M. Poulus[1]

Wifi-tracking: de cookie is op

Computerrecht 2018/112

Het volgen van mensen via wifi-tracking vindt anno nu op grote schaal plaats. Op het gebruik van wifi-tracking is vaak de Algemene verordening gegevensbescherming van toepassing. Deze bijdrage onderzoekt of ook de 'cookieregels' uit de e-Privacyrichtlijn (in Nederland geïmplementeerd in art. 11.7a Telecommunicatiewet) op wifi-tracking van toepassing kunnen zijn. Wanneer de cookieregels van toepassing zijn, heeft dit grote gevolgen; het maakt wifi-tracking vrijwel onmogelijk. Ook bespreekt dit artikel de regels voor wifi-tracking uit het voorstel voor de e-Privacyverordening. Tot slot behandelt deze bijdrage de vraag of toepasbaarheid van huidige en toekomstige e-Privacyregels op wifi-tracking wenselijk is.

1. Inleiding

Het vermogen te weten waar de ander is, behoort tot de diepste verlangens van de mens. Ook voor organisaties en overheden zijn locatiegegevens van personen interessant; weten waar iemand zich bevindt, hoe hij zich beweegt en hoe vaak hij op een bepaalde plek terugkomt, levert waardevolle informatie op. Het grootschalige gebruik van mobiele apparatuur, zoals met name smartphones, zorgt ervoor dat de locatie van personen via verschillende technologieën in kaart kan worden gebracht. Mensen dragen hun smartphone dag en nacht bij zich en lenen dit apparaat bijna nooit uit.[2] De locatie van een smartphone – en dus van een persoon – kan onder andere worden bepaald aan de hand van gps-technologie, informatie ontvangen via zendmasten en door het opvangen van wifi- en bluetooth-signalen.[3]

Moderne mobiele apparatuur beschikt vaak over zowel wifi- als bluetooth-functionaliteiten om verbinding te kunnen maken met een router, of andere randapparatuur. Veel mensen zijn zich er niet van bewust dat unieke identificatie- en locatiegegevens van hun mobiele apparatuur, wanneer de wifi- en/of bluetooth-functionaliteit van de apparatuur aan staat, meerdere keren per dag en door verschillende partijen worden opgevangen, verwerkt en geanalyseerd. Scanners in winkels, langs wegen, op stations en vliegvelden vangen door middel van wifi- en bluetooth-tracking-technologie unieke gegevens op van mobiele apparatuur die zich binnen het bereik van de meetapparatuur bevindt.[4]

Wanneer bij de toepassing van wifi-tracking persoonsgegevens worden verwerkt is in Nederland de Algemene verordening gegevensbescherming (AVG),[5] voorheen de Wet bescherming persoonsgegevens (Wbp),[6] op de verwerking van toepassing.

In de praktijk en literatuur bestaat onduidelijkheid en discussie over de vraag of de 'cookiebepaling', zoals neergelegd in art. 5 lid 3 e-Privacyrichtlijn[7] en in Nederland geïmplementeerd in art. 11.7a Telecommunicatiewet (Tw), naast de regels uit de AVG op wifi-tracking van toepassing kan zijn.

Als art. 11.7a Tw op wifi-tracking van toepassing kan zijn, brengt dit voor de praktijk grote gevolgen met zich mee, nu art. 11.7a lid 1 Tw voorschrijft dat het verkrijgen van toegang tot informatie die is opgeslagen op de randapparatuur van een gebruiker, slechts is toegestaan nadat aan twee cumulatieve voorwaarden is voldaan. De gebruiker van de randapparatuur dient, (sub a) voordat toegang wordt verkregen tot de informatie, volledig en duidelijk te zijn geïnformeerd en (sub b) hij moet voorafgaande toestemming hebben verleend. In de praktijk vindt wifi-tracking, voor zover mij bekend, uitsluitend plaats zonder dat gebruikers hiervoor toestemming verlenen. Daarnaast is het, gelet op de wijze waarop wifi-tracking in de praktijk wordt toegepast, nog maar de vraag of (voorafgaande) toestemming überhaupt kan worden verleend.

De vraag of art. 11.7a Tw van toepassing kan zijn op wifi-tracking blijft relevant totdat de toekomstige e-Privacyverordening van toepassing wordt, die de e-Privacyrichtlijn zal gaan vervangen. Zodra de e-Privacyverordening van toepassing wordt, zal art. 11.7a Tw worden ingetrokken.

Op 10 januari 2017 heeft de Europese Commissie (Commissie) het voorstel voor de e-Privacyverordening gepubli-

1 Mr. Martijn Poulus is advocaat bij Ploum. Dit artikel is een bewerking van de scriptie die de auteur schreef ter afronding van de master Informatierecht aan de Universiteit van Amsterdam. De auteur dankt dr. Frederik Zuiderveen Borgesius voor zijn waardevolle commentaar.

2 Artikel 29-werkgroep, *Opinion 13/2011 on Geolocation services on smart mobile devices*, WP 185, 16 mei 2011 (hierna: WP29 Geolocation smart mobile devices 13/2011), p. 7.

3 E. Valgaeren & L. Leitner, 'Smartphones en privacy – Vrienden, vijanden of ergens tussenin?', *Computerrecht* 2012/2, afl. 1, p. 2-9.

4 Omwille van de leesbaarheid is ervoor gekozen in deze bijdrage in veel gevallen 'wifi' te schrijven waar wifi en bluetooth kan worden gelezen. De technologische eigenschappen van wifi- en bluetooth-tracking zijn zeer vergelijkbaar.

5 Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

6 Autoriteit Persoonsgegevens, *Wifi-tracking van mobiele apparaten in en rond winkels door Bluetrace*, Rapport definitieve bevindingen, 13 oktober 2015 (hierna: Bluetrace-rapport), p. 28.

7 Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), laatstelijk gewijzigd door Richtlijn 2009/136/EG.

ceerd.[8] De e-Privacyverordening bevat nieuwe regels die, naast de regels uit de AVG, expliciet op wifi-tracking van toepassing zullen zijn.[9] De Commissie burgerlijke vrijheden, justitie en binnenlandse zaken (LIBE-commissie) van het Europees Parlement (EP), presenteerde op 23 oktober 2017 een geamendeerde versie van de e-Privacyverordening.[10] Op 26 oktober 2017 stemde het EP in met het door de LIBE-commissie geamendeerde voorstel. Het was de bedoeling van de Commissie dat de e-Privacyverordening tegelijk met de AVG op 25 mei 2018 van toepassing zou worden.[11] Dit streven is niet gehaald. Op het moment van afronding van deze bijdrage dient de Raad van de Europese Unie (Raad) zijn standpunt over de e-Privacyverordening nog in te nemen en moeten de triloogonderhandelingen over de verordening nog beginnen.[12]

Na een introductie van wifi-trackingtechnologie (2) bespreek ik hierna (3) of de cookiebepaling, zoals neergelegd in art. 5 lid 3 e-Privacyrichtlijn en in Nederland geïmplementeerd in art. 11.7a Tw, op wifi-tracking van toepassing kan zijn. Kort gezegd, denk ik dat dit het geval is. Vervolgens (4) sta ik stil bij de vraag welke gevolgen toepasbaarheid van de cookiebepaling heeft op wifi-tracking in de praktijk. Deze gevolgen zijn groot en maken wifi-tracking in de praktijk moeilijk uitvoerbaar. Daarna (5) bespreek ik het toekomstige art. 8 lid 2 e-Privacyverordening, waarvan duidelijk is dat het artikel expliciet op wifi-tracking van toepassing zal zijn en vergelijk ik de bepaling met art. 5 lid 3 e-Privacyrichtlijn en art. 11.7a Tw. Het toekomstige regime lijkt minder streng te zijn dan het huidige. Tot slot (6) sta ik stil bij de vraag of toepasbaarheid van huidige en toekomstige e-Privacyregels op wifi-tracking wenselijk is. Ondanks dat toepasbaarheid van e-Privacyregels de uitvoering van wifi-tracking in de praktijk lastig maakt, denk ik dat toepasbaarheid, gelet op de grote privacyrisico's waaraan gebruikers worden blootgesteld, wenselijk is. Ik sluit af met een conclusie (7).

2. Wifi-trackingtechnologie

Mobiele apparatuur, zoals smartphones en tablets, zijn voorzien van verschillende antennes waarmee de apparatuur verbinding kan maken met andere apparatuur, zoals routers, carkits, autoradio's en smartwatches. Een smartphone bevat vaak zowel een wifi- als een bluetooth-antenne. Deze antennes sturen met kleine tussenpozen via radiofrequenties een signaal (*probe request*) met daarin het Media Access Control (MAC)-adres van de antenne de lucht in. Dit MAC-adres is een uniek identificatienummer, dat door de fabrikant van de apparatuur aan de antenne is toegekend. Een MAC-adres wordt in hexadecimale vorm aangeduid en ziet er bijvoorbeeld als volgt uit: 00:C0:CA:8D:9B:62. De eerste zes karakters van een MAC-adres identificeren de fabrikant van de antenne.[13] De laatste zes karakters zijn uniek voor ieder apparaat.

Door het opvangen van het MAC-adres, in combinatie met registratie van de signaalsterkte, locatie en het tijdstip van de waarneming, is het mogelijk om zeer nauwkeurig te bepalen waar en op welk moment een bepaald apparaat (en dus zijn eigenaar) zich bevindt.[14] Wifi-tracking kan op een actieve en passieve wijze worden toegepast. Bij actieve wifi-tracking wordt toegang verkregen tot het MAC-adres wanneer de apparatuur van een gebruiker verbinding maakt met een wifi-netwerk, zoals een wifi-hotspot. Bij passieve wifi-tracking wordt geen verbinding gemaakt met de randapparatuur die het signaal uitzendt, zoals de smartphone of de tablet. De scanapparatuur vangt – op passieve wijze – signalen op, die het MAC-adres van de apparatuur bevatten. De gebruiker merkt hier niets van. Ook de apparatuur van de gebruiker registreert niet wanneer informatie wordt opgevangen, die de antenne van de randapparatuur van de gebruiker uitzendt. Deze bijdrage beperkt zich tot een bespreking van deze passieve vorm van wifi-tracking.

Wifi-tracking wordt in de praktijk voor verschillende doeleinden toegepast. In de retailsector wordt wifi-tracking ingezet om winkelbezoekers te tellen, te bepalen hoelang winkelbezoekers zich op een bepaalde plek (bijvoorbeeld voor een schap) bevinden en om loopstromen in winkels of winkelstraten in kaart te brengen.[15] In het kader van verkeersonderzoek wordt wifi-tracking toegepast om te bepalen hoelang auto's erover doen om van punt A naar B te komen.[16] Op basis van deze informatie kan *real time* verkeersinformatie worden gegenereerd. Ook op vliegvelden, waaronder in Nederland,[17] wordt wifi-tracking toegepast. Zo wordt bijvoorbeeld onderzocht hoelang reizigers erover doen om door de veiligheids- en paspoortcontrole van een luchthaven te komen.[18] Daarnaast wordt wifi-tracking ook voor niet-commerciële doeleinden gebruikt, bijvoorbeeld door studenten[19] en voor hobbyprojecten. Zo paste een Franse hobbyist wifi-tracking toe om een meetsysteem te

8 Voorstel voor een verordening van het Europees Parlement en de Raad met betrekking tot de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie, en tot intrekking van Richtlijn 2002/58/EG, COM(2017)10 def. (hierna: Commissievoorstel EPV).

