persoonsgegevens verwerkt en dat het bedrijf (mede)verantwoordelijk is voor de gegevensverwerkingen.

Geldige grondslag

De AP oordeelt, in tegenstelling tot het eerdere rapport, dat Bluetrace een gerechtvaardigd bedrijfsbelang toekomt voor het registreren van het verplaatsingsgedrag van de *winkelbezoekers*. Het bedrijf heeft maatregelen genomen om de persoonsgegevens van winkelbezoekers te verwijderen of anonimiseren na ten hoogste 24 uur en verschaft nadere informatie over het bestaan van de mogelijkheid tot opt-out van de verwerking op haar website. Vanwege getroffen maatregelen weegt het belang van de vrijheid van ondernemerschap aan de zijde van Bluetrace zwaarder dan het belang van de winkelbezoekers bij het niet plaatsvinden van de gegevensverwerking.

Ten aanzien van de *omwonenden* stelt de AP dat het bedrijf geen gerechtvaardigd belang toekomt als grondslag voor de verwerking. Het doel is om informatie over winkelbezoekers en voorbijgangers te registreren. Daarvoor is het niet noodzakelijk dat het gedrag van omwonenden wordt geregistreerd. De verwerking is niet proportioneel en raakt aan het huisrecht van de omwonenden: in eigen woning dient men ongestoord zichzelf te kunnen zijn.

Met betrekking tot de *voorbijgangers* meent de AP dat Bluetrace in beginsel een gerechtvaardigd belang kan toekomen om de voorbijgangers- en bezoekersstromen te kunnen meten. Bluetrace heeft haar werkwijze aangepast en de metingen beperkt tot de winkelopeningstijden, beperkt tot een straal van één meter buiten de winkels en bewaart de (versleutelde) gegevens ten hoogste 24 uur. De AP stelt dat het niet noodzakelijk is om de wifi-gegevens van voorbijgangers in herleidbare vorm vast te leggen, aangezien het ook mogelijk is om alleen tellingen te verrichten (*subsidiariteit*). Voor de metingen *buiten* de winkel ontbreekt Bluetrace een toereikende verwerkingsgrondslag concludeert de AP en handelt daarmee in strijd met artikel 8 Wbp.

Bewaartermijn

Bluetrace heeft de bewaartermijn van alle gegevens verkort tot 24 uur. Dit is voor winkelbezoekers voldoende. Echter, zo stelt de AP, de gegevens van voorbijgangers dient men direct na het verzamelen op het kastje te anonimiseren of te verwijderen. Het meten van het verplaatsingsgedrag van omwonenden is sowieso niet toegestaan.

Informatieverplichting

Bluetrace heeft maatregelen genomen om het publiek van informatie te voorzien met een privacybeleid op de website en het beschikbaar maken van stickers en informatiebrochures. Deze informatie is volgens de AP deels onjuist en onvolledig. Bluetrace dient te vermelden dat zij de verantwoordelijke is voor de gegevensverwerkingen. Omdat de hashingmaatregel niet tot anonimisering van de gegevens leidt, bewaart Bluetrace gedurende maximaal 24 uur persoonsgegevens. Hierover zou het bedrijf moeten informeren en daarnaast over alle verschillende verwerkte categorieën persoonsgegevens. De omwonenden en voorbijgangers dienen ook op de hoogte te worden gebracht. Daarnaast is het vereist dat betrokkenen uiterlijk op het moment van vastlegging van de gegevens geïnformeerd worden. Bluetrace zou daartoe maatregelen moeten nemen door bijvoorbeeld het plaatsen van borden op straat voor voorbijgangers en stickers op de winkelramen voor winkelbezoekers.

5 In vergelijking: de Verenigde Staten

Het is interessant om de Bluetrace-zaak te vergelijken met een overeenkomstig geval in de Verenigde Staten waar retailtrackingaanbieder Nomi Technologies, Inc. (Nomi) door de Federal Trade Commission (FTC) is onderzocht.[27] We beperken ons hierbij tot een beschrijving van het wettelijk kader, de case-beschrijving en de uitkomsten op de punten die ook in de Bluetrace-zaak centraal stonden.