9 Zie art. 8 lid 2 en overweging 25 Commissievoorstel EPV.

10 Europees Parlement, Verslag over het voorstel voor een verordening van het Europees Parlement en de Raad met betrekking tot de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie, en tot intrekking van Richtlijn 2002/58/EG, A8-0324/2017 (hierna: LIBE-rapport EPV).

11 Art. 27 lid 1 Commissievoorstel EPV. Het EP heeft de datum 25 mei 2018 uit het voorstel voor de e-Privacyverordening verwijderd. Zie art. 27 lid 1 (Amendement 166) LIBE-rapport EPV.

12 Zie over de onrealistische tijdsplanning van de e-Privacyverordening H.W. Roerdink, 'Over the top: Het voorstel voor de Europese e-Privacyverordening', *IR* 2017, afl. 5/6 (hierna: Roerdink, *IR* 2017), p. 192.

13 Zie voor een overzicht van deze fabrikanten en de bijbehorende eerste zes karakters http://standards-oui.ieee.org/oui.txt.

14 WP29 Geolocation smart mobile devices 13/2011, p. 5-7.

15 Zie over retailtracking J. Turow, *The Aisles Have Eyes*, New Haven: Yale University Press 2017. Zie ook W. Raas e.a., 'Het veranderende retail landschap: De opkomst van nieuwe technologieën', *WR* 2017/177, afl. 2, p. 53-55.

16 M. Hijink, 'Duizenden scanners langs de weg leggen onze gegevens vast', *NRC* 26 april 2015 (hierna: Hijink, *NRC* 2015).

17 J-H. Hoepman, 'Ongezien over de Wallen', *FD* 23 juni 2017.

18 C. Negroni, 'Tracking Your Wi-Fi Trail', *The New York Times* 21 maart 2011.

19 Zie bijvoorbeeld M. Nadeem, 'How we tracked and analyzed over 200,000 people's footsteps at MIT', 9 juli 2017, https://goo.gl/H8Fi12.

creëren, dat hem waarschuwt wanneer een parkeerwachter zich in de buurt van zijn auto bevindt. Net als een smartphone stuurt ook de apparatuur waarmee Franse parkeerwachters parkeerboetes uitdelen (wanneer de wifi-functionaliteit van deze apparatuur aan staat) signalen uit, die het MAC-adres van de apparatuur bevatten.[20]

In reactie op wifi-tracking hebben verschillende fabrikanten van smartphones mogelijkheden voor randomisatie van MAC-adressen ontwikkeld. Deze maatregelen tegen wifi-tracking blijken echter niet effectief te zijn.[21]

3. Mogelijke toepasbaarheid huidige e-Privacyregels op wifi-tracking

Hierna bespreek ik of art. 5 lid 3 e-Privacyrichtlijn en art. 11.7a Tw op wifi-tracking van toepassing kunnen zijn. Ter beantwoording van deze vraag sta ik stil bij de ratio en totstandkomingsgeschiedenis van de cookiebepaling. Daarnaast toets ik wifi-tracking aan een relevante uitzondering op de cookiebepaling. Ook bespreek ik of wifi-tracking een vorm van 'device fingerprinting' kan zijn, waarop art. 5 lid 3 e-Privacyrichtlijn mogelijk van toepassing is.

3.1 *Artikel 5 lid 3 e-Privacyrichtlijn*

Art. 11.7a Tw is een implementatie van art. 5 lid 3 e-Privacyrichtlijn. De e-Privacyrichtlijn is in 2002 in werking getreden, als opvolger van de ISDN-richtlijn.[22] De e-Privacyrichtlijn is één van de basisrichtlijnen over privacy en gegevensbescherming in de Europese Unie. Het voornaamste doel van de e-Privacyrichtlijn is het garanderen van een hoge mate van privacy bij de communicatie via openbare communicatienetwerken, ongeacht welke technologie daarbij wordt gebruikt.[23]

Art. 5 lid 3 e-Privacyrichtlijn was niet opgenomen in het oorspronkelijke voorstel van de Commissie voor de e-Privacyrichtlijn,[24] maar werd geïntroduceerd in een amendement van het EP[25] en later aangepast door de Raad.[26] De bepaling werd in 2009 gewijzigd door de Richtlijn Burgerrechten.[27]

In de op dit moment geldende variant[28] ziet art. 5 lid 3 e-Privacyrichtlijn er als volgt uit:

> "De lidstaten dragen ervoor zorg dat de opslag van informatie of het verkrijgen van toegang tot informatie die reeds is opgeslagen in de eindapparatuur van een abonnee of gebruiker, alleen is toegestaan op voorwaarde dat de betrokken abonnee of gebruiker toestemming heeft verleend, na te zijn voorzien van duidelijke en volledige informatie overeenkomstig [de Privacyrichtlijn][29] (lees sinds 25 mei 2018: de AVG),[30] onder meer over de doeleinden van de verwerking. Zulks vormt geen beletsel voor enige vorm van technische opslag of toegang met als uitsluitend doel de uitvoering van de verzending van een communicatie over een elektronisch communicatienetwerk, of, indien strikt noodzakelijk, om ervoor te zorgen dat de aanbieder van een uitdrukkelijk door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij deze dienst levert."

Art. 5 lid 3 e-Privacyrichtlijn is onderdeel van art. 5 e-Privacyrichtlijn, dat 'Vertrouwelijk karakter van de communicatie' als titel heeft. Het eerste lid van art. 5 e-Privacyrichtlijn beoogt communicatie en de daarmee verband houdende verkeersgegevens te beschermen. Art. 5 lid 3 e-Privacyrichtlijn wordt in de literatuur aangeduid als een

20 J. Saint-Clair, 'WIFI tracker (aka avoid electronic ticketing for unpaid parking fees)', https://goo.gl/7g5U7u.

21 J. Martin e.a., 'A Study of MAC Address Randomization in Mobile Devices and When it Fails', *Proceedings on Privacy Enhancing Technologies* (4) 2017, afl. 4, p. 268-286. Zie ook S. van Voorst, 'Maatregels telefoonfabrikanten tegen tracking via mac-adres schieten tekort', *Tweakers* 10 maart 2017.

22 Richtlijn 97/66/EG van het Europees Parlement en de Raad van 15 december 1997 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector. Zie over de wijzigingen van de e-Privacyrichtlijn ten opzichte van de ISDN-richtlijn W.A.M. Steenbruggen, 'Herziening hoofdstuk 11 Tw: tijd voor een heroverweging?', *Computerrecht* 2003, afl. 1, p. 27-37.

23 Overweging 4 e-Privacyrichtlijn.

24 Voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, COM(2000)385 def.

25 Europees Parlement, Tweede verslag over het voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, A5-0374/2001 (hierna: LIBE-rapport EPR) (Amendement 26), p. 22.

26 Raad van de Europese Unie, Gemeenschappelijk Standpunt (EG) nr. 26/2002 van 28 januari 2002, vastgesteld door de Raad, volgens de procedure van artikel 251 van het Verdrag tot oprichting van de Europese Gemeenschap, met het oog op de aanneming van een richtlijn van het Europees Parlement en de Raad betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (2002/C 113 E/03).

27 Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische communicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming.

28 Zie over de totstandkomingsgeschiedenis en achtergrond van art. 5 lid 3 e-Privacyrichtlijn E. Kosta, 'Peeking into the Cookie Jar: The European Approach Towards the Regulation of Cookies', *International Journal of Law and Information Technology* (21) 2013 (hierna: Kosta, *Int'l JL & Info Tech* 2013), p. 380-406.

29 Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

30 Sinds de AVG van toepassing is gelden alle verwijzingen in de e-Privacyrichtlijn naar de Privacyrichtlijn als verwijzingen naar de AVG. Zie art. 94 lid 2 AVG. Zie ook Artikel 29-werkgroep, *Guidelines on Consent under Regulation 2016/679*, WP 259 rev. 01, 28 november 2017, zoals laatst aangepast en aangenomen op 10 april 2018 (hierna: WP29 Consent under the GDPR), p. 4.

'vooruitgeschoven verdedigingslinie' met betrekking tot het communicatiegeheim van art. 5 lid 1 e-Privacyrichtlijn.[31] De ratio van art. 5 lid 3 e-Privacyrichtlijn is gelegen in het idee dat de informatie op de apparatuur van een gebruiker, zoals een computer of smartphone, deel uitmaakt van de persoonlijke levenssfeer van de gebruiker.[32] Het begrip 'informatie' is niet gedefinieerd in de e-Privacyrichtlijn. Duidelijk is echter, dat deze informatie geen persoonsgegevens hoeft te betreffen.[33]

Al sinds de introductie van de e-Privacyrichtlijn is onduidelijk op welke technologieën art. 5 lid 3 e-Privacyrichtlijn – naast cookies – van toepassing is. De reden dat de reikwijdte van het artikel niet expliciet in de richtlijn is gespecificeerd, is gelegen in de wens om de bepaling zo techniekneutraal mogelijk te formuleren.[34] De considerans van de e-Privacyrichtlijn noemt, naast cookies, als voorbeelden van technologieën waarop art. 5 lid 3 e-Privacyrichtlijn van toepassing is: spionagesoftware, webtaps, verborgen identificatoren en andere 'soortgelijke programmatuur'.[35]

Het techniekneutrale karakter van de e-Privacyrichtlijn werd nog eens benadrukt in de considerans van de Richtlijn Burgerrechten, die een aantal bepalingen, waaronder art. 5 lid 3 e-Privacyrichtlijn,[36] in de e-Privacyrichtlijn wijzigde:

> "(…) technologische vooruitgang maakt de ontwikkeling mogelijk van nieuwe toepassingen die zijn gebaseerd op systemen voor gegevensverzameling en identificatie, zoals contactloze radiofrequentiesystemen. RFID-systemen (Radio Frequency Identification Devices) bijvoorbeeld maken gebruik van radiofrequenties om gegevens op te vangen van op unieke wijze geïdentificeerde RFI-chips, gegevens die vervolgens kunnen worden verstuurd over bestaande communicatienetwerken. (…) Wanneer dergelijke systemen aan openbare elektronischecommunicatienetwerken worden gekoppeld of gebruikmaken van elektronischecommunicatiediensten als basisinfrastructuur gelden de relevante bepalingen van [de e-Privacyrichtlijn] inclusief die in verband met veiligheids-, verkeers- en locatiegegevens en vertrouwelijkheid."[37]

Net als RFID-technologie is wifi-trackingtechnologie een nieuwe toepassing, die is gebaseerd op systemen voor gegevensverzameling en identificatie van op unieke wijze geïdentificeerde chips (door een MAC-adres) via contactloze radiofrequentiesystemen (wifi-meetsystemen). Ook wifi-trackingapparatuur vangt, gebruikmakend van radiofrequenties, gegevens op die worden verstuurd over bestaande communicatienetwerken.

In het evaluatierapport van de e-Privacyrichtlijn, dat in 2016 in opdracht van de Commissie tot stand is gekomen, wordt wifi-tracking aangehaald als voorbeeld van een technologie waarvan in de praktijk onduidelijk is of deze onder het bereik van art. 5 lid 3 e-Privacyrichtlijn valt.[38] Ook de Artikel 29-werkgroep, het Europese samenwerkingsverband van nationale privacytoezichthouders dat sinds 25 mei 2018 is opgevolgd door de European Data Protection Board (EDPB),[39] stelt in Opinie 03/2016 over de evaluatie van de e-Privacyrichtlijn dat door de wijze waarop art. 5 lid 3 e-Privacyrichtlijn is geformuleerd, in de praktijk niet geheel helder is of de bepaling op wifi-tracking van toepassing kan zijn.[40] In de praktijk en literatuur wordt met name geworsteld met de vraag of het opvangen van signalen, waarin het MAC-adres van de eindapparatuur is meegezonden, kan worden aangemerkt als "het verkrijgen van toegang tot informatie die is opgeslagen in de eindapparatuur van een gebruiker".

Bosch en Van Eijk voeren aan dat uit art. 5 lid 3 en de preambule van de e-Privacyrichtlijn volgt dat het artikel beoogt apparatuur en de inhoud ervan te beschermen tegen onbevoegde toegang ('access to').[41] Door het opvangen van signalen die een apparaat automatisch uitzendt zou, volgens de auteurs, geen toegang worden verkregen tot informatie op de apparatuur. Bosch en Van Eijk lijken te veronderstellen dat art. 5 lid 3 e-Privacyrichtlijn slechts van toepassing is op technologieën waarbij daadwerkelijk – fysiek – toegang wordt verkregen tot apparatuur, waarna informatie wordt uitgelezen, zoals bij cookies.

Een enge en rigide uitleg van art. 5 lid 3 e-Privacyrichtlijn lijkt voort te komen uit een verkeerd begrepen ratio van de cookiebepaling. Wellicht dat de term 'cookiebepaling' te erg aan art. 5 lid 3 e-Privacyrichtlijn is gaan kleven en het artikel door velen niet los van cookies kan worden gezien. Er lijkt een – nergens op gestoelde – overtuiging te bestaan, dat voordat informatie 'uit' randapparatuur wordt gelezen, er eerst informatie (door dezelfde partij) op de randapparatuur moet worden geplaatst om art. 5 lid 3 e-Privacyrichtlijn van toepassing te laten zijn.

31 W.A.M. Steenbruggen, *Publieke dimensies van privé-communicatie: een onderzoek naar de verantwoordelijkheid van de overheid bij de bescherming van vertrouwelijke communicatie in het digitale tijdperk* (diss. Amsterdam UvA), Amsterdam: Otto Cramwinckel 2009, p. 186.

32 Overweging 24 en 25 e-Privacyrichtlijn. Zie ook LIBE-rapport EPR, p. 21 en *Kamerstukken II* 2013/14, 33902, 3, p. 1.

33 Overweging 24 e-Privacyrichtlijn. Zie ook Artikel 29-werkgroep, *Opinion 2/2010 on online behavioural advertising*, WP 171, 22 juni 2010 (hierna: WP29 Online behavioural advertising 2/2010), p. 9 en F.J. Zuiderveen Borgesius, 'De nieuwe cookieregels: alwetende bedrijven en onwetende internetgebruikers?', *P&I* 2011, afl. 1, p. 6.

34 F. Debusseré, 'The EU E-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster?', *International Journal of Law and Information Technology* (13) 2005, p. 82-83.

35 Overweging 24 e-Privacyrichtlijn.

36 B. van der Sloot & F.J. Zuiderveen Borgesius, 'De amendementen van de Richtlijn Burgerrechten op de e-Privacyrichtlijn', *P&I* 2010, afl. 4, p. 166-167.

37 Overweging 56 Richtlijn 2009/136/EG.

38 Deloitte, *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector*, 2016, p. 135.

39 Zie art. 68 en overweging 139 AVG.

40 Artikel 29-werkgroep, *Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC)*, WP 240, 19 juli 2016, p. 11.

41 B.F.E. Bosch & N.A.N.M. van Eijk, 'Wifi-tracking in de winkel(straat): inbreuk op de privacy?' *P&I* 2016, afl. 6 (hierna: Bosch & Van Eijk, *P&I* 2016), p. 245.

In dit kader is interessant dat de Artikel 29-werkgroep van mening is dat de bewoording 'opslag of verkrijgen van toegang' ('stored or accessed') in art. 5 lid 3 e-Privacyrichtlijn, erop wijst dat de opslag en toegang tot informatie niet tijdens dezelfde handeling hoeft te gebeuren, of hoeft te worden uitgevoerd door dezelfde partij. Informatie die is opgeslagen door een bepaalde partij (inclusief informatie opgeslagen door de fabrikant) en waar *later* door een andere partij toegang tot wordt verkregen, valt, volgens de Artikel 29-werkgroep, onder het bereik van art. 5 lid 3 e-Privacyrichtlijn. De Artikel 29-werkgroep benadrukt dat ook wanneer toegang wordt verkregen tot een *read-only value*, art. 5 lid 3 e-Privacyrichtlijn van toepassing is. De Artikel 29-werkgroep noemt daarbij, als (enig) voorbeeld, het uitlezen van een MAC-adres.[42]

Zowel uit een tekstuele interpretatie van art. 5 lid 3 e-Privacyrichtlijn, als de ratio van de e-Privacyrichtlijn en de Richtlijn Burgerrechten, volgt dat het artikel van toepassing is op *alle* technologieën die toegang verkrijgen tot informatie die is opgeslagen in apparatuur van een gebruiker. Hieronder worden ook expliciet technologieën begrepen die gegevens opvangen, gebruikmakend van radiofrequenties 'zoals', dus niet uitsluitend, RFID-technologie. Uit niets volgt dat bepaalde technologieën, zoals wifi-tracking, niet onder het bereik van de bepaling kunnen vallen. Integendeel, de techniekneutrale formulering van art. 5 lid 3 e-Privacyrichtlijn en de ratio van de e-Privacyrichtlijn en de Richtlijn Burgerrechten geven naar mijn mening juist alle reden te concluderen dat het artikel ook op wifi-tracking (en soortgelijke technologieën) van toepassing kan zijn.

3.2 *Artikel 11.7a Telecommunicatiewet*

Zoals eerder in deze bijdrage aangegeven, is art. 5 lid 3 e-Privacyrichtlijn in Nederland geïmplementeerd in art. 11.7a Tw. De bepaling is sinds 2012 van toepassing.[43] Het eerste lid ziet er, in de huidige vorm,[44] als volgt uit:

> "Onverminderd de [Wbp] (lees sinds 25 mei 2018: de AVG)[45] is het via een elektronisch communicatienetwerk opslaan van of toegang verkrijgen tot informatie in de randapparatuur van een gebruiker, alleen toegestaan op voorwaarde dat de betrokken gebruiker:
>
> a. is voorzien van duidelijke en volledige informatie overeenkomstig de [Wbp] (lees: de AVG), in ieder geval over de doeleinden waarvoor deze informatie wordt gebruikt, en
> b. daarvoor toestemming heeft verleend."

Uit de parlementaire geschiedenis van art. 11.7a Tw volgt dat de wetgever uitdrukkelijk duidelijk heeft willen maken dat het toepassingsbereik van het artikel niet beperkt is tot het gebruik van cookies, maar – in lijn met de bedoeling van de e-Privacyrichtlijn – van toepassing is op *alle* technologieën die opslag van informatie op randapparatuur of het verkrijgen van toegang tot informatie mogelijk maken.[46]

De Autoriteit Consument en Markt (ACM), toezichthouder op de cookiebepaling, stelt dat het toepassingsbereik van art. 11.7a Tw 'veel verder' gaat dan alleen het plaatsen van cookies. De ACM geeft aan dat alleen in de situatie waarin in het geheel geen sprake is van het opslaan, dan wel uitlezen van gegevens op de randapparatuur van de gebruiker, art. 11.7a Tw niet van toepassing is.[47]

Bosch en Van Eijk stellen dat art. 11.7a Tw zich richt tot aanbieders van een 'telecommunicatienetwerk'. De auteurs vragen zich vervolgens af of wifi-tracking via een telecommunicatienetwerk wordt toegepast.[48] Art. 11.7a Tw is echter van toepassing op "het via een *elektronisch communicatienetwerk* opslaan van of toegang verkrijgen tot informatie in de randapparatuur van de gebruiker". Uit de parlementaire geschiedenis volgt dat het begrip 'elektronisch communicatienetwerk' netwerken betreft waarmee, onder meer via radiogolven, signalen worden overgebracht. Ook het *ontvangen* van signalen die "strikt genomen niet als communicatie zouden kunnen worden opgevat" vallen, volgens de wetgever, onder het overbrengen van signalen.[49]

Daarnaast bepaalt het tweede lid van art. 11.7a Tw dat ook wanneer op een andere wijze dan via een elektronisch communicatienetwerk informatie wordt opgeslagen of "toegang wordt verleend tot op het randapparatuur opgeslagen informatie", het artikel van toepassing is. Het tweede lid van art. 11.7a Tw brengt de cookiebepaling in lijn met het idee dat art. 5 lid 3 e-Privacyrichtlijn – in tegenstelling tot de rest van de e-Privacyrichtlijn[50] – een 'algemeen karakter' heeft, en niet uitsluitend van toepassing is wanneer toegang wordt verkregen tot informatie via een 'elektronisch communicatienetwerk'.[51] In de parlementaire geschiedenis komt naar voren dat op grond van art. 11.7a lid 2 Tw de informatieplicht en het toestemmingsvereiste van art. 11.7a lid 1 Tw bijvoorbeeld tevens gelden als via een draadloos

42 Artikel 29-werkgroep, *Advies 9/2014 over de toepassing van Richtlijn 2002/58/EG op device fingerprinting,* WP 224, 25 november 2014 (hierna: WP29 Device fingerprinting 9/2014), p. 8.

43 Voordat art. 5 lid 3 e-Privacyrichtlijn werd geïmplementeerd in art. 11.7a Tw, was de cookiebepaling geïmplementeerd in art. 4.1 van het Besluit universele dienstverlening en eindgebruikersbelangen. Zie Besluit van 7 mei 2004, houdende regels met betrekking tot universele dienstverlening en eindgebruikersbelangen (Besluit universele dienstverlening en eindgebruikersbelangen), *Stb.* 2004, 203, p. 27-29.

44 Zie voor de oorspronkelijke bewoording van het artikel Wet van 10 mei 2012 tot wijziging van de Telecommunicatiewet ter implementatie van de herziene telecommunicatierichtlijnen, *Stb.* 2012, 235. De huidige tekst is in 2015 in werking getreden. Zie Wet van 4 februari 2015 tot wijziging van de Telecommunicatiewet (wijziging artikel 11.7a), *Stb.* 2015, 100. Zie over de Nederlandse implementatie van de cookiebepaling E. Kosta, 'The Dutch Regulation of Cookies', *European Data Protection Law Review* (2) 2016, p. 97-102.

45 Art. 94 lid 2 AVG.

46 *Kamerstukken II* 2010/11, 32549, 3, p. 78.

47 Autoriteit Consument en Markt, *Veelgestelde vragen over de cookiebepaling*, versie november 2016, p. 4.

48 Bosch & Van Eijk, *P&I* 2016, p. 245.

49 *Kamerstukken II* 2002/03, 25851, 3, p. 89.

50 Art. 3 lid 1 e-Privacyrichtlijn.

51 Kosta, *Int'l JL & Info Tech* 2013, p. 380-406. Zie ook WP29 Online behavioural advertising 2/2010, p. 9 en Artikel 29-werkgroep, *Opinion 1/2008 on data protection issues related to search engines*, WP 148, 4 april 2008, p. 12.

transmissiesysteem, zoals Bluetooth of Near Field Communication (NFC), iets op het randapparaat van een gebruiker wordt geplaatst of informatie uitgelezen.[52] Mede op grond van deze overweging kan worden gesteld dat ook het uitlezen van informatie uit (bijvoorbeeld Bluetooth-)signalen die zich in de openbaarheid (de lucht) bevinden, onder het bereik van art. 11.7a lid 1 jo. lid 2 Tw kan vallen. Immers, door het opvangen van de signalen wordt toegang verkregen tot unieke informatie die is opgeslagen op de randapparatuur die de signalen uitzendt.