5.1 *Wettelijk kader*

De Verenigde Staten kennen geen omnibusprivacyregulering zoals in de Europese Unie, maar verschillende vormen van privacybescherming, waaronder grondwettelijke bescherming, sectorspecifieke regulering,[28] wettelijke aansprakelijkheden, staatsspecifieke reguleringen, algemene en specifieke consumentenregulering.[29] Met name wordt het leerstuk van misleidende en oneerlijke handelspraktijken toegepast op privacykwesties waar geen sectorspecifieke regulering voor is, zoals (retail)tracking. Op grond van Section 5 van de Federal Trade Commission Act (FTC-Act) zijn alle misleidende

27 FTC, *Agreement containing consent order, Nomi Technologies, Inc.*, File no. 132 3251, 23 april 2015.
28 I.S. Rubinstein e.a., *Privacy Bridges: EU and US privacy experts in search of transatlantic privacy solutions*, Amsterdam/Cambridge 2015, p. 16.
29 D.J. Solove & W. Hartzog, 'The FTC and the new common law of privacy', *Columbia Law Review* (144) 2014 (hierna: Solove & Hartzog), p. 587.

en oneerlijke handelspraktijken verboden en houdt de Federal Trade Commission (FTC) daar toezicht op.[30]

Door de gefragmenteerde regulering op het gebied van privacy en het feit dat veel bedrijven buiten de sectorspecifieke regulering vallen, is de FTC daarmee de voornaamste waker over consumentenprivacy.[31] De FTC behandelt ongeveer veertig privacyzaken per jaar.[32] In het geval van een overtreding wordt meestal een schikking bereikt tussen de FTC en het betrokken bedrijf of instelling. De schikkingen en de daartoe gemaakte afspraken worden vastgelegd in een *consent agreement*, doorgaans voor de duur van twintig jaar.[33]

5.2 *Case: Nomi*

In 2013 is de FTC een onderzoek gestart naar retailtrackingbedrijf Nomi. Het bedrijf bood retailtrackingtechnologie aan winkeliers, enerzijds door sensoren voor wifitracking te plaatsen en anderzijds door te tracken via reeds bestaande wifi access points. Het bedrijf past wifitracking toe overeenkomstig met paragraaf 2.2.

De FTC kwam in haar onderzoek tot de conclusie dat de informatie in de privacypolicy van Nomi misleidend was, omdat Nomi de beloftes maar gedeeltelijk nakwam. Op haar website had Nomi de volgende tekst geplaatst: 'Nomi pledges to (…) Always allow consumers to opt out of Nomi's service on its Web site as well as at any retailer using Nomi's technology.' De belofte in deze privacypolicy is tweeledig: het kunnen aangeven van de opt-out op de website en in de winkel. Op de website kon de consument zijn MAC-adres invoeren en hiermee de opt-outkeuze aangeven. Het MAC-adres kwam hierdoor op een blacklist te staan. De verzamelde gegevens werden vervolgens niet opgeslagen wanneer een consument een winkel bezocht met Nomi's wifi-trackingtechnologie. In tegenstelling tot de belofte had Nomi geen voorzieningen getroffen om een opt-out in de winkel mogelijk te maken. De FTC was daarbij van mening dat de tweede belofte, een opt-out-mogelijkheid in de winkel, ook een impliciete belofte inhield om de consument te informeren wanneer de winkel gebruiktmaakt van de wifi-trackingtechnologie. Deze impliciete belofte kwam Nomi niet na. Deze handelspraktijken achtte de FTC misleidend en leverde daarom een schending van Section 5 van de FTC-Act op.

Nomi en de FTC hebben de zaak geschikt en de afspraken in een *consent agreement* neergelegd. In de schikking is een verbod op misleidende informatie opgenomen en allerlei rapportering- en compliancemaatregelen.[34] Zo moet Nomi alle documenten die toezien op de naleving minimaal vijf jaar bewaren en binnen negentig dagen na de *order* (en periodiek daarna) een compliancerapport aan de FTC uitbrengen.

5.3 *Toepassing centrale aspecten uit de Bluetrace-zaak*

Persoonsgegevens

In de Verenigde Staten speelt het begrip 'persoonsgegevens' een andere rol dan in Nederland. Ondanks dat 'personal identifiable information' een voorwaarde kan zijn voor de toepassing van wetgeving in de Verenigde Staten,[35] vormt het leerstuk van misleidende en oneerlijke handelspraktijken in de Nomi-zaak het wettelijk kader en daarvoor is alleen het consumentenperspectief van belang en niet of er persoonsgegevens in het geding zijn.