3.3 *Uitzondering op cookiebepaling*

De cookiebepaling uit de Tw kent een aantal uitzonderingen. Deze uitzonderingen zijn neergelegd in art. 11.7a lid 3 Tw en zien er als volgt uit:

> "Het bepaalde in het eerste lid is niet van toepassing indien het de opslag of toegang betreft:
> a. met als uitsluitend doel de communicatie over een elektronisch communicatienetwerk uit te voeren,
> b. die strikt noodzakelijk is om de door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij te leveren of – mits dit geen of geringe gevolgen heeft voor de persoonlijke levenssfeer van de betrokken abonnee of gebruiker – om informatie te verkrijgen over de kwaliteit of effectiviteit van een geleverde dienst van de informatiemaatschappij."

Hierna sta ik stil bij de vraag of de uitzondering in art. 11.7a lid 3 sub b Tw op wifi-tracking van toepassing kan zijn. Wanneer de uitzondering van toepassing is, kan wifi-tracking plaatsvinden zonder voorafgaande toestemming van de gebruiker en zonder dat de gebruiker over de toepassing hoeft te worden geïnformeerd.

Het voor mijn analyse relevante gedeelte van art. 11.7a lid 3 sub b Tw bepaalt dat art. 11.7a lid 1 Tw niet van toepassing is, indien sprake is van opslag van of toegang tot gegevens:

> "die strikt noodzakelijk is (…) mits dit geen of geringe gevolgen heeft voor de persoonlijke levenssfeer van de betrokken abonnee of gebruiker – om informatie te verkrijgen over de kwaliteit of effectiviteit van een geleverde dienst van de informatiemaatschappij."

De uitzondering in art. 11.7a lid 3 sub b Tw is tot stand gekomen om – met name[53] – websitehouders analytische cookies te kunnen laten plaatsen, zonder dat hiervoor voorafgaande toestemming benodigd is, mits het plaatsen van de analytische cookies nauwelijks nadelige gevolgen heeft voor de persoonlijke levenssfeer van de gebruiker.[54] Door het plaatsen van analytische cookies kan een websitehouder bijvoorbeeld bijhouden hoeveel unieke bezoekers een website ontvangt.

Het is de vraag waar de grens ligt tussen een simpele telling en een meer gedetailleerde analyse. Ook op grond van een enkele registratie van een MAC-adres in combinatie met gegevens over signaalsterkte, locatie en tijdstip van waarneming kan immers een analyse worden gemaakt, waaraan conclusies kunnen worden verbonden. Van Canneyt is van mening dat wanneer wifi-tracking beperkt blijft tot het tellen van winkelbezoekers, op grond van art. 11.7a lid 3 sub b Tw geen toestemming voor toepassing van wifi-tracking hoeft te worden verkregen.[55] Nu, zoals Van Canneyt terecht aangeeft, wifi-tracking vaak een ruimer doel dient dan een simpele telling, zal de uitzondering uit art. 11.7a lid 3 sub b Tw in veel situaties niet van toepassing zijn.

Daarnaast is de uitzondering slechts van toepassing wanneer informatie wordt verkregen over de kwaliteit of effectiviteit van een 'geleverde dienst van de informatiemaatschappij', zoals een website.[56] Eén van de voorwaarden om te kunnen spreken van een 'dienst van de informatiemaatschappij' is dat de dienst op individueel verzoek van een afnemer wordt verricht.[57] Van zo'n 'individueel verzoek' zal bij passieve wifi-tracking geen sprake zijn. Dit kan mogelijk anders zijn wanneer MAC-adressen en tijd- en locatiegegevens worden verwerkt, wanneer gebruikers verbinding maken met een wifi-netwerk dat gratis ter beschikking is gesteld om de aandacht van potentiele klanten te vestigen op de waren of diensten van een winkel.[58]

3.4 *Device fingerprinting en artikel 5 lid 3 e-Privacyrichtlijn*

Naar mijn mening kan art. 5 lid 3 e-Privacyrichtlijn op wifi-tracking van toepassing zijn. Dit volgt uit de formulering van het artikel en de totstandkomingsgeschiedenis en ratio van de bepaling. Daarnaast kan wifi-tracking in mijn optiek worden aangemerkt als een vorm van 'device fingerprinting', waarop art. 5 lid 3 e-Privacyrichtlijn van toepassing is.

In Advies 9/2014 stelt de Artikel 29-werkgroep dat art. 5 lid 3 e-Privacyrichtlijn op device fingerprinting van toepassing kan zijn.[59] Een device fingerprint wordt gedefinieerd als een verzameling van informatie-elementen waarmee een apparaat of applicatie kan worden geïdentificeerd.[60] Deze identificatie kan plaatsvinden door gebruikers (of een apparaat)

52 *Kamerstukken II* 2013/14, 33902, 3, p. 2.

53 Het artikel heeft volgens de wetgever een 'toekomstbestendige' techniekneutrale formulering gekregen, zodat de bepaling niet uitsluitend van toepassing is op (analytische) cookies. Zie *Kamerstukken II* 2013/14, 33902, 3, p. 7.

54 *Kamerstukken II* 2013/14, 33902, 3, p. 6-8. Zie ook M. Bolhuis, 'Cookieregulering revisited', *Mediaforum* 2013, afl. 11, p. 264-265.

55 T. van Canneyt, 'Big brother in de winkel? – wifi-tracking en de verwerking van persoonsgegevens', *Computerrecht* 2016/125, afl. 4 (hierna: Van Canneyt, *Computerrecht* 2016), p. 216.

56 *Kamerstukken II* 2013/14, 33902, 3, p. 4.

57 Art. 1 lid 1 sub b Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij.

58 HvJ EU 15 september 2016, C-484/14, ECLI:EU:C:2016:689 (*Mc Fadden/Sony Music*).

59 WP29 Device fingerprinting 9/2014, p. 7-8.

60 A Cooper e.a., *Privacy Considerations for Internet Protocols*, RFC 6973, juli 2013, p. 8.

in de tijd te onderscheiden of te herleiden ('singling out'), te koppelen of te deduceren.[61] Ook in Opinie 8/2014 over the Internet of Things (IoT) stelt de Artikel 29-werkgroep zich expliciet op het standpunt dat art. 5 lid 3 e-Privacyrichtlijn van toepassing is op het verkrijgen van toegang tot informatie, waarmee een device fingerprint van een (mobiel) apparaat kan worden gecreëerd.[62]

Van Canneyt is van mening dat het verwerken van een MAC-adres, in combinatie met registratie van de signaalsterkte, locatie en het tijdstip van waarneming van een apparaat, als het nemen van een device fingerprint kan worden aangemerkt, waarop art. 5 lid 3 e-Privacyrichtlijn van toepassing is.[63] Dit standpunt lijkt juist nu, zoals Van Canneyt terecht opmerkt, het apparaat van de gebruiker door het verwerken van een MAC-adres, de signaalsterkte, locatie en het tijdstip van de waarneming, van een ander apparaat kan worden onderscheiden (singling out).

Bosch en Van Eijk stellen dat bij toepassing van wifi-tracking geen sprake is van device fingerprinting, nu volgens de auteurs bij wifi-tracking slechts gebruik wordt gemaakt van één gegeven (het MAC-adres), terwijl device fingerprinting het opstellen van een profiel inhoudt, op basis van een combinatie van (niet-unieke) apparaatgegevens.[64] De uitleg die Bosch en Van Eijk hanteren, is een vrij beperkte uitleg van het begrip device fingerprinting, ten opzichte van de ruimere definitie zoals door de Artikel 29-werkgroep wordt gehanteerd. Daarnaast wordt bij wifi-tracking niet alleen het MAC-adres verwerkt, maar tevens een aantal niet-unieke apparaatgegevens; namelijk de signaalsterkte, locatie en het tijdstip van de waarneming. In dat opzicht kan naar mijn mening dus wel degelijk worden gesproken van een combinatie van (unieke en niet-unieke) apparaatgegevens.

3.5 *Standpunt Autoriteit Persoonsgegevens en regering*

De Autoriteit Persoonsgegevens (AP) heeft zich in het Bluetrace-rapport eind 2015 voor het eerst over wifi-tracking uitgelaten. In het rapport heeft de AP wifi-tracking uitsluitend getoetst aan de Wbp.[65] De tweede keer dat de AP zich uitliet over wifi-tracking was in juni 2016. In twee vrijwel identieke brieven aan Detailhandel Nederland en de Vereniging van Nederlandse Gemeenten wijst de AP op de wettelijke eisen die gelden wanneer winkels en gemeenten gebruikmaken van wifi-tracking.[66] Opvallend is dat de AP in beide brieven slechts in twee voetnoten wijst op de mogelijke toepasbaarheid van art. 11.7a Tw op wifi-tracking.

In de brieven van de AP stelt de toezichthouder in voetnoot 3 dat "Afhankelijk van de gebruikte technologie, (…) ook de [Tw] van toepassing [kan] zijn". In voetnoot 5 is de volgende tekst opgenomen:

> "Daarnaast wijst de [AP] op artikel 11.7a [Tw]. Dit artikel kan van toepassing zijn op tracking technieken waarbij gegevens worden geplaatst op het apparaat van de consument, of daarvan worden afgelezen."

De reden waarom deze voor de praktijk belangrijke constatering slechts vermelding in een voetnoot verdient, is waarschijnlijk gelegen in het feit dat de AP geen toezicht houdt op naleving van art. 11.7a Tw. Deze taak is, zoals eerder aangegeven, wettelijk voorbehouden aan de ACM.[67] De ACM heeft zich, voor zover mij bekend, tot op heden nog niet publiekelijk uitgelaten over de mogelijke toepasbaarheid van art. 11.7a Tw op wifi-tracking.

Met de e-Privacyverordening op komst, wordt in kamerstukken over de toekomstige verordening naar de huidige cookiebepaling verwezen. Dit levert interessante inzichten op. Zo is opvallend dat, net als de AP, ook de regering van mening lijkt te zijn dat art. 11.7a Tw op wifi-tracking van toepassing kan zijn. In het Beoordeling Nieuwe Commissievoorstellen (BNC)-fiche over de e-Privacyverordening stelt de regering dat het 'lezen/verwerken' van MAC-adressen "tot nu viel (…) onder het toestemmingsvereiste van de [e-Privacyrichtlijn], respectievelijk artikel 11.7a van de [Tw]".[68]

4. Gevolgen toepasbaarheid huidige e-Privacyregels op wifi-tracking

Nu ik eerder in deze bijdrage heb vastgesteld dat art. 11.7a Tw in bepaalde situaties op wifi-tracking van toepassing kan zijn, bespreek ik hierna welke gevolgen toepasbaarheid heeft voor de praktijk. Naast alle vereisten uit de AVG dient de toepassing van wifi-tracking, wanneer geen sprake is van een uitzonderingssituatie als bedoeld in art. 11.7a lid 3 sub b Tw, te voldoen aan de vereisten uit art. 11.7a lid 1 Tw. Uit het eerste lid van art. 11.7a Tw volgt dat wifi-tracking slechts is toegestaan op voorwaarde dat (sub a) de gebruiker wordt voorzien van duidelijke en volledige informatie en (sub b) toestemming heeft verleend voor het verkrijgen van toegang tot informatie die is opgeslagen op zijn randapparatuur.

4.1 *Duidelijke en volledige informatie*

Art. 11.7a lid 1 sub a Tw schrijft voor dat de gebruiker moet worden voorzien van duidelijke en volledige informatie

61 WP29 Device fingerprinting 9/2014, p. 4.
62 Artikel 29-werkgroep, *Opinion 8/2014 on the Recent Developments on the Internet of Things*, WP 223, 16 september 2014, p. 14.
63 Van Canneyt, *Computerrecht* 2016, p. 216.
64 Bosch & Van Eijk, *P&I* 2016, p. 245.
65 Bluetrace-rapport, p. 21-26.
66 Autoriteit Persoonsgegevens, *Wifi-tracking en de Wet bescherming persoonsgegevens*, brieven aan Detailhandel Nederland en Vereniging Nederlandse Gemeenten, 15 juni 2016, p. 2 en p. 4.
67 Zodra de e-Privacyverordening van toepassing wordt, zal mogelijk niet langer de ACM, maar de AP toezicht gaan houden op naleving van cookie- en devicetrackingregelgeving. Hierover bestaat nog onduidelijkheid en discussie. Zie art. 18 lid 1 Commissievoorstel EPV, art. 18 lid 1 LIBE-rapport EPV en *Kamerstukken II* 2016/17, 22112, 2306, p. 8-10.
68 *Kamerstukken II* 2016/17, 22112, 2306, p. 4.

overeenkomstig de Wbp (lees sinds 25 mei 2018: de AVG),[69] "in ieder geval over de doeleinden waarvoor deze informatie wordt gebruikt". In de openbare versie van de brief van de AP waarin de toezichthouder aan Bluetrace een last onder dwangsom oplegt, heeft de AP uiteengezet hoe aan de informatieverplichting kan worden voldaan wanneer wifi-tracking wordt toegepast.[70] De AP stelt dat de informatie op getrapte wijze kan worden gegeven in de, in de praktijk veel voorkomende, situatie dat de beschikbare ruimte voor informatie beperkt is.

In een eerste (zeer) korte kennisgeving dient ten minste te worden opgenomen: (i) de naam van het bedrijf dat de gegevens verwerkt; (ii) het doeleinde van de verwerking; en (iii) de vermelding waar nadere informatie over de verwerking kan worden verkregen. Het is denkbaar en in de praktijk voorkomend, dat wordt verwezen naar een webpagina waar nadere informatie wordt gegeven. Dit is in lijn met het idee dat informeren op een website met name geschikt is in situaties waarin, door de technische complexiteit van een verwerking, het voor de betrokkene moeilijk is om te begrijpen of, door wie en met welk doel zijn persoonsgegevens worden verwerkt.[71]

De AP geeft aan dat door partijen die wifi-tracking toepassen pictogrammen kunnen worden gebruikt om aan het informatievereiste te voldoen.[72] In de praktijk gebruiken partijen die wifi-tracking toepassen verschillende varianten van een pictogram, die het uitzenden (of ontvangen) van signalen symboliseert. Het is de vraag in hoeverre een pictogram, al dan niet voorzien van een begeleidende tekst, kan voldoen aan het vereiste dat duidelijke en volledige informatie dient te worden gegeven. Immers, een gemiddelde passant van een dergelijke pictogram zal – als hij de pictogram in een druk gebied al waarneemt[73] – gelet op de technische complexiteit van wifi-trackingtechnologie niet direct begrijpen wat het pictogram[74] of zelfs de begeleidende tekst betekent.

De AP geeft verder aan dat in een tweede en eventueel derde informatielaag, de gebruiker (nader) kan worden geïnformeerd door het ter beschikking stellen van flyers of informatiebrochures.

69 Art. 13 AVG.

70 Autoriteit Persoonsgegevens, *Last onder dwangsom Bluetrace*, brief aan Bluetrace, 30 juni 2016, p. 15.

71 Overweging 58 AVG.

72 Zie ook art. 12 lid 7 en overweging 60 AVG.

73 Bits of Freedom, *Standpunt Bits of Freedom na eerste analyse van voorstel ePrivacy Verordening*, brief aan ministers Kamp en Van der Steur, 18 januari 2017, p. 5.

74 Op Nederlandse stations is in het verleden geëxperimenteerd met het informeren van reizigers over de toepassing van wifi-tracking via slechts een pictogram. Deze pictogram werd niet begrepen; reizigers dachten dat ze op het station gratis toegang tot een wifi-netwerk konden krijgen. Zie V. Wever, 'Met wifi-tracking naar optimaal netwerk', *OV-Magazine* 13 juni 2017.

4.2 *Toestemming*

Onder toestemming van de gebruiker ex art. 11.7a lid 1 sub b Tw wordt toestemming verstaan als bedoeld in de AVG. De AVG specificeert toestemming als "Elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt".[75]

De vraag hoe rechtsgeldige toestemming kan worden verleend voor de toepassing van wifi-tracking kan, gezien de technische eigenschappen van wifi-trackingtechnologie, niet gemakkelijk worden beantwoord. Zoals in deze bijdrage uiteengezet, wordt bij het gebruik van wifi-tracking op passieve wijze informatie uitgelezen uit (en via de signalen afkomstig van) een apparaat: de gebruiker merkt hier niets van. Zodra een gebruiker binnen het meetgebied van de trackingapparatuur komt, vindt het uitlezen van informatie automatisch plaats. In het geval de gebruiker eventuele informatie over de toepassing van wifi-tracking heeft gemist, of de informatie wel heeft gezien maar niet begrepen, is het MAC-adres van de gebruiker al uitgelezen. Toestemming kan dan niet meer, of niet meer op informatie berustend, worden gegeven.

Op grond van de AVG komt de gebruiker het recht toe om zijn toestemming voor de toepassing van wifi-tracking te allen tijde in te trekken.[76] Dit leidt ertoe dat alle partijen die wifi-tracking toepassen, een opt-outmogelijkheid aan de gebruiker moeten aanbieden. In de praktijk bieden verschillende partijen die wifi-tracking toepassen aan gebruikers de mogelijkheid om middels een opt-outconstructie op een website aan te geven (achteraf) niet akkoord te gaan met de verwerking van hun MAC-adres en locatiegegevens. Het bieden van een opt-outmogelijkheid, nadat een verwerking heeft plaatsgevonden, voldoet niet aan de vereisten voor toestemming als bedoeld in de AVG. De AP heeft in het Bluetrace-rapport aangegeven dat het aanbieden van een opt-outmogelijkheid slechts in de context van art. 8 sub f Wbp (lees sinds 25 mei 2018: art. 6 lid 1 sub f AVG) bijdraagt aan de belangenafweging tussen enerzijds het belang van de aanbieder van wifi-tracking en, anderzijds, het belang van de betrokkene op eerbiediging van de persoonlijke levenssfeer.[77] In Opinie 15/2011 over de definitie van toestemming heeft ook de Artikel 29-werkgroep aangegeven dat toestemming in de context van art. 5 lid 3 e-Privacyrichtlijn moet zijn verkregen *voordat* de handeling (in het geval van wifi-tracking: het opvangen van wifi-signalen) plaatsvindt.[78] Ook de wetgever heeft benadrukt dat onder art. 11.7a Tw toestemming *voorafgaand* aan de handeling moet worden verkregen.[79]

75 Art. 4 lid 11 AVG. Zie ook overweging 32 AVG.

76 Art. 7 lid 3 AVG.

77 Bluetrace-rapport, p. 66.

78 Artikel 29-werkgroep, *Opinie 15/2011 over de definitie van toestemming*, WP 187, 13 juli 2011, p. 35.

79 *Kamerstukken II* 2013/14, 33902, 3, p. 12.

Om in de praktijk aan het toestemmingsvereiste te kunnen voldoen, zijn verschillende oplossingen denkbaar. Een voorbeeld van zo'n oplossing is het plaatsen van een toegangspoort (een offline 'trackingmuur') voor een gebied waar wifi-tracking wordt toegepast, zoals een winkel of winkelgebied. Een dergelijke toegangspoort kan slechts worden geopend wanneer een bezoeker van het gebied aangeeft akkoord te gaan met het opvangen van de wifi-signalen van zijn randapparatuur. De gebruiker kan bijvoorbeeld toestemming geven door het aantikken van een akkoord-knop op een beeldscherm. Voordat de gebruiker toestemming geeft, moet hij zijn voorzien van duidelijke en volledige informatie, die bijvoorbeeld op het beeldscherm is afgebeeld en gelezen moet zijn, voordat de akkoord-knop verschijnt. Het is echter de vraag of winkeliers bereid zullen zijn een dergelijke toegangspoort voor hun winkel te plaatsen. Een toegangspoort zal voor veel bezoekers – zacht gezegd – even wennen zijn.

Daarnaast dient het intrekken van toestemming op grond van de AVG even eenvoudig te zijn als het geven ervan.[80] Dit moet ook duidelijk zijn voor de gebruiker.[81] Het is zeer de vraag of het aanbieden van een opt-outmogelijkheid op een website, zoals sommige partijen dat nu doen, aan dit vereiste voldoet, wanneer toestemming bijvoorbeeld bij de ingang van een winkel(gebied) door het aantikken van een akkoord-knop is gegeven.

Voornoemde 'oplossing' is helemaal problematisch op vliegvelden en stations. Als een reiziger zijn vlucht of trein moet halen, zal hij per definitie zijn toestemming voor de toepassing van wifi-tracking moeten geven. Er is dan geen sprake van een vrije wilsuiting: de gebruiker heeft geen keuzevrijheid.[82] Ook wanneer wifi-tracking wordt toegepast om verkeersstromen in kaart te brengen – zoals dat in Nederland op grote schaal wordt gedaan[83] – is lastig te bedenken hoe aan het toestemmingsvereiste kan worden voldaan.

De Artikel 29-werkgroep stelt in Opinie 01/2017 dat toestemming voor wifi-tracking kan worden verkregen met behulp van een app.[84] In Opinie 6/2017 van de European Data Protection Supervisor (EDPS) brengt de EDPS naar voren dat partijen die wifi-tracking toepassen een database kunnen creëren, waarin MAC-adressen worden opgenomen van gebruikers die hebben aangegeven toestemming te geven voor wifi-tracking.[85] Beide ideeën lijken door de technologische eigenschappen van wifi-tracking echter lastig uitvoerbaar. De meetapparatuur die voor wifi-tracking wordt gebruikt, vangt *alle* signalen op die zich binnen het bereik van de meetapparatuur bevinden. Het lijkt mij, gelet op de huidige stand van de techniek, lastig om slechts de signalen op te vangen van gebruikers die via een app of een online opt-inregister hebben aangegeven akkoord te gaan met de toepassing van wifi-tracking. Om te controleren of een MAC-adres op een 'witte lijst' staat, moet het MAC-adres immers eerst worden opgevangen en verwerkt. Ook wanneer een MAC-adres dat niet op een witte lijst staat meteen wordt verwijderd, is al toegang verkregen tot informatie die is opgeslagen op de randapparatuur van de gebruiker.

Wanneer een gebruiker geen toestemming wil geven voor de toepassing van wifi-tracking, maar wel een gebied wil betreden waar wifi-tracking wordt toegepast (en daar gebruik wil blijven maken van de wifi-functionaliteit van zijn apparatuur), bestaat er maar één mogelijkheid waarmee een gebruiker zich aan wifi-tracking kan onttrekken: het uitzetten van de wifi-functionaliteit op zijn randapparatuur.[86] Zoals Bosch en Van Eijk terecht opmerken, is het de vraag in hoeverre het aan de gebruiker moet worden gelaten om een actieve handeling te verrichten om zich te onttrekken aan wifi-tracking. Het continu aan en uit moeten zetten van de wifi-functionaliteit op randapparatuur is anno nu een onevenredige (en uit praktisch oogpunt onwenselijke) inspanning.[87] Daarnaast leidt dit tot een ongewenst *chilling effect*: omdat gebruikers weten dat ze kunnen worden gevolgd, zullen ze de wifi-functionaliteit van hun apparatuur mogelijk uitschakelen en daarmee hun gedrag aanpassen.