De FTC meent dat Nomi's wifi-trackingdienst bestaat uit het verzamelen en verwerken van locatiegegevens van consumenten. De FTC stelt vast dat er vijf soorten gegevens door Nomi worden verzameld: het MAC-adres, de signaalsterkte, de maker van het apparaat (af te leiden van het MAC-adres), de locatie van de sensor en de datum en tijd van de meting. Nomi hasht het MAC-adres voordat zij deze opslaat op de server. De FTC is van mening dat de gehashte waarde een uniek identificatiemiddel blijft.[36] Deze analyse heeft echter niet tot resultaat dat er andere regels op de gegevensverwerking van toepassing zijn. De herleidbaarheid van de gegevens tot een individu speelt als zodanig geen rol.

Verantwoordelijke

Nomi is de retailtrackingaanbieder die de diensten aanbiedt, de gegevens verzamelt, de gegevens analyseert en tot geaggregeerde rapporten verwerkt. Nomi geldt daardoor als de verantwoordelijke voor wat betreft te onderzoeken gedrag.

Geldige grondslag

Een geldige grondslag voor de gegevensverwerking is geen vereiste met betrekking tot de toelaatbaarheid hiervan in de Verenigde Staten.[37] De verwerking van persoonsgegevens is in beginsel toegestaan, tenzij dit wordt verboden door een specifieke wet. Amerikaanse regulering waarbij privacy-aspecten in het geding zijn legt de focus op *consumer harm* en de juiste balans vinden tussen privacy en efficiënte commerciële transacties.[38] De winkelier en retailtrackingaanbieder hebben een le-

30 Section 5 FTC-Act - 15 U.S. Code § 45.
31 Solove & Hartzog, p. 588.
32 FTC, *Privacy & Security update 2015*, p. 2.
33 C.J. Hoofnagle, *Federal Trade Commission, Privacy Law and Policy*, New York: Cambridge University Press 2016, p. 167.
34 FTC, *Decision and Order, Nomi Technologies, Inc.*, File no. 132 3251, 3 september 2015.
35 P.M. Schwartz & D.J. Solove, 'Reconciling Personal Information in the United States and European Union', 102 *California Law Review* 877 (2014), UC Berkeley Public Law Research Paper No. 2271442, GWU Legal Studies Research Paper No. 2013-77, GWU Law School Public Law Research Paper No. 2013-77 (hierna: Schwartz & Solove), p. 887-891.
36 FTC, *Nomi Technologies, Inc.; Analysis of Proposed Consent Order to Aid Public Comment*, File no. 132 3251, Federal Register, Vol. 80, No. 84, 1 mei 2015, Notices, p. 24925.
37 P.M. Schwartz, *Preemption and Privacy*, 118 *Yale Law Journal* 902, 913 (2009).
38 Schwartz & Solove, p. 877.

gitiem bedrijfsbelang voor wifi-tracking om hiermee bedrijfsinzichten te verwerven en bijvoorbeeld winkelindeling te verbeteren en wachtrijen te verkorten.[39] De FTC erkent dat er privacyrisico's zijn, maar maakt geen afweging tussen de belangen van beide partijen in haar beoordeling. De FTC bevestigt in de Nomi-zaak dat het verzamelen van informatie door Nomi is toegestaan en derhalve geen grondslag vereist is voor (retail)tracking. De FTC voegt daaraan toe dat het feit dat wifi-tracking is toegestaan niet betekent dat de consument mag worden misleid over wifi-tracking.[40]

Bewaartermijn

Er zijn geen juridische vereisten met betrekking tot de bewaartermijn van de verzamelde gegevens. De FTC benadrukt in de *consent agreement* met Nomi alleen dat het hashen van de gegevens niet wegneemt dat er unieke identificatiemiddelen worden opgeslagen.

Informatieverplichtingen

Uit de Nomi-zaak blijkt dat het als zodanig niet verplicht is om de consument te informeren over de gegevensverwerking, maar dat het wel noodzakelijk is dat de verstrekte informatie daaromtrent correct is.

6 Analyse en knelpunten

Hiervoor is besproken dat winkeliers consumentengedrag in toenemende mate in de gaten houden. Wifi-tracking is daar een belangrijke technologie voor. Uit Nederlands en Amerikaans perspectief is gekeken naar de juridische toelaatbaarheid van wifi-tracking aan de hand van twee cases van de nationale privacytoezichthouders: Bluetrace en Nomi. Vijf privacygerelateerde aspecten zijn daarbij nader uitgewerkt. Hieronder zullen deze aspecten nader worden geanalyseerd. Tot slot worden enkele knelpunten geformuleerd met betrekking tot de transparantie van de gegevensverwerkingen en de mogelijkheid tot opt-out.