Verder bepaalt de AVG dat het geven van toestemming niet mogelijk is, wanneer sprake is van een duidelijke wanverhouding tussen de gebruiker en de partij die wifi-tracking toepast.[88] Uit de AVG volgt dat van een dergelijke wanverhouding met name sprake kan zijn, wanneer de partij die wifi-tracking toepast een overheidsinstantie is, en dit het onwaarschijnlijk maakt dat de toestemming vrijelijk is verleend.[89] Nu wifi-tracking in Nederland vaak wordt toegepast door (of in opdracht van) overheidsinstanties, zoals met name gemeenten,[90] is het de vraag of de toepassing van wifi-tracking door overheidsinstanties überhaupt nog mogelijk is, sinds de AVG van toepassing is.

80 Art. 7 lid 3 AVG.
81 Art. 13 lid 2 sub c AVG.
82 Zie hierover in het kader van online trackingmuren overweging 22 LIBE-rapport EPV en F.J. Zuiderveen Borgesius e.a., 'Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation', *European Data Protection Law Review* (3) 2017, p. 353-368.
83 Hijink, *NRC* 2015.
84 Artikel 29-werkgroep, *Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)*, WP 247, 4 april 2017 (hierna: WP29 ePrivacy Regulation 01/2017), p. 11.
85 European Data Protection Supervisor, *Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)*, 24 april 2017 (hierna: EDPS ePrivacy Regulation 6/2017), p. 20.
86 Overigens is het voor bezitters van een iPhone sinds iOS 11 een stuk moeilijker geworden om de wifi- en bluetoothfunctionaliteit van het apparaat daadwerkelijk uit te zetten. Zie 'Wifi en bluetooth in bedieningspaneel iOS 11 gaan niet echt uit', *NOS* 21 september 2017 en https://support.apple.com/en-us/HT208086.
87 Bosch & Van Eijk, *P&I* 2016, p. 245. Zie ook EDPS ePrivacy Regulation 6/2017, p. 20.
88 Overweging 43 AVG.
89 Overweging 43 AVG. Zie ook WP29 Consent under the GDPR, p. 6.
90 D. Verlaan, 'Zorgen om privacy: in alle grote steden word je via je telefoon gevolgd', *RTL Z* 16 juni 2016.

5. Toekomstige regels voor wifi-tracking: de e-Privacyverordening

Op 10 januari 2017 publiceerde de Commissie het voorstel voor de e-Privacyverordening. De verordening is onderdeel van de strategie van de Commissie voor de digitale eengemaakte markt (*Digital Single Market Strategy*). Deze strategie heeft als doelstelling het vertrouwen in en de veiligheid van digitale diensten te vergroten.[91] Het voorstel voor de e-Privacyverordening is een *lex specialis* bij de AVG[92] en voorziet in een nadere omschrijving en aanvulling voor elektronische communicatiegegevens die als persoonsgegevens worden aangemerkt.[93]

Zonder een uitgebreide algemene analyse van de toekomstige e-Privacyverordening te willen geven, sta ik hierna stil bij art. 8 lid 2 e-Privacyverordening dat, zodra de e-Privacyverordening van toepassing wordt, expliciet op wifi-tracking van toepassing zal zijn.[94]

5.1 *Commissievoorstel e-Privacyverordening*

In het voorstel voor de e-Privacyverordening van 10 januari 2017 geeft de Commissie aan op de hoogte te zijn van wifi-trackingtechnologie en de gevaren ervan voor de persoonlijke levenssfeer.[95] Op grond van de 'devicetracking-bepaling' in het voorstel voor de e-Privacyverordening is wifi-tracking toegestaan op voorwaarde dat gebruikers worden geïnformeerd, en door de partij die wifi-tracking toepast beveiligingsmaatregelen worden genomen.[96]

Het bericht dat wifi-tracking wordt toegepast, dient duidelijk en zichtbaar te zijn aangebracht en een aantal cumulatieve gegevens te bevatten. Zo moet worden vermeld: (1) de wijze waarop gegevensverzameling plaatsvindt; (2) de doeleinden voor de gegevensverzameling; (3) de persoon die ervoor verantwoordelijk is; en (4) de maatregelen die de gebruiker kan nemen om het verzamelen van gegevens te beperken of te beëindigen. Indien bij de toepassing van wifi-tracking persoonsgegevens worden verwerkt, wat vaak het geval zal zijn, dient ook aan de informatievereisten van art. 13 AVG te worden voldaan.

Met andere woorden, een zichtbaar bordje met daarop de tekst "In dit gebied wordt wifi-tracking toegepast door partij A voor doeleinden B. Indien u niet wenst dat uw gegevens worden verzameld, kunt u (de wifi- en/of bluetooth-functionaliteit van) uw mobiele apparatuur uitschakelen" zou – wanneer geen persoonsgegevens worden verwerkt – voldoende zijn om aan de vereisten van de e-Privacyverordening te voldoen.[97]

De Commissie stelt tevens voor dat de te leveren informatie in combinatie met gestandaardiseerde iconen kan worden verstrekt.[98] De bevoegdheid om te bepalen welke informatie de iconen dienen weer te geven en op welke wijze de iconen moeten worden aangebracht, komt, zo stelt de Commissie voor, toe aan de Commissie.[99]

5.2 *Kritiek op Commissievoorstel e-Privacyverordening*

De soepele benadering ten opzichte van het gebruik van wifi-tracking is de Commissie op veel kritiek komen te staan.

Een belangrijk en in mijn optiek terecht punt van kritiek is dat wanneer voor de toepassing van wifi-tracking slechts een informatieverplichting geldt, er een continue angst voor surveillance kan ontstaan.[100] Gebruikers zullen, zodra zij de voordeur achter zich dichttrekken, voortdurend moeten zoeken naar bordjes of posters waarop staat aangegeven dat wifi-tracking wordt toegepast in het gebied waar zij zich bevinden. Met name argeloze burgers zullen de bordjes waarschijnlijk niet eens opmerken. Ook is het in veel situaties nog maar de vraag of het mogelijk is om gebruikers voorafgaand aan de toepassing van wifi-tracking te informeren. Wanneer wifi-tracking bijvoorbeeld voor verkeersonderzoek wordt toegepast, zal een automobilist met hoge snelheid langs een meetsysteem en een daarbij in de buurt geplaatst informatiebord rijden.[101] Het is de vraag of zo'n informatiebord wordt waargenomen, laat staan of er voldoende tijd bestaat om de wifi-functionaliteit van alle in de auto aanwezige apparatuur uit te schakelen.

Bij de toepassing van wifi-tracking worden locatiegegevens verwerkt. Deze informatie wordt over het algemeen als gevoelig beschouwd en kan soms zelfs zeer gevoelig zijn. De EDPS noemt als voorbeeld de toepassing van wifi-tracking in de buurt van een religieuze instelling of een ziekenhuis.[102] Het is vreemd dat de verwerking van locatiegegevens in het voorstel van de Commissie een zwakker regime kent dan elders in het voorstel, waar voor de verwerking van locatiegegevens wel toestemming is vereist.[103] Ook op grond van de AVG zal voor de verwerking van locatiegegevens het verkrijgen van toestemming in bepaalde gevallen vereist zijn. Het voorgestelde (en soepele) regime van de e-Privacyverordening lijkt het beschermingsniveau van de gebruiker ten

91 Europese Commissie, 'Proposal for an ePrivacy Regulation', 10 januari 2017, https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation.

92 Dit in tegenstelling tot de verhouding tussen de e-Privacyrichtlijn en de Privacyrichtlijn, waar geen sprake lijkt te zijn van een *lex specialis/lex generalis*-relatie, maar van elkaar complementerende richtlijnen. Zie F.J. Zuiderveen Borgesius, 'Personal Data Processing for Behavioural Targeting: Which Legal Basis?', *International Data Privacy Law* (5) 2015, p. 163-176.

93 Commissievoorstel EPV, p. 3.

94 Zie voor een uitgebreide analyse van het voorstel voor de e-Privacyverordening Roerdink, *IR* 2017 en M.A.M. Verveld-Suijkerbuijk, 'Het Europese voorstel voor een e-Privacyverordening', *P&I* 2017, afl. 2, p. 70-76.

95 Overweging 25 Commissievoorstel EPV.

96 Art. 8 lid 2 sub b Commissievoorstel EPV.

97 F.J. Zuiderveen Borgesius e.a., *An Assessment of the Commission's Proposal on Privacy and Electronic Communications*, Brussel: Europese Unie 2017 (hierna: Zuiderveen Borgesius e.a. 2017), p. 83.

98 Art. 8 lid 3 Commissievoorstel EPV.

99 Art. 8 lid 4 Commissievoorstel EPV.

100 Zuiderveen Borgesius e.a. 2017, p. 82.

101 N. Härting, *Study on the Impact of the Proposed ePrivacy Regulation*, 19 oktober 2017, p. 43-44, https://goo.gl/gTKG2m.

102 EDPS ePrivacy Regulation 6/2017, p. 19.

103 Zie art. 6 lid 2 sub c en overweging 17 Commissievoorstel EPV.

opzichte van de AVG te verlagen, hetgeen in strijd is met de algemene doelstelling van de e-Privacyverordening.[104]

5.3 *Geamendeerde versie e-Privacyverordening door Europees Parlement*

Het EP heeft in een geamendeerde versie van de e-Privacyverordening een strenger regime voor de toepassing van wifi-tracking voorgesteld. Op grond van de geamendeerde devicetrackingbepaling in de e-Privacyverordening is wifi-tracking slechts in twee situaties toegestaan: (1) nadat de gebruiker is geïnformeerd en toestemming heeft verleend[105] en (2) indien 'de risico's zijn verlaagd'.[106] In de laatste situatie hoeft dus geen toestemming voor de toepassing van wifi-tracking te worden verkregen.

Om 'risico's te verlagen' dient de toepassing van wifi-tracking aan de volgende voorwaarden te voldoen: (a) het doel van de verzameling van gegevens uit de eindapparatuur wordt beperkt tot louter statistisch tellen; (b) de verwerking is beperkt in tijd en ruimte tot hetgeen voor dit doeleinde strikt noodzakelijk is; (c) onmiddellijk nadat het doeleinde bereikt is, worden de gegevens verwijderd of anoniem gemaakt; en (d) de gebruikers worden effectieve mogelijkheden geboden om bezwaar te maken die geen gevolgen hebben voor het functioneren van de eindapparatuur.[107]

Zoals in deze bijdrage al eerder aangegeven, is het de vraag wanneer sprake is van strikt 'statistisch tellen'. Het woord 'tellen' impliceert dat er geen enkele nadere analyse mag plaatsvinden. Wanneer een partij wifi-tracking wil toepassen voor andere doeleinden dan het tellen van gebruikers, zal hiervoor dus altijd toestemming van de gebruiker benodigd zijn.

Het vereiste dat de gegevens 'onmiddellijk nadat het doeleinde is bereikt' worden verwijderd of geanonimiseerd, roept ook vragen op. Immers, veel partijen die wifi-tracking toepassen, pseudonimiseren de verkregen gegevens slechts, door het *hashen* van de opgevangen MAC-adressen. Het hashen van gegevens, eventueel met toevoeging van additionele informatie 'salting', heeft, volgens de Artikel 29-werkgroep, niet tot gevolg dat de oorspronkelijk verkregen gegevens worden geanonimiseerd.[108] In de praktijk zullen partijen opgevangen MAC-adressen dus daadwerkelijk en definitief moeten verwijderen of – voor zover mogelijk[109] – anonimiseren.