Persoonsgegevens

Alhoewel de FTC de gegevens niet als persoonsgegevens als zodanig kwalificeert, bestempelen beide toezichthouders de verzamelde gegevens als gegevens herleidbaar tot het individu. Zowel in Nederland en in de Verenigde Staten is kritiek geleverd op dit standpunt. Zo is Zwenne de mening toegedaan dat de Wbp niet van toepassing is op wifi-tracking. Naar zijn mening is het begrip 'identificatie' opgerekt en is er geen sprake van persoonsgegevens.[41] Hij stelde het een en ander ook al in zijn inaugurele rede.[42] In een dissenting opinion, schrijft FTC Commissioner Ohlhausen dat Nomi geen *personally identifiable information* verzamelt en de eveneens dissenting Commissioner Wright stelt dat Nomi's technologie geen personen identificeert.[43]

Gelet op de aard van de gemeten gegevens, MAC-adres in combinatie met locatiegegevens, maken beide toezichthouders zich zorgen om de privacy van de consument. Zij achten het hashen van de gegevens geen maatregel voor anonimisering en dus geen maatregel waardoor de herleidbaarheid wordt weggenomen. De AP voegt daaraan toe dat hashen eerder een beveiligingsmaatregel is tegen inbreuken van derden.

Verantwoordelijke

Gelet op de ingestelde onderzoeken naar de wifi-trackingaanbieders en de opgelegde sancties zijn in beide landen de bedrijven als verantwoordelijke voor de verzameling en analyse van de gegevens aan te merken. Van Canneyt meent dat het ook goed mogelijk is dat de wifi-trackingaanbieder bewerker is in plaats van verantwoordelijke.[44]

Grondslag

In beide landen wordt erkend dat winkeliers een legitiem belang kunnen hebben om consumentengedrag te observeren. In Nederland maakt dit belang deel uit van de vrijheid van ondernemerschap en kan dit belang zwaarder wegen dan het belang op de bescherming van de persoonlijke levenssfeer van de consument zolang er voldoende waarborgen zijn geïmplementeerd. Onder het Amerikaanse systeem is geen grondslag vereist voor de verwerking en is misleiding of *consumer harm* eerder de grens voor de toelaatbaarheid van de verwerking. De *consent agreement* van de FTC beargumenteert dat de valse belofte tot opt-out in de winkel en impliciete belofte tot informatie de consument schaadt. Commissarissen Ohlhausen en Wright richten zich tegen dit argument van de rest van de commissie en stellen dat er geen sprake is van *consumer harm*. Wright betoogt dat de *consent order* juist *consumer harm* tot gevolg heeft, omdat het bedrijven zou afschrikken om vrijwillig een opt-out aan te bieden of transparant te zijn. Commissioner Brill, die deel uitmaakt van de meerderheid, brengt tegen deze argumenten in dat de *order* bedrijven juist de prikkel geeft om periodiek de privacypolicy te herzien en na te leven.[45]

---

39 FTC, *Nomi Technologies, Inc.; Analysis of Proposed Consent Order to Aid Public Comment*, File no. 132 3251, Federal Register, Vol. 80, No. 84, 1 mei 2015, Notices, p. 24925.

40 D.S. Clark, FTC, *Letter to commenter: The Information Technology & Innovation Foundation*, File no. 132 3251, Nomi Technologies, Inc., 28 augustus 2015.

41 'CBP beperkt wifi-tracking', *De Telegraaf* 1 december 2010.

42 G.J. Zwenne, *De verwaterde privacywet* (oratie Leiden), 2013, zwenneblog.weblog.leidenuniv.nl/files/2013/09/G-J.-Zwenne-De-verwaterde-privacywet-oratie-Leiden-12-apri-2013-NED.pdf.

43 FTC, *Dissenting Statement of Commissioner Ohlhausen, in the matter of Nomi Technologies, Inc.*, 28 augustus 2015; FTC, *Dissenting Statement of Commissioner Wright, in the matter of Nomi Technologies, Inc.*, 23 april 2015.

44 T. Van Canneyt, 'Big brother in de winkel? – wifi-tracking en de verwerking van persoonsgegevens', *Computerrecht* 2016/125, p. 211-219 (hierna: Van Canneyt), p. 214.

45 FTC, *Statement of Commissioner Brill, in the matter of Nomi Technologies, Inc.*, Matter no. 1233251, 28 augustus 2015.