Het 'statistisch tellen' dient te worden beperkt 'in tijd en ruimte tot hetgeen voor dit doeleinde strikt noodzakelijk is'. Met andere woorden: wanneer wifi-tracking bijvoorbeeld wordt toegepast voor het tellen van bezoekers van een winkel, dient de meetapparatuur zo te worden ingesteld dat het tellen stopt wanneer de winkel is gesloten (tijd), en geen voorbijgangers worden geteld (ruimte).

Uit het vereiste dat gebruikers 'effectieve mogelijkheden' dienen te worden geboden om bezwaar te maken tegen wifi-tracking, volgt dat altijd een opt-outmogelijkheid aanwezig moet zijn. Het bieden van de 'oplossing' dat (de wifi-functionaliteit van) een apparaat kan worden uitgeschakeld, heeft immers 'gevolgen voor het functioneren van de eindapparatuur'. Het aanbieden van een opt-outmogelijkheid op een website kan eventueel kwalificeren als een 'effectieve mogelijkheid' om bezwaar te maken. Mogelijk kunnen partijen die wifi-tracking toepassen, naar Amerikaans voorbeeld,[110] gezamenlijk een website ontwikkelen waarop een gebruiker kan aangeven dat hij niet wil dat zijn MAC-adres en locatiegegevens worden verwerkt.

Tegen het aanbieden van een opt-outmogelijkheid op een website zijn echter een aantal bezwaren te bedenken. Ten eerste dient een gebruiker diep in de instellingen van zijn apparatuur te duiken om het MAC-adres van zijn apparaat te vinden. Dit kan met name een opgave zijn voor niet-technisch onderlegde gebruikers. Ten tweede dienen gebruikers het MAC-adres van de apparatuur handmatig over te typen. Ten derde zal de partij die een dergelijke online opt-outmogelijkheid beheert, het MAC-adres waarschijnlijk onbeperkt bewaren. Ten vierde zal een gebruiker, wanneer er geen initiatief voor een gezamenlijke opt-outwebsite wordt genomen, zijn MAC-adres op verschillende websites moeten invullen. Ten vijfde bieden bepaalde apparaten, zoals fitness trackers, geen toegang tot het MAC-adres van de apparatuur.[111]

Recent hebben Franse auteurs een alternatieve opt-outmogelijkheid geïntroduceerd, die mogelijk als een 'effectieve mogelijkheid' om bezwaar te maken tegen wifi-tracking kan dienen. De auteurs stellen voor dat partijen die in een bepaald gebied wifi-tracking toepassen, in dat gebied een (zichtbaar) access point aanbieden waarmee gebruikers kunnen verbinden.[112] De *Service Set Identifier* (SSID / netwerknaam) van dit access point kan bijvoorbeeld zijn: "Opt-out wifi-tracking" of "Do not track". Wanneer een gebruiker zijn apparatuur met dit access point verbindt, wordt het MAC-adres van de apparatuur op een zwarte lijst gezet. Wanneer een gebruiker weer in de buurt van hetzelfde access point komt, zal zijn apparatuur (wanneer de wifi-functionaliteit aan staat) automatisch met het access point verbinden. Als partijen die wifi-tracking toepassen deze opt-outmogelijkheid gezamenlijk aanbieden, hoeft een gebruiker slechts eenmaal met het access point te verbinden om ook op andere locaties (en aan andere partijen

104 Zie WP29 ePrivacy Regulation 01/2017, p. 11-12, EDPS ePrivacy Regulation 6/2017, p. 19-20 en Zuiderveen Borgesius e.a. 2017, p. 82.
105 Art. 8 lid 2 alinea 1 letter a bis (Amendement 95) LIBE-rapport EPV.
106 Art. 8 lid 2 alinea 1 letter a ter (Amendement 96) LIBE-rapport EPV.
107 Art. 8 lid 2 bis (Amendement 99) LIBE-rapport EPV.
108 Artikel 29-werkgroep, *Opinion 05/2014 on Anonymisation Techniques*, WP 216, 10 april 2014, p. 20. Zie ook WP29 ePrivacy Regulation 01/2017, p. 11.
109 N. Lomas, 'How "anonymous" wifi data can still be a privacy risk', *TechCrunch* 7 oktober 2017.
110 https://optout.smart-places.org.
111 C. Matte, *Wi-Fi Tracking: Fingerprinting Attacks and Counter-Measures* (diss. Lyon), 2017 (hierna: Matte 2017), p. 132.
112 C. Matte & M. Cunche, 'Wombat: An experimental Wi-Fi tracking system', 8e édition de l'Atelier sur la Protection de la Vie Privée (APVP), 2017, p. 6-7.

die wifi-tracking toepassen) aan te geven dat hij zich aan wifi-tracking wil onttrekken. Een lastig (of misschien wel onmogelijk) op te lossen probleem blijft echter dat een MAC-adres eerst dient te worden opgevangen, voordat kan worden gecontroleerd of het MAC-adres op een zwarte lijst staat. Het enige effect van een opt-out via een website of door het verbinden met een access point is dat het MAC-adres niet wordt meegenomen in een telling nadat het wel is opgevangen en vastgesteld dat het MAC-adres niet mag worden verwerkt.

5.4 *Vergelijking artikel 8 lid 2 e-Privacyverordening met huidige e-Privacyregels*

De vereisten uit de door het EP geamendeerde versie van art. 8 lid 2 e-Privacyverordening sluiten aan bij de inhoud van art. 5 lid 3 e-Privacyrichtlijn en art. 11.7a Tw. Op grond van deze bepalingen is wifi-tracking immers ook toegestaan op voorwaarde dat de gebruiker is geïnformeerd en toestemming heeft verleend. De informatieverplichting van de devicetrackingbepaling uit de door het EP geamendeerde e-Privacyverordening[113] is ten opzichte van art. 11.7a lid 1 sub a Tw soepeler. Ook wanneer bij de toepassing van wifi-tracking geen persoonsgegevens worden verwerkt, dient op grond van art. 11.7a lid 1 sub a Tw aan alle informatievereisten uit de AVG te worden voldaan.

De door het EP voorgestelde uitzondering in de e-Privacyverordening heeft een aantal overeenkomsten met art. 11.7a lid 3 sub b Tw. Eerder in deze bijdrage heb ik verdedigd dat wifi-tracking op grond van art. 11.7a lid 3 sub b Tw zonder voorafgaande toestemming is toegestaan wanneer sprake is van een 'simpele telling' en er geen of geringe gevolgen zijn voor de persoonlijke levenssfeer van de gebruiker. Deze uitzondering is echter slechts van toepassing op een 'dienst van de informatiemaatschappij' waar door de gebruiker uitdrukkelijk om wordt verzocht. Hiervan zal bij de toepassing van wifi-tracking niet snel sprake zijn.

Op grond van de door het EP geamendeerde devicetrackingbepaling zal wifi-tracking dus in meer situaties – zonder voorafgaande toestemming – zijn toegestaan. Het artikel vereist echter, dat slechts sprake mag zijn van in tijd en ruimte beperkt 'statistisch tellen'. Ook op grond van de e-Privacyverordening zal dus in veel gevallen voorafgaande toestemming voor de toepassing van wifi-tracking moeten worden verkregen.

Zoals in de inleiding van deze bijdrage is aangegeven, dient de Raad zijn standpunt over de e-Privacyverordening nog in te nemen[114] en moeten de triloogonderhandelingen over de e-Privacyverordening nog beginnen. Het is daarom ten tijde van afronding van deze publicatie nog onduidelijk hoe de uiteindelijke versie van art. 8 lid 2 e-Privacyverordening er zal uitzien.

6. Wenselijkheid toepasbaarheid e-Privacyregels op wifi-tracking

In mijn optiek kan de e-Privacyrichtlijn op wifi-tracking van toepassing zijn. In het voorstel voor de e-Privacyverordening is meer expliciet opgenomen dat gebruik van wifi-tracking aan de vereisten van de voorgestelde verordening moet voldoen. Wanneer de e-Privacyrichtlijn en de door het EP geamendeerde versie van de e-Privacyverordening op wifi-tracking van toepassing zijn, leidt dit ertoe dat het gebruik van wifi-tracking aan meer regels is gebonden dan welke volgen uit de AVG. De vraag is of dit wenselijk is.

Het toepassen van wifi-tracking kan – zeker wanneer individuen gedurende een lange periode en op verschillende locaties worden gevolgd – grote privacyrisico's[115] met zich meebrengen, zoals ook de Artikel 29-werkgroep in Opinie 01/2017 over de e-Privacyverordening aan de orde stelt. De Artikel 29-werkgroep noemt, ter illustratie van zulke risico's, de situatie waarin wifi-tracking wordt toegepast om MAC-adressen en de locatie van winkelbezoekers te verzamelen, om zo de bewegingen van gebruikers over een lange periode in kaart te brengen, mogelijk zelfs in verschillende vestigingen van een winkel.[116]

In voornoemde situatie kan sprake zijn van een ernstige inbreuk op de persoonlijke levenssfeer van de gebruiker. Locatiegegevens zijn in combinatie met een uniek identificatiegegeven, zoals een MAC-adres, zeer gevoelige persoonsgegevens.[117] Uit onderzoek is gebleken dat op basis van slechts vier locatiewaarnemingen 95% van de personen in een populatie van anderhalf miljoen mensen kan worden geïdentificeerd.[118] Daarnaast zeggen locatiegegevens mogelijk iets over de gewoonten en gedragspatronen van een gebruiker.[119] Locatiegegevens kunnen – onder andere – informatie prijsgeven over consumptiegedrag (welke winkels bezoekt een gebruiker?), persoonlijkheid (welke plekken bezoekt een gebruiker in zijn vrije tijd?), seksualiteit (bezoekt een gebruiker prostituees, en/of homobars?) en relaties (komt een gebruiker vaak op een bepaalde plek terug?).[120]

Dat het verkrijgen van toegang tot MAC-adressen en locatiegegevens door middel van wifi- en bluetooth-tracking daadwerkelijk privacygevoelig is, blijkt bijvoorbeeld uit het

113 Art. 8 lid 2 ter (Amendement 100) LIBE-rapport EPV.

114 Zie voor de aanpassingen van art. 8 lid 2 e-Privacyverordening die het Voorzitterschap van de Raad tot nu toe heeft voorgesteld Examination of the Presidency text, 2017/0003 (COD), 7820/18, 13 april 2018, p. 50.

115 Zie over zulke risico's M. Goodman, *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World*, Londen (VK): Transworld Publishers 2015, p. 173-174 en International Working Group on Data Protection in Telecommunications, *Working Paper on Location Tracking from Communications of Mobile Devices*, 14 oktober 2015, p. 3-4.

116 WP29 ePrivacy Regulation 01/2017, p. 11.

117 J. Angwin, *Dragnet Nation: A Quest for Privacy, Security and Freedom in a World of Relentless Surveillance*, New York (VS): Times Books 2014, p. 149-150.

118 Y-A. de Montjoye e.a., 'Unique in the Crowd: The privacy bounds of human mobility', *Scientific Reports* 2013/1376, afl. 3.

119 WP29 Geolocation smart mobile devices 13/2011, p. 7.

120 Matte 2017, p. 32.

feit dat informatie verkregen uit bluetooth-tracking in het kader van verkeersonderzoek in verschillende strafzaken als bewijs voor de locatie van een verdachte is gebruikt.[121]

Vrijwel alle partijen die wifi-tracking toepassen, verwerken de gegevens van gebruikers omdat zij de verwerking noodzakelijk achten voor het gerechtvaardigd belang (bedrijfsbelang) van de onderneming.[122] Op basis van deze grondslag is het verkrijgen van toestemming van de gebruiker niet vereist. Wanneer de gebruiker niet de mogelijkheid krijgt om het uitlezen van informatie – voorafgaand aan het uitlezen – te weigeren, verliest de gebruiker de controle over zijn gegevens en privacy in de openbare ruimte. De gebruiker kan zich, wanneer hij zijn smartphone bij zich draagt, vaak niet meer anoniem door de openbare ruimte bewegen.[123] Het gevaar dat de gebruiker aan wifi-tracking wordt blootgesteld ligt, wanneer e-Privacyregels niet naast algemene privacyregels op wifi-tracking van toepassing zijn, altijd op de loer.

Bij de ernst van de inbreuk op de persoonlijke levenssfeer speelt een grote rol dat veel mensen zich niet bewust zijn van het feit dat wifi-tracking wordt toegepast. De gemiddelde gebruiker verwacht, met name door het ontbreken van adequate informatie, waarschijnlijk niet dat meetapparatuur op talloze locaties in Nederland de signalen van zijn mobiele apparatuur opvangt.[124] Gebruikers worden in de praktijk vaak niet, of in ieder geval niet voldoende, voorzien van duidelijke en volledige informatie voordat meetapparatuur toegang verkrijgt tot informatie op de randapparatuur van de gebruiker.

Wanneer het toestemmingsvereiste uit de huidige en toekomstige e-Privacyregels van toepassing is, zal de gebruiker te allen tijde 'gedwongen' worden geïnformeerd, alvorens de gebruiker – welbewust – kiest of hij aan wifi-tracking wil worden blootgesteld.

Hierbij dient de kanttekening te worden geplaatst dat het nog maar de vraag is of het verkrijgen van geïnformeerde toestemming, door de technische complexiteit van wifi-trackingtechnologie, überhaupt mogelijk is. De gemiddelde burger heeft misschien niet voldoende technische kennis om te begrijpen waarmee hij precies akkoord gaat. Het valt te betwijfelen of een gebruiker begrijpt hoe wifi-tracking werkt, welke gegevens worden verwerkt en wat de consequenties van de verwerking zijn. In een dergelijke situatie is sprake van informatieasymmetrie, vergelijkbaar met de situatie waarin internetgebruikers 'geïnformeerde' toestemming geven voor het plaatsen van cookies. Ook voor websitebezoekers is het, wanneer zij toestemming geven voor het plaatsen van cookies, vaak moeilijk, of in het geheel niet mogelijk, om te begrijpen of hun gegevens worden verzameld en wat er met de verzamelde informatie gebeurt.[125] Men kan zich afvragen of het toepassen van wifi-tracking in algemene zin wenselijk en toelaatbaar is, wanneer het verkrijgen van geïnformeerde toestemming wellicht niet mogelijk is.

Ondanks het voorgaande is toepasbaarheid van e-Privacyregels op wifi-tracking in mijn optiek wenselijk. Op dit moment bestaat er geen empirisch onderzoek naar (het ontbreken van) kennis van burgers over wifi-tracking. Het valt, vooralsnog, niet met zekerheid te zeggen dat het verkrijgen van geïnformeerde toestemming voor de toepassing van wifi-tracking *de facto* niet mogelijk is. Daarnaast is het verdedigbaar dat door opkomst van aandacht voor wifi-tracking in mainstream media[126] en voorlichtingsinitiatieven zoals de overheidswebsite www.veiliginternetten.nl,[127] het kennisniveau van de gemiddelde burger over wifi-tracking steeds groter wordt. Wanneer burgers meer kennis (kunnen) opdoen over het bestaan en de werking van wifi-tracking, wordt de mogelijkheid van het geven van geïnformeerde toestemming steeds reëler.

Toepasbaarheid van de vereisten uit art. 11.7a lid 1 Tw is in mijn ogen niet in alle denkbare situaties waarin wifi-tracking plaatsvindt wenselijk. Wanneer wifi-tracking wordt toegepast voor (simpele) analytische doeleinden, staat het vereiste om voorafgaande toestemming te verkrijgen niet altijd in verhouding tot de (relatief geringe) inbreuk op de persoonlijke levenssfeer van de gebruiker. Een voorbeeld van een simpel analytisch doeleinde is het tellen van bezoekers van een winkel of festival. Wanneer de verkregen informatie onmiddellijk wordt geanonimiseerd of verwijderd, blijft de inbreuk op de persoonlijke levenssfeer van de gebruiker beperkt.

In dergelijke situaties biedt de uitzondering in art. 11.7a lid 3 sub b Tw echter geen soelaas: de uitzondering is slechts van toepassing op een geleverde 'dienst van de informatiemaat-

121 Rb. Zeeland-West-Brabant 28 juni 2016, ECLI:NL:RBZWB:2016:3865 (*doodslag verkeer*), Hof Arnhem-Leeuwarden 27 november 2014, ECLI:NL:GHARL:2014:9050 (*medeplichtigheid moord op sportschoolhouder*), Rb. Midden-Nederland 12 februari 2014, ECLI:NL:RBMNE:2014:509 (*vrijspraak moord, dan wel doodslag op partner en ongeboren kind*), Rb. Midden-Nederland 4 november 2013, ECLI:NL:RBMNE:2013:5423 (*vrijspraak overval op woning*).

122 Art. 6 lid 1 sub f AVG. Zie ook Bluetrace-rapport, p. 40-48.

123 B. Zhao, 'Exposure and Concealment in Digitalized Public Spaces', in: B.C. Newell, T. Timan & B-J. Koops (red.), *Privacy in Public Space: Conceptual and Regulatory Challenges*, Cheltenham (VK): Edward Elgar Publishing 2017, p. 139-163. Zie ook M. Martijn & D. Tokmetzis, *Je hebt wél iets te verbergen*, Amsterdam: De Correspondent 2016, p. 42.

124 Zie over verwachtingen van informatiestromen in relatie tot privacy H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford (VS): Stanford University Press 2010.

125 Zie met name hoofdstuk 6 en 7 in F.J. Zuiderveen Borgesius, *Improving privacy protection in the area of behavioural targeting* (diss. Amsterdam UvA; Information Law Series, deel 33), Alphen aan den Rijn: Kluwer Law International 2015.

126 Zie bijvoorbeeld 'Radar', AVROTROS NPO 1, 17 oktober 2016, 'Al jaren wifi-tracking in grote steden', *NOS* 29 januari 2014 en P. Zandstra, 'Winkeliers kunnen gedrag klant volgen via wifi op smartphone', *NRC* 23 januari 2014.

127 www.veiliginternetten.nl/nieuws/wifi-tracking-wat-het-en-mag-het/. Opmerking verdient dat de zinsnede "De aanwezigheid van een wifi-netwerk is ook voor jou handig" op deze website, ten onrechte doet vermoeden dat de gebruiker in 'ruil' voor wifi-tracking altijd gratis toegang tot een wifi-netwerk krijgt.

schappij', waar door de gebruiker om moet zijn verzocht. In het geval van passieve wifi-tracking (dus wanneer slechts signalen worden opgevangen) zal hiervan geen sprake zijn.

In de door het EP geamendeerde versie van de e-Privacyverordening is een uitzondering opgenomen die het gebruik van wifi-tracking voor simpele analytische doeleinden, zonder voorafgaande toestemming van de gebruiker, mogelijk maakt. Deze naar mijn mening welkome uitzondering zal echter pas gaan gelden wanneer de e-Privacyverordening van toepassing wordt. Daarnaast is het mogelijk dat de uitzondering de uiteindelijke versie van de e-Privacyverordening niet, of niet in de door het EP voorgestelde vorm, zal halen.

7. Conclusie

In deze bijdrage is onderzocht of de cookiebepaling, zoals neergelegd in art. 5 lid 3 e-Privacyrichtlijn en in Nederland geïmplementeerd in art. 11.7a Tw, op wifi-tracking van toepassing kan zijn. Vervolgens is besproken welke gevolgen toepasbaarheid van de cookiebepaling heeft op wifi-tracking in de praktijk. Ook zijn de regels voor wifi-tracking uit de toekomstige e-Privacyverordening geanalyseerd en vergeleken met de huidige regels uit de e-Privacyrichtlijn. Tot slot is in deze bijdrage stilgestaan bij de vraag of toepasbaarheid van huidige en toekomstige e-Privacyregels op wifi-tracking wenselijk is.

Op basis van de ratio, totstandkomingsgeschiedenis en een tekstuele interpretatie van art. 5 lid 3 e-Privacyrichtlijn en art. 11.7a Tw ben ik van mening dat art. 11.7a Tw op wifi-tracking van toepassing kan zijn. Voor de praktijk betekent dit dat toepassing van wifi-tracking naast alle vereisten van de AVG, totdat de e-Privacyverordening van toepassing wordt, tevens dient te voldoen aan de vereisten van art. 11.7a Tw. Het toepassen van wifi-tracking is op grond van art. 11.7a lid 1 Tw slechts mogelijk nadat de gebruiker is voorzien van duidelijke en volledige informatie en indien hij voorafgaande toestemming heeft verleend. Aan de vereisten van art. 11.7a lid 1 Tw hoeft niet te worden voldaan, wanneer wifi-tracking uitsluitend wordt toegepast voor eenvoudige tellingen en de toepassing kan worden aangemerkt als een 'dienst van de informatiemaatschappij' – hetgeen in de praktijk niet veel voorkomt.

Begin 2017 introduceerde de Commissie het voorstel voor de e-Privacyverordening. De voorgestelde verordening bevat regels die expliciet op wifi-tracking van toepassing zullen zijn. Deze regels zijn door het EP geamendeerd. De vereisten van art. 11.7a Tw sluiten in grote mate aan bij de door het EP voorgestelde versie van art. 8 lid 2 e-Privacyverordening. Hoe de 'devicetrackingbepaling' in de e-Privacyverordening er uiteindelijk gaat uitzien en wanneer de e-Privacyverordening in werking treedt en van toepassing wordt, is ten tijde van afronding van deze publicatie nog niet duidelijk.

Door het passieve en voor gebruikers onzichtbare en abstracte karakter van wifi-trackingtechnologie, is het in veel praktijksituaties lastig voor te stellen hoe aan de vereisten van huidige en toekomstige e-Privacyregelgeving kan worden voldaan. Daarnaast is het de vraag of het verkrijgen van (geïnformeerde) toestemming, gezien de technische complexiteit van wifi-trackingtechnologie, mogelijk is. Ondanks dat wifi-tracking onder de voorwaarden van de e-Privacyrichtlijn en de e-Privacyverordening waarschijnlijk nog maar beperkt kan worden toegepast, is toepasbaarheid in mijn optiek in veel situaties wenselijk, gelet op de grote privacyrisico's die het gebruik van wifi-tracking met zich kan meebrengen.

De ACM, toezichthouder op art. 11.7a Tw, heeft zich tot op heden nog niet publiekelijk uitgelaten over de mogelijke toepasbaarheid van de huidige e-Privacyregels op wifi-tracking. Nu het waarschijnlijk nog enige tijd duurt totdat de e-Privacyverordening van toepassing wordt en art. 11.7a Tw tot die tijd naast de AVG blijft gelden, zou een standpunt over de toepasbaarheid van art. 11.7a Tw op wifi-tracking van de ACM – eventueel gezamenlijk met de AP – zeer welkom zijn.