Bewaartermijn

In tegenstelling tot de Verenigde Staten waar de bewaartermijn van gegevens niet is gelimiteerd, dienen in Nederland strikte bewaartermijnen in acht te worden genomen van ten hoogste 24 uur. Gegevens van voorbijgangers moeten direct onomkeerbaar worden geanonimiseerd of verwijderd en omwonenden mogen niet worden gevolgd.

Informatieverplichting

Onder de Wbp zijn verantwoordelijken voor wifi-tracking verplicht om de consument van gedetailleerde informatie te voorzien en benadrukt de AP dat transparantie de hoofdverplichting van de verantwoordelijke is. Hoewel in de Verenigde Staten geen wettelijke plicht tot informeren bestaat, is de les die uit Nomi getrokken kan worden dat bedrijven hun privacypolicy periodiek dienen te herzien en zorg dienen te dragen dat de beloftes worden nagekomen.

Knelpunten

Retailmarketing via wifi-tracking is een groeiend fenomeen, dat inmiddels ook de aandacht van toezichthouders heeft getrokken. Hiervoor zijn de ontwikkelingen in Nederland en in de Verenigde Staten besproken en geanalyseerd. Duidelijk wordt dat er ten minste twee knelpunten, transparantie en het bieden van een opt-out, zijn die verdere aandacht behoeven.

Transparantie

Het wringt dat er ten aanzien van wifi-tracking een gebrek is aan afdoende transparantie. Het transparantiebeginsel, uitgewerkt tot de plicht tot informatieverstrekking in de Wbp, heeft tot doel om de verwerkingen van de verantwoordelijke kenbaar te maken zodat de betrokkene in staat is om de verantwoordelijke in rechte aan te spreken.[46] Op dit moment heeft de consument geen idee door wie, op welke locaties, wanneer en met welk doel zijn verplaatsingsgedrag wordt gemeten. Het AP-rapport en de last onder dwangsom hebben, samen met het algemeen beleid middels haar brieven aan de Detailhandel Nederland en Vereniging Nederlandse Gemeenten, tot doel om te zorgen dat de verantwoordelijken hun kernverplichting tot het bieden van transparantie naleven. Ondanks dat transparantie de inbreuk niet wegneemt, en de consument doorgaans niet bewust let op informatietekens in een winkel en op straat,[47] is het van belang dat er inzicht is in de gegevensverwerking als zodanig. De consument krijgt hierdoor in ieder geval de kans om zijn rechten te kunnen uitoefenen, verantwoordelijken op hun plichten te wijzen of zijn gedrag aan te passen. Dat in beginsel deze informatie onder de Wbp opvraagbaar is, doet aan een en ander niet af.

Opt-out

Uit beide cases blijkt dat een opt-outkeuze aanbieden niet verplicht is. Van Canneyt suggereert dat het onder de Europese wetgeving mogelijk zou zijn dit verplicht te stellen door artikel 5 lid 3 e-Privacyrichtlijn, geïmplementeerd in artikel 11.7a Nederlandse Telecommunicatiewet (Tw), toe te passen op wifi-tracking in het kader van *device fingerprinting*.[48] Deze technische methode, *device fingerprinting*, is het combineren van een aantal (niet-unieke) informatie-elementen om een unieke 'vingerafdruk' te maken van een apparaat om hiermee dit apparaat op langere termijn te kunnen volgen en analyseren.[49] Het is echter de vraag of artikel 11.7a Tw wel van toepassing is. Het betreft de zogenaamde 'cookie-bepaling', die stelt dat voor het plaatsen en uitlezen van informatie op een randapparaat voorafgaande toestemming is vereist. Echter, de bepaling richt zich tot aanbieders van een telecommunicatienetwerk en het is de vraag of daar bij wifi-tracking sprake van is. Daar komt bij dat gelet op overweging 24 preambule en de tekst van artikel 5 lid 3 e-Privacyrichtlijn, het evenmin zeker is of een opt-out hierop te baseren valt. Volgens de preambule beoogt het artikel het apparaat en de inhoud hiervan te beschermen tegen onbevoegde toegang[50] en benadrukt artikel 5 lid 3 e-Privacyrichtlijn dat de bepaling het 'opslaan van of toegang krijgen tot de informatie in de randapparatuur' betreft. Wifi-trackingtechnologie registreert de wifi-signalen die het apparaat automatisch uitzendt waardoor er geen toegang wordt verkregen ('access to') tot informatie op de telefoon. Daarnaast maakt wifi-tracking slechts gebruik van één apparaatgegeven: het unieke MAC-adres, terwijl voor *device fingerprinting* een profiel wordt opgesteld van een combinatie van (niet-unieke) apparaatgegevens.

Los van de vraag of er al dan niet een afdoende wettelijke grondslag is voor een opt-outregime, blijft de vraag of het aan de consument moet worden gelaten om een actieve handeling te verrichten om zich te onttrekken aan wifi-tracking door het aangeven van een opt-out of het uitschakelen van zijn apparaten. In toenemende mate maakt de consument gebruik van apparaten die wifi- of bluetoothsignalen afgeven die geregistreerd kunnen worden. Wanneer winkeliers, maar ook gemeentes in het kader van *smart cities*, in toenemende mate deze signalen registreren en daardoor het verplaatsingsgedrag van de consument, is het wellicht niet wenselijk om deze verantwoordelijkheid geheel bij de consument neer te leggen. Zoals ook de AP stelde, dient men zich onbespied te wanen in de openbare ruimte, daarvoor is het continu uit- en aanzetten van de telefoon of functionaliteiten een onevenredige inspanning.

---

46 *Kamerstukken II* 1997/98, 25892, 3 (MvT bij artikel 33 en 34).
47 Westerman.
48 Van Canneyt, p. 216.
49 Artikel 29-werkgroep, *Advies 9/2014 over device fingerprinting*, WP 224, 25 november 2014, p. 4.
50 J. van Hoboken & F.J. Zuiderveen Borgesius, 'Scoping Electronic Communications Privacy Rules: Data, Services and Values', *JIPITEC* 2015, 3, p. 198-230, p. 202.

Conclusie

Een duidelijke juridische kwalificatie van een nieuwe technologie draagt bij aan de beperking van de risico's. De Nederlandse en Amerikaanse toezichthouders zijn het eens: wifi-tracking in de winkel(straat) levert privacyrisico's op. Maar retailtrackingaanbieders en winkeliers hebben eveneens een bedrijfsbelang om wifi-tracking toe te passen. De vraag of wifi-tracking is toegestaan wordt in Nederland en de Verenigde Staten anders benaderd, maar het antwoord is in essentie hetzelfde: wifi-tracking is (onder voorwaarden) toegestaan.

In Nederland wordt het fundamentele recht op de vrijheid van ondernemerschap aan de zijde van de retailtrackingaanbieder en winkelier afgewogen tegen het recht op de persoonlijke levenssfeer en het recht op bescherming van persoonsgegevens van winkelbezoekers. In de Verenigde Staten wordt vanuit een consumentenperspectief gekeken of er sprake is van een misleidende of oneerlijke handelspraktijk. Beide toezichthouders concluderen dat wifi-tracking in beginsel toegestaan kan zijn onder de toepasselijke regelgeving. In de Verenigde Staten mag er geen sprake zijn van misleiding of *consumer harm* en concludeert de FTC in de Nomi-zaak dat opgelet dient te worden dat de privacypolicy correcte informatie bevat en regelmatig wordt herzien.

In Nederland dienen retailtrackingaanbieders en winkeliers aan striktere wettelijke vereisten te voldoen. Uit de Bluetrace-zaak blijkt dat het registreren van het verplaatsingsgedrag van omwonenden niet is toegestaan. Van voorbijgangers is slechts het tellen toegestaan en mogen dus geen herleidbare gegevens worden vastgelegd. Winkelbezoekers dienen voordat het verplaatsingsgedrag wordt geregistreerd volledig en juist geïnformeerd te zijn. Daarbij dienen de metingen beperkt te zijn tot hetgeen strikt noodzakelijk is (bijvoorbeeld openingstijden van de winkel) en mogen de gegevens ten hoogste 24 uur in herleidbare vorm worden vastgelegd.

Deze juridische kwalificatie van wifi-tracking geeft de marktpartijen en consumenten duidelijkheid omtrent de eisen die de wet stelt en de grenzen waarbinnen bewogen kan worden. Toch zorgt het gebrek aan transparantie op dit moment ook nog voor onduidelijkheid. De consument heeft geen inzicht in de toepassing van wifi-trackingtechnologie en wordt momenteel verhinderd om enige controle te kunnen uitoefenen over de metingen van zijn verplaatsingsgedrag. Gelet op de aankondiging van de Autoriteit Persoonsgegevens om te gaan handhaven en de opgelegde dwangsom aan Bluetrace, zijn de winkeliers en technologieaanbieders gewaarschuwd om hun wettelijke verplichtingen na te komen, waaronder hun kernverplichting tot transparantie